U.S. PTO
14/757638
12/23/2015

02205 U.S. PTO
122315

PTO/SB/17 (03-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

FEE TRANSMITTAL

Complete if known	
Application Number	
Filing Date	December 23, 2015
First Named Inventor	David K. AHN
Examiner Name	TBA
Art Unit	TBA
Practitioner Docket No.	007742.00059

☑ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29. Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

TOTAL AMOUNT OF PAYMENT ($) 1,200

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☑ Deposit Account Deposit Account Number: 19-0733 Deposit Account Name: _____

For the above-identified deposit account, the Director is hereby authorized to (check all that apply):

☑ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, **except for the filing fee**

☑ Charge any additional fee(s) or underpayment of fee(s) under 37 CFR 1.16 and 1.17 ☑ Credit any overpayment of fee(s)

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES (U = undiscounted fee; S = small entity fee; M = micro entity fee)

	FILING FEES			SEARCH FEES			EXAMINATION FEES			
Application Type	U ($)	S ($)	M ($)	U ($)	S ($)	M ($)	U ($)	S ($)	M ($)	Fees Paid ($)
Utility	280	140*	70	600	300	150	720	360	180	800
Design	180	90	45	120	60	30	460	230	115	
Plant	180	90	45	380	190	95	580	290	145	
Reissue	280	140	70	600	300	150	2,160	1,080	540	
Provisional	260	130	65	0	0	0	0	0	0	

* The $140 small entity status filing fee for a utility application is further reduced to $70 for a small entity status applicant who files the application via EFS-Web.

2. EXCESS CLAIM FEES

Fee Description	Undiscounted Fee ($)	Small Entity Fee ($)	Micro Entity Fee ($)
Each claim over 20 (including Reissues)	80	40	20
Each independent claim over 3 (including Reissues)	420	210	105
Multiple dependent claims	780	390	195

Total Claims		Extra Claims		Fee ($)		Fee Paid ($)
25	-20 or HP =	5	x	40	=	200

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims		Extra Claims		Fee ($)		Fee Paid ($)
	-3 or HP =		x		=	

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims	Fee ($)	Fee Paid ($)

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $400 ($200 for small entity) ($100 for micro entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets		Extra Sheets		Number of each additional 50 or fraction thereof		Fee ($)		Fee Paid ($)
	- 100 =		/ 50 =		(round **up** to a whole number) x		=	

4. OTHER FEE(S)

	Fees Paid ($)
Non-English specification, $130 fee (no small or micro entity discount)	
Non-electronic filing fee under 37 CFR 1.16(t) for a utility application, $400 fee ($200 small or micro entity)	200
Other (e.g., late filing surcharge): _____	

SUBMITTED BY

Signature	William E. Wooten	Registration No. (Attorney/Agent) 60,049	Telephone (202) 824-3000
Name (Print/Type)	William E. Wooten		Date December 23, 2015

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

02205 U.S. PTO
122315

RULE-BASED NETWORK-THREAT DETECTION FOR ENCRYPTED COMMUNICATIONS

BACKGROUND

[01] Network security is becoming increasingly important as the information age continues to unfold. Network threats may take a variety of forms (e.g., unauthorized requests or data transfers, viruses, malware, large volumes of traffic designed to overwhelm resources, and the like). Network-threat services provide information associated with network threats, for example, reports that include listings of network-threat indicators (e.g., network addresses, domain names, uniform resource identifiers (URIs), and the like). Such information may be utilized to identify network threats. Encrypted communications, however, may obfuscate data corresponding to network threats. Accordingly, there is a need for rule-based network-threat detection for encrypted communications.

SUMMARY

[02] The following presents a simplified summary in order to provide a basic understanding of some aspects of the disclosure. It is intended neither to identify key or critical elements of the disclosure nor to delineate the scope of the disclosure. The following summary merely presents some concepts of the disclosure in a simplified form as a prelude to the description below.

[03] Aspects of this disclosure relate to rule-based network-threat detection for encrypted communications. In accordance with embodiments of the disclosure, a packet-filtering system configured to filter packets in accordance with packet-filtering rules may receive data indicating network-threat indicators and may configure the packet-filtering rules to cause the packet-filtering system to identify packets comprising unencrypted data, and packets comprising encrypted data. A portion of the unencrypted data may correspond to one or more of the network-threat indicators, and the packet-filtering rules may be configured to cause the packet-filtering system to determine, based on the portion of the unencrypted data, that the packets comprising encrypted data correspond to the one or more network-threat indicators.

EX1002
CISCO SYSTEMS, INC. / Page 2 of 1453

BRIEF DESCRIPTION OF THE DRAWINGS

[04] The present disclosure is pointed out with particularity in the appended claims. Features of the disclosure will become more apparent upon a review of this disclosure in its entirety, including the drawing figures provided herewith.

[05] Some features herein are illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings, in which like reference numerals refer to similar elements, and wherein:

[06] **FIG. 1** depicts an illustrative environment for rule-based network-threat detection for encrypted communications in accordance with one or more aspects of the disclosure;

[07] **FIG. 2** depicts an illustrative packet-filtering system for rule-based network-threat detection for encrypted communications in accordance with one or more aspects of the disclosure;

[08] **FIGs. 3A-C**, **4A-C**, **5A-B**, and **6A-B** depict illustrative event sequences for rule-based network-threat detection for encrypted communications in accordance with one or more aspects of the disclosure; and

[09] **FIG. 7** depicts an illustrative method for rule-based network-threat detection for encrypted communications in accordance with one or more aspects of the disclosure.

DETAILED DESCRIPTION

[10] In the following description of various illustrative embodiments, reference is made to the accompanying drawings, which form a part hereof, and in which is shown, by way of illustration, various embodiments in which aspects of the disclosure may be practiced. It is to be understood that other embodiments may be utilized, and structural and functional modifications may be made, without departing from the scope of the disclosure.

EX1002
CISCO SYSTEMS, INC. / Page 3 of 1453

[11] Various connections between elements are discussed in the following description. These connections are general and, unless specified otherwise, may be direct or indirect, wired or wireless. In this respect, the specification is not intended to be limiting.

[12] **FIG. 1** depicts an illustrative environment for rule-based network-threat detection for encrypted communications in accordance with one or more aspects of the disclosure. Referring to **FIG. 1**, environment **100** may include networks **102** and **104**. Network **102** may comprise one or more networks (e.g., Local Area Networks (LANs), Wide Area Networks (WANs), Virtual Private Networks (VPNs), or combinations thereof) associated with one or more individuals or entities (e.g., governments, corporations, service providers, or other organizations). Network **104** may comprise one or more networks (e.g., LANs, WANs, VPNs, or combinations thereof) that interface network **102** with one or more other networks (not illustrated). For example, network **104** may comprise the Internet, a similar network, or portions thereof.

[13] Environment **100** may also include one or more hosts, such as computing or network devices (e.g., servers, desktop computers, laptop computers, tablet computers, mobile devices, smartphones, routers, gateways, firewalls, switches, access points, or the like). For example, network **102** may include hosts **106**, **108**, and **110**, proxy devices **112**, **114**, and **116**, web proxy **118**, rule gates **120**, **122**, **124**, **126**, and **128**, domain name system (DNS) **130**, Internet content adaptation protocol (ICAP) server **132**, and gateway **134**. As used herein, "host" (or "hosts") refers to any type of network device (or node) or computing device; while such devices may be assigned (or configured to be assigned) one or more network-layer addresses, the term "host" (or "hosts") does not imply such devices necessarily are assigned (or configured to be assigned) one or more network-layer addresses.

[14] Gateway **134** may be located at border **136** between networks **102** and **104** and may interface network **102** or one or more hosts located therein with network **104** or one or more hosts located therein. For example, network **104** may include one or more rule

EX1002
CISCO SYSTEMS, INC. / Page 4 of 1453

providers **138**, one or more threat-intelligence providers **140**, and hosts **142**, **144**, and **146**, and gateway **134** may interface hosts **106**, **108**, and **110**, proxy devices **112**, **114**, and **116**, web proxy **118**, rule gates **120**, **122**, **124**, **126**, and **128**, DNS **130**, and ICAP server **132** with rule providers **138**, threat-intelligence providers **140**, and hosts **142**, **144**, and **146**.

[15] **FIG. 2** depicts an illustrative packet-filtering system for rule-based network-threat detection for encrypted communications in accordance with one or more aspects of the disclosure. Referring to **FIG. 2**, packet-filtering system **200** may be associated with network **102** and may include one or more of rule gates **120**, **122**, **124**, **126**, and **128**. Packet-filtering system **200** may comprise one or more processors **202**, memory **204**, one or more communication interfaces **206**, and data bus **208**. Data bus **208** may interface processors **202**, memory **204**, and communication interfaces **206**. Memory **204** may comprise one or more program modules **210**, rules **212**, and logs **214**. Program modules **210** may comprise instructions that when executed by processors **202** cause packet-filtering system **200** to perform one or more of the functions described herein. Rules **212** may comprise one or more packet-filtering rules in accordance with which packet-filtering system **200** is configured to filter packets received via communication interfaces **206**. Logs **214** may include one or more entries generated by processors **202** in accordance with rules **212** for packets received by packet-filtering system **200** via communication interfaces **206**.

[16] Communication interfaces **206** may interface packet-filtering system **200** with one or more communication links of environment **100** (e.g., of networks **102** and **104**). In some embodiments, one or more of communication interfaces **206** may interface directly with a communication link of environment **100**. For example, interfaces **216** and **224** may interface directly with links **236** and **244**, respectively. In some embodiments, one or more of communication interfaces **206** may interface indirectly with a communication link of environment **100**. For example, interface **220** may interface with links **236** and **244** via one or more network devices **240**. Network devices **240** may provide interface

EX1002
CISCO SYSTEMS, INC. / Page 5 of 1453

220 with access to (or copies of) packets traversing one or more of links **236** and **244**, for example, via a switched port analyzer (SPAN) port of network devices **240**. Additionally or alternatively, interfaces **218** and **222** may interface with links **236** and **244** via tap devices **238** and **242**. For example, packet-filtering system **200** may provision tap device **238** with one or more of rules **212** configured to cause tap device **238** to identify packets traversing link **236** that correspond to specified criteria and route (or forward) the packets (or copies thereof) to interface **218**, and packet-filtering system **200** may provision tap device **242** with one or more of rules **212** configured to cause tap device **242** to identify packets traversing link **244** that correspond to specified criteria and route (or forward) the packets (or copies thereof) to interface **222**. Similarly, interfaces **226** and **234** may interface directly with links **246** and **254**, respectively; network devices **250** may provide interface **230** with access to (or copies of) packets traversing one or more of links **246** and **254**; packet-filtering system **200** may provision tap device **248** with one or more of rules **212** configured to cause tap device **248** to identify packets traversing link **246** that correspond to specified criteria and route (or forward) the packets (or copies thereof) to interface **228**; and packet-filtering system **200** may provision tap device **252** with one or more of rules **212** configured to cause tap device **252** to identify packets traversing link **254** that correspond to specified criteria and route (or forward) the packets (or copies thereof) to interface **232**. In some embodiments, packet-filtering system **200** may comprise one or more of tap devices **238**, **242**, **248**, and **252** or network devices **240** and **250**.

[17] **FIGs. 3A-C**, **4A-C**, **5A-B**, and **6A-B** depict illustrative event sequences for rule-based network-threat detection for encrypted communications in accordance with one or more aspects of the disclosure. The depicted steps are merely illustrative and may be omitted, combined, or performed in an order other than that depicted; the numbering of the steps is merely for ease of reference and does not imply any particular ordering is necessary or preferred.

[18] Referring to **FIG. 3A**, at step **#1**, threat-intelligence providers **140** may communicate one or more threat-intelligence reports to rule providers **138**. The threat-intelligence reports may include one or more network-threat indicators, for example, domain names (e.g., fully qualified domain names (FQDNs)), URIs, network addresses, or the like. At step **#2**, rule providers **138** may utilize the threat-intelligence reports to generate one or more packet-filtering rules configured to identify packets comprising data corresponding to the network-threat indicators. At step **#3**, rule providers **138** may communicate the packet-filtering rules to rule gate **120**. As indicated by the crosshatched boxes over the lines extending downward from network **104**, rule gate **128**, and gateway **134**, the packet-filtering rules may traverse network **104**, rule gate **128**, and gateway **134**. For example, network **104** and gateway **134** may interface rule providers **138** and rule gate **120**, and rule gate **128** may interface a communication link interfacing network **104** and gateway **134**. Rule gate **120** may receive the packet-filtering rules generated by rule providers **138** and, at step **#4**, may utilize the received packet-filtering rules to configure rules **212** to cause packet-filtering system **200** to identify packets comprising data corresponding to at least one of the plurality of network-threat indicators.

[19] At step **#5**, host **106** may generate a request. For example, host **106** may execute a web browser, and the web browser may generate a request in response to user input (e.g., navigation of the web browser to a URI). The request may comprise a domain name, and host **106** may generate a DNS query comprising the domain name and, at step **#6**, may communicate the DNS query toward DNS **130**. Rule gate **126** may interface a communication link interfacing host **106** and DNS **130**, the domain name included in the request may correspond to one or more of the network-threat indicators, and rules **212** may be configured to cause rule gate **126** to one or more of identify one or more packets comprising the DNS query, determine that the packets comprise the domain name corresponding to the network-threat indicators, and responsive to one or more of identifying the packets or determining that the packets comprise the domain name corresponding to the network-threat indicators, one or more of log (as indicated by the diamond-patterned box over the line extending downward from rule gate **126**) or drop

EX1002
CISCO SYSTEMS, INC. / Page 7 of 1453

the packets. Rule gate **126** may generate log data (e.g., one or more entries in logs **214**) for the packets. For example, the packets may comprise a network address of host **106** (e.g., as a source address in their network-layer headers), and rule gate **126** may generate log data indicating the network address of host **106**. As depicted by step **#6A**, the packets may be communicated to DNS **130**. In some embodiments, rules **212** may be configured to cause rule gate **126** to, responsive to one or more of identifying the packets or determining that the packets comprise the domain name corresponding to the network-threat indicators, drop the packets, preventing them from reaching DNS **130**, as depicted by step **#6B**.

[20] DNS **130** may generate a reply to the DNS query and, at step **#7**, may communicate the reply toward host **106**. The reply may comprise the domain name corresponding to the network-threat indicators, and rules **212** may be configured to cause rule gate **126** to one or more of identify one or more packets comprising the reply, determine that the packets comprise the domain name corresponding to the network-threat indicators, and responsive to one or more of identifying the packets or determining that the packets comprise the domain name corresponding to the network-threat indicators, one or more of log or drop the packets. Rule gate **126** may generate log data (e.g., one or more entries in logs **214**) for the packets. For example, the packets may comprise the network address of host **106** (e.g., as a destination address in their network-layer headers), and rule gate **126** may generate log data indicating the network address of host **106**. Similarly, the domain name may correspond to host **142**, the packets may comprise a network address of host **142** (e.g., DNS **130** may have resolved the domain name included in the query to the network address of host **142**.), and rule gate **126** may generate log data indicating the network address of host **142**. As depicted by step **#7A**, the packets may be communicated to host **106**. In some embodiments, rules **212** may be configured to cause rule gate **126** to, responsive to determining that the packets comprise the domain name corresponding to the network-threat indicators, drop the packets, preventing them from reaching host **106**, as depicted by step **#7B**.

[21] Packet-filtering system **200** may be configured to correlate packets identified by packet-filtering system **200** (e.g., the packets comprising the reply to the DNS query) with packets previously identified by packet-filtering system **200** (e.g., the packets comprising the DNS query). For example, packet-filtering system **200** may be configured to determine that packets identified by packet-filtering system **200** (e.g., the packets comprising the reply to the DNS query) are one or more of associated with, related to, or the product of packets previously identified by packet-filtering system **200** (e.g., the packets comprising the DNS query). Packet-filtering system **200** may be configured to correlate packets identified by packet-filtering system **200** with packets previously identified by packet-filtering system **200** based on data stored in logs **214** (e.g., the log data generated by rule gate **126** in steps **#6** and **#7**).

[22] For example, for one or more packets logged by packet-filtering system **200** (e.g., the packets comprising the DNS query or the packets comprising the reply to the DNS query), logs **214** may comprise one or more entries indicating one or more of network-layer information (e.g., information derived from one or more network-layer header fields of the packets, such as a protocol type, a destination network address, a source network address, a signature or authentication information (e.g., information from an Internet protocol security (IPsec) encapsulating security payload (ESP)), or the like), transport-layer information (e.g., a destination port, a source port, a checksum or similar data (e.g., error detection or correction values, such as those utilized by the transmission control protocol (TCP) or the user datagram protocol (UDP)),or the like), application-layer information (e.g., information derived from one or more application-layer header fields of the packets, such as a domain name, a uniform resource locator (URL), a uniform resource identifier (URI), an extension, a method, state information, media-type information, a signature, a key, a timestamp, an application identifier, a session identifier, a flow identifier, sequence information, authentication information, or the like), other data in the packets (e.g., payload data), or one or more environmental variables (e.g., information associated with but not solely derived from the packets themselves, such as one or more arrival (or receipt) or departure (or transmission) times

EX1002
CISCO SYSTEMS, INC. / Page 9 of 1453

of the packets (e.g., at or from one or more of rule gates **120**, **122**, **124**, **126**, or **128**, tap devices **238**, **242**, **248**, or **252**, or network devices **240** or **250**), one or more ingress or egress identifiers (e.g., associated with one or more physical or logical network interfaces, ports, or communication-media types of one or more of rule gates **120**, **122**, **124**, **126**, or **128**, tap devices **238**, **242**, **248**, or **252**, or network devices **240** or **250** via which the packets were one or more of received or transmitted), one or more device identifiers (e.g., associated with one or more of rule gates **120**, **122**, **124**, **126**, or **128**, tap devices **238**, **242**, **248**, or **252**, or network devices **240** or **250** via which the packets were one or more of received or transmitted), or the like), and packet-filtering system **200** may utilize such entries to correlate one or more packets identified by packet-filtering system **200** with one or more packets previously identified by packet-filtering system **200**.

[23] In some embodiments, packet-filtering system **200** may implement one or more aspects of the technology described in U.S. Patent Application Serial No. 14/618,967, filed February 10, 2015, and entitled "CORRELATING PACKETS IN COMMUNICATIONS NETWORKS," the disclosure of which is incorporated by reference herein in its entirety and made part hereof, or similar technology (e.g., to correlate one or more packets identified by packet-filtering system **200** with one or more packets previously identified by packet-filtering system **200**).

[24] Host **106** may generate one or more packets destined for host **142** comprising data (e.g., a TCP: SYN handshake message) configured to establish a connection (e.g., a TCP connection or tunnel) between hosts **106** and **142** and, at step **#8**, may communicate the packets toward host **142**. Rule gate **120** may interface a communication link interfacing hosts **106** and **142**, and rules **212** may be configured to cause rule gate **120** to one or more of identify the packets or determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more of the packets comprising the DNS query or the reply to the

DNS query based on data stored in logs **214** (e.g., the log data generated by rule gate **126** in one or more of steps **#6** or **#7**).

[25] At step **#9**, rule gate **120** may route the packets comprising the data configured to establish the connection between hosts **106** and **142** to proxy device **112** and, at step **#10**, may communicate the packets to proxy device **112**. For example, rules **212** may be configured to cause rule gate **120** to route the packets to proxy device **112** based on data in the packets, for example, one or more ports (e.g., port 443) indicated by transport-layer headers in the packets, indicating the connection between hosts **106** and **142** will be utilized to establish an encrypted communication session or tunnel (e.g., a session established in accordance with the transport layer security (TLS) protocol, secure sockets layer (SSL) protocol, secure shell (SSH) protocol, or the like). In some embodiments, rules **212** may be configured to cause rule gate **120** to route the packets to proxy device **112** based on a determination that one or more of hosts **106** or **142** is associated with a network address for which rules **212** indicate encrypted communications should be established via one or more of proxy devices **112**, **114**, or **116**. For example, proxy devices **112**, **114**, and **116** may be part of a proxy system (e.g., a SSL/TLS proxy system) that enables packet-filtering system **200** to filter packets comprising encrypted data based on information within the encrypted data, and rules **212** may be configured to cause rule gate **120** to route the packets to proxy device **112** based on a determination that host **142** is associated with a network address of a domain corresponding to the network-threat indicators.

[26] Additionally or alternatively, network **102** may include one or more hosts for which rules **212** indicate connections utilized to establish encrypted communication sessions (e.g., connections with hosts corresponding to network-threat indicators) should be established via one or more of proxy devices **112**, **114**, or **116**, as well as one or more hosts for which rules **212** indicate connections utilized to establish encrypted communication sessions should not be established via one or more of proxy devices **112**, **114**, and **116**, for example, hosts that generate sensitive data (e.g., personally

identifiable information (PII)), inspection of which may present privacy or regulatory concerns (e.g., data subject to the health insurance portability and accountability act (HIPAA), or the like), and rules **212** may be configured to cause rule gate **120** to route the packets to proxy device **112** based on a determination that host **106** is associated with a network address for which rules **212** indicate encrypted communications should be established via one or more of proxy devices **112**, **114**, or **116**.

[27] For example, link **236** may interface host **106** with rule gate **120**, link **244** may interface rule gate **120** with host **142**, link **246** may interface rule gate **120** with proxy device **112**, link **254** may interface proxy devices **112** and **114** and may comprise a communication link internal to a proxy system comprising proxy devices **112** and **114**, and rules **212** may be configured to cause rule gate **120** to route (or redirect) packets received from host **106** via one or more of interfaces **216**, **218**, or **220** and destined for host **142** (or a portion thereof (e.g., packets comprising data configured to establish a connection between hosts **106** and **142** and indicating the connection will be utilized to establish an encrypted communication session)) to host **142** via interface **226**. Additionally or alternatively, rules **212** may be configured to cause rule gate **120** to forward copies of (or mirror) packets received from host **106** via one or more of interfaces **216**, **218**, **220**, or **222** and destined for host **142** (or a portion thereof (e.g., packets comprising data configured to establish a connection between hosts **106** and **142** and indicating the connection will be utilized to establish an encrypted communication session)) to proxy device **112** via interface **226**.

[28] At step **#11**, proxy devices **112** and **114** may exchange one or more parameters determined from the packets comprising the data configured to establish the connection between hosts **106** and **142**, for example, one or more network addresses in network-layer headers of the packets (e.g., network addresses of hosts **106** and **142**) or ports indicated by transport-layer headers in the packets (e.g., indicating the type of encrypted communication session the connection will be utilized to establish). Proxy device **112** may utilize the parameters to generate packets comprising data configured

to establish a connection between proxy device **112** and host **106** (e.g., a TCP: SYN-ACK handshake message) and, at step **#12**, may communicate the packets to host **106**. Rules **212** may be configured to cause rule gate **120** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more of the packets comprising the DNS query or the reply to the DNS query based on data stored in logs **214** (e.g., the log data generated by rule gate **126** in one or more of steps **#6** or **#7**), and one or more of log or drop the packets.

[29] Similarly, proxy device **114** may utilize the parameters to generate packets comprising data configured to establish a connection between proxy device **114** and host **142** (e.g., a TCP: SYN handshake message) and, at step **#13**, may communicate the packets to host **142**. Rule gate **128** may interface a communication link interfacing proxy device **114** and host **142**, and rules **212** may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of steps **#6**, **#7**, or **#12**), and one or more of log or drop the packets.

[30] Responsive to receiving the packets from proxy device **112**, host **106** may generate packets comprising data configured to establish the connection between proxy device **112** and host **106** (e.g., a TCP: ACK handshake message) and, at step **#14**, may communicate the packets to proxy device **112**. Rules **212** may be configured to cause rule gate **120** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by

correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of steps **#6**, **#7**, **#12**, or **#13**), and one or more of log or drop the packets.

[31] Responsive to receiving the packets from proxy device **114**, host **142** may generate packets comprising data configured to establish the connection between proxy device **114** and host **142** (e.g., a TCP: SYN-ACK handshake message) and, at step **#15**, may communicate the packets to proxy device **114**. Rules **212** may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6**, **7**, or **12-14**), and one or more of log or drop the packets.

[32] Responsive to receiving the packets from host **142**, proxy device **114** may generate packets comprising data configured to establish the connection between proxy device **114** and host **142** (e.g., a TCP: ACK handshake message) and, at step **#16**, may communicate the packets to host **142**. Rules **212** may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6**, **7**, or **12-15**), and one or more of log or drop the packets.

[33] Referring to **FIG. 3B**, proxy device **112** may receive the packets comprising data configured to establish the connection between proxy device **112** and host **106**

EX1002
CISCO SYSTEMS, INC. / Page 14 of 1453

communicated by host **106** in step **#14**, and connection **302** (e.g., a TCP connection) between proxy device **112** and host **106** may be established. Similarly, host **142** may receive the packets comprising data configured to establish the connection between proxy device **114** and host **142** communicated by proxy device **114** in step **#16**, and connection **304** (e.g., a TCP connection) between proxy device **114** and host **142** may be established.

[34] At step **#17**, proxy device **112** and host **106** may communicate packets comprising data configured to establish encrypted communication session **306** (e.g., a SSL/TLS session) between proxy device **112** and host **106** via connection **302**. Rules **212** may be configured to cause rule gate **120** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6**, **7**, or **12-16**), and one or more of log or drop the packets. Additionally or alternatively, rules **212** may be configured to cause rule gate **120** to one or more of identify the packets or determine that the packets comprise data corresponding to the network-threat indicators based on data included in the packets. For example, in some embodiments, host **106** may comprise a client (e.g., web browser), host **142** may comprise a server (e.g., web server), the packets may comprise one or more handshake messages configured to establish session **306** that comprise unencrypted data including a domain name corresponding to the network-threat indicators, for example, a hello message generated by the client (e.g., including the domain name in the server name indication extension, or the like) or a certificate message generated by the server (e.g., including the domain name in one or more of the subject common name field or the extension subjectAltName (of type dNSName), or the like), and rules **212** may be configured to cause rule gate **120** to one or more of identify the packets or determine that the packets comprise data corresponding to the network-

threat indicators based on data included in the one or more handshake messages configured to establish session **306**. In such embodiments, rules **212** may be configured to cause packet-filtering system **200** to one or more of identify the packets or determine that the packets comprise data corresponding to the network-threat indicators based on the certificate message comprising other data (e.g., in addition to or in lieu of the domain name) corresponding to one or more of the network-threat indicators, for example, data indicating at least one of a serial number (or type thereof) indicated by rules **212**, an issuer (or type thereof) indicated by rules **212**, a validity time-range (or type thereof) indicated by rules **212**, a key (or type thereof) indicated by rules **212**, a digital signature (e.g., fingerprint) (or type thereof) indicated by rules **212**, or a signing authority (or type thereof) indicated by rules **212**.

[35] Similarly, at step **#18**, proxy device **114** and host **142** may communicate packets comprising data configured to establish encrypted communication session **308** (e.g., a SSL/TLS session) between proxy device **114** and host **142** via connection **304**, and rules **212** may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6**, **7**, or **12-17**) or the packets comprising one or more handshake messages configured to establish session **308** that comprise unencrypted data (e.g., including the domain name) corresponding to the network-threat indicators, and one or more of log or drop the packets.

[36] Host **106** may generate packets comprising data encrypted in accordance with one or more parameters of session **306** and, at step **#19**, may communicate the packets to proxy device **112** via session **306**. Rules **212** may be configured to cause rule gate **120** to one or more of identify the packets, determine (e.g., based on one or more network

addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6**, **7**, or **12-18**), and one or more of log (as indicated by the triangles over the line extending downward from rule gate **120**) or drop the packets.

[37] Proxy device **112** may receive the packets and decrypt the data in accordance with the parameters of session **306**. The packets may comprise a request (e.g., a hypertext transfer protocol (HTTP) request), and proxy device **112** may comprise an ICAP client, which, at step **#20**, may communicate the packets to ICAP server **132**. Rule gate **126** may interface a communication link interfacing proxy device **112** and ICAP server **132**, and rules **212** may be configured to cause rule gate **126** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6**, **7**, or **12-19**), and one or more of log or drop the packets.

[38] ICAP server **132** may generate packets comprising data responsive to the request (e.g., a response, modified request, or the like) and, at step **#21**, may communicate the packets to proxy device **112**. Rules **212** may be configured to cause rule gate **126** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g.,

log data generated by packet-filtering system **200** in one or more of step **#s 6**, **7**, or **12-20**), and one or more of log or drop the packets. Additionally or alternatively, rules **212** may be configured to cause rule gate **126** to one or more of identify the packets or determine that the packets comprise data corresponding to the network-threat indicators based on data included in the packets, for example, the data responsive to the request (e.g., a modified request) may comprise data (e.g., a domain name, URI, or the like) corresponding to the network-threat indicators.

[39] Proxy device **112** may generate packets (e.g., based on the data generated by ICAP server **132**) and, at step **#22**, may communicate the packets to proxy device **114**. Rule gate **124** may interface a communication link internal to the proxy system comprising proxy devices **112** and **114**, and thus packets traversing the communication link may comprise unencrypted data (e.g., rule gate **124** may be "the man in the middle" of proxy devices **112** and **114**), and rules **212** may be configured to cause rule gate **124** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6**, **7**, or **12-21**), and one or more of log or drop the packets.

[40] Additionally or alternatively, rules **212** may be configured to cause rule gate **124** to one or more of identify the packets or determine that the packets comprise data corresponding to the network-threat indicators based on data included in the packets, for example, unencrypted data in the packets corresponding to one or more of the network-threat indicators. For example, in some embodiments, packet-filtering system **200** may implement one or more aspects of the technology described in U.S. Patent Application Serial No. 13/795,822, filed March 12, 2013, and entitled "FILTERING NETWORK DATA TRANSFERS," the disclosure of which is incorporated by reference

herein in its entirety and made part hereof, or similar technology, and rules **212** may be configured to cause rule gate **124** to one or more of identify the packets or determine that the packets comprise data corresponding to the network-threat indicators based on the packets comprising one or more of a URI specified by rules **212**, data indicating a protocol version specified by rules **212**, data indicating a method specified by rules **212**, data indicating a request specified by rules **212**, or data indicating a command specified by rules **212**. Additionally or alternatively, rules **212** may be configured to cause rule gate **124** to one or more of identify the packets or determine that the packets comprise data corresponding to the one or more network-threat indicators based on unencrypted data in the packets comprising a URI meeting or exceeding a threshold size specified by rules **212** (e.g., a URI likely being utilized to exfiltrate data).

[41] Proxy device **114** may receive the packets and generate one or more corresponding packets comprising data encrypted in accordance with one or more parameters of session **308** and, at step **#23**, may communicate the packets to host **142**. Rules **212** may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6**, **7**, or **12-22**), and one or more of log or drop the packets.

[42] Host **142** may generate one or more packets comprising data encrypted in accordance with one or more parameters of session **308** and, at step **#24**, may communicate the packets to proxy device **114**. Rules **212** may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets

with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6**, **7**, or **12-23**), and one or more of log or drop the packets.

[43] Proxy device **114** may receive the packets and generate one or more corresponding packets comprising unencrypted data and, at step **#25**, may communicate the packets to proxy device **112**. Rules **212** may be configured to cause rule gate **124** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6**, **7**, or **12-24**), and one or more of log or drop the packets.

[44] Proxy device **112** may receive the packets and generate one or more corresponding packets comprising data encrypted in accordance with one or more parameters of session **306** and, at step **#26**, may communicate the packets to host **106**. Rules **212** may be configured to cause rule gate **120** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6**, **7**, or **12-25**), and one or more of log or drop the packets.

[45] Host **106** may generate one or more packets comprising data encrypted in accordance with one or more parameters of session **306** and, at step **#27**, may communicate the packets toward proxy device **112**. Rules **212** may be configured to cause rule gate **120**

EX1002
CISCO SYSTEMS, INC. / Page 20 of 1453

to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6**, **7**, or **12-26**), and one or more of log or drop the packets.

[46] Proxy device **112** may receive one or more of the packets and generate one or more corresponding packets comprising unencrypted data and, at step **#28**, may communicate the packets toward proxy device **114**. Rules **212** may be configured to cause rule gate **124** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6**, **7**, or **12-27**), and one or more of log or drop the packets.

[47] Proxy device **114** may receive one or more of the packets and generate one or more corresponding packets comprising data encrypted in accordance with one or more parameters of session **308** and, at step **#29**, may communicate the packets toward host **142**. Rules **212** may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6**, **7**, or **12-28**), and one or more of log or drop the packets.

[48] Host **142** may generate one or more packets comprising data encrypted in accordance with one or more parameters of session **308** and, at step **#30**, may communicate the packets toward proxy device **114**. Rules **212** may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6**, **7**, or **12-29**), and one or more of log or drop the packets.

[49] Proxy device **114** may receive one or more of the packets and generate one or more corresponding packets comprising unencrypted data and, at step **#31**, may communicate the packets toward proxy device **112**. Rules **212** may be configured to cause rule gate **124** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6**, **7**, or **12-30**), and one or more of log or drop the packets.

[50] Proxy device **112** may receive one or more of the packets and generate one or more corresponding packets comprising data encrypted in accordance with one or more parameters of session **306** and, at step **#32**, may communicate the packets toward host **106**. Rules **212** may be configured to cause rule gate **120** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to

the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6**, **7**, or **12-31**), and one or more of log or drop the packets.

[51] Referring to **FIG. 3C**, at step **#33**, rule gate **120** may one or more of update a console (or interface) associated with packet-filtering system **200** running on host **108** or receive one or more updates to rules **212** via the console. For example, the console may provide data regarding one or more threats to network **102** corresponding to the network-threat indicators, and rule gate **120** may update the console based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6**, **7**, or **12-32**). In some embodiments, the console may provide data identifying network threats associated with one or more of hosts **106**, **108**, **110**, **142**, **144**, or **146**, and rule gate **120** may update data associated with one or more of hosts **106** or **142** based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6**, **7**, or **12-32**).

[52] At step **#34**, rule gate **120** may reconfigure rules **212** based on one or more of updates received via the console or data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6**, **7**, or **12-32**). For example, packet-filtering system **200** may implement one or more aspects of the technology described in U.S. Patent Application Serial No. 14/690,302, filed April 17, 2015, and entitled "RULE-BASED NETWORK-THREAT DETECTION," the disclosure of which is incorporated by reference herein in its entirety and made part hereof, or similar technology, and rule gate **120** may reconfigure rules **212** based on one or more risk scores updated to reflect data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6**, **7**, or **12-32**).

[53] Host **106** may generate one or more packets comprising data encrypted in accordance with one or more parameters of session **306** and, at step **#35**, may communicate the packets toward proxy device **112**. Rules **212** (e.g., one or more of rules **212** reconfigured in step **#34**) may be configured to cause rule gate **120** to one or more of

identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6**, **7**, or **12-32**), and one or more of log or drop the packets.

[54] Proxy device **112** may receive one or more of the packets and generate one or more corresponding packets comprising unencrypted data and, at step **#36**, may communicate the packets toward proxy device **114**. Rules **212** (e.g., one or more of rules **212** reconfigured in step **#34**) may be configured to cause rule gate **124** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6**, **7**, **12-32**, or **35**), and one or more of log or drop the packets.

[55] Proxy device **114** may receive one or more of the packets and generate one or more corresponding packets comprising data encrypted in accordance with one or more parameters of session **308** and, at step **#37**, may communicate the packets toward host **142**. Rules **212** (e.g., one or more of rules **212** reconfigured in step **#34**) may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering

EX1002
CISCO SYSTEMS, INC. / Page 24 of 1453

system **200** in one or more of step **#s 6**, **7**, **12-32**, **35**, or **36**), and one or more of log or drop the packets.

[56] Host **142** may generate one or more packets comprising data encrypted in accordance with one or more parameters of session **308** and, at step **#38**, may communicate the packets toward proxy device **114**. Rules **212** (e.g., one or more of rules **212** reconfigured in step **#34**) may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6**, **7**, **12-32**, or **35-37**), and one or more of log or drop the packets.

[57] Proxy device **114** may receive one or more of the packets and generate one or more corresponding packets comprising unencrypted data and, at step **#39**, may communicate the packets toward proxy device **112**. Rules **212** (e.g., one or more of rules **212** reconfigured in step **#34**) may be configured to cause rule gate **124** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6**, **7**, **12-32**, or **35-38**), and one or more of log or drop the packets.

[58] Proxy device **112** may receive one or more of the packets and generate one or more corresponding packets comprising data encrypted in accordance with one or more parameters of session **306** and, at step **#40**, may communicate the packets toward host **106**. Rules **212** (e.g., one or more of rules **212** reconfigured in step **#34**) may be

configured to cause rule gate **120** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6**, **7**, **12-32**, or **35-39**), and one or more of log or drop the packets.

[59] Host **142** may generate one or more packets destined for one or more of hosts **106**, **108**, or **110** and, at step **#41**, may communicate the packets toward gateway **134**. Rules **212** (e.g., one or more of rules **212** reconfigured in step **#34**) may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6**, **7**, **12-32**, or **35-40**), and one or more of log or drop the packets.

[60] Host **108** may generate one or more packets and, at step **#42**, may communicate the packets to host **142**. Rules **212** (e.g., one or more of rules **212** reconfigured in step **#34**) may be configured to cause rule gates **120** and **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated

by packet-filtering system **200** in one or more of step **#s 6**, **7**, **12-32**, or **35-41**), and one or more of log or drop the packets.

[61] Host **106** may generate one or more packets destined for hosts **108**, **142**, **144**, and **146** and, at step **#43**, may communicate the packets toward hosts **108**, **142**, **144**, and **146**. Rules **212** (e.g., one or more of rules **212** reconfigured in step **#34**) may be configured to cause rule gate **120** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6**, **7**, **12-32**, or **35-42**), and one or more of log or drop the packets.

[62] Referring to **FIG. 4A**, step **#s 1-5** substantially correspond to step **#s 1-5** of **FIG. 3A**.

[63] Host **106** (e.g., the web browser) may be configured to utilize web proxy **118** and responsive to the request, may generate packets comprising data configured to establish a connection between host **106** and web proxy **118** (e.g., a TCP: SYN handshake message) and, at step **#6**, may communicate the packets to web proxy **118**. Rule gate **120** may interface a communication link interfacing host **106** and web proxy **118**, and rules **212** may be configured to cause rule gate **120** to one or more of identify the packets, for example, based on one or more network addresses included in their network-layer headers (e.g., a network address of web proxy **118**) or one or more ports (e.g., port 80) indicated by transport-layer headers in the packets, and one or more of log or drop the packets.

[64] Responsive to receiving the packets from host **106**, web proxy **118** may generate packets comprising data configured to establish the connection between host **106** and web proxy **118** (e.g., a TCP: SYN-ACK handshake message) and, at step **#7**, may

communicate the packets to host **106**. Rules **212** may be configured to cause rule gate **120** to one or more of identify the packets, for example, based on one or more network addresses included in their network-layer headers (e.g., a network address of web proxy **118**) or one or more ports (e.g., port 80) indicated by transport-layer headers in the packets, and one or more of log or drop the packets.

[65] Responsive to receiving the packets from web proxy **118**, host **106** may generate packets comprising data configured to establish the connection between host **106** and web proxy **118** (e.g., a TCP: ACK handshake message) and, at step **#8**, may communicate the packets to web proxy **118**. Rules **212** may be configured to cause rule gate **120** to one or more of identify the packets, for example, based on one or more network addresses included in their network-layer headers (e.g., a network address of web proxy **118**) or one or more ports (e.g., port 80) indicated by transport-layer headers in the packets, and one or more of log or drop the packets.

[66] Web proxy **118** may receive the packets from host **106**, and connection **402** (e.g., a TCP connection) between host **106** and web proxy **118** may be established. Host **106** may generate packets comprising a request (e.g., an HTTP CONNECT request), and, at step **#9**, may communicate the packets to web proxy **118** via connection **402**. Rules **212** may be configured to cause rule gate **120** to one or more of identify the packets, for example, based on one or more network addresses included in their network-layer headers (e.g., a network address of web proxy **118**) or one or more ports (e.g., port 80) indicated by transport-layer headers in the packets, determine the packets comprise data corresponding to the network-threat indicators, for example, a domain name (e.g., FQDN) in the request, and one or more of log or drop the packets.

[67] Web proxy **118** may generate a DNS query comprising the domain name and, at step **#10**, may communicate the DNS query toward DNS **130**. The domain name included in the request may correspond to one or more of the network-threat indicators, and rules **212** may be configured to cause rule gate **126** to one or more of identify one or more packets comprising the DNS query, determine that the packets comprise the domain

EX1002
CISCO SYSTEMS, INC. / Page 28 of 1453

name corresponding to the network-threat indicators, and one or more of log or drop the packets. For example, the packets may comprise a network address of web proxy **118** (e.g., as a source address in their network-layer headers), and rule gate **126** may generate log data indicating the network address of web proxy **118**. As depicted by step **#10A**, the packets may be communicated to DNS **130**. In some embodiments, rules **212** may be configured to cause rule gate **126** to, responsive to determining that the packets comprise the domain name corresponding to the network-threat indicators, drop the packets, preventing them from reaching DNS **130**, as depicted by step **#10B**.

[68] DNS **130** may generate a reply to the DNS query and, at step **#11**, may communicate the reply toward web proxy **118**. The reply may comprise the domain name corresponding to the network-threat indicators, and rules **212** may be configured to cause rule gate **126** to one or more of identify one or more packets comprising the reply, determine that the packets comprise the domain name corresponding to the network-threat indicators, and one or more of log or drop the packets. For example, the packets may comprise the network address of web proxy **118** (e.g., as a destination address in their network-layer headers), and rule gate **126** may generate log data indicating the network address of web proxy **118**. Similarly, the domain name may correspond to host **142**, the packets may comprise a network address of host **142** (e.g., DNS **130** may have resolved the domain name included in the query to the network address of host **142**.), and rule gate **126** may generate log data indicating the network address of host **142**. As depicted by step **#11A**, the packets may be communicated to web proxy **118**. In some embodiments, rules **212** may be configured to cause rule gate **126** to, responsive to determining that the packets comprise the domain name corresponding to the network-threat indicators, drop the packets, preventing them from reaching web proxy **118**, as depicted by step **#11B**.

[69] Web proxy **118** may generate one or more packets destined for host **142** comprising data (e.g., a TCP: SYN handshake message) configured to establish a connection (e.g., a TCP connection or tunnel) between web proxy **118** and host **142** and, at step **#12**, may

communicate the packets toward host **142**. Rule gate **122** may interface a communication link interfacing web proxy **118** and host **142**, and rules **212** may be configured to cause rule gate **122** to one or more of identify the packets or determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more of the packets comprising the request, the DNS query, or the reply to the DNS query based on data stored in logs **214** (e.g., the log data generated by rule gates **120** and **126** in one or more of step **#s 6-11**).

[70] At step **#13**, rule gate **122** may route the packets comprising the data configured to establish the connection between web proxy **118** and host **142** to proxy device **112** and, at step **#14**, may communicate the packets to proxy device **112**. For example, rules **212** may be configured to cause rule gate **122** to route the packets to proxy device **112** based on data in the packets, for example, one or more ports (e.g., port 443) indicated by transport-layer headers in the packets, indicating the connection between web proxy **118** and host **142** will be utilized to establish an encrypted communication session or tunnel (e.g., a session established in accordance with the transport layer security (TLS) protocol, secure sockets layer (SSL) protocol, secure shell (SSH) protocol, or the like).

[71] Referring to **FIG. 4B**, at step **#15**, proxy devices **112** and **114** may exchange one or more parameters determined from the packets comprising the data configured to establish the connection between web proxy **118** and host **142**, for example, one or more network addresses in network-layer headers of the packets (e.g., network addresses of web proxy **118** and host **142**) or ports indicated by transport-layer headers in the packets (e.g., indicating the type of encrypted communication session the connection will be utilized to establish). Proxy device **112** may utilize the parameters to generate packets comprising data configured to establish a connection between proxy device **112** and web proxy **118** (e.g., a TCP: SYN-ACK handshake message) and, at step **#16**, may communicate the packets to web proxy **118**. Rules **212** may be configured to cause rule gate **122** to one or more of identify the packets or determine (e.g., based on one or

more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more of the packets comprising the request, the DNS query, or the reply to the DNS query based on data stored in logs **214** (e.g., the log data generated by rule gates **120** and **126** in one or more of step **#s 6-11**).

[72] Similarly, proxy device **114** may utilize the parameters to generate packets comprising data configured to establish a connection between proxy device **114** and host **142** (e.g., a TCP: SYN handshake message) and, at step **#17**, may communicate the packets to host **142**. Rules **212** may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6-11** or **16**), and one or more of log or drop the packets.

[73] Responsive to receiving the packets from proxy device **112**, web proxy **118** may generate packets comprising data configured to establish the connection between proxy device **112** and web proxy **118** (e.g., a TCP: ACK handshake message) and, at step **#18**, may communicate the packets to proxy device **112**. Rules **212** may be configured to cause rule gate **122** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6-11**, **16**, or **17**), and one or more of log or drop the packets.

[74] Responsive to receiving the packets from proxy device **114**, host **142** may generate packets comprising data configured to establish the connection between proxy device **114** and host **142** (e.g., a TCP: SYN-ACK handshake message) and, at step **#19**, may communicate the packets to proxy device **114**. Rules **212** may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6-11** or **16-18**), and one or more of log or drop the packets.

[75] Responsive to receiving the packets from host **142**, proxy device **114** may generate packets comprising data configured to establish the connection between proxy device **114** and host **142** (e.g., a TCP: ACK handshake message) and, at step **#20**, may communicate the packets to host **142**. Rules **212** may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6-11** or **16-19**), and one or more of log or drop the packets.

[76] Proxy device **112** may receive the packets comprising data configured to establish the connection between proxy device **112** and web proxy **118** communicated by web proxy **118** in step **#18**, and connection **404** (e.g., a TCP connection) between proxy device **112** and web proxy **118** may be established. Similarly, host **142** may receive the packets comprising data configured to establish the connection between proxy device **114** and

EX1002
CISCO SYSTEMS, INC. / Page 32 of 1453

host **142** communicated by proxy device **114** in step **#20**, and connection **406** (e.g., a TCP connection) between proxy device **114** and host **142** may be established.

[77] At step **#21**, proxy device **112** and host **106** may communicate packets comprising data configured to establish encrypted communication session **408** (e.g., a SSL/TLS session) between proxy device **112** and host **106** via connections **402** and **404**. Rules **212** may be configured to cause one or more of rule gates **120** or **122** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6-11** or **16-20**) or the packets comprising one or more handshake messages configured to establish session **408** that comprise unencrypted data (e.g., including the domain name) corresponding to the network-threat indicators, and one or more of log or drop the packets.

[78] Similarly, at step **#22**, proxy device **114** and host **142** may communicate packets comprising data configured to establish encrypted communication session **410** (e.g., a SSL/TLS session) between proxy device **114** and host **142** via connection **406**, and rules **212** may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6-11** or **16-21**) or the packets comprising one or more handshake messages configured to establish session **410** that comprise unencrypted data (e.g., including the domain name) corresponding to the network-threat indicators, and one or more of log or drop the packets.

[79] Referring to **FIGs. 4B-C**, step **#s 23-47** substantially correspond to step **#s 19-43** of **FIGs. 3B-C**; however, rules **212** may be configured to cause one or more of rule gates **120** or **122** to one or more of identify, drop, or log the packets communicated in one or more of step **#s 23**, **30**, **31**, **36**, **39**, or **44** of **FIGs. 4B-C**.

[80] Referring to **FIG. 5A**, step **#s 1-7** substantially correspond to step **#s 1-7** of **FIG. 3A**.

[81] Host **106** may generate one or more packets destined for host **142** comprising data (e.g., a TCP: SYN handshake message) configured to establish a connection (e.g., a TCP connection or tunnel) between hosts **106** and **142** and, at step **#8**, may communicate the packets to host **142**. Rules **212** may be configured to cause one or more of rule gates **120** or **128** to one or more of identify the packets or determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more of the packets comprising the DNS query or the reply to the DNS query based on data stored in logs **214** (e.g., the log data generated by rule gate **126** in one or more of steps **#6** or **#7**).

[82] Responsive to receiving the packets from host **106**, host **142** may generate packets comprising data configured to establish the connection between hosts **106** and **142** (e.g., a TCP: SYN-ACK handshake message) and, at step **#9**, may communicate the packets to host **106**. Rules **212** may be configured to cause one or more of rule gates **120** or **128** to one or more of identify the packets or determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more of the packets comprising the DNS query or the reply to the DNS query based on data stored in logs **214** (e.g., the log data generated by rule gate **126** in one or more of steps **#6** or **#7**).

[83] Responsive to receiving the packets from host **142**, host **106** may generate packets comprising data configured to establish the connection between hosts **106** and **142**

(e.g., a TCP: ACK handshake message) and, at step **#10**, may communicate the packets to host **142**. Rules **212** may be configured to cause one or more of rule gates **120** or **128** to one or more of identify the packets or determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more of the packets comprising the DNS query or the reply to the DNS query based on data stored in logs **214** (e.g., the log data generated by rule gate **126** in one or more of steps **#6** or **#7**).

[84] Host **142** may receive the packets comprising data configured to establish the connection between hosts **106** and **142** communicated by host **106** in step **#10**, and connection **502** (e.g., a TCP connection) between hosts **106** and **142** may be established.

[85] At step **#11**, hosts **106** and **142** may communicate packets comprising data configured to establish encrypted communication session **504** (e.g., a SSL/TLS session) between hosts **106** and **142** via connection **502**. Rules **212** may be configured to cause one or more of rule gates **120** or **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6-10**) or the packets comprising one or more handshake messages configured to establish session **504** that comprise unencrypted data (e.g., including the domain name) corresponding to the network-threat indicators, and one or more of log or drop the packets.

[86] Host **106** may generate packets comprising data encrypted in accordance with one or more parameters of session **504** and, at step **#12**, may communicate the packets to host **142**. Rules **212** may be configured to cause one or more of rule gates **120** or **128** to one or more of identify the packets, determine (e.g., based on one or more network

addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6-11**), and one or more of log or drop the packets.

[87] Host **142** may generate packets comprising data encrypted in accordance with one or more parameters of session **504** and, at step **#13**, may communicate the packets to host **106**. Rules **212** may be configured to cause one or more of rule gates **120** or **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6-12**), and one or more of log or drop the packets.

[88] Host **106** may generate packets comprising data encrypted in accordance with one or more parameters of session **504** and, at step **#14**, may communicate the packets toward host **142**. Rules **212** may be configured to cause one or more of rule gates **120** or **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6-13**), and one or more of log or drop the packets.

[89] Host **142** may generate packets comprising data encrypted in accordance with one or more parameters of session **504** and, at step **#15**, may communicate the packets toward

host **106**. Rules **212** may be configured to cause one or more of rule gates **120** or **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6-14**), and one or more of log or drop the packets.

[90] Referring to **FIG. 5B**, steps **#16** and **#17** substantially correspond to steps **#33** and **#34** of **FIG. 3C**.

[91] Host **106** may generate packets comprising data encrypted in accordance with one or more parameters of session **504** and, at step **#18**, may communicate the packets toward host **142**. Rules **212** (e.g., one or more of rules **212** reconfigured in step **#17**) may be configured to cause one or more of rule gates **120** or **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6-15**), and one or more of log or drop the packets.

[92] Host **142** may generate packets comprising data encrypted in accordance with one or more parameters of session **504** and, at step **#19**, may communicate the packets toward host **106**. Rules **212** (e.g., one or more of rules **212** reconfigured in step **#17**) may be configured to cause one or more of rule gates **120** or **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets

EX1002
CISCO SYSTEMS, INC. / Page 37 of 1453

previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6-15** and **18**), and one or more of log or drop the packets.

[93] Step **#s 20-22** substantially correspond to step **#s 41-43** of **FIG. 3C**.

[94] Referring to **FIG. 6A**, step **#s 1-11** substantially correspond to step **#s 1-11** of **FIG. 4A**.

[95] Web proxy **118** may generate one or more packets destined for host **142** comprising data (e.g., a TCP: SYN handshake message) configured to establish a connection (e.g., a TCP connection or tunnel) between web proxy **118** and host **142** and, at step **#12**, may communicate the packets to host **142**. Rules **212** may be configured to cause one or more of rule gates **122** or **128** to one or more of identify the packets or determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more of the packets comprising the DNS query or the reply to the DNS query based on data stored in logs **214** (e.g., the log data generated by rule gate **126** in one or more of steps **#10** or **#11**).

[96] Responsive to receiving the packets from web proxy **118**, host **142** may generate packets comprising data configured to establish the connection between web proxy **118** and host **142** (e.g., a TCP: SYN-ACK handshake message) and, at step **#13**, may communicate the packets to web proxy **118**. Rules **212** may be configured to cause one or more of rule gates **122** or **128** to one or more of identify the packets or determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more of the packets comprising the DNS query or the reply to the DNS query based on data stored in logs **214** (e.g., the log data generated by rule gate **126** in one or more of steps **#10** or **#11**).

[97] Responsive to receiving the packets from host **142**, web proxy **118** may generate packets comprising data configured to establish the connection between web proxy **118** and host **142** (e.g., a TCP: ACK handshake message) and, at step **#14**, may communicate the packets to host **142**. Rules **212** may be configured to cause one or more of rule gates **122** or **128** to one or more of identify the packets or determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more of the packets comprising the DNS query or the reply to the DNS query based on data stored in logs **214** (e.g., the log data generated by rule gate **126** in one or more of steps **#10** or **#11**).

[98] Referring to **FIG. 6B**, host **142** may receive the packets comprising data configured to establish the connection between web proxy **118** and host **142** communicated by web proxy **118** in step **#14**, and connection **604** (e.g., a TCP connection) between web proxy **118** and host **142** may be established.

[99] At step **#15**, hosts **106** and **142** may communicate packets comprising data configured to establish encrypted communication session **606** (e.g., a SSL/TLS session) between hosts **106** and **142** via connections **602** and **604**. Rules **212** may be configured to cause one or more of rule gates **120**, **122**, or **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step **#s 6-15**) or the packets comprising one or more handshake messages configured to establish session **606** that comprise unencrypted data (e.g., including the domain name) corresponding to the network-threat indicators, and one or more of log or drop the packets.

EX1002
CISCO SYSTEMS, INC. / Page 39 of 1453

[100] Step **#s 16-26** substantially correspond to step **#s 12-22** of **FIGs. 5A-B**; however, rules **212** may be configured to cause one or more of rule gates **120**, **122**, or **128** to one or more of identify, drop, or log the packets communicated in one or more of step **#s 16-19**, **22**, or **23** of **FIG. 6B**.

[101] **FIG. 7** depicts an illustrative method for rule-based network-threat detection for encrypted communications in accordance with one or more aspects of the disclosure. Referring to **FIG. 7**, in step **702**, a packet-filtering system may receive data indicating network-threat indicators. For example, packet-filtering system **200** may receive packet-filtering rules generated by rule provides **138** based on network-threat indicators provided by threat-intelligence providers **140**. In step **704**, the packet-filtering system may configure packet-filtering rules in accordance with which it is configured to filter packets. For example, packet-filtering system **200** may configure rules **212**.

[102] In step **706**, the packet-filtering system may identify packets comprising unencrypted data. For example, packet-filtering system **200** may identify packets comprising a DNS query, a reply to a DNS query, or a handshake message configured to establish an encrypted communication session. In step **708**, the packet-filtering system may identify packets comprising encrypted data. For example, packet-filtering system **200** may identify packets encrypted in accordance with one or more parameters of sessions **306**, **308**, **408**, **410**, **504**, or **606**.

[103] In step **710**, the packet-filtering system may determine based on a portion of the unencrypted data corresponding to the network-threat indicators that the packets comprising encrypted data correspond to the network-threat indicators. For example, packet-filtering system **200** may determine that a domain name included in the DNS query, the reply to the DNS query, or the handshake message corresponds to the network-threat indicators, and packet-filtering system **200** may determine that one or more of the packets encrypted in accordance with the parameters of sessions **306**, **308**, **408**, **410**, **504**, or **606** correlate to one or more packets comprising the DNS query, the reply to the DNS query, or the one or more handshake messages.

[104] The functions and steps described herein may be embodied in computer-usable data or computer-executable instructions, such as in one or more program modules, executed by one or more computers or other devices to perform one or more functions described herein. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types when executed by one or more processors in a computer or other data-processing device. The computer-executable instructions may be stored on a computer-readable medium such as a hard disk, optical disk, removable storage media, solid-state memory, RAM, etc. As will be appreciated, the functionality of the program modules may be combined or distributed as desired. In addition, the functionality may be embodied in whole or in part in firmware or hardware equivalents, such as integrated circuits, application-specific integrated circuits (ASICs), field-programmable gate arrays (FPGA), and the like. Particular data structures may be used to more effectively implement one or more aspects of the disclosure, and such data structures are contemplated to be within the scope of computer-executable instructions and computer-usable data described herein.

[105] Although not required, one of ordinary skill in the art will appreciate that various aspects described herein may be embodied as a method, system, apparatus, or one or more computer-readable media storing computer-executable instructions. Accordingly, aspects may take the form of an entirely hardware embodiment, an entirely software embodiment, an entirely firmware embodiment, or an embodiment combining software, hardware, and firmware aspects in any combination.

[106] As described herein, the various methods and acts may be operative across one or more computing devices and networks. The functionality may be distributed in any manner or may be located in a single computing device (e.g., a server, client computer, or the like).

[107] Aspects of the disclosure have been described in terms of illustrative embodiments thereof. Numerous other embodiments, modifications, and variations within the scope and spirit of the appended claims will occur to persons of ordinary skill in the art from a

review of this disclosure. For example, one of ordinary skill in the art will appreciate that the steps illustrated in the illustrative figures may be performed in other than the recited order and that one or more illustrated steps may be optional. Any and all features in the following claims may be combined or rearranged in any way possible.

EX1002
CISCO SYSTEMS, INC. / Page 42 of 1453

What is claimed is:

1. A method comprising:

receiving, by a packet-filtering system configured to filter packets in accordance with a plurality of packet-filtering rules, data indicating a plurality of network-threat indicators; and

configuring, by the packet-filtering system, the plurality of packet-filtering rules to cause the packet-filtering system to:

identify packets comprising unencrypted data;

identify packets comprising encrypted data; and

determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, that the packets comprising encrypted data correspond to the one or more network-threat indicators.

2. The method of claim 1, wherein:

the one or more network-threat indicators comprise a domain name;

the packets comprising unencrypted data comprise one or more packets comprising at least one of a domain name system (DNS) query or a reply to the DNS query; and

the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to determine that the at least one of the DNS query or the reply to the DNS query comprises the domain name.

3. The method of claim 2, wherein:

the portion of the unencrypted data comprises one or more network addresses included in the at least one of the DNS query or the reply to the DNS query; and

the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to determine that the packets comprising encrypted data comprise

EX1002
CISCO SYSTEMS, INC. / Page 43 of 1453

one or more packet headers comprising at least one of the one or more network addresses.

4. The method of claim 2, wherein:

the portion of the unencrypted data comprises one or more network addresses included in one or more headers of the one or more packets comprising the at least one of the DNS query or the reply to the DNS query; and

the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to determine that the packets comprising encrypted data comprise one or more packet headers comprising at least one of the one or more network addresses.

5. The method of claim 4, wherein:

the one or more network addresses comprise a network address of a web proxy that generated the DNS query in response to a request received from a host; and

the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to identify one or more packets comprising the request.

6. The method of claim 1, wherein:

one or more packets of the packets comprising unencrypted data comprise data configured to establish an encrypted communication session between a first host and a second host; and

the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to route the one or more of the packets to a proxy system.

7. The method of claim 6, wherein:

the one or more network-threat indicators comprise a domain name; and

the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to route the one or more of the packets to the proxy system based

EX1002
CISCO SYSTEMS, INC. / Page 44 of 1453

on a determination that at least one of the first host or the second host corresponds to the domain name.

8. The method of claim 6, wherein:

the plurality of packet-filtering rules indicate:

one or more network addresses for which encrypted communications should be established via the proxy system, and

one or more network addresses for which encrypted communications should not be established via the proxy system; and

the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to route the one or more of the packets to the proxy system based on a determination that at least one of the first host or the second host corresponds to the one or more network addresses for which encrypted communications should be established via the proxy system.

9. The method of claim 6, wherein:

the packet-filtering system comprises:

one or more interfaces interfacing the packet-filtering system with one or more communication links interfacing the first host and the second host, and

one or more interfaces interfacing the packet-filtering system with the proxy system; and

the configuring the packet-filtering system to route the one or more of the packets to the proxy system comprises configuring the packet-filtering system to redirect packets received via the one or more interfaces interfacing the packet-filtering system with the one or more communication links interfacing the first host and the second host to the one or more interfaces interfacing the packet-filtering system with the proxy system.

10. The method of claim 6, wherein:

the packet-filtering system comprises:

one or more interfaces interfacing the packet-filtering system with one or more communication links interfacing the first host and the second host, and

one or more interfaces interfacing the packet-filtering system with the proxy system; and

the configuring the packet-filtering system to route the one or more of the packets to the proxy system comprises configuring the packet-filtering system to forward copies of packets received via the one or more interfaces interfacing the packet-filtering system with the one or more communication links interfacing the first host and the second host to the one or more interfaces interfacing the packet-filtering system with the proxy system.

11. The method of claim 6, wherein the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to:

identify, via a communication link interfacing the first host and the proxy system, the packets comprising encrypted data; and

identify, via an internal communication link of the proxy system, packets corresponding to the packets comprising encrypted data.

12. The method of claim 11, wherein the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to identify, via a communication link interfacing the proxy system and the second host, packets generated by the proxy system based on the packets corresponding to the packets comprising encrypted data.

13. The method of claim 6, wherein the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to, responsive to determining that one or more packets generated by the proxy system based on one or more of the packets comprising encrypted data correspond to one or more criteria specified by the plurality of packet-filtering rules, at least one of:

drop the one or more packets generated by the proxy system;

log the one or more packets generated by the proxy system;

drop one or more other packets generated by the proxy system;

log one or more other packets generated by the proxy system;

drop one or more other packets of the packets comprising encrypted data; or

log one or more other packets of the packets comprising encrypted data.

14. The method of claim 13, wherein the determining comprises determining that the one or more packets generated by the proxy system comprise at least one of a uniform resource identifier (URI) specified by the plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules.

15. The method of claim 13, wherein the determining comprises determining that the one or more packets generated by the proxy system comprise a uniform resource identifier (URI) meeting a threshold size specified by the plurality of packet-filtering rules.

16. The method of claim 6, wherein the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to identify, via a communication link interfacing the proxy system and an Internet content adaptation protocol (ICAP) server, one or more packets comprising at least one of an ICAP request, a response generated by the ICAP server, or a modified request generated by the ICAP server.

17. The method of claim 1, wherein the packets comprising encrypted data comprise packets received from a first host and destined for a second host, the method comprising configuring the plurality of packet-filtering rules to cause the packet-filtering system to at least one of drop or log packets other than the packets comprising encrypted data based on a determination that the packets other than the packets comprising encrypted data were at least one of received from the second host or destined for the first host.

18. The method of claim 1, wherein:

the one or more network-threat indicators comprise a domain name;

the packets comprising unencrypted data comprise one or more packets comprising one or more handshake messages configured to establish an encrypted communication session between a client and a server; and

the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to determine that the one or more handshake messages comprise the domain name.

19. The method of claim 18, wherein the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to, responsive to determining that the one or more handshake messages comprise the domain name, at least one of drop or log the packets comprising encrypted data.

20. The method of claim 18, wherein:

the one or more handshake messages comprise at least one of a hello message generated by the client or a certificate message generated by the server; and

the configuring the packet-filtering system to determine that the one or more handshake messages comprise the domain name comprises configuring the packet-filtering system to determine the at least one of the hello message generated by the client or the certificate message generated by the server comprises the domain name.

21. The method of claim 18, wherein:

the portion of the unencrypted data comprises one or more network addresses included in one or more headers of the one or more packets comprising the one or more handshake messages; and

the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to determine that the packets comprising encrypted data comprise

one or more packet headers comprising at least one of the one or more network addresses.

22. The method of claim 21, wherein:

the one or more network addresses comprise a network address of the server and a network address of a web proxy; and

the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to:

identify one or more packets comprising one or more packet headers comprising the network address of the web proxy and a network address of the client; and

determine that the packets comprising encrypted data comprise one or more packet headers comprising the network address of the server and the network address of the client.

23. The method of claim 1, wherein:

the packets comprising unencrypted data comprise a certificate message for an encrypted communication session; and

the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to at least one of drop or log one or more of the packets comprising encrypted data based on a determination that the certificate message comprises data indicating at least one of a serial number indicated by the plurality of packet-filtering rules, an issuer indicated by the plurality of packet-filtering rules, a validity time-range indicated by the plurality of packet-filtering rules, a key indicated by the plurality of packet-filtering rules, or a signing authority indicated by the plurality of packet-filtering rules.

24. A packet-filtering system comprising:

at least one processor; and

a memory storing instructions that when executed by the at least one processor cause the packet-filtering system to:

receive data indicating a plurality of network-threat indicators;

configure a plurality of packet-filtering rules, in accordance with which the packet-filtering system is configured to filter packets, to cause the packet-filtering system to:

identify packets comprising unencrypted data;

identify packets comprising encrypted data; and

determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, that the packets comprising encrypted data correspond to the one or more network-threat indicators.

25. One or more non-transitory computer-readable media comprising instructions that when executed by at least one processor of a packet-filtering system cause the packet-filtering system to:

receive data indicating a plurality of network-threat indicators;

configure a plurality of packet-filtering rules, in accordance with which the packet-filtering system is configured to filter packets, to cause the packet-filtering system to:

identify packets comprising unencrypted data;

identify packets comprising encrypted data; and

determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, that the packets comprising encrypted data correspond to the one or more network-threat indicators.

EX1002
CISCO SYSTEMS, INC. / Page 50 of 1453

ABSTRACT

A packet-filtering system configured to filter packets in accordance with packet-filtering rules may receive data indicating network-threat indicators and may configure the packet-filtering rules to cause the packet-filtering system to identify packets comprising unencrypted data, and packets comprising encrypted data. A portion of the unencrypted data may correspond to one or more of the network-threat indicators, and the packet-filtering rules may be configured to cause the packet-filtering system to determine, based on the portion of the unencrypted data, that the packets comprising encrypted data correspond to the one or more network-threat indicators.

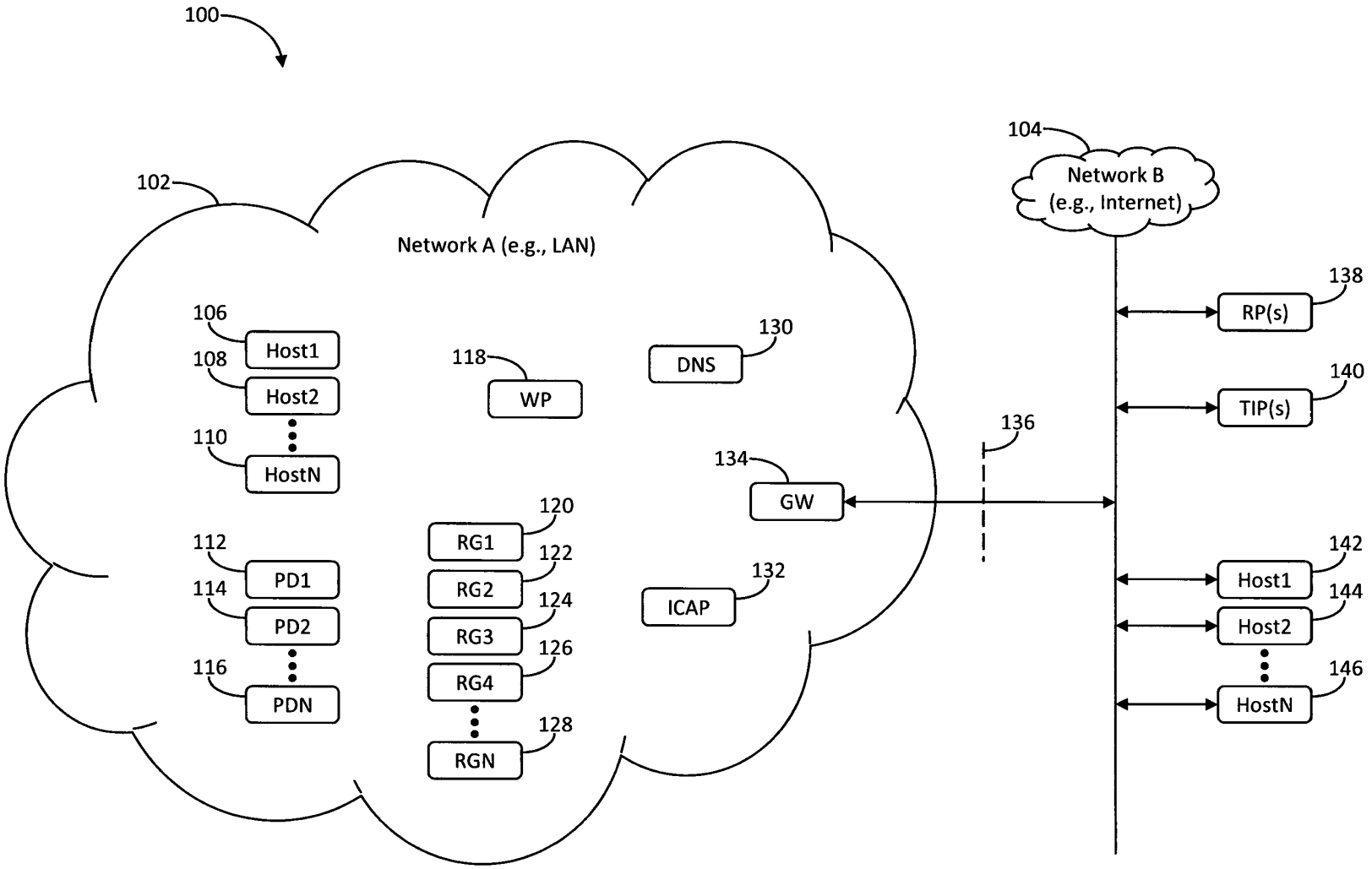


FIG. 1

EX1002
CISCO SYSTEMS, INC. / Page 52 of 1453

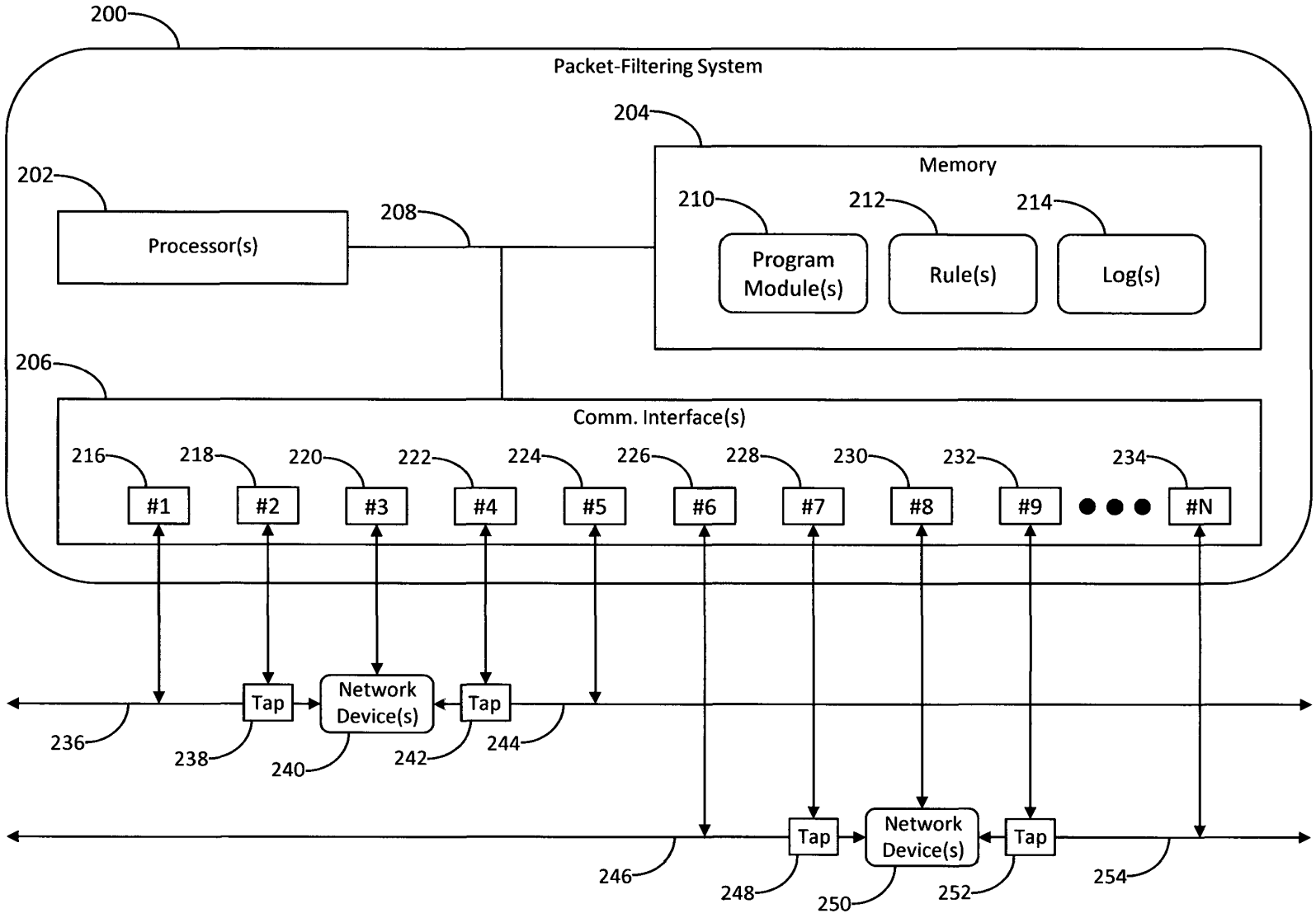


FIG. 2

CISCO SYSTEMS, INC. / Page 53 of 1453
EX1002

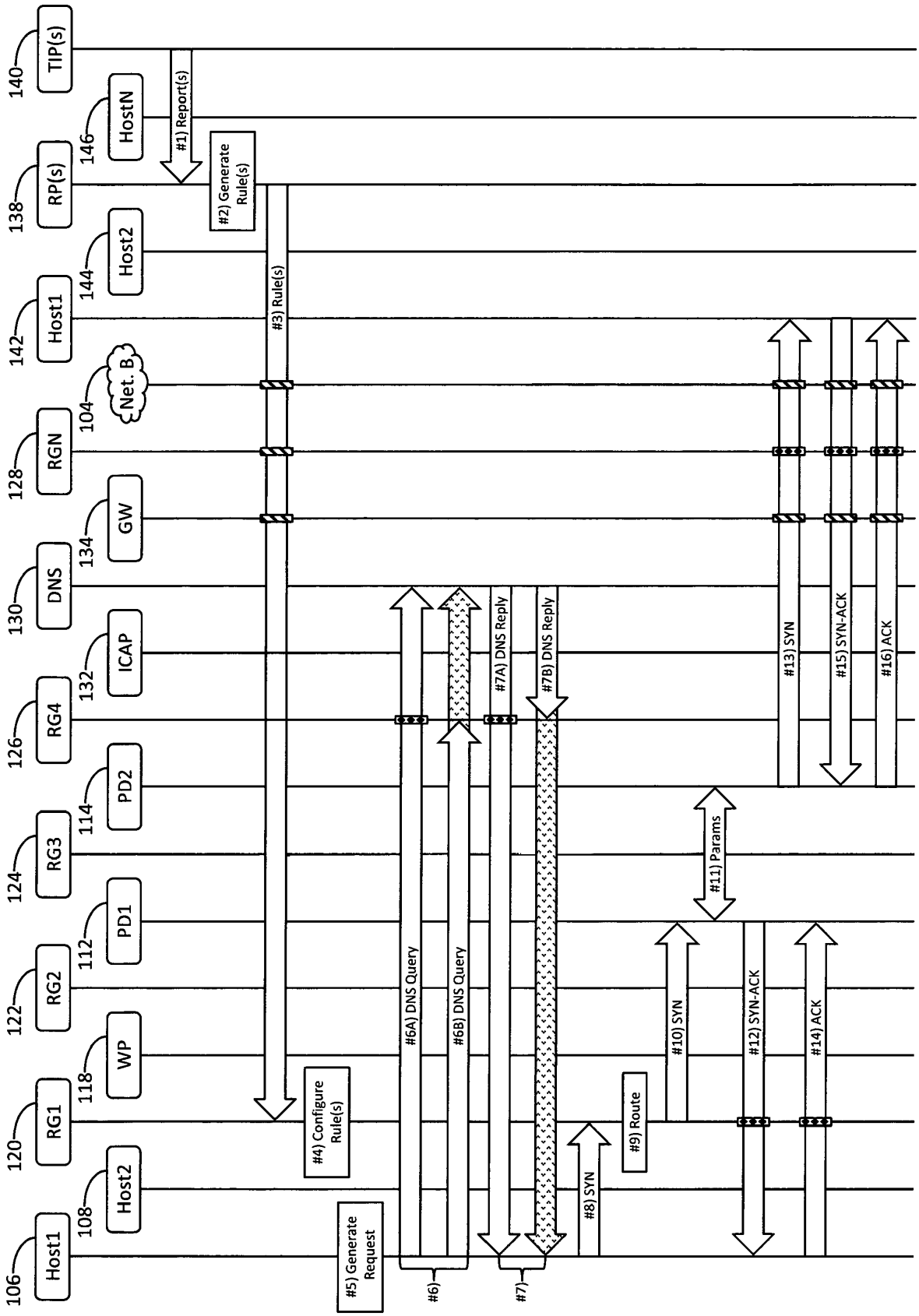

106 Host1
108 Host2
120 RG1
118 WP
122 RG2
112 PD1
124 RG3
114 PD2
126 RG4
132 ICAP
130 DNS
134 GW
128 RGN
104 Net. B
142 Host1
144 Host2
138 RP(s)
146 HostN
140 TIP(s)
#1) Report(s)
#2) Generate Rule(s)
#3) Rule(s)
#4) Configure Rule(s)
#5) Generate Request
#6A) DNS Query
#6B) DNS Query
#6)
#7A) DNS Reply
#7B) DNS Reply
#7)
#8) SYN
#9) Route
#10) SYN
#11) Params
#12) SYN-ACK
#13) SYN
#14) ACK
#15) SYN-ACK
#16) ACK

FIG. 3A

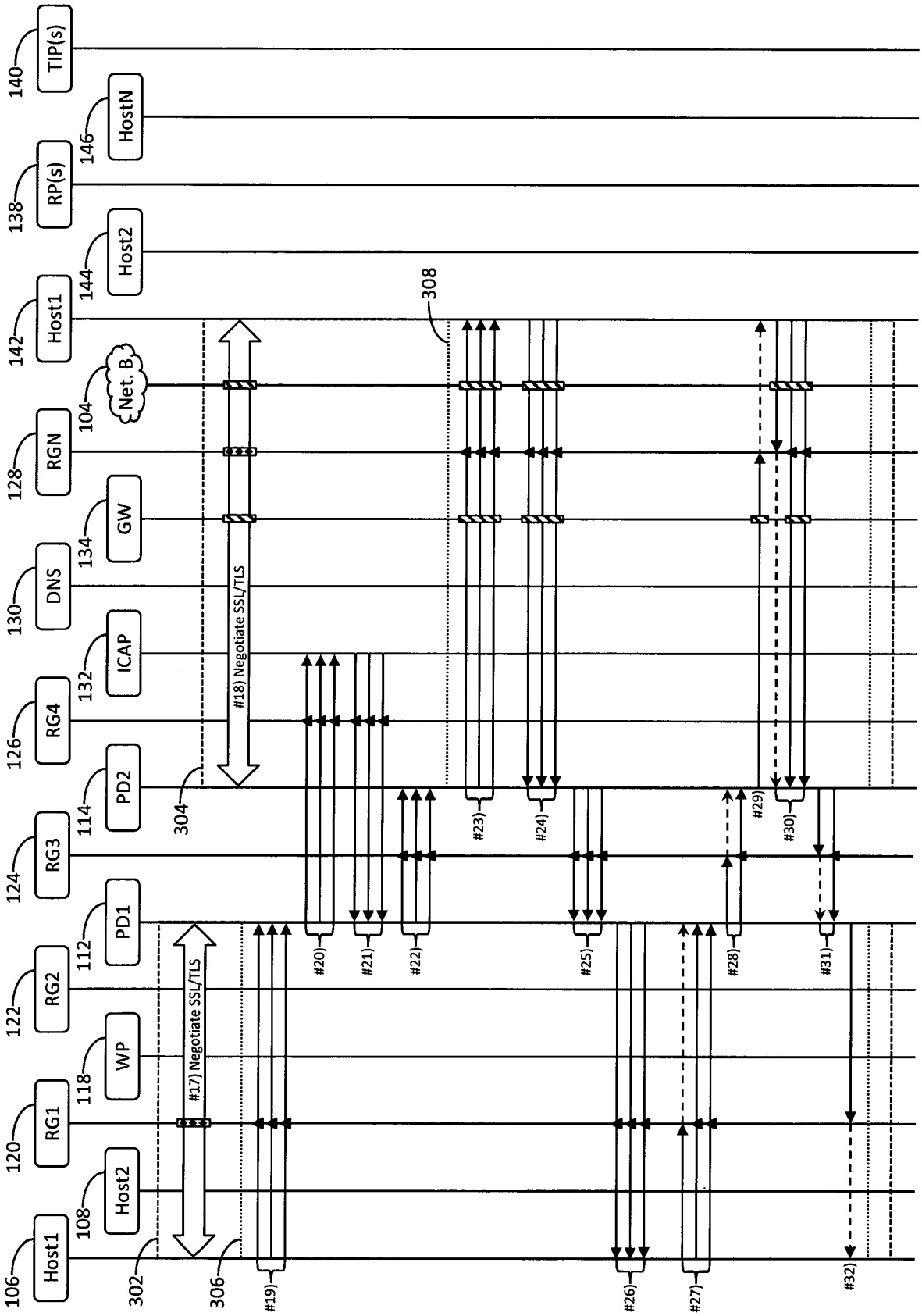

106 Host1
108 Host2
120 RG1
118 WP
122 RG2
112 PD1
124 RG3
114 PD2
126 RG4
132 ICAP
130 DNS
134 GW
128 RGN
104 Net. B
142 Host1
144 Host2
138 RP(s)
146 HostN
140 TIP(s)
302
306
304
308
#17) Negotiate SSL/TLS
#18) Negotiate SSL/TLS
#19)
#20)
#21)
#22)
#23)
#24)
#25)
#26)
#27)
#28)
#29)
#30)
#31)
#32)

FIG. 3B

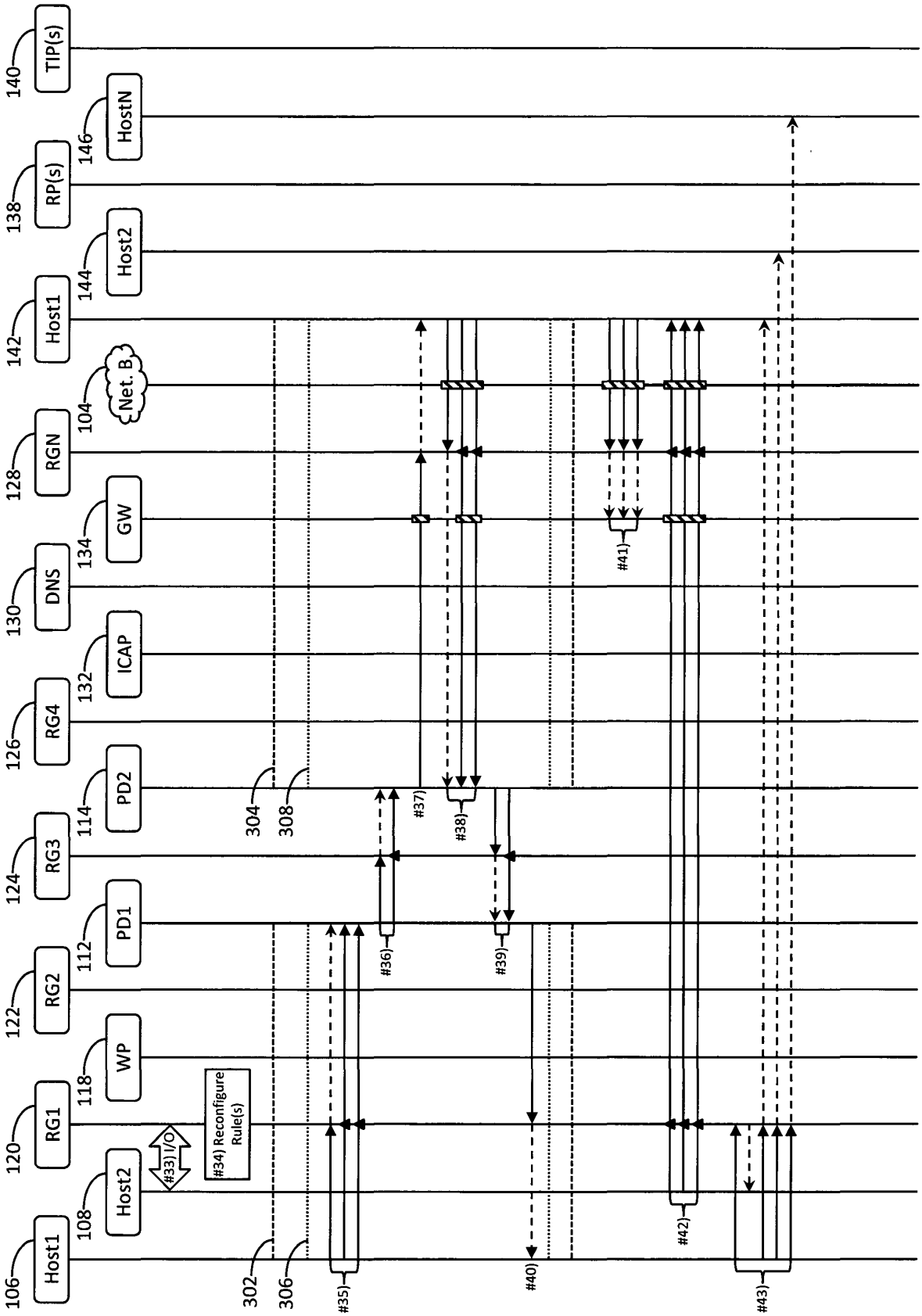

106 Host1
108 Host2
120 RG1
118 WP
122 RG2
112 PD1
124 RG3
114 PD2
126 RG4
132 ICAP
130 DNS
134 GW
128 RGN
104 Net. B
142 Host1
144 Host2
138 RP(s)
146 HostN
140 TIP(s)
#33) I/O
#34) Reconfigure Rule(s)
302
306
304
308
#35)
#36)
#37)
#38)
#39)
#40)
#41)
#42)
#43)

FIG. 3C

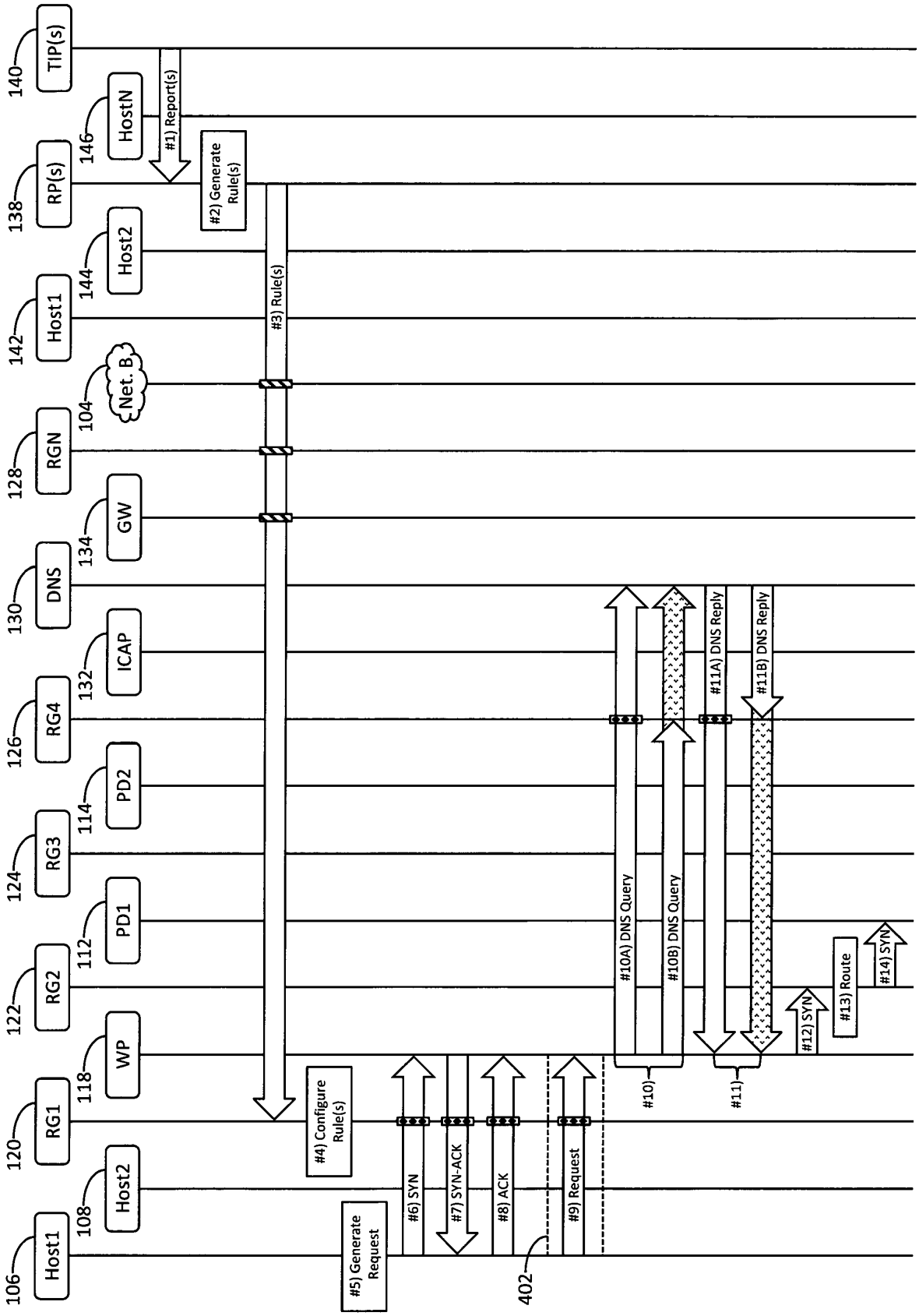

106 Host1
108 Host2
120 RG1
122 RG2
124 RG3
126 RG4
128 RGN
130 DNS
132 ICAP
134 GW
104 Net. B
142 Host1
144 Host2
138 RP(s)
146 HostN
140 TIP(s)
118 WP
112 PD1
114 PD2
#1) Report(s)
#2) Generate Rule(s)
#3) Rule(s)
#4) Configure Rule(s)
#5) Generate Request
#6) SYN
#7) SYN-ACK
#8) ACK
#9) Request
402
#10A) DNS Query
#10B) DNS Query
#10)
#11A) DNS Reply
#11B) DNS Reply
#11)
#12) SYN
#13) Route
#14) SYN

FIG. 4A

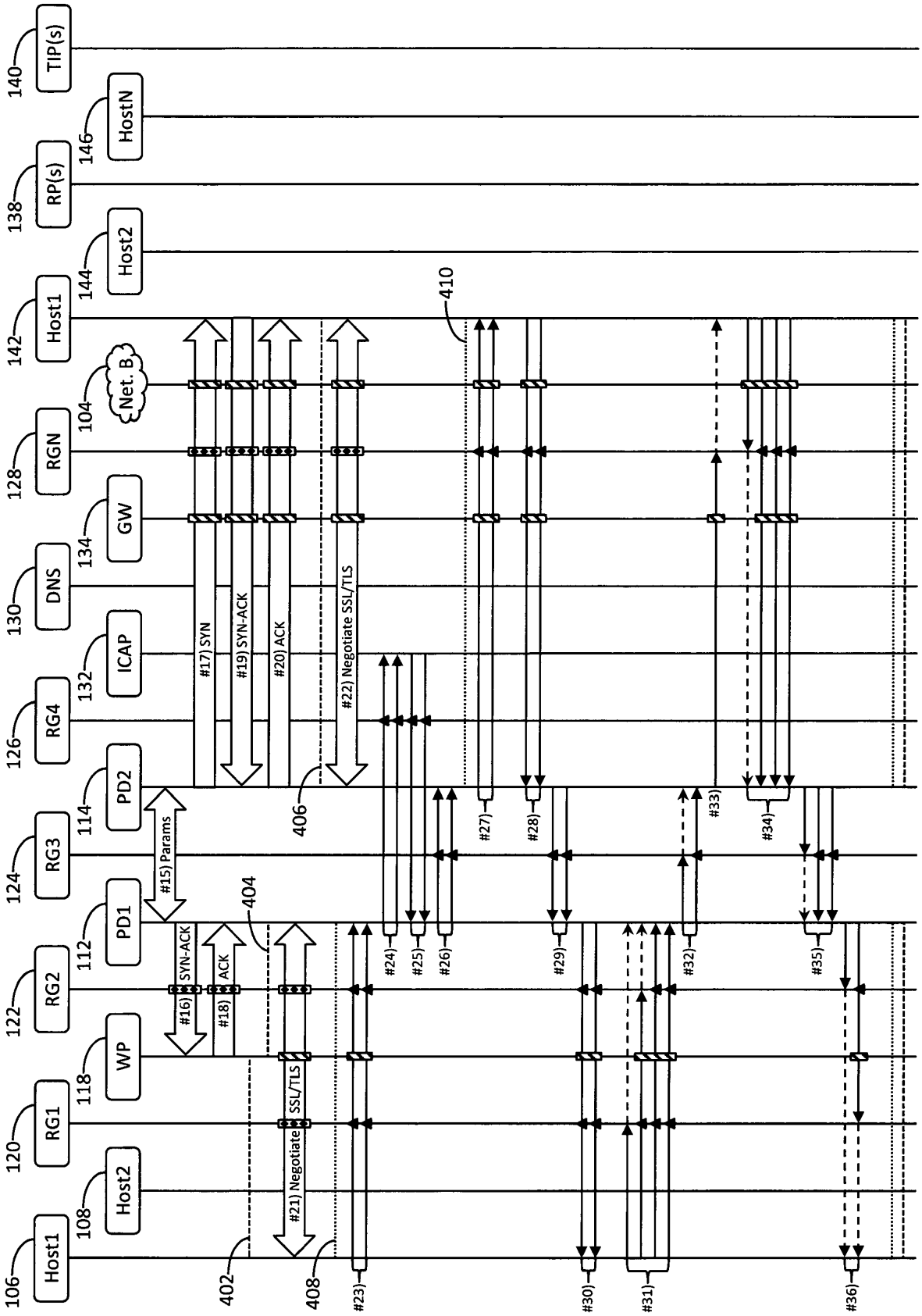

106 Host1
108 Host2
120 RG1
118 WP
122 RG2
112 PD1
124 RG3
114 PD2
126 RG4
132 ICAP
130 DNS
134 GW
128 RGN
104 Net. B
142 Host1
144 Host2
138 RP(s)
146 HostN
140 TIP(s)
#15) Params
#16) SYN-ACK
#17) SYN
#18) ACK
#19) SYN-ACK
#20) ACK
#21) Negotiate SSL/TLS
#22) Negotiate SSL/TLS
#23)
#24)
#25)
#26)
#27)
#28)
#29)
#30)
#31)
#32)
#33)
#34)
#35)
#36)
402
404
406
408
410

FIG. 4B

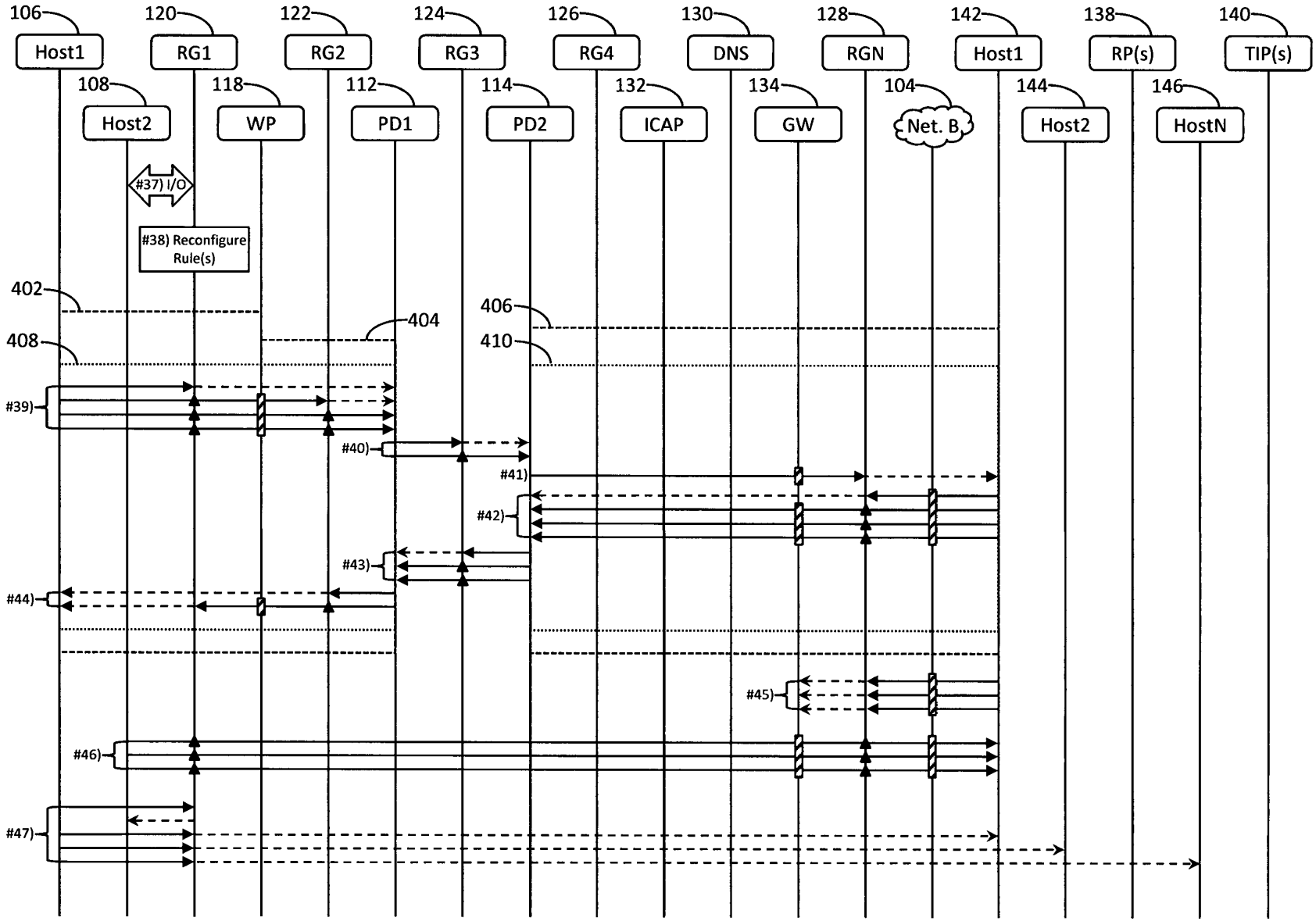


FIG. 4C

CISCO SYSTEMS, INC. / Page 59 of 1453
EX1002

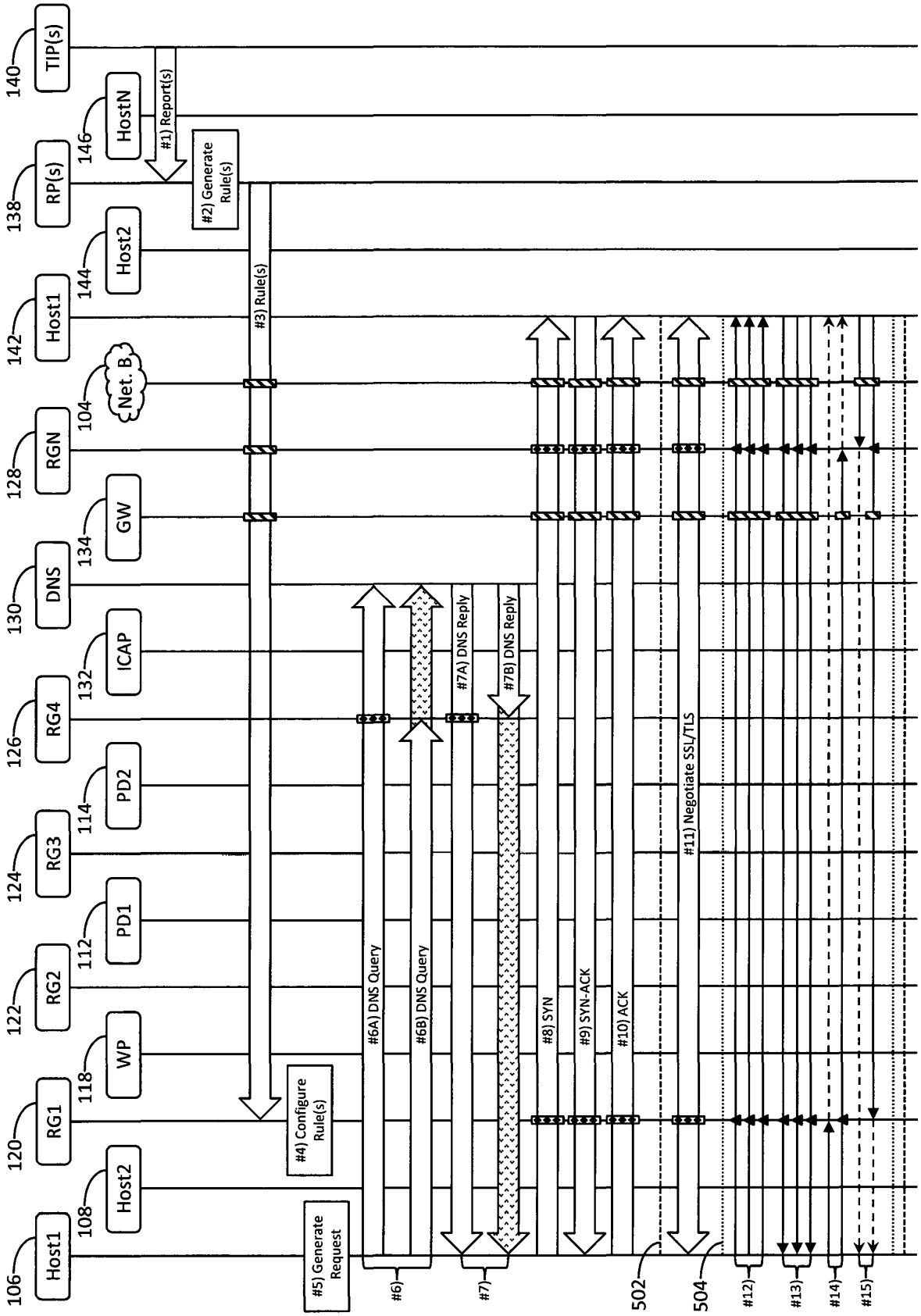

106 Host1
108 Host2
120 RG1
118 WP
122 RG2
112 PD1
124 RG3
114 PD2
126 RG4
132 ICAP
130 DNS
134 GW
128 RGN
104 Net. B
142 Host1
144 Host2
138 RP(s)
146 HostN
140 TIP(s)
#1) Report(s)
#2) Generate Rule(s)
#3) Rule(s)
#4) Configure Rule(s)
#5) Generate Request
#6A) DNS Query
#6B) DNS Query
#7A) DNS Reply
#7B) DNS Reply
#8) SYN
#9) SYN-ACK
#10) ACK
#11) Negotiate SSL/TLS
#6)
#7)
502
504
#12)
#13)
#14)
#15)

FIG. 5A

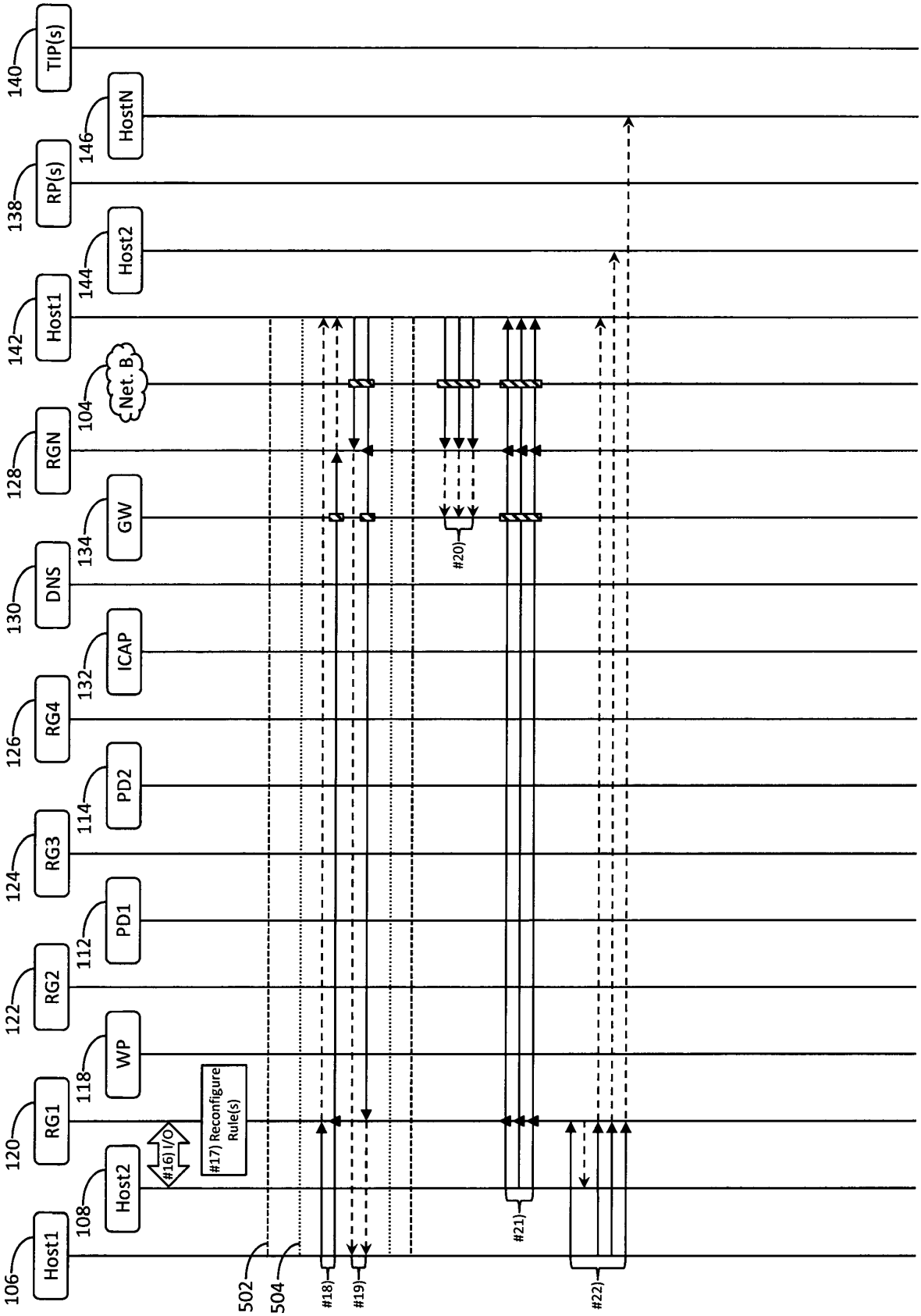

106 Host1
108 Host2
120 RG1
122 RG2
124 RG3
126 RG4
130 DNS
128 RGN
142 Host1
138 RP(s)
140 TIP(s)
118 WP
112 PD1
114 PD2
132 ICAP
134 GW
104 Net. B
144 Host2
146 HostN
#16) I/O
#17) Reconfigure Rule(s)
502
504
#18)
#19)
#20)
#21)
#22)

FIG. 5B

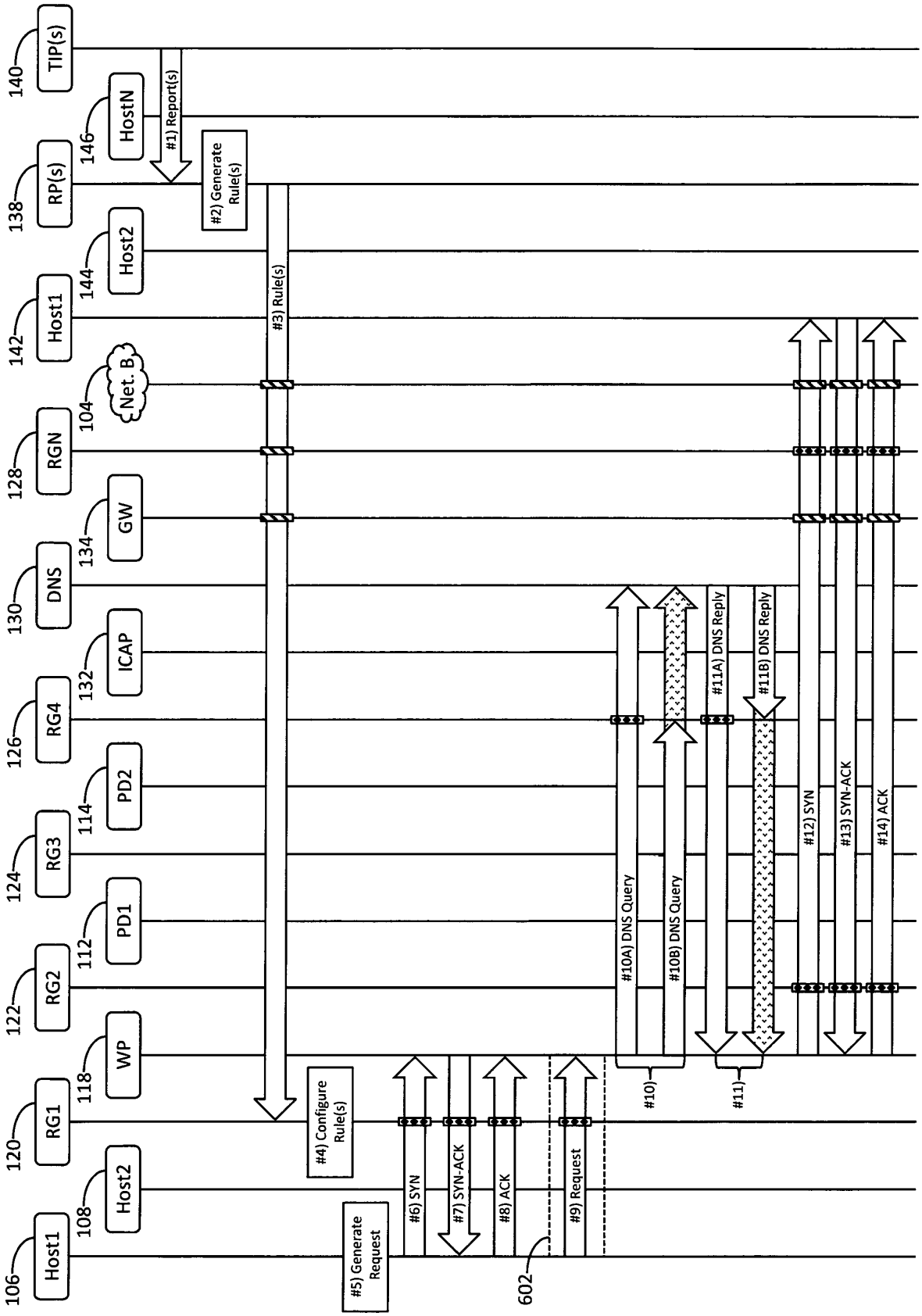

106 Host1
108 Host2
120 RG1
118 WP
122 RG2
112 PD1
124 RG3
114 PD2
126 RG4
132 ICAP
130 DNS
134 GW
128 RGN
104 Net. B
142 Host1
144 Host2
138 RP(s)
146 HostN
140 TIP(s)
#1) Report(s)
#2) Generate Rule(s)
#3) Rule(s)
#4) Configure Rule(s)
#5) Generate Request
#6) SYN
#7) SYN-ACK
#8) ACK
#9) Request
602
#10A) DNS Query
#10B) DNS Query
#10)
#11A) DNS Reply
#11B) DNS Reply
#11)
#12) SYN
#13) SYN-ACK
#14) ACK

FIG. 6A

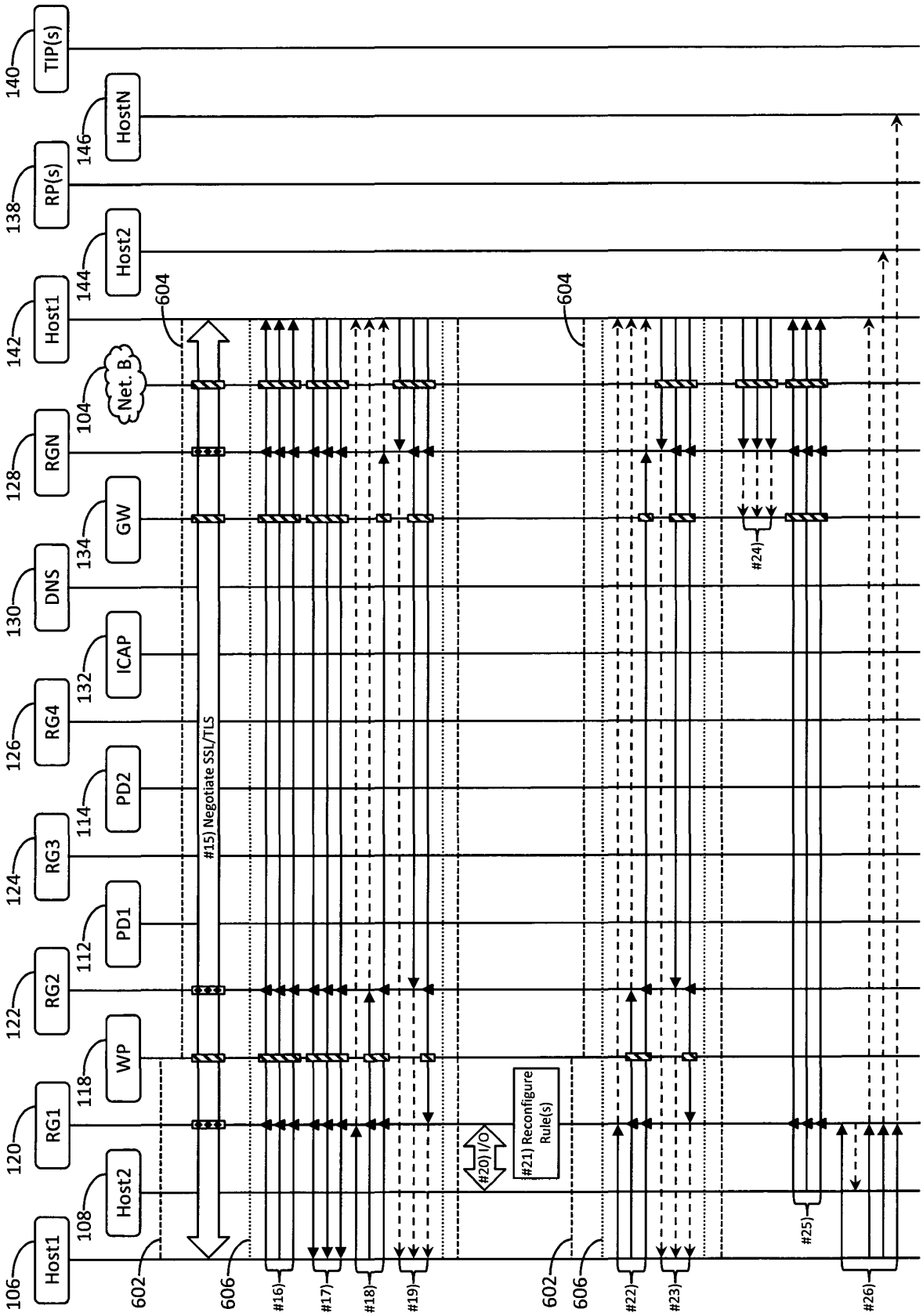

106 Host1
108 Host2
120 RG1
118 WP
122 RG2
112 PD1
124 RG3
114 PD2
126 RG4
132 ICAP
130 DNS
134 GW
128 RGN
104 Net. B
142 Host1
144 Host2
138 RP(s)
146 HostN
140 TIP(s)
602
606
604
#15) Negotiate SSL/TLS
#16)
#17)
#18)
#19)
#20) I/O
#21) Reconfigure Rule(s)
#22)
#23)
#24)
#25)
#26)

FIG. 6B

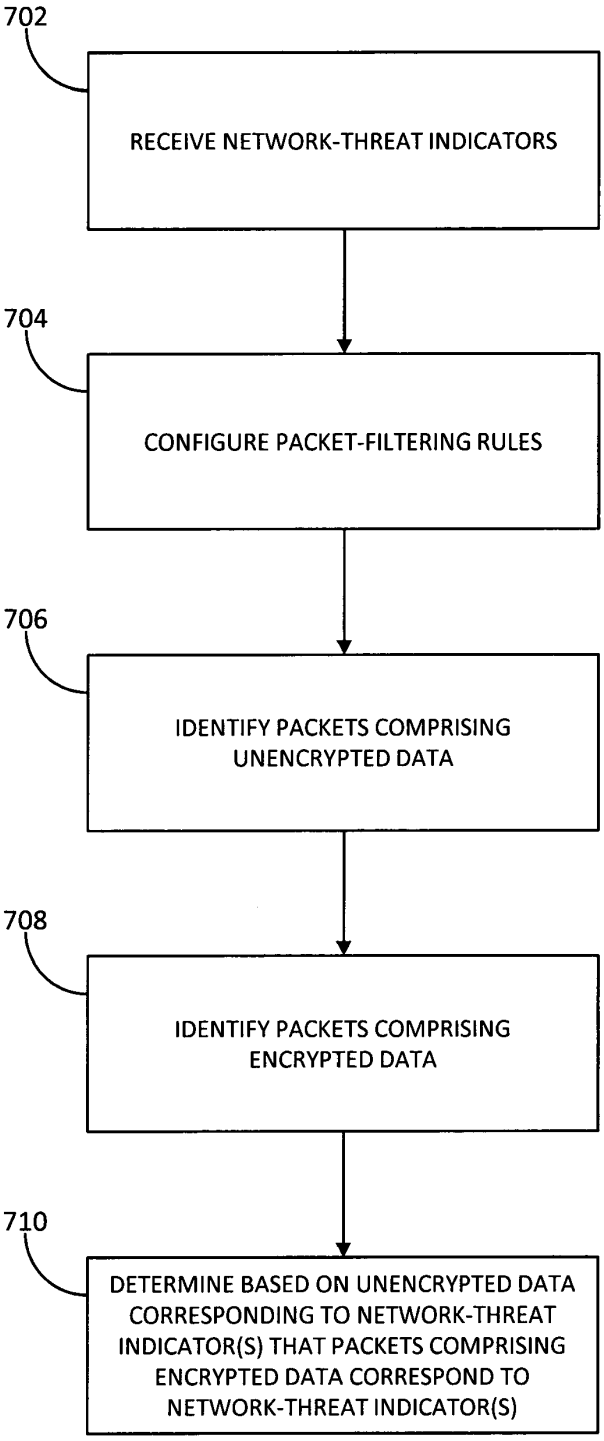

702
RECEIVE NETWORK-THREAT INDICATORS
704
CONFIGURE PACKET-FILTERING RULES
706
IDENTIFY PACKETS COMPRISING UNENCRYPTED DATA
708
IDENTIFY PACKETS COMPRISING ENCRYPTED DATA
710
DETERMINE BASED ON UNENCRYPTED DATA CORRESPONDING TO NETWORK-THREAT INDICATOR(S) THAT PACKETS COMPRISING ENCRYPTED DATA CORRESPOND TO NETWORK-THREAT INDICATOR(S)

FIG. 7

02205 U.S.PTO
122315

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	007742.00059
	Application Number	
Title of Invention	RULE-BASED NETWORK-THREAT DETECTION FOR ENCRYPTED COMMUNICATIONS	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2:

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	David	K.	Ahn	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Winston-Salem	State/Province	NC	Country of Residence	US

Mailing Address of Inventor:

Address 1	c/o Centripetal Networks, Inc.
Address 2	2251 Corporate Park Drive, Suite 150

City	Herndon	State/Province	VA
Postal Code	20171	Country	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Sean		Moore	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Hollis	State/Province	NH	Country of Residence	US

Mailing Address of Inventor:

Address 1	c/o Centripetal Networks, Inc.
Address 2	2251 Corporate Park Drive, Suite 150

City	Herndon	State/Province	VA
Postal Code	20171	Country	US

Inventor 3 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Douglas	M.	DiSabello	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	007742.00059
	Application Number	
Title of Invention	RULE-BASED NETWORK-THREAT DETECTION FOR ENCRYPTED COMMUNICATIONS	

City	Leesburg	State/Province	VA	Country of Residence	US

Mailing Address of Inventor:

Address 1	c/o Centripetal Networks, Inc.		
Address 2	2251 Corporate Park Drive, Suite 150		
City	Herndon	State/Province	VA
Postal Code	20171	Country	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	22907		
Email Address		Add Email	Remove Email

Application Information:

Title of the Invention	RULE-BASED NETWORK-THREAT DETECTION FOR ENCRYPTED COMMUNICATIONS		
Attorney Docket Number	007742.00059	Small Entity Status Claimed	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	13	Suggested Figure for Publication (if any)	2

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	007742.00059
	Application Number	
Title of Invention	RULE-BASED NETWORK-THREAT DETECTION FOR ENCRYPTED COMMUNICATIONS	

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	22907		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status		Remove	
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)[i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

			Remove
Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	007742.00059
	Application Number	
Title of Invention	RULE-BASED NETWORK-THREAT DETECTION FOR ENCRYPTED COMMUNICATIONS	

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	007742.00059
	Application Number	
Title of Invention	RULE-BASED NETWORK-THREAT DETECTION FOR ENCRYPTED COMMUNICATIONS	

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	007742.00059
	Application Number	
Title of Invention	RULE-BASED NETWORK-THREAT DETECTION FOR ENCRYPTED COMMUNICATIONS	

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

◉ Assignee	○ Legal Representative under 35 U.S.C. 117	○ Joint Inventor
○ Person to whom the inventor is obligated to assign.	○ Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor:

If the Applicant is an Organization check here. ☒

Organization Name	Centripetal Networks, Inc.		
Mailing Address Information For Applicant:			
Address 1	2251 Corporate Park Drive, Suite 150		
Address 2			
City	Herndon	**State/Province**	VA
Country	US	Postal Code	20171
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button.

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	007742.00059
	Application Number	
Title of Invention	RULE-BASED NETWORK-THREAT DETECTION FOR ENCRYPTED COMMUNICATIONS	

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.

Signature:

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature				Date (YYYY-MM-DD)	2015-12-23
First Name	William	Last Name	Wooten	Registration Number	60049

Additional Signature may be generated within this form by selecting the Add button.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	007742.00059
	Application Number	
Title of Invention	RULE-BASED NETWORK-THREAT DETECTION FOR ENCRYPTED COMMUNICATIONS	

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

PATENT APPLICATION SERIAL NO._____

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET

12/30/2015 ZJUHAR1 00000046 190733 14757638

01 FC:2011 140.00 DA
02 FC:2111 300.00 DA
03 FC:2311 360.00 DA
04 FC:2090 200.00 DA
05 FC:2202 200.00 DA

PTO-1556
(5/87)

*U.S. Government Printing Office: 2002- 489-267/69033

Document code: WFEE

United States Patent and Trademark Office
Sales Receipt for Accounting Date: 01/27/2016

ASAHLE SALE #00000038 Mailroom Dt: 12/23/2015 190733 14757638
01 FC : 2051 70.00 DA

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 14/757,638

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	140		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	25 minus 20 =	* 5	x 40 =	200	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 210 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	1000		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)	OR	RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/757,638	12/23/2015	2431	1270	007742.00059	25	3

CONFIRMATION NO. 9492

FILING RECEIPT

22907
BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051



Date Mailed: 01/29/2016

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

David K. Ahn, Winston-Salem, NC;
Sean Moore, Hollis, NH;
Douglas M. DiSabello, Leesburg, VA;

Applicant(s)

Centripetal Networks, Inc., Herndon, VA;

Power of Attorney: None

Domestic Applications for which benefit is claimed - None.
A proper domestic benefit claim must be provided in an Application Data Sheet in order to constitute a claim for domestic benefit. See 37 CFR 1.76 and 1.78.

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted:

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/757,638**

Projected Publication Date: To Be Determined - pending completion of Security Review

Non-Publication Request: No

Early Publication Request: No
** **SMALL ENTITY** **
Title

Rule-based network-threat detection for encrypted communications

Preliminary Class

713

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/757,638	12/23/2015	David K. Ahn	007742.00059

CONFIRMATION NO. 9492

22907
BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

INFORMAL NOTICE

OC000000080189730

Date Mailed: 01/29/2016

INFORMATIONAL NOTICE TO APPLICANT

Applicant is notified that the above-identified application contains the deficiencies noted below. No period for reply is set forth in this notice for correction of these deficiencies. However, if a deficiency relates to the inventor's oath or declaration, the applicant must file an oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each actual inventor no later than the expiration of the time period set in the "Notice of Allowability" to avoid abandonment. See 37 CFR 1.53(f).

The item(s) indicated below are also required and should be submitted with any reply to this notice to avoid further processing delays.

- A properly executed inventor's oath or declaration has not been received for the following inventor(s):
  David K. Ahn
  Sean Moore
  Douglas M. DiSabello

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/hchin/

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82A (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	14/757,638
Filing Date	December 23, 2015
First Named Inventor	David K. Ahn et al.
Title	Rule-Based Network-Threat Detection For Encrypted Communications
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	007742.00059\US

SIGNATURE of Applicant or Patent Practitioner

Signature	/Bradley C. Wright/	Date (Optional)	February 12, 2016
Name	Bradley C. Wright	Registration Number	38,061
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ *Total of 1 forms are submitted.

17717459

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82B(07-12)
Approved for use through 11/30/2014. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in the attached transmittal letter.

☒ I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A or equivalent):

22907

OR

☐ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A or equivalent):

Name	Registration Number	Name	Registration Number

Please recognize or change the correspondence address for the application identified in the attached transmittal letter to:

☒ The address associated with the above-mentioned Customer Number.

OR

☐ The address associated with Customer Number:

OR

☐ Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant:

☐ Inventor or Joint Inventor

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor

☒ Assignee or Person to Whom the Inventor is Under an Obligation to Assign

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (*e.g.*, a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document)

SIGNATURE of Applicant for Patent

Signature		Date	July 19 2013
Name	Steven Rogers	Telephone	(571) 252-5082
Title and Company	Chief Executive Officer, Centripetal Networks, Inc.		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms for more than one signature, see below *.

☒ *Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Acknowledgement Receipt

EFS ID:	24899684
Application Number:	14757638
International Application Number:	
Confirmation Number:	9492
Title of Invention:	Rule-based network-threat detection for encrypted communications
First Named Inventor/Applicant Name:	David K. Ahn
Customer Number:	22907
Filer:	Bradley C. Wright/Holly Parker
Filer Authorized By:	Bradley C. Wright
Attorney Docket Number:	007742.00059
Receipt Date:	12-FEB-2016
Filing Date:	23-DEC-2015
Time Stamp:	12:02:15
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Oath or Declaration filed	Signed_Declaration_-_Ahn_17715101.PDF	83770 446e82ffb33e11551cfa47d4c3f77bb190af8bb6	no	1

Warnings:	
Information:	

2	Oath or Declaration filed	Signed_Declaration_-_Moore_17714989.PDF	713213 ca19a792114b7e1ff9d85f646192b81e0461a949	no	1
Warnings:					
Information:					
3	Oath or Declaration filed	Signed_Declaration_-_DiSabello_17714956.PDF	149262 c2b9ec9a5abe5529f97ac5e4c42282fdaa7b0fe8	no	1
Warnings:					
Information:					
4	Power of Attorney	POA_or_Authorization_of_Agent_17717709.pdf	16578 d54fd26a36b3c5202ffdbc39cdb8ea191c6f347e	no	1
Warnings:					
Information:					
5	Power of Attorney	Centripetal_POA_17717422.PDF	184376 21c73e74c207437bda0e0eb884e1e57c7f141552	no	1
Warnings:					
Information:					
			Total Files Size (in bytes):	1147199	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	Rule-Based Network-Threat Detection for Encrypted Communications

As the below named inventor, I hereby declare that:

This declaration is directed to:

☐ The attached application, or

☒ United States application or PCT international application number 14/757,638 filed on December 23, 2015.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: David K. Ahn Date (Optional): 2-10-2016

Signature: _____

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Declaration Sean Moore

PTO/AIA/01 (08-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	Rule-Based Network-Threat Detection for Encrypted Communications

As the below named inventor, I hereby declare that:

This declaration is directed to:

- ☐ The attached application, or
- ☒ United States application or PCT international application number 14/757,638 filed on December 23, 2015

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Sean Moore Date (Optional): 05-FEB-2016

Signature: Sean Moore

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	Rule-Based Network-Threat Detection for Encrypted Communications

As the below named inventor, I hereby declare that:

This declaration is directed to:

☐ The attached application, or

☒ United States application or PCT international application number 14/757,638 filed on December 23, 2015.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

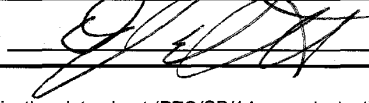
I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Douglas M. DiSabello Date (Optional): 2/2/16

Signature: 

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Patent Application Fee Transmittal

Application Number:	14757638
Filing Date:	23-Dec-2015
Title of Invention:	Rule-based network-threat detection for encrypted communications
First Named Inventor/Applicant Name:	David K. Ahn
Filer:	Bradley C. Wright/Holly Parker
Attorney Docket Number:	007742.00059

Filed as Micro Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Late Filing Fee for Oath or Declaration	3051	1	35	35
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**35**

Electronic Acknowledgement Receipt

EFS ID:	24899907
Application Number:	14757638
International Application Number:	
Confirmation Number:	9492
Title of Invention:	Rule-based network-threat detection for encrypted communications
First Named Inventor/Applicant Name:	David K. Ahn
Customer Number:	22907
Filer:	Bradley C. Wright/Holly Parker
Filer Authorized By:	Bradley C. Wright
Attorney Docket Number:	007742.00059
Receipt Date:	12-FEB-2016
Filing Date:	23-DEC-2015
Time Stamp:	12:14:11
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$35
RAM confirmation Number	8908
Deposit Account	190733
Authorized User	WRIGHT, BRADLEY
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 CFR 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 CFR 1.19 (Document supply fees)

Charge any Additional Fees required under 37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Fee Worksheet (SB06)	fee-info.pdf	30530 e01d4dadb9fdcc5418a16cf85be5093f6373e506	no	2

Warnings:

Information:

Total Files Size (in bytes):	30530

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/757,638	12/23/2015	David K. Ahn	007742.00059

CONFIRMATION NO. 9492

22907
BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

POA ACCEPTANCE LETTER

OC000000080896399

Date Mailed: 02/25/2016

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 02/12/2016.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/sleutchit/

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14757638
Filing Date	2015-12-23
First Named Inventor	David K. Ahn
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	007742.00059\US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6226372		2001-05-01	Beebe et al.	
	2	7721084		2010-05-18	Salminen et al.	
	3	7684400		2010-03-23	Govindarajan et al.	
	4	7539186		2009-05-26	Aerrabotu et al.	
	5	7710885		2010-05-04	Ilnicki et al.	
	6	8856926		2014-10-07	Narayanaswamy et al.	
	7	6611875		2003-08-26	Chopra et al.	
	8	8806638		2014-08-12	Mani	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

	9	8004994		2011-08-23	Darisi et al.	
	10	6098172		2000-08-01	Coss et al.	
	11	7331061	B1	2008-02-12	Ramsey et al.	
	12	7299353	B2	2007-11-20	Le Pennec et al.	
	13	7227842	B1	2007-06-05	Ji et al.	
	14	7107613	B1	2006-09-12	Chen et al.	
	15	7263099	B1	2007-08-28	Woo et al.	
	16	7237267	B2	2007-06-26	Rayes et al.	
	17	7089581	B1	2006-08-08	Nagai et al.	
	18	6662235	B1	2003-12-09	Callis et al.	
	19	6484261	B1	2002-11-19	Wiegel	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

	20	8042167	B2	2011-10-18	Fulp et al.	
	21	8037517	B2	2011-10-11	Fulp et al.	
	22	7954143	B2	2011-05-31	Aaron	
	23	8495725	B2	2013-07-23	Ahn	
	24	8935785	B2	2015-01-13	Pandrangi	
	25	8726379	B1	2014-05-13	Stiansen et al.	
	26	8306994	B2	2012-11-06	Kenworthy	
	27	7818794	B2	2010-10-19	Wittman	
	28	7478429	B2	2009-01-13	Lyon	
	29	6317837	B1	2001-11-13	Kenworthy	
	30	9124552	B2	2015-09-01	Moore	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

	31	9160713	B2	2015-10-13	Moore	
	32	9094445	B2	2015-07-28	Moore et al.	
	33	9137205	B2	2015-09-15	Rogers et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20030123456	A1	2003-07-03	Denz et al.	
	2	20070083924	A1	2007-04-12	Lu	
	3	20060195896		2006-08-31	Fulp et al.	
	4	20060248580		2006-11-02	Fulp et al.	
	5	20060048142		2006-03-02	Roese et al.	
	6	20100011434		2010-01-14	Kay	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

	7	20120113987	A1	2012-05-10	Riddoch et al.	
	8	20110270956	A1	2011-11-03	McDysan et al.	
	9	20100211678	A1	2010-08-19	McDysan et al.	
	10	20050117576		2005-06-02	McDysan et al.	
	11	20040151155	A1	2004-08-05	Jouppi	
	12	20030212900	A1	2003-11-13	Liu et al.	
	13	20030188192	A1	2003-10-02	Tang et al.	
	14	20120264443	A1	2012-10-18	Ng et al.	
	15	20130059527	A1	2013-03-07	HASESAKA et al.	
	16	20010039624		2001-11-08	Kellum	
	17	20030035370	A1	2003-02-20	Brustoloni, Jose	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

	18	20030142681		2003-07-31	Chen et al.	
	19	20030145225		2003-07-31	Bruton et al.	
	20	20050138204		2005-06-23	Iyer et al.	
	21	20050141537		2005-06-30	Kumar et al.	
	22	20060212572		2006-09-21	Afek et al.	
	23	20080072307		2008-03-20	Maes	
	24	20100082811		2010-04-01	Van Der Merwe et al.	
	25	20100296441		2010-11-25	Barkan	
	26	20110088092		2011-04-14	Nguyen et al.	
	27	20080005795	A1	2008-01-03	Acharya et al.	
	28	20090172800	A1	2009-07-02	WOOL	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

	29	20030097590	A1	2003-05-22	Syvanne	
	30	20090328219	A1	2009-12-31	Narayanaswamy	
	31	20120240135	A1	2012-09-20	Risbood et al.	
	32	20120314617	A1	2012-12-13	Erichsen et al.	
	33	20040088542	A1	2004-05-06	Daude et al.	
	34	20080235755	A1	2008-09-25	Blaisdell et al.	
	35	20100132027	A1	2010-05-27	Ou	
	36	20110055916	A1	2011-03-03	Ahn	
	37	20020016858	A1	2002-02-07	Sawada et al.	
	38	20060262798	A1	2006-11-23	Joshi et al.	
	39	20080043739	A1	2008-02-21	SUH et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

	40	20080279196	A1	2008-11-13	Friskney et al.	
	41	20130254766	A1	2013-09-26	Zuo et al.	
	42	20030154297	A1	2003-08-14	Suzuki et al.	
	43	20060114899	A1	2006-06-01	Toumura et al.	
	44	20120331543	A1	2012-12-27	Bostrom et al.	
	45	20110185055	A1	2011-07-28	NAPPIER et al.	
	46	20060070122	A1	2006-03-30	Bellovin	
	47	20050010765	A1	2005-01-13	Swander et al.	
	48	20020198981	A1	2002-12-26	Corl et al.	
	49	20090138938	A1	2009-05-28	Harrison et al.	
	50	20060104202	A1	2006-05-18	Reiner	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

	51	20050229246	A1	2005-10-13	Rajagopal et al.	
	52	20040177139	A1	2004-09-09	Schuba et al.	
	53	20040010712	A1	2004-01-15	Hui et al.	
	54	20030120622	A1	2003-06-26	Nurmela et al.	
	55	20080301765	A1	2008-12-04	Nicol et al.	
	56	20050251570	A1	2005-11-10	Heasman et al.	
	57	20050183140	A1	2005-08-18	Goddard	
	58	20050125697	A1	2005-06-09	Tahara	
	59	20040193943	A1	2004-09-30	Angelino et al.	
	60	20020165949	A1	2002-11-07	Na et al.	
	61	20020038339	A1	2002-03-28	Xu	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

	62	20050114704	A1	2005-05-26	Swander	
	63	20100268799	A1	2010-10-21	Maestas	
	64	20110055923	A1	2011-03-03	Thomas	
	65	20100303240	A1	2010-12-02	Beachem et al.	
	66	20100199346	A1	2010-08-05	Ling et al.	
	67	20100011433	A1	2010-01-14	HARRISON et al.	
	68	20080077705	A1	2008-03-27	Li et al.	
	69	20050286522	A1	2005-12-29	Paddon et al.	
	70	20040205360	A1	2004-10-14	Norton et al.	
	71	20140366132	A1	2014-12-11	Stiansen et al.	
	72	20130061294	A1	2013-03-07	Kenworthy	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

	73	20100242098	A1	2010-09-23	Kenworthy	
	74	20070240208	A1	2007-10-11	Yu et al.	
	75	20060146879	A1	2006-07-06	Anthias et al.	
	76	20060136987	A1	2006-06-22	Okuda	
	77	20020049899	A1	2002-04-25	Kenworthy	
	78	20140281030	A1	2014-09-18	Cui et al.	
	79	20040073655	A1	2004-04-15	Kan et al.	
	80	20150237012	A1	2015-08-20	Moore	
	81	20150304354	A1	2015-10-22	Rogers et al.	
	82	20140115654	A1	2014-04-24	Rogers et al.	
	83	20140201123	A1	2014-07-17	Ahn et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

	84	20140283004	A1	2014-09-18	Moore	
	85	20140283030	A1	2014-09-18	Moore et al.	
	86	20080229415	A1	2008-09-18	Kapoor et al.	
	87	20140215574	A1	2014-07-31	Erb et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	1677484	EP	A2	2006-07-05	Microsoft Corp		
	2	1313290	EP	A1	2003-05-21	Stonesoft Corp		
	3	2005046145	WO	A1	2005-05-19	Ericsson Telefon Ab L M		
	4	2385676	EP	A1	2011-11-09	Alcatel Lucent		
	5	2498442	EP	A1	2012-09-12	Openet Telecom Ltd		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

	6	20010079361	KR	A	2001-08-22	Kim, Sang Wook		
	7	1006701	EP	A2	2000-06-07	Lucent Technologies Inc		
	8	2006105093	WO	A2	2006-10-05	Univ Wake Forest		
	9	2006093557	WO	A2	2006-09-08	Univ Wake Forest		
	10	2005328336	AU	B2	2011-09-15	Univ Wake Forest		
	11	2011038420	WO	A2	2011-03-31	Great Wall Systems		
	12	1484884	EP	A2	2004-12-08	Microsoft Corp		
	13	2006230171	AU	B2	2012-06-21	Univ Wake Forest		
	14	1864226	EP	B1	2013-05-15	Univ Wake Forest		
	15	2600236	CA	A1	2006-10-05	Univ Wake Forest		
	16	2012146265	WO	A1	2012-11-01	Voipfuture Gmbh		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

If you wish to add additional Foreign Patent Document citation information please click the Add button [Add]

NON-PATENT LITERATURE DOCUMENTS [Remove]

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	Copy of ISR for PCT/US2013/057502, dated November 7, 2013.	
	2	International Search Report off International Application No. PCT/US2014/023286, dated June 24, 2014.	
	3	ISR off International Application No. PCT/US2013/072566, dated March 24, 2014.	
	4	ISR off International Application No. PCT/US2014/027723, dated June 26, 2014.	
	5	"Control Plane Policing Implementation Best Practices"; Cisco Systems; March 13, 2013; <https://web.archive.org/web/20130313135143/http:www.cisco.com/web/about/security/intelligence/coppwp_gs.html>	
	6	Reumann, John; "Adaptive Packet Filters"; IEEE, 2001, Department of Electrical Engineering and Computer Science, The University of Michigan, Ann Arbor, MI	
	7	Greenwald, Michael; "Designing an Academic Firewall: Policy, Practice, and Experience with SURF"; IEEE, Proceedings of SNDSS, 1996.	
	8	Mizuno et al., A New Remote Configurable Firewall System for Home-use Gateways, January 2005. Second IEEE Consumer Communications and Networking Conference, pp. 599-601.	
	9	"SBIR Case Study: Centripetal Networks Subtitle: How CNI Leveraged DHS S&T SBIR Funding to Launch a Successful Cyber Security Division 2012 Principal Investigators' Meeting"; Sean Moore, October 10, 2014.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

	10	John Kindervag; "Build Security Into Your Network's DNA: The Zero Trust Network Architecture", Forrester Research Inc.; Novermber 5, 2010, pps: 1-26.	
	11	Palo Alto Networks; "Designing A Zero Trust Network With Next-Generation Firewalls"; pps. 1-10; last viewed on October 21, 2012.	
	12	2016 Jan 11 - (US) Non Final Rejection - App 14/698,560	
	13	2011 Apr 27 - (WO) International Search Report and Written Opinion - App PCT/US2010/054520	
	14	2011 Mar 04 - (US) Notice of Allowance - App 11/316,331	
	15	2011 Mar 03 - (EP) Communication Pursuant to Rules 70(2) and 70a(2) - App 06758213.0	
	16	2011 Feb 14 - (EP) Search Report - App 06758213.0	
	17	Fulp, Errin: "Errin Fulp," XP002618346, www.cs.wfu.edu/fulp/ewfPub.html, pgs. 1-5 (Copyright 2010)	
	18	2010 Sept 30 - (US) Office Action - App 11/390,976	
	19	2010 Sept 10 - (AU) Office Action - App 2006230171	
	20	2010 Aug 20 - (AU) Office Action - App 2005328336	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

	21	2010 Jun 23 - (US) Final Rejection - App 11/316,331	
	22	2010 Apr 29 - (US) Interview Summary - App 11/390,976	
	23	2010 Mar 26 - (US) Final Rejection - App 11/390,976	
	24	2009 Sept 14 (US) Office Action - App 11/316,331	
	25	2009 Jun 24 - (US) Office Action - App 11/390,976	
	26	2008 Jul 03 - (WO) Written Opinion of the International Searching Authority - App PCT/US06/11291	
	27	2007 Aug 31 - (EP) Communication Pursuant to Rules 109 and 110 - App 05857614.1	
	28	Acharya et al, "OPTWALL: A Hierarchical Traffic-Aware Firewall," Department of Computer Science, Telecommunications Program, University of Pittsburgh, pgs. 1-11 (2007)	
	29	2006 Sept 11 - (WO) Written Opinion of the International Searching Authority - App PCT/US05/47008	
	30	Tarsa et al., "Balancing Trie-Based Policy representations for Network Firewalls," Department of Computer Science, Wake Forest University, pgs. 1-6 (2006)	
	31	Fulp, "Trie-Based Policy Representations for Network Firewalls," Proceedings of the IEEE International Symposium on Computer Communications (2005)	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

	32	E. Fulp, "Optimization of Network Firewall Policies Using Ordered Sets and Directed Acyclical Graphs", Technical Report, Computer Scient Department, Wake Forest University, January 2004	
	33	E. Fulp et al., "Network Firewall Policy Tries", Technical Report, Computer Science Department, Wake Forest University, 2004	
	34	E. Al-Shaer et al., "Modeling and Management of Firewall Policies", IEEE Transactions on Network and Service Management, 1(1): 2004	
	35	E.W. Fulp, "Firewall Architectures for High Speed Networks", U.S. Department of Energy Grant Application, Funded September 2003	
	36	E. Al-Shaer et al., "Firewall Policy Advisor for Anomaly Discovery and Rule Editing", Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management, 2003	
	37	V.P. Ranganath, "A Set-Based Approach to Packet Classification", Proceedings of the IASTED International Conference on Parallel and Distributed Computing and Systems, 889-894, 2003	
	38	M. Christiansen et al., "Using IDDsfor Packet Filtering", Technical Report, BRICS, October 2002	
	39	Lee et al., "Development Framework for Firewall Processors," IEEE, pgs. 352-355 (2002)	
	40	L. Qui et al., "Fast Firewall Implementations for Software and Hardware-Based Routers", Proceedings of ACM Sigmetrics, June 2001	
	41	D. Eppstein et al., "Internet Packet Filter Management and Rectangle Geometry", Proceedings of the Symposium on Discrete Algorithms, 827-835, 2001	
	42	E. Fulp, "Preventing Denial of Service Attacks on Quality of Service", Proceedings of the 2001 DARPA Information Survivability Conference and Exposition II, 2001	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

	43	S. Goddard et al., "An Unavailability Analysis of Firewall Sandwich Configurations", Proceedings of the 6th IEEE Symposium on High Assurance Systems Engineering, 2001	
	44	G.V. Rooij, "Real Stateful TCP Packet Filtering in IP Filter", Proceedings of the 10th USENIX Security Symposium, 2001	
	45	P. Warkhede et al., "Fast Packet Classification for Two-Dimensional Conflict-Free Filters", Proceedings of IEEE INFOCOM, 1434-1443, 2001	
	46	D. Decasper et al., "Router Plugins: A Software Architecture for Next-Generation Routers", IEEE/ACM Transactions on Networking, 8(1): February 2000	
	47	A. Feldmann et al., "Tradeoffs for Packet Classification", Proceedings of the IEEE INFOCOM, 397-413, 2000	
	48	X. Gan et al., "LSMAC vs. LSNAT: Scalable Cluster-based Web servers", Journal of Networks, Software Tools, and Applications, 3(3): 175-185, 2000	
	49	A. Hari et al., "Detecting and Resolving Packet Filter Conflicts", Proceedings of IEEE INFOCOM, 1203-1212, 2000	
	50	O. Paul et al., "A full Bandwidth ATM Firewall", Proceedings of the 6th European Symposium on Research in Computer Security ESORICS'2000, 2000	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Bradley C. Wright/	Date (YYYY-MM-DD)	2016-03-30
Name/Print	Bradley C. Wright	Registration Number	38061

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	25345015
Application Number:	14757638
International Application Number:	
Confirmation Number:	9492
Title of Invention:	Rule-based network-threat detection for encrypted communications
First Named Inventor/Applicant Name:	David K. Ahn
Customer Number:	22907
Filer:	Bradley C. Wright/Holly Parker
Filer Authorized By:	Bradley C. Wright
Attorney Docket Number:	007742.00059
Receipt Date:	30-MAR-2016
Filing Date:	23-DEC-2015
Time Stamp:	13:39:20
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	NPL_-_ISR_from_007742_16712474.PDF	879049 0c802d5b79a6d7cc80dc33c3685743441eceec44	no	8
Warnings:					
Information:					

2	Non Patent Literature	NPL-ISR_dated_24-6-147742_16806852.PDF	519073 8f3879c91d1dd61cd1a7d73ef98e53309964ad85	no	9
Warnings:					
Information:					
3	Non Patent Literature	NPL-ISR_16811120.PDF	8697440 386f3734edd4d1111a0ce5eb49f047d48a7df8e4	no	66
Warnings:					
Information:					
4	Non Patent Literature	NPL-ISR_dated_2606_16818779.PDF	744984 e1ca96f7cd5b5a2fa2cccc54367d9a3ea7ad69bc	no	11
Warnings:					
Information:					
5	Non Patent Literature	NPL-Cisco_16818946.PDF	2472590 e14c692da0b6acaa6bb75cbae061bdd60efaea86	no	26
Warnings:					
Information:					
6	Non Patent Literature	NPL_Reumann_as_filed_17029214.PDF	506812 7ce72f2f751d31ee0dbebfba3e269204ac309c28	no	5
Warnings:					
Information:					
7	Non Patent Literature	NPL_Greenwald_as_filed_17029228.PDF	1453816 f534647935f58bfb9e25964260695c7bb3863dda	no	14
Warnings:					
Information:					
8	Non Patent Literature	NPL-Mizuno_17259625.PDF	363361 4fd1c88496c3f87fd05dd88cbf06087f412ac8d6	no	3
Warnings:					
Information:					
9	Non Patent Literature	NPL-Moore_16818826.PDF	1932721 7f7362dd6ca63b62d069e3a66279ca0175c2da98	no	9
Warnings:					
Information:					
10	Non Patent Literature	NPL-Kindervag_16712444.PDF	2836187 7320c5df93a3c25807d980d1ff9302ac28250a18	no	27
Warnings:					
Information:					

11	Non Patent Literature	NPL-PaloAltoNetworks_16712439.PDF	2240313 1a612b6fe32ae1fdcce919ae95025d31865f5c76	no	11
Warnings:					
Information:					
12	Non Patent Literature	Non-Final_Rejection__892__1449_17666796.pdf	3313609 f94b21bf5072e9131e28903be6edbe2c064d83d3	no	82
Warnings:					
Information:					
13	Non Patent Literature	12871806_17760757.pdf	133950 d087d3fbbe5474766fb472b2fee3ab27b0b1d25c	no	3
Warnings:					
Information:					
14	Non Patent Literature	128718063_17748716.pdf	1885109 ff333809c196b7f7a899c06c24df7be6148b7b74	no	27
Warnings:					
Information:					
15	Non Patent Literature	128718063_17748705.pdf	72597 651be9b6f8516e40bd49cb8fea3b32608f57ad50	no	1
Warnings:					
Information:					
16	Non Patent Literature	128718063_17748704.pdf	280016 221a9d9fc8b69cd190f9a5e0c1fa7680eb10d7d4	no	8
Warnings:					
Information:					
17	Non Patent Literature	128718063_17748700.pdf	219866 2ff7ed11de580c33fbb1b4952953d81e9b627c07	no	6
Warnings:					
Information:					
18	Non Patent Literature	128718063_17748691.pdf	1056941 bfadf021c891e2d729069fdda5bb30ab7fbf6763	no	16
Warnings:					
Information:					
19	Non Patent Literature	128718063_17748689.pdf	93553 aeebc179c8fe4b8652ce76890598f0a71ce1aaa8	no	2
Warnings:					
Information:					

20	Non Patent Literature	128718063_17748686.pdf	66979 3884e538b6229e78e030c0dadc818f3747c9c505	no	1
Warnings:					
Information:					
21	Non Patent Literature	128718063_17748681.pdf	996456 64c55e7adf26bce0057805bbce8893d9484d48a2	no	30
Warnings:					
Information:					
22	Non Patent Literature	128718063_17748678.pdf	156743 31b7acfb7a47df115a561685241059d1d659011d	no	3
Warnings:					
Information:					
23	Non Patent Literature	128718063_17748674.pdf	954410 43e217a062cbd30d39f335589611d5c666afc0b0	no	22
Warnings:					
Information:					
24	Non Patent Literature	128718063_17748670.pdf	2407621 8036abd1045aaa8ace8ddc328d101c5e3756a533	no	40
Warnings:					
Information:					
25	Non Patent Literature	128718063_17748667.pdf	2047479 88a901174011cc43df79b97eefab85b253c4402e	no	29
Warnings:					
Information:					
26	Non Patent Literature	WO2006105093_17760770.pdf	130515 ffedf6884c4fc8189503e9ff67e119dd3c780109	no	3
Warnings:					
Information:					
27	Non Patent Literature	128718063_17748664.pdf	237193 7e270b000e2db4b9499e9c0955d46568991f37b2	no	4
Warnings:					
Information:					
28	Non Patent Literature	128718063_17748659.pdf	954305 3f4b7c0c39cc5a790a91fb62c5377170c2dd5d5b	no	11
Warnings:					
Information:					

29	Non Patent Literature	WO2006093557_17760776.pdf	330618 8b1a7002192e2958fc5a052a07ea100d87f170f4	no	6
Warnings:					
Information:					
30	Non Patent Literature	128718063_17748656.pdf	680644 f6452d529346441b5a7b66f39d8cb7b835fc821f	no	6
Warnings:					
Information:					
31	Non Patent Literature	128718063_17748652.pdf	809858 22ec24e861a9992648686b98ef88ea8c83a07bab	no	8
Warnings:					
Information:					
32	Non Patent Literature	128718063_17748644.pdf	843872 c9065af421ba9ec73f59a3c0abbae1bf99b75614	no	12
Warnings:					
Information:					
33	Non Patent Literature	128718063_17748638.pdf	1048051 62d2f5d39bb17ff27c66337e49aee4f6c9830c66	no	17
Warnings:					
Information:					
34	Non Patent Literature	128718063_17748635.pdf	910845 6e552f84cff6cf8d14434127ae71adb7df616dec	no	10
Warnings:					
Information:					
35	Non Patent Literature	128718063_17748632.pdf	1400185 d1485e17039f0972c9bca74d770ed585d940bd53	no	20
Warnings:					
Information:					
36	Non Patent Literature	128718063_17748622.pdf	1289250 fcdde68b1fc3570582a7a07ca4720c19537e39da	no	14
Warnings:					
Information:					
37	Non Patent Literature	128718063_17748618.pdf	585331 8f5ff661f447eb4f39db56058ccd1229bcaa0dfc	no	6
Warnings:					
Information:					

38	Non Patent Literature	128718063_17748614.pdf	1233391 f84378a5a084fed2aaf6cba80ecece4a98f2ba0	no	28
Warnings:					
Information:					
39	Non Patent Literature	128718063_17748610.pdf	266637 d6500988f54cbcebcbe36d73eca657359214084b	no	4
Warnings:					
Information:					
40	Non Patent Literature	128718063_17748605.pdf	888581 179b281ea068d86062d3084a0dbbc4632778ce46	no	10
Warnings:					
Information:					
41	Non Patent Literature	128718063_17748600.pdf	943167 06b16c35524d8f1d1a800b00e6f9293a6e11f14b	no	9
Warnings:					
Information:					
42	Non Patent Literature	128718063_17748594.pdf	1313706 cb35a896663a5ce778fd6ac66689f1bbdee57433	no	14
Warnings:					
Information:					
43	Non Patent Literature	128718063_17748590.pdf	1117022 140263fcd5145fb1e2e2a099b1e98f18b8d6d360	no	10
Warnings:					
Information:					
44	Non Patent Literature	128718063_17748585.pdf	897641 06520e07f43a9afbc0f7b7ad730dff8247a967af	no	15
Warnings:					
Information:					
45	Non Patent Literature	128718063_17748581.pdf	1165960 0c1b258923b72f80b1dc6cdf7b6363c8a95a44dd	no	10
Warnings:					
Information:					
46	Non Patent Literature	128718063_17748578.pdf	1551967 88a0f067f9a24decfbe884fa2df29cc25ab0d0b5	no	14
Warnings:					
Information:					

47	Non Patent Literature	128718063_17748577.pdf	1143829 25ac578781f5ed2e25f8b34aa201a16e82b83daa	no	10
Warnings:					
Information:					
48	Non Patent Literature	128718063_17748574.pdf	1347663 c2f845908e887514e60f22eea11e9ec7546ca129	no	11
Warnings:					
Information:					
49	Non Patent Literature	128718063_17748567.pdf	1222050 3962296f0c45ec3f80f4d5cbf25eedfe9ef404b1	no	10
Warnings:					
Information:					
50	Non Patent Literature	128718063_17748564.pdf	1118094 8e2f6a7b03a382382e26a106186d64dd475fcedb	no	16
Warnings:					
Information:					
51	Non Patent Literature	128718063_17748559.pdf	959293 0848229de6e141860751e8e14d6e021a7da1b25f	no	11
Warnings:					
Information:					
52	Non Patent Literature	128718063_17748527.pdf	655973 538c772956eacec011f7a184a5ac5a01ee34d6bd	no	8
Warnings:					
Information:					
53	Non Patent Literature	128718063_17748517.pdf	527673 ec48fa1268dddc8f6dcd05783730b341339a1371	no	5
Warnings:					
Information:					
54	Non Patent Literature	128718063_17748507.pdf	214277 aa3925bbab5f9517b3d068f7238a2985fbc4eec9	no	2
Warnings:					
Information:					
55	Non Patent Literature	128718063_17748503.pdf	1104955 9a812673586643b63a12e826cdd6cb53c332b895	no	18
Warnings:					
Information:					

56	Non Patent Literature	128718063_17748500.pdf	1428072 2b7e6fb1104bdca0e149137487d7ed7da7f11317	no	12
Warnings:					
Information:					
57	Non Patent Literature	128718063_17748492.pdf	1206677 9796972ed4e3a9278f61305fd084edf6b1d8e87c	no	12
Warnings:					
Information:					
58	Non Patent Literature	128718063_17748477.pdf	820708 3b06c3828c0a94ea80bec34368675ee9b0d9661f	no	8
Warnings:					
Information:					
59	Non Patent Literature	128718063_17748473.pdf	1310896 32621dc86ff0594ecbf95b9eae06e336a994092c	no	15
Warnings:					
Information:					
60	Information Disclosure Statement (IDS) Form (SB08)	Information_Disclosure_Statement_Fillable_PDF_1_of_2_17791346.pdf	1041471 cf1824ab7364a427445c81cc975b3d0fc3b284f5	no	20
Warnings:					
Information:					
		Total Files Size (in bytes):	69032045		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
Wright, Bradley
BANNER & WITCOFF, LTD.
1100 13th Street, N.W. Suite 1200
Washington, DC 20005-4051
ETATS-UNIS D'AMERIQUE

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

	Date of mailing *(day/month/year)* 7 November 2013 (07-11-2013)
Applicant's or agent's file reference 007742.00023	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US2013/057502	International filing date *(day/month/year)* 30 August 2013 (30-08-2013)
Applicant CENTRIPETAL NETWORKS, INC.	

1. [X] The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the International Search Report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Fascimile No.: (41-22) 338.82.70

   For more detailed instructions, see *PCT Applicant's Guide*, International Phase, paragraphs 9.004 - 9.011.

2. [ ] The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. [ ] **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   [ ] the protest together with the decision thereon has been transmitted to the International Bureau together with any request to forward the texts of both the protest and the decision thereon to the designated Offices.

   [ ] no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.

   Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before completion of the technical preparations for international publication (Rules 90*bis*.1 and 90*bis*.3).

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

   In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

   For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the *PCT Applicant's Guide*, National Chapters.

Name and mailing address of the International Searching Authority	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040 Fax: (+31-70) 340-3016	VINCI, Rossana Tel: +31 (0)70 340-2812

NOV 12 2013

Form PCT/ISA/220 (July 2010)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	FOR FURTHER ACTION	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
007742.00023		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2013/057502	30 August 2013 (30-08-2013)	22 October 2012 (22-10-2012)
Applicant		
CENTRIPETAL NETWORKS, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 3 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language**, the international search was carried out on the basis of:
      [X] the international application in the language in which it was filed
      [ ] a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. [ ] This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).
   c. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. [ ] **Certain claims were found unsearchable** (See Box No. II)

3. [ ] **Unity of invention is lacking** (see Box No III)

4. With regard to the **title,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings,**
   a. the figure of the **drawings** to be published with the abstract is Figure No. 1
      [ ] as suggested by the applicant
      [X] as selected by this Authority, because the applicant failed to suggest a figure
      [ ] as selected by this Authority, because this figure better characterizes the invention
   b. [ ] none of the figures is to be published with the abstract

NOV 12 2013

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2013/057502

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 677 484 A2 (MICROSOFT CORP [US]) 5 July 2006 (2006-07-05) paragraphs [0011], [0017] - [0019]	1-20
X	US 6 226 372 B1 (BEEBE TODD [US] ET AL) 1 May 2001 (2001-05-01) column 3, line 38 - column 4, line 32; claims 1-11	1-20

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 October 2013	07/11/2013

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Veen, Gerardus

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2013/057502

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1677484 A2	05-07-2006	CN 1777179 A	24-05-2006
		EP 1677484 A2	05-07-2006
		JP 4914052 B2	11-04-2012
		JP 2006146891 A	08-06-2006
		KR 20060056231 A	24-05-2006
		US 2006129808 A1	15-06-2006
		US 2009172774 A1	02-07-2009
US 6226372 B1	01-05-2001	AU 1950301 A	18-06-2001
		US 6226372 B1	01-05-2001
		US 2001014150 A1	16-08-2001
		WO 0143343 A1	14-06-2001

Form PCT/ISA/210 (patent family annex) (April 2005)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2013/057502	30.08.2013	22.10.2012

International Patent Classification (IPC) or both national classification and IPC
INV. H04L29/06

Applicant
CENTRIPETAL NETWORKS, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

NOV 1 2 2013

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Fax: +31 70 340 - 3016	see form PCT/ISA/210	Veen, Gerardus Telephone No. +31 70 340-3811

Form PCT/ISA/237 (Cover Sheet) (July 2009)

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

   a. (means)

      ☐ on paper

      ☐ in electronic form

   b. (time)

      ☐ in the international application as filed

      ☐ together with the international application in electronic form

      ☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	
	No:	Claims	1-20
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-20
Industrial applicability (IA)	Yes:	Claims	1-20
	No:	Claims	

2. Citations and explanations

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1 The following documents are referred to:

D1 EP 1 677 484 A2 (MICROSOFT CORP [US]) 5 July 2006 (2006-07-05)

D2 US 6 226 372 B1 (BEEBE TODD [US] ET AL) 1 May 2001 (2001-05-01)

2 The present application does not meet the criteria of Article 33(2) PCT, because the subject-matter of claims 1-20 is not new.

2.1 In the words of independent claim 1, D1 discloses:

'A method (column 4, line 13), comprising:

at each of one or more packet security gateways (c.4, l.16, 'enforcement engine') associated with a security policy management server (c.4, l.15, 'policy server'):

receiving a dynamic security policy from the security policy management server (c.4, l.16-19);

receiving packets associated with a network protected by each respective packet security gateway; and

performing, on a packet by packet basis, at least one of multiple packet transformation functions specified by the dynamic security policy on the packets (c.4, l.19-20, 'enforcing the security policies'), wherein performing the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets comprises performing at least one packet transformation function other than forwarding or dropping the packets (c.5, l.30-36)'.

Claim 1 is thus not new (Art. 33(2) PCT).

2.2 The same reasoning applies, mutatis mutandis, to independent claims 19 and 20 which are, therefore, also not new.

2.3 Dependent claims 2-18 do not contain any features which, in combination with the features of the claims to which they refer, meet the requirements of the PCT in respect of novelty and inventive step, see D1, D2 and the corresponding citations in the search report.

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

PCT

To:
Wright, Bradley C.
BANNER & WITCOFF, LTD.
1100 13th Street, N.W. Suite 1200
Washington, DC 20005-4051
ETATS-UNIS D'AMERIQUE

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

Applicant's or agent's file reference 007742.00030	Date of mailing *(day/month/year)* 24 June 2014 (24-06-2014)
International application No. PCT/US2014/023286	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
Applicant CENTRIPETAL NETWORKS, INC.	International filing date *(day/month/year)* 11 March 2014 (11-03-2014)

1. [X] The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the International Search Report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Fascimile No.: (41-22) 338.82.70

   For more detailed instructions, see *PCT Applicant's Guide*, International Phase, paragraphs 9.004 - 9.011.

2. [ ] The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. [ ] **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   [ ] the protest together with the decision thereon has been transmitted to the International Bureau together with any request to forward the texts of both the protest and the decision thereon to the designated Offices.

   [ ] no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.

   Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before completion of the technical preparations for international publication (Rules 90*bis*.1 and 90*bis*.3).

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

   In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

   For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the *PCT Applicant's Guide*, National Chapters.

Name and mailing address of the International Searching Authority	Authorized officer	
European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040 Fax: (+31-70) 340-3016	ROTHENBüCHER, Anita Tel: +31 (0)70 340-9872	JUN 24 2014 BANNER & WITCOFF LTD

Form PCT/ISA/220 (July 2010)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
007742.00030		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2014/023286	11 March 2014 (11-03-2014)	12 March 2013 (12-03-2013)
Applicant		
CENTRIPETAL NETWORKS, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 3 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language,** the international search was carried out on the basis of:
      [X] the international application in the language in which it was filed
      [ ] a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. [ ] This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).
   c. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. [ ] **Certain claims were found unsearchable** (See Box No. II)

3. [ ] **Unity of invention is lacking** (see Box No III)

4. With regard to the **title,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings,**
   a. the figure of the **drawings** to be published with the abstract is Figure No. 2
      [ ] as suggested by the applicant
      [X] as selected by this Authority, because the applicant failed to suggest a figure
      [ ] as selected by this Authority, because this figure better characterizes the invention
   b. [ ] none of the figures is to be published with the abstract

RECEIVED
JUN 24 2014
BANNER & WITCOFF LTD

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2014/023286

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2003/123456 A1 (DENZ PETER R [US] ET AL) 3 July 2003 (2003-07-03) paragraphs [03.7], [0008], [0025] - [0027]	1-20
X	US 2007/083924 A1 (LU HONGQIAN K [US]) 12 April 2007 (2007-04-12) paragraphs [0054] - [0055]	1-20

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 June 2014	24/06/2014

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Veen, Gerardus

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2014/023286

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003123456 A1	03-07-2003	NONE	
US 2007083924 A1	12-04-2007	NONE	

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY
(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2014/023286	11.03.2014	12.03.2013

International Patent Classification (IPC) or both national classification and IPC
INV. H04L29/06

Applicant
CENTRIPETAL NETWORKS, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☒ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

JUN 24 2014
BANNER & WITCOFF LTD

Name and mailing address of the ISA:
European Patent Office
P.B. 5818 Patentlaan 2
NL-2280 HV Rijswijk - Pays Bas
Tel. +31 70 340 - 2040
Fax: +31 70 340 - 3016

Date of completion of this opinion
see form PCT/ISA/210

Authorized Officer
Veen, Gerardus
Telephone No. +31 70 340-3811

Form PCT/ISA/237 (Cover Sheet) (July 2009)

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

   a. (means)

   ☐ on paper

   ☐ in electronic form

   b. (time)

   ☐ in the international application as filed

   ☐ together with the international application in electronic form

   ☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	
	No:	Claims	1-20
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-20
Industrial applicability (IA)	Yes:	Claims	1-20
	No:	Claims	

2. Citations and explanations

see separate sheet

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

The following documents are referred to:

D1 US 2003/123456 A1 (DENZ PETER R [US] ET AL) 3 July 2003 (2003-07-03)

D2 US 2007/083924 A1 (LU HONGQIAN K [US]) 12 April 2007 (2007-04-12)

1 The present application does not meet the criteria of Article 33(2) PCT, because the subject-matter of claims 1-20 is not new.

1.1 Independent claim 1 (as far as it is clear, see **Item VIII**) defines a method for filtering a packet, the method having two stages:

1) in the first stage, a first operation ('operator') is performed upon the packet, based on a first header field value;

2) in the second stage, a second operation ('transformation') is performed upon the packet, based on a second header field value.

Moreover, these two steps are interrelated in the sense that the criteria, with which the second header field value is compared during the second stage, are determined during the first stage.

Such a method is also disclosed in D1 (see the passages cited in the search report).

Present claim 1 is thus not new according to Art. 33(2) PCT.

1.2 The same reasoning applies, mutatis mutandis, to independent claims 11 and 20 which are, therefore, also not new.

1.3 Dependent claims 2-10 and 12-19 do not appear to contain any features which, in combination with the features of the claims to which they refer, meet the requirements of the PCT in respect of novelty and inventive step, see D1, D2 and the corresponding references cited in the search report.

1.4 It is further noted that a reasoning based on D2 would lead to very similar conclusions.

Re Item VIII

Certain observations on the international application

2 Claims 1-20 do not meet the requirements of Article 6 PCT for, at least, the following reasons:

- in claim 1, the expressions 'header field' and 'application header field', and especially how they differ from each other, are not clear;

- a similar remark applies to the expressions 'operator' and 'packet transformation function', respectively.

Similar observations apply to independent claims 11 and 20.

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
Wright, Bradley C.
BANNER & WITCOFF, LTD.
1100 13th Street, N.W. Suite 1200
Washington, DC 20005-4051
ETATS-UNIS D'AMERIQUE

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

Applicant's or agent's file reference 007742.00025	Date of mailing *(day/month/year)* 24 March 2014 (24-03-2014) **FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US2013/072566	International filing date *(day/month/year)* 2 December 2013 (02-12-2013)
Applicant CENTRIPETAL NETWORKS, INC.	

1. [X] The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the International Search Report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Facsimile No.: (41-22) 338.82.70

   For more detailed instructions, see *PCT Applicant's Guide*, International Phase, paragraphs 9.004 - 9.011.

2. [ ] The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. [ ] **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   [ ] the protest together with the decision thereon has been transmitted to the International Bureau together with any request to forward the texts of both the protest and the decision thereon to the designated Offices.

   [ ] no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.

Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before completion of the technical preparations for international publication (Rules 90*bis*.1 and 90*bis*.3).

Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the *PCT Applicant's Guide*, National Chapters.

Name and mailing address of the International Searching Authority European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040 Fax: (+31-70) 340-3016	Authorized officer ROTHENBüCHER, Anita Tel: +31 (0)70 340-9872

RECEIVED
MAR 28 2014
BANNER & WITCOFF, LTD.

Form PCT/ISA/220 (July 2010)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	FOR FURTHER ACTION	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
007742.00025		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2013/072566	2 December 2013 (02-12-2013)	11 January 2013 (11-01-2013)
Applicant		
CENTRIPETAL NETWORKS, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 4 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language**, the international search was carried out on the basis of:
      [X] the international application in the language in which it was filed
      [ ] a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. [ ] This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).
   c. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. [ ] **Certain claims were found unsearchable** (See Box No. II)

3. [ ] **Unity of invention is lacking** (see Box No III)

4. With regard to the **title,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings,**
   a. the figure of the **drawings** to be published with the abstract is Figure No. 2
      [ ] as suggested by the applicant
      [X] as selected by this Authority, because the applicant failed to suggest a figure
      [ ] as selected by this Authority, because this figure better characterizes the invention
   b. [ ] none of the figures is to be published with the abstract

RECEIVED
MAR 26 2014
BANNER & WITCOFF, LTD.

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2013/072566

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 313 290 A1 (STONESOFT CORP [FI]) 21 May 2003 (2003-05-21) abstract paragraph [0010] paragraph [0022] paragraph [0024] paragraph [0029] paragraph [0040] paragraph [0025] --- -/--	1-24

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 March 2014	24/03/2014

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Oliveira, Joel

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2013/072566

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2005/046145 A1 (ERICSSON TELEFON AB L M [SE]) 19 May 2005 (2005-05-19) abstract page 3, line 14 - line 28 page 4, line 10 - line 11 page 5, line 10 page 5, line 23 - line 32 page 7, line 2 - line 8 page 7, line 30 - page 8, line 8 page 11, line 20 - line 25 -----	1-24
A	US 2011/055916 A1 (AHN DAVID K [US]) 3 March 2011 (2011-03-03) paragraph [0017] paragraph [0021] - paragraph [0022] -----	1-24

1

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

EX1002
CISCO SYSTEMS, INC. / Page 140 of 1453

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2013/072566

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1313290 A1	21-05-2003	AT 346446 T	15-12-2006
		DE 60216218 T2	08-03-2007
		EP 1313290 A1	21-05-2003
		US 2003097590 A1	22-05-2003
WO 2005046145 A1	19-05-2005	CN 1879361 A	13-12-2006
		EP 1683313 A1	26-07-2006
		JP 4323523 B2	02-09-2009
		JP 2007534219 A	22-11-2007
		US 2005111434 A1	26-05-2005
		WO 2005046145 A1	19-05-2005
US 2011055916 A1	03-03-2011	AU 2010297968 A1	22-03-2012
		EP 2471218 A2	04-07-2012
		US 2011055916 A1	03-03-2011
		US 2014007216 A1	02-01-2014
		WO 2011038420 A2	31-03-2011

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2013/072566	02.12.2013	11.01.2013

International Patent Classification (IPC) or both national classification and IPC
INV. H04L29/06

Applicant
CENTRIPETAL NETWORKS, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

RECEIVED
MAR 28 2014

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Fax: +31 70 340 - 3016	see form PCT/ISA/210	BANNER & WITCOFF, LTD. Oliveira, Joel Telephone No. +31 70 340-3334

Form PCT/ISA/237 (Cover Sheet) (July 2009)

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

   a. (means)

   ☐ on paper

   ☐ in electronic form

   b. (time)

   ☐ in the international application as filed

   ☐ together with the international application in electronic form

   ☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	2, 3, 6-9, 11, 13, 14, 17-22, 24
	No:	Claims	1, 4, 5, 10, 12, 15, 16, 23
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-24
Industrial applicability (IA)	Yes:	Claims	1-24
	No:	Claims	

2. Citations and explanations

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

Reference is made to the following documents:

D1 EP 1 313 290 A1 (STONESOFT CORP [FI]) 21 May 2003 (2003-05-21)

D2 WO 2005/046145 A1 (ERICSSON TELEFON AB L M [SE]) 19 May 2005 (2005-05-19)

D3 US 2011/055916 A1 (AHN DAVID K [US]) 3 March 2011 (2011-03-03)

1 The present application does not meet the criteria of Article 33(2) PCT, because the subject-matter of claims **1, 12 and 23** is not new.

1.1 **D1** discloses a method comprising, at a network protection device **(abstract)**:

receiving a first rule set **(paragraph [0010], column3 lines 4-7)**;

receiving a second rule set **(paragraph [0010], column3 lines 4-7)**;

preprocessing the first rule set and the second rule set **(considered to be implicit from paragraphs [0010], [0013], [0040]: when a new set of rules is made available it must be made certain that they do not contain errors which could stop the filtering of the firewall)**;

configuring the network protection device to process packets in accordance with the first rule set **(paragraph [0010], column3 lines 13-18)**;

receiving packets **(column 6 lines 23-26)**;

processing a first portion of the packets in accordance with the first rule set **(paragraphs [0010], [0020])**;

reconfiguring the network protection device to process packets in accordance with the second rule set **(paragraphs [0010], [0024])**; and

processing a second portion of the packets in accordance with the second rule set **(paragraphs [0010], [0024])**.

1.2 The same reasoning applies, mutatis mutandis, to the subject-matter of the corresponding independent apparatus and computer-readable media claims **12 and 23**, which therefore are also considered not new.

1.3 Dependent claims **2-11, 13-22 and 24** do not contain any features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT in respect of novelty (for claims **4, 5, 10, 15, 16**) and/or inventive step (for claims **2, 3, 6, 7, 8, 9, 11, 13, 14, 17, 18, 19, 20, 21, 22, 24**) see passages cited in the Search Report.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 313 290 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
21.05.2003 Bulletin 2003/21

(51) Int Cl.[7]: **H04L 29/06**

(21) Application number: **02102581.2**

(22) Date of filing: **14.11.2002**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **19.11.2001 US 988356**

(71) Applicant: **Stonesoft Corporation**
00210 Helsinki (FI)

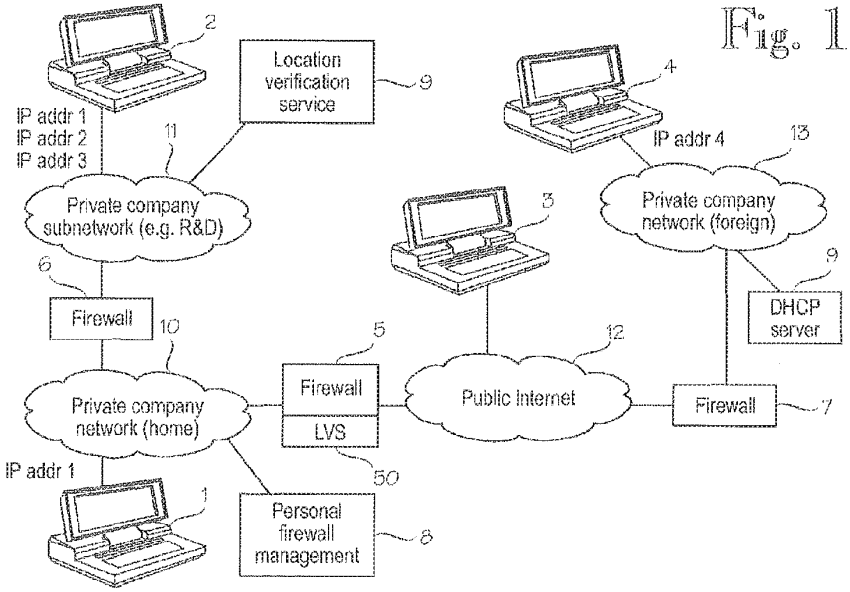
(72) Inventor: **Syvänne, Tuomo**
Fin-01450, Vantaa (FI)

(74) Representative: **Äkräs, Tapio Juhani**
Kolster Oy Ab,P.O. Box 148,
Iso Roobertinkatu 23
00121 Helsinki (FI)

(54) A personal firewall with location dependent functionality

(57) A computer device is provided with a local security mechanism, a personal firewall, for protecting the computer device from attacks from a foreign network, in addition to or instead of a firewall in the internal network which protects the computer when connected to a home network. The personal firewall is provided with different sets of security rules for the home network and foreign networks. The personal firewall is arranged to detect its current location, i.e. determine to which network it is connected to at each particular moment. The personal firewall activates one of the given sets of security rules according to the detected current location of the computer device, i.e. the personal firewall automatically uses the security rules predefined for the network to which the computer device is connected at each particular moment. Upon detecting a change in the location, the personal firewall immediately adapts to use security rules predefined for the new location.

Fig. 1



EP 1 313 290 A1

Printed by Jouve, 75001 PARIS (FR)

BNSDOCID: <EP_____1313290A1_I_>

Description

Field of the Invention

[0001] The present invention relates to network security and, more particularly, to personal firewalls.

Background of the Invention

[0002] Traditionally, a firewall is considered as a set of components forming a gateway between two or more networks. Thus, a firewall has been a gateway which operates at the same time as a connector and a separator between the networks in a sense that the firewall keeps track of the traffic that passes through it from one network to another and restricts connections and packets that are defined as unwanted by the administrator of the system. Physically a firewall is a machine with appropriate software to do the tasks assigned to it. It can be a router, a personal computer (PC), or any other device that can be used for such purposes. Although firewalls are mostly used to connect Local Area Networks (LANs), i.e. internal networks, to the Internet and to protect against attackers or undesired traffic in general, they may also be used to separate and connect different segments of internal network for security purposes. The advantages of having a firewall are numerous. A firewall secures the network and can be used as a tool for monitoring the traffic especially from the outside to the inside of the network guarded by a firewall. Because all traffic intended for the internal network must pass through the firewall, most of the network security actions and policies can be concentrated in this particular point. This is of course a cost and administrative advantage.

[0003] Nowadays, laptop computers and other portable computer devices are widely used. While outside the internal network, the laptop cannot make benefit of the protection provided by the conventional "gateway-type" firewall. Therefore, approaches to improve security of a client located in a foreign network (a public network or an internal network of a foreign organisation) have been proposed. These approaches are based on protecting the laptop itself by means of a local security mechanism, called a personal firewall herein, installed in the laptop (in addition to or instead of a firewall in an internal network, which protects the computers connected to the internal network). The personal firewall may be implemented as software installed in the computer device, or as a separate electronic device connected to the computer device.

[0004] European patent application EP 0 952 715 discloses a firewall security device connected to an external communication port of a computer device. The incoming communications stream to the computer device from e.g. public networks is passed through the firewall security device. The firewall device applies standard security measures, thereby protecting the computer device.

[0005] There is a particular need for such protection by means of a personal firewall if the laptop is allowed to have a remote access, e.g. make a VPN (Virtual Private Network) connection to company network while being connected to a foreign network. In order to improve security of the VPN connections, one prior art solution is to enforce a protection level of a laptop, when a VPN tunnel to a company network is created. This means for example that, during a VPN connection, the IP address forwarding is not allowed, or that any connection attempts to the laptop are denied.

[0006] Clearly this is not enough, since the laptop must be protected as soon as it is connected to a foreign network, not only during a VPN connection. The laptops are often used by non-technical people, which increases the risk of overlooking security aspects. Laptops contain sensitive material, such as customer emails. If a laptop is unprotected, when connected to a foreign network, even for a short period of time, there is a risk of getting infected by a hostile application. Such application can be activated later, when the laptop is connected to an internal network and offer inside help for attacks.

[0007] Thus, there is a need to protect the laptop by means of a personal firewall always when the laptop is connected to a foreign network. However, when the laptop is connected to a company internal network, such personal firewall may unduly prevent some essential traffic. For example, the personal firewall should allow use of a laptop at home (internal) network and access to all services, such as disk-share. In a home network even non-IP protocols are sometimes used. Therefore, it is not feasible to have a personal firewall running at all times, at least not with the same configuration, since the protection needs in an internal network are different from those in a foreign network.

[0008] Some of the current solutions allow changing the set of rules used in the personal firewall, that is, they allow the user of the laptop to use different rule sets when connected to the internal network and when connected to a foreign network. However this is a manual operation. Since manual action is required, there is a high risk that operation is not done. Risk is even higher if the end user does not fully understand the need of a firewall.

Summary of the Invention

[0009] An object of the invention is to improve the security and flexibility of a personal firewall. The object is achieved by the invention disclosed in the attached independent claims. Preferred embodiments are disclosed in the attached dependent claims.

[0010] A computer device which can be connected to a home network (such as an internal network of a company or other organisation where the user is employed) and to a foreign network (such as a public network or an internal network of a foreign organisation) is provided with a local security mechanism, called a personal fire-

EPNSDOCID: <EP 1313290A1_I_>

EX1002
CISCO SYSTEMS, INC. / Page 147 of 1453

wall herein, for protecting the computer device from attacks from a foreign network, in addition to or instead of a firewall in the internal network which protects the computer when connected to the internal network. The personal firewall is provided with different sets of security rules, at least one set of rules for the home network and at least one set of rules for foreign networks. In its simplest form, the set of rules for the home network contains no restrictions for the communication or use of service in the home network. The personal firewall is arranged to detect its current location, i.e. to determine the network to which it is connected at each particular moment. The personal firewall activates one of the given sets of security rules according to the detected current location of the computer device, i.e. the personal firewall automatically uses the security rules predefined for the network to which the computer device is connected at each particular moment. Upon detecting a change in the location, the personal firewall immediately adapts to use security rules predefined for the new location. A benefit of the invention is that the protection of a personal firewall is always enabled at the correct level, depending on the current location. On the other hand, when the computer device is located in the home network, a lower level of protection, or no protection at all, can be automatically provided by the personal firewall, so that the communication and services are not unduly restricted in the home network. Thus, the automated location-dependent management of different sets of rules offers optimal protection in different networks, while not unduly restricting operation in the home network.

[0011] The current location of the computer device is preferably determined on the basis of a currently used IP address of the computer device. This is based on the common practice that a computer device has a different IP address, either a fixed address or a dynamic address, in different networks. The IP address can thereby be utilized for identifying the current network and the location of the computer device.

[0012] However, there are situations where the IP address fails to indicate current location of the computer device. Therefore, in an embodiment of the invention, the current location determined on the basis of the current IP address of the computer device is verified by carrying out an additional location verification procedure with a predetermined network element. In a still further embodiment of the invention, availability of said predetermined network element related to the current IP address is checked. The predetermined network element is such that it responses only if the computer device is located in the network in which it is assumed to be on the basis of the current IP address. If the predetermined network element responses and identifies itself properly, the current location determined based on the current IP address is considered to be verified. Otherwise the computer device determines that the current IP address fails to indicate current location of the computer device. The additional verification process makes it even possible to automatically create a secured tunnel, such as a VPN tunnel to a home network even if the computer device uses the same IP address in the current location as in the internal (home) network. The present invention offers benefits even with stand alone personal firewalls wherein the security rules can be defined locally by the user, although the use of these rules is automated and location-dependent. However, more advantages are achieved when the basic invention is used with a central management of personal firewalls.

[0013] According to an aspect of the invention, security rules are defined, updated and distributed centrally by a centralized rule-based server. Especially the updating of the rules is challenging, because the rule updates must be applied as soon as possible, and therefore the process of updating rules in the personal firewalls must be automated. Updating of rules by push method from the centralized rule base server is not a sufficient option in this case. Use of DHCP (Dynamic Host Configuration Protocol), frequent travelling and the fact that at times the laptop may not be connected to any network makes it next to impossible for the centralized management to initiate contacts with the personal firewalls in the computer devices, because there is no way for the centralized management to know the IP address the computer device is using at a given moment. Therefore, according to an aspect of the invention, the personal firewall is configured to periodically query the availability of updated security rules from the centralized management. The queries should only be made, while the computer device is located in the home network, or optionally, when the computer device has a remote access (e.g. VPN connection) to the home network while being located in a foreign network. In other words, also the updating process is dependent on the current location of the computer device in a similar manner as the selection of the active rules, and similar methods can be utilized for determining the current location.

[0014] According to another aspect of the invention, log files containing information of a status and usage of resources of the computer device are handled in a centralized management location. This enables personnel aware of security aspects to verify whether there have been any attacks against the computer device or not. To that end, the personal firewall sends the log files to the central management, such as to a centralized log server, when the computer device is located in the home network. However, when the computer device is disconnected from the home network, the log files are collected and stored locally in the firewall. In order to enable central handling of the log files, the personal firewall transfers the collected log files to the central log server when such is available. This is performed automatically, whenever the computer device is located in, or optionally, connected to the home network. Again, the handling of the log files in the personal firewall is automated and location dependent in a way similar to the selection of active rules, and similar methods can be used for de-

BNSDOCID: <EP_____1313290A1_I_>

EX1002
CISCO SYSTEMS, INC. / Page 148 of 1453

termining the current location of the computer device.

[0015] The present invention allows use of a computer device in a home (internal) network and access to all services, such as disc-share, and even use of non-IP protocols, which are often denied in foreign networks.

Brief description of the drawings

[0016] Preferred embodiments of the invention will now be described with reference to the attached drawings, in which

Figure 1 is a schematic block diagram of an exemplary network configuration where the present invention can be applied;
Figure 2 shows an exemplary protocol stack of a computer device containing a personal firewall according to the present invention,
Figure 3 illustrates exemplary selection rules and a security rule basis, and the association therebetween,
Figure 4 is a flow diagram illustrating a location-dependent rule base selection according to an embodiment of the invention;
Figures 5 and 6 are flow diagrams illustrating the location verification procedure according to an embodiment of the invention;
Figures 7 and 8 are flow diagrams illustrating the rule base updating according to an embodiment of the invention; and
Figure 9 is a flow diagram illustrating the handling of log files according to an embodiment of the invention.

Preferred embodiments of the invention

[0017] The present invention can be applied in personal firewalls in any computer device which can be moved and connected to different networks. Typically such devices are portable computer devices, such as laptop computers, PDAs, communicators, smart phones, intelligent telecommunication devices, etc. In the following illustrative embodiments of the invention, a laptop computer is used as an example of suitable computer devices.

[0018] Figure 1 shows a schematic block diagram of an exemplary network configuration. The configuration is shown only to facilitate the understanding and description of the present invention. The present invention is not intended to be restricted to any particular network configuration. Further, in order to improve clarity, only network elements which are somehow involved with the present invention are shown in Figure 1.

[0019] As illustrated in Figure 1, private local networks 10 and 13 are coupled to a public network, such as the Internet 12 via firewalls 5 and 7, respectively. Naturally, the coupling between the private networks and the public Internet 12 may include also routers and Internet service providers (ISPs not shown in Figure 1). As is well known in the art, private networks 10 and 13 may be, for example, company networks, such as local area networks (LANs) which connect users and resources, such as workstations, servers, printers and the like of the company. A private internal network may also consist of several sub-networks separated by internal firewalls. In the exemplary network configuration shown in Figure 1, the private company sub-network 11 is connected via a firewall 6 to the private local network 10. Such a sub-network 11 may be, for example, a dedicated network for a specific department of the organisation, such as the research and development (R&D) department which must have a restrictive access and higher protection level compared with other part of the company network. Sub-networks of the company, such as the local networks of organisation headquarters and branch offices may be interconnected by secure connections, such as virtual private network (VPN).

[0020] As already described above, the firewalls 5, 6 and 7 are gateways which operate at the same time as connectors and separators between the networks in a sense that the firewall keeps track of the traffic that passes through it from one network to another and restricts connections and packets that are defined as unwanted by the administrator of the system. Physically a firewall is a machine with appropriate software to perform the task assigned to it. It can be a router, a personal computer (PC), or whatever that can be used for such purposes.

[0021] However, the firewalls between the networks, or the implementations thereof, are not relevant to the present invention.

[0022] The present invention relates to protecting of the computer device, e.g. laptop itself, by means of a local security mechanism, called a personal firewall herein, installed on the laptop in addition to or instead of a firewall in a private network. The personal firewall may be implemented as software installed and run in the computer device, which is a preferred embodiment, or as a separate electronic device connected to the computer device. In Figure 1, the laptops 1, 2, 3 and 4 illustrate laptops provided with a personal firewall.

[0023] Figure 2 illustrates the basic principle of a personal firewall installed in a laptop. Physical and network layers 200 refer to all protocols and physical connections required for transferring protocol data units (PDUs) of the upper layers. The upper layers 200 include applications and any transmission protocols employed, such as Internet protocol (IP) transmission control protocol (TCP), NetPEUI, IPX, etc. Basically the personal firewall protection layer 201 operates in a manner analogue to a firewall between networks. More particularly, the personal firewall protection layer 201 operates at the same time as a connector and a separator between the underlying layers and the upper layer in a sense that the personal firewall keeps track of the traffic that passes through it from underlying layers to the upper layers, and

EPNSDOCID: <EP_____1313290A1_I_>

EX1002
CISCO SYSTEMS, INC. / Page 149 of 1453

vice versa, and restricts connections and packets that are defined as unwanted according to the security rules used. The personal firewall protection layer 201 is implemented or controlled by a personal firewall application 203 run in the laptop. In a preferred embodiment of the invention, the personal firewall application 203 carries out the location detection and the location-dependent functions described below, such as the selection of the active rule base according to the current location of the laptop. However, it should be appreciated that the present invention is not intended to be restricted to any specific practical implementation of the personal firewall.

[0024] In accordance with the principles of the present invention, the personal firewall has different sets of rules for the home network (such as the private company network 10) and foreign network, such as the public Internet 12, or the foreign private network 13, or a network of another department of the company. It is not relevant to the present invention what kind of security rules are applied, but some examples are given in Figure 3. For example, a rule base 301 for the foreign company network may list as allowed connections of protocols: hypertext transfer protocol (http), secured http (Https), domain name service (DNS), single message transfer protocol (SMTP) and a VPN connection with IPsec. In the preferred embodiment of the invention these rules are exclusive, in other words, other protocols and connections are denied and blocked by the personal firewall. For a default network, which may be the public Internet 12, the rule base 302 is similar to the rule base 301, except that the SMTP protocol is no longer allowed. For the home network 10, a rule base 300 is defined. The allowed protocols include, in addition to the http, https and the SMTP, also other transmission protocols, such as NetBEUI and IPX. The rule base 300 also allows a disc-share for predefined servers using NetBIOS. Other protocols and connections are denied. It is also possible that the rule base 300 allows all protocols and connections in the home network. Since the home network is protected by a company firewall, the use of a personal firewall in the home network may be regarded as unnecessary. However, the company firewall gives protection only against attacks from the outside of the home network, and the use of a personal firewall protection may be necessary for protecting against attacks from within the home network.

[0025] The different rule bases could be activated manually by a user. However, according to the basic principle of the present invention, the personal firewall automatically selects and activates the proper rule base according to the current location of the laptop.

[0026] Figure 4 is a flow diagram illustrating the selection of the rule base according to one embodiment of the present invention. The simplest way to determine the current location of the laptop is to do it on the basis of the currently used IP address only. This is possible in the cases where the laptop has a different IP address, either a fixed or a dynamic address, in different networks. As is well known in the art, a part of the IP address identifies the network, and can thus be used for detecting the current network of the laptop. The personal firewall may, for example, contain information on the IP address space of home network, and optionally, foreign networks, or a list of addresses available for the laptop in the home network.

[0027] When the current IP address of the laptop matches to a given address space or a list of addresses of the home network 10, for example, it can be assumed that the laptop is located in the home network 10 and the rule base 300 of the home network 10 is used. Thus, the current IP address is used as a selection rule for activating the rule base 300. However, there is some uncertainty in determining the location based on the current IP address only, and some approaches to overcome this problem are described with reference to further embodiments of the invention below.

[0028] Referring again to the generic flow diagram shown in Figure 4, the current IP address of the laptop is firstly determined in the step 401. The current IP address may be obtained simply by asking for it from the operating system of the laptop by means of using IP configuration routine. The current location of the laptop is monitored constantly, and therefore the personal firewall may be configured to periodically query the current IP address from the operating system. More preferably, the operating system of the laptop may be configured to inform any changes in the IP address to the personal firewall, and therefore a need for query the IP address time-to-time can be avoided. The step 401 may also include verification of the location determined based on the IP address by a verification procedure described below. In step 402, the personal firewall compares the current IP address with the current IP address stored in the personal firewall. If the IP address has not changed, the present active rule base can be maintained. However, if the IP address has changed, the personal firewall checks whether the new IP address matches to any IP address space or IP address belonging to one of the networks on the selection rule list in the personal firewall (step 403). If the new IP address does not belong to any of the networks on the selection rule list, the personal firewall considers the current network an unidentified network, and a default rule base 302 is selected (step 404). If the network cannot be identified and the default rule base must be used, it is normally assumed that the laptop is in a potentially hostile environment, most likely in the public Internet 12. Therefore, the default rule base is typically defined to provide the maximum protection needed. If the new IP address belongs to one of the networks defined on the selection rule list in step 403, it means that the network has been identified and a rule base linked to the identified network (or the corresponding selection rule) is selected and activated (step 405). In the simplest implementation, the selection rules include only the home network of the laptop and the cor-

BNSDOCID: <EP_____1313290A1_I_>

EX1002
CISCO SYSTEMS, INC. / Page 150 of 1453

responding IP address space or list of addresses . If the current IP address belongs to the home network, the rule base 300 of the home network 10 is used. Otherwise the rule base 310 for foreign network or the default rule base 302 is used. In a more complicated implementation, there are selection rules (i.e. IP addresses and associated rule bases) also for at least one foreign network and/or different segments of the home network 10.

[0029] In the examples described above there are two or more rule bases which are enabled or disabled on the basis of the current location of the laptop. However, there are also alternative ways to implement different rule bases. One alternative is to provide only one rule base in which the rules are enabled and disabled in different combinations on the basis of the current location of the laptop.

[0030] As noted above, there are situations where the location (the current network) determined on the basis of the current IP address is uncertain, i.e. the IP address fails to indicate the current location of the laptop. If the IP address does not match the current network, use of the Internet protocol (IP) to attack against the laptop is not likely, and one may reason that in that case a personal firewall does not need to be used. However, there is still a possibility that there is an attack using other protocols, such NetBEUI or IPX. By detecting the situation where the IP address of the laptop is not an IP address of the current network, it is possible to block such protocols while in foreign networks. Further, NAT (network address translation) and private IP addresses are frequently used. This means that the same IP address is in use in several networks. In that case it is not enough to trust IP address information only when determining the location of the laptop. It is even possible that while being connected to a hostile network, the DHCP (dynamic host configuration protocol) gives familiar IP address to make it easier to attack the laptop. Basically, the DHCP enables individual computers on a network to connect to a DHCP server, such as the server 9 in Figure 1, and be assigned a dynamic IP address of the current network.

[0031] Thus, according to an aspect of the invention, in addition to the detection of location based on the current IP address described above, a further location verification procedure is carried out with a predetermined network element, which is preferably reachable only from the location to be verified. More generally, the network element is selected in such a way that it responses to the verification request only if the request originates from the location (i.e. the network) to be verified. Preferably, the specific network element is provided with a location verification service supporting the verification according to the invention. The verification procedure requires that the verification method be specified for the personal firewall, preferably at the same time as the different locations are specified. In other words, the methods to verify the location are specified for the personal firewall in the initial configuration, for example. It is also possible that the verification methods are updated or changed by means of the updating procedure described below, in a manner similar to other security rules.

[0032] A generic location verification procedure according to one embodiment of the invention is described with reference to Figures 5 and 6. Firstly, the current location is determined on the basis of the currently used IP address as described above (step 501). Next, the personal firewall selects a predetermined network element that should be available for verification from the determined current location (step 502). Then the personal firewall sends to the selected network element a request to send a response with some data proving the identity of the network element (step 503). Referring now to Figure 6, the verifying network element receives the verification request (step 601) from a personal firewall. Then, either always in response to the verification request or only if predetermined requirements are met, the network element sends the response with the required identity data to the personal firewall (step 602). Referring again to Figure 5, the personal firewall waits for a response (step 504), and if no response is received (preferably within a predetermined period of time), the location determined on the basis of the current IP address is rejected, and the location is determined to be unknown (step 505). In that case, a default location and an associated rule base, such as the rule base 302, can be used.

[0033] However, if the response is received from the network element in the step 504, the personal firewall verifies the identity of the network element on the basis of the received identity data, e.g. by comparing the received identity data with identity data stored in the personal firewall (step 506). If the verification of the identity is unsuccessful (step 507), the procedure proceeds to the step 505 described above. However, if the verification of the identity of the network element is successful, also the location of the laptop determined on the basis of the current IP address has been successfully verified and can be accepted.

[0034] Additionally, it is possible that one IP address is included in more than one selection rule in the personal firewall. In that case, if the verification of the laptop being located in a first network indicated by the current IP address fails, it is checked if the laptop is located in a second network indicated by the current IP address. There are various ways to implement the generic location verification procedure described above. The simplest way to implement the location verification service is to probe some known (known to the personal firewall) element. For example, it is possible to ask the MAC address of the known network element located in the home network and having a known IP address. The network element returns the MAC address in response, and if the AMC address is the one that it is assumed to be (e. g. matches with a MAC address stored in the personal firewall), it is verified that the laptop is located in the home network. If the MAC address is not the correct one, the laptop is determined to be outside the internal

BNSDOCID: <EP_____1313290A1_I_>

EX1002
CISCO SYSTEMS, INC. / Page 151 of 1453

network.

[0035] One possible implementation is that the location verification service is implemented in such network element in an internal network which can be reached only from inside the internal network. For example, the firewall protecting the internal network, such as firewall 5 in Figure 1, may be configured to discard all connections from outside the internal network to this network element. If the personal firewall is able to reach this specific network element, it is verified that the personal firewall resides inside the internal network. Otherwise the personal firewall resides outside the internal network. There may be a plurality of such location verification services in a plurality of internal networks or sub-networks, and if the personal firewall cannot reach any of them, then it is assumed to be outside this plurality of internal networks or sub-networks.

[0036] The location verification service may be incorporated into the network firewall, such as the location verification service 50 in the firewall 5 in Figure 1. For example, verification requests only from the direction of the internal network (such as home network 10) may be responded by the location verification service 50. This implementation is rather straightforward, since the present firewalls are readily capable of detecting from which direction, that is, from which interface, a data packet is coming from.

[0037] In any case it is preferred that the personal firewall communicates with the location verification service by using some cryptographically strong method, such as public key encryption. For example SSL can be used. The certainty of the location verification can be further improved by setting the TTL (time-to-live) field in the location verification request to a relatively low value, so that the request is capable of reaching only a nearby location verification service. The TTL value is decremented each time the verification request passes through a router connecting different networks or network segments. If the TTL value is set to, for example, a zero value the verification request is not able to pass through a router to a different network or a network segment.

[0038] The use of additional location verification makes it even possible to automatically create a VPN tunnel to the home network even if the current location (a foreign network) is using the same IP address as in the internal network.

[0039] All the embodiments described above are effective both in standalone computers and in centrally managed computers. The central management of personal firewalls enables a uniform protection level in all computer devices using the private network. One feature of the central management is that preferably all of the personal firewalls have essentially similar security rules. It should also be possible to update these. It is preferable that rule updates are applied in the personal firewalls as soon as possible after they have been made in the central management. Because it is not sufficient to rely on the manual updating by the user, the process of updating the rules must be automated. However, distribution of the updated rules by a push transmission from the central management is not a sufficient option in a case where the personal firewalls can move from one network to another. Therefore, according to an aspect of the invention, the personal firewalls are arranged to periodically query the availability of updated rules from the central management. An updating procedure according to one embodiment of the invention is described with reference to Figures 7 and 8.

[0040] Firstly, a personal firewall measures a predetermined updating period, which can be any period of time, preferably one day or a few days (step 701). In step 702, the personal firewall checks whether the updating period has expired, and if not, the procedure returns to the step 701. When the updating period has expired, the personal firewall checks whether the current location of the laptop is in the home network (step 703) or in another subnetwork of the same company. The location determination is preferably based on the methods described above. If the current location is in the home network, the process proceeds directly to the step 705. However, if the current location is not in the home network, the personal firewall waits for the laptop to return to or establish a connection (e.g. VPN) to the home network (step 704), before proceeding to the step 705. In the step 705, the personal firewall sends a rule update query to the central management, such as the personal firewall management server 8 in Figure 1. Referring now to Figure 8, the personal firewall management 8 receives the rule update query from the personal firewall (step 801) and sends updated rules, if there are any, to the personal firewall (step 802). Referring again to Figure 7, the personal firewall checks whether the reply received from the personal firewall management 8 contains rule updatings (step 706), and if not, the process returns to the step 701 to measure the next updating period. However, if rule updatings have been received, the personal firewall updates the relevant rule bases stored in the laptop (step 707).

[0041] It is also preferable that the logs relating to the communication transactions of the laptop are handled in a central location. Since the laptops are frequently disconnected from the home network, logs must be collected locally. In order to enable central handling, the logs must be transferred to a central log server, such as the personal firewall management 8, when such is available. This should take place automatically when the computer device provided with a personal firewall is connected to the home network. Figure 9 illustrates log handling according to one embodiment of the invention.

[0042] Firstly, the personal firewall creates a log file each time the laptop is involved with a communication transaction, such as an Internet session (step 91). Then the personal firewall determines the current location of the laptop, preferably based on the location determining methods described above (steps 92 and 93). If the lo-

BNSDOCID: <EP_____1313290A1_I_>

EX1002
CISCO SYSTEMS, INC. / Page 152 of 1453

cation of the laptop is in the home network or in another subnetwork of the same company, the personal firewall sends the log file to the central log server 8 immediately (step 94). However, if the current location of the laptop is not in the home network, the process proceeds to the step 95, where the log file is stored locally. Similarly, a number of log files is collected locally while the laptop is disconnected from the home network. When the personal firewall next time detects that the computer device is relocated in the home network, it sends the collected log files to the central log server 8. Optionally, the personal firewall may also send the collected log files to the personal firewall management 8 when the laptop has established a (e.g. VPN) connection to the home network.

[0043] It is apparent for those skilled in the art that the illustrative embodiments described are only examples and that various modifications can be made within the scope and spirit of the invention as defined in the appended claims.

Claims

1. A method of controlling a personal firewall in a client computer, said method comprising
   providing said personal firewall with at least one set of security rules to be used when said client computer is connected to a home network of said client computer, and at least one set of security rules to be used when said client computer is connected to foreign networks,
   monitoring the current location of said client computer based on an Internet Protocol (IP) address currently used by said client computer, and
   automatically selecting one of said sets of security rules by said personal firewall according to said current location of said client computer.

2. A method according to claim 1, wherein
   said step of providing comprises providing said client computer with said set of security rules in form of at least two rule bases,
   said step of selecting comprises enabling one of said rule bases at a time according to the current location of said client computer.

3. A method according to claim 1, wherein
   said step of providing comprises providing said client computer with said set of security rules in form of one rule base, and
   said step of selecting comprises enabling and disabling rules in said one rule base in different combinations according to the current location of said client computer.

4. A method according to claim 1, wherein said step of monitoring comprises
   storing in said client computer an IP address space of said home network,
   comparing the current IP address of said client computer with said IP address space, and
   if the current IP address of said client computer matches said IP address space, determining said personal firewall to be located in said home network.

5. A method according to any one of claims 1, 2 or 3, wherein said step of monitoring comprises
   storing in said client computer a list of IP addresses of said home network,
   comparing the current IP address of said client computer with said list of IP addresses, and
   if the current IP address of said client computer matches one of said addresses on said list, determining said client computer to be located in said home network.

6. A method according to any one of claims 1, 2 or 3, comprising
   verifying the current location determined on the basis of the current IP address of said client computer by carrying out a location verification procedure with a predetermined network element.

7. A method according to claim 6, wherein said step of verifying comprises
   checking availability of said predetermined network element related to the current IP address, said predetermined network element responding only if said client computer is located in the network in which it is assumed to be on the basis of the current IP address,
   verifying the current location determined based on said current IP address, if said predetermined network element responses with a specific identity data.

8. A method according to claim 7, wherein said specific identity data is a Media Access Control (MAC) address of said predetermined network element.

9. A method of managing a personal firewall in a client computer, comprising
   storing in said personal firewall at least one set of security rules to be used when said client computer is connected to a home network of said client computer, and at least one set of security rules to be used when said client computer is connected to foreign networks,
   storing updated sets of security rules, if any, in a centralized unit in said home network of said client computer,
   configuring said personal firewall to periodically query the availability of said updated sets of security rules from said centralized rule base server

BNSDOCID: <EP_____1313290A1_I_>

EX1002
CISCO SYSTEMS, INC. / Page 153 of 1453

when being located in said home network, or when having a remote access to said home network while being located in a foreign network, and

loading said updated sets of security rules from said centralized rule base server to said personal firewall in response to said query, if such updated sets of security rules are available.

10. A method according to claim 9, comprising

monitoring the current location of said client computer based on an Internet Protocol (IP) address currently used by said client computer, and

automatically activating said periodical query, when the current location of said client computer is in said home network.

11. A method according to claim 9, comprising

monitoring the current location of said client computer based on an Internet Protocol (IP) address currently used by said client computer,

sending log files to a centralized log server from said personal firewall, when the current location of said client computer is in said home network, said log files containing information on communication transactions in said client computer,

collecting log files locally at said personal firewall, when the current location of said client computer is not in said home network, and

transferring said locally collected log files from said personal firewall to said centralized log server, when said client computer is connected to said home network.

12. A computer terminal, comprising

a personal firewall provided with at least one set of security rules to be used when said computer terminal is connected to a home network of said computer terminal, and at least one set of security rules to be used when said computer terminal is connected to foreign networks,

said personal firewall having a mechanism monitoring the current location of said computer terminal based on an Internet Protocol (IP) address currently used by said computer terminal, and

said personal firewall having a mechanism automatically selecting one of said sets of security rules by said personal firewall according to said current location of said computer terminal.

13. A computer terminal according to claim 12, further comprising

a mechanism verifying the current location determined on the basis of the current IP address of said computer terminal by carrying out a location verification procedure with a predetermined network element.

14. A computer-readable medium, containing a computer software which, when executed in a computer device, causes the computer device to provide a personal firewall routine comprising

storing at least one set of security rules to be used when said computer device is connected to a home network of said computer device, and at least one set of security rules to be used when said computer device is connected to foreign networks,

monitoring the current location of said computer device based on an Internet Protocol (IP) address currently used by said computer device, and

automatically selecting one of said sets of security rules by said personal firewall according to said current location of said computer device.

15. A computer-readable medium according to claim 14, said personal firewall routine further comprising

verifying the current location determined on the basis of the current IP address of said client computer by carrying out a location verification procedure with a predetermined network element

16. A computer device, comprising a personal firewall routine configured to store security rules for a home network of said computer device, and for foreign networks,

periodically query the availability of updated security rules from a centralized rule base server in said home network of said computer device when said computer device is located in said home network, and

download said updated security rules from said centralized rule base server, if such updated security rules are available in said centralized rule base server.

17. A computer device according to claim 16, said personal firewall routine being further configured to

activate said periodical query also when said computer device has a remote access to said home network while being located in a foreign network.

18. A computer device, comprising a personal firewall routine configured to

send log files to a centralized log server, when a current location of said computer device is in a home network of said computer device, said log files containing information on communication transactions in said computer device,

collect log files locally in said computer device, when the current location of said client device is not in said home network,

transfer said locally collected log files to said centralized log server, when said computer device is reconnected to said home network.

19. A computer-readable medium, containing computer software which, when executed in a computer de-

BNSDOCID: <EP_____1313290A1_I_>

EX1002
CISCO SYSTEMS, INC. / Page 154 of 1453

vice, causes the computer device to provide a personal firewall routine comprising

storing security rules for a home network of said computer device, and for foreign networks,

periodically querying the availability of updated security rules from a centralized rule base server in said home network of said computer device when said computer device is located in said home network, and

downloading said updated security rules from said centralized rule base server, if such updated security rules are available in said centralized rule base server.

20. A computer-readable medium, containing computer software which, when executed in a computer device, causes the computer device to provide a personal firewall routine comprising

sending log files to a centralized log server, when a current location of said computer device is in a home network of said computer device, said log files containing information on communication transactions in said computer device,

collecting log files locally in said computer device, when the current location of said client device is not in said home network,

transferring said locally collected log files to said centralized log server, when said computer device is reconnected to said home network.

21. A computer program comprising program code means for performing all the steps of any one of claims 1 to 11 when the program is run on a computer.

BNSDOCID: <EP_____1313290A1_I_>

EX1002
CISCO SYSTEMS, INC. / Page 155 of 1453

Fig. 1

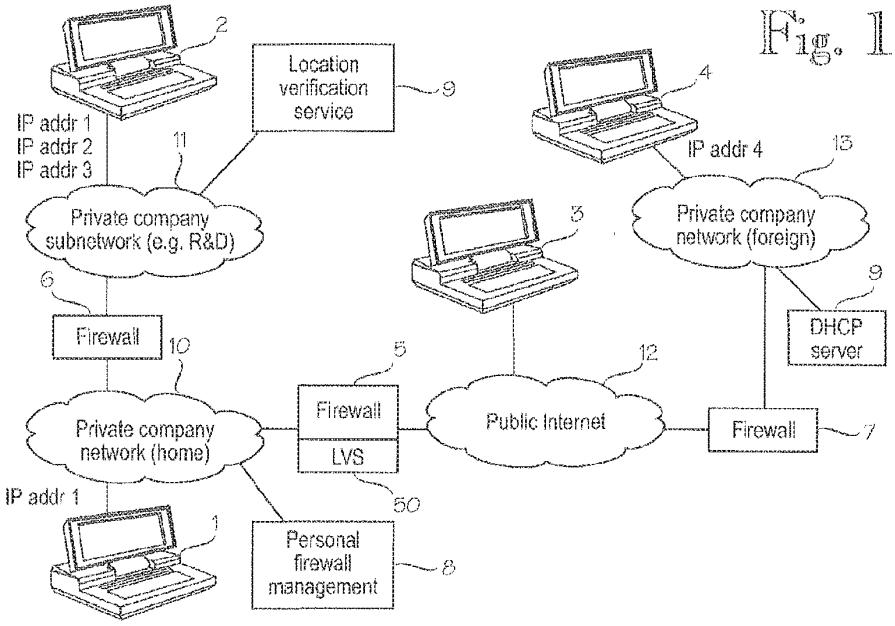


Fig. 2

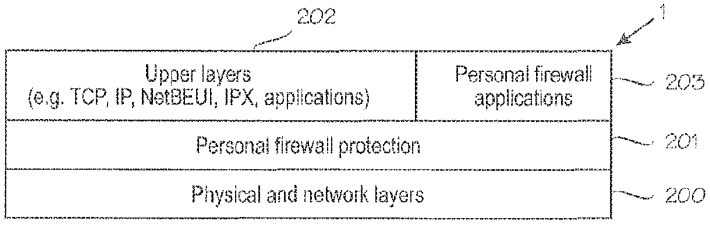
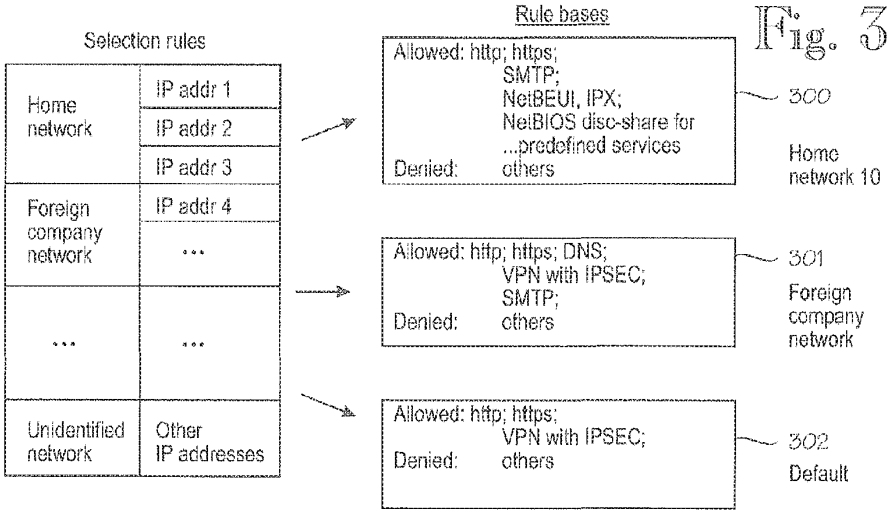


Fig. 3



BNSDOCID: <EP_____1313290A1_I_>

EX1002
CISCO SYSTEMS, INC. / Page 156 of 1453

Fig. 4

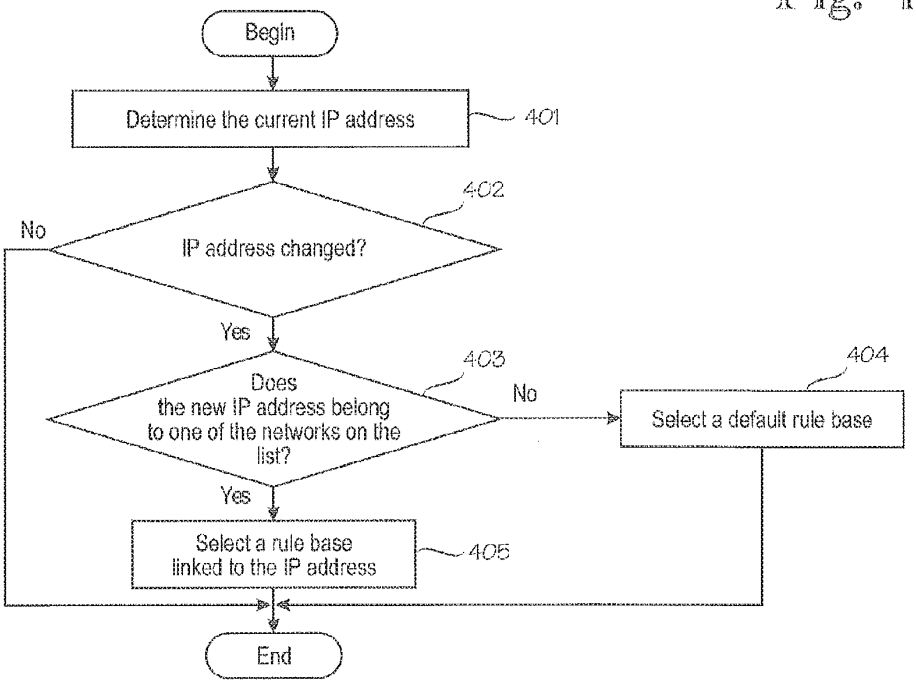
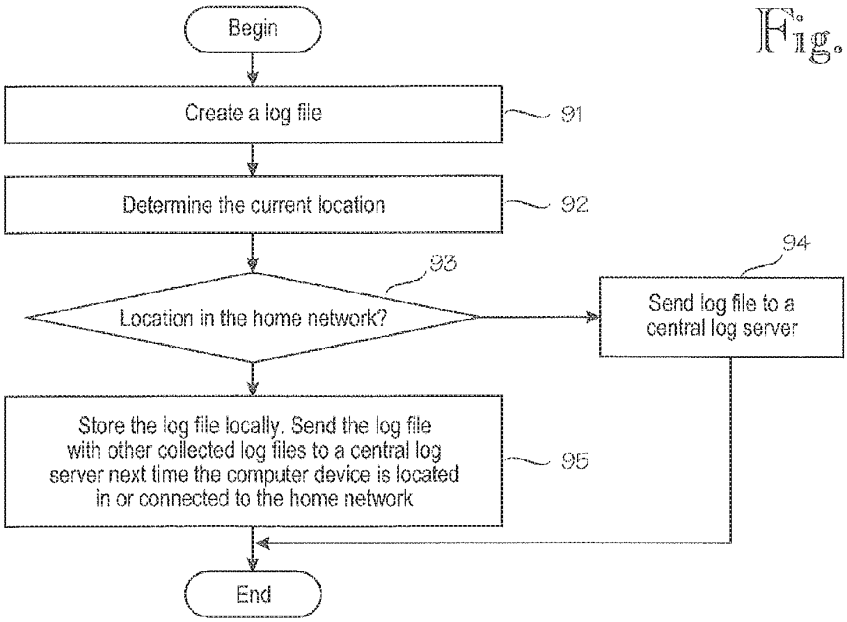


Fig. 9



BNSDOCID: <EP_____1313290A1_I_>

EX1002
CISCO SYSTEMS, INC. / Page 157 of 1453

Fig. 5

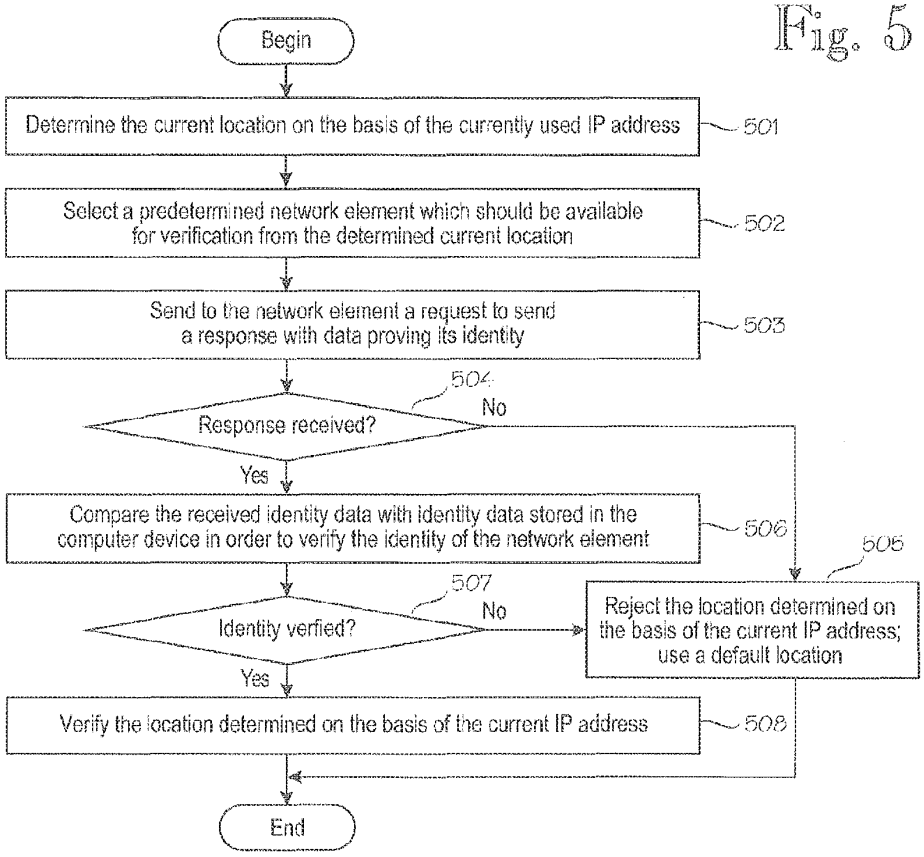


Fig. 6

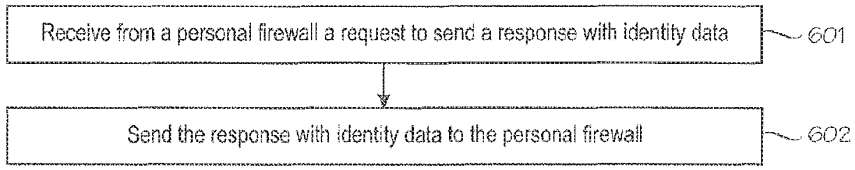
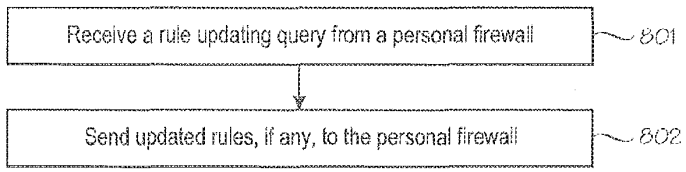


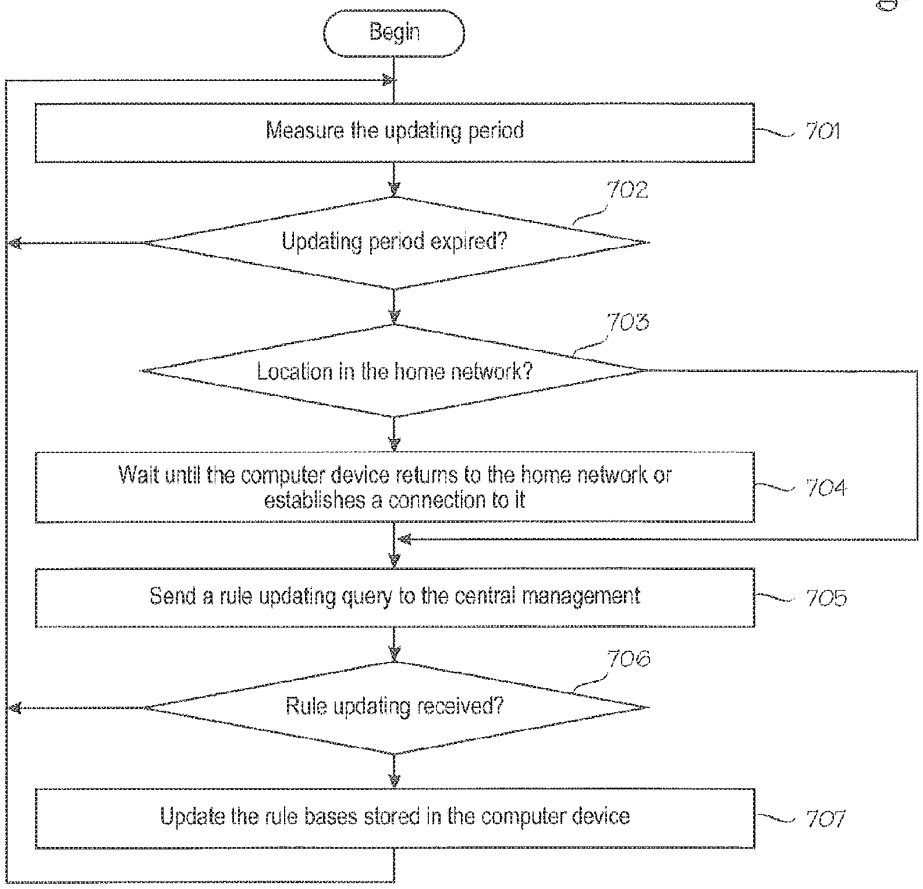
Fig. 8



BNSDOCID: <EP_____1313290A1_I_>

EX1002
CISCO SYSTEMS, INC. / Page 158 of 1453

Fig. 7



BNSDOCID: <EP_____1313290A1_I_>

EX1002
CISCO SYSTEMS, INC. / Page 159 of 1453

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 02 10 2581

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	EP 0 854 621 A (AT & T CORP) 22 July 1998 (1998-07-22) * page 4, line 28 - line 47 *	1-21	H04L29/06
A	US 6 158 008 A (OWENS LESLIE DALE ET AL) 5 December 2000 (2000-12-05) * claim 1 *	1-21	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)

H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	14 March 2003	Veen, G

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

BNSDOCID: <EP_____1313290A1_I_>

EX1002
CISCO SYSTEMS, INC. / Page 160 of 1453

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 02 10 2581

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

14-03-2003

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0854621 A	22-07-1998	US 6233686 B1	15-05-2001
		CA 2226814 A1	17-07-1998
		EP 0854621 A1	22-07-1998
		JP 10229418 A	25-08-1998
US 6158008 A	05-12-2000	WO 9921339 A1	29-04-1999

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

BNSDOCID: <EP_____1313290A1_I_>

EX1002
CISCO SYSTEMS, INC. / Page 161 of 1453

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 May 2005 (19.05.2005)

PCT

(10) International Publication Number
WO 2005/046145 A1

(51) International Patent Classification[7]: H04L 12/56, 12/46

(21) International Application Number: PCT/SE2004/001611

(22) International Filing Date: 5 November 2004 (05.11.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/517,737 6 November 2003 (06.11.2003) US
10/977,724 29 October 2004 (29.10.2004) US

(71) Applicant: TELEFONAKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S-164 83 Stockholm (SE).

(72) Inventor: HALEN, Joacim; Anhaltsvägen 8, S-191 40 Sollentuna (SE).

(74) Agent: KARIN BOESTAD et al.; Ericsson AB, Patent Unit Core Networks Kista, S-164 80 Stockholm (SE).

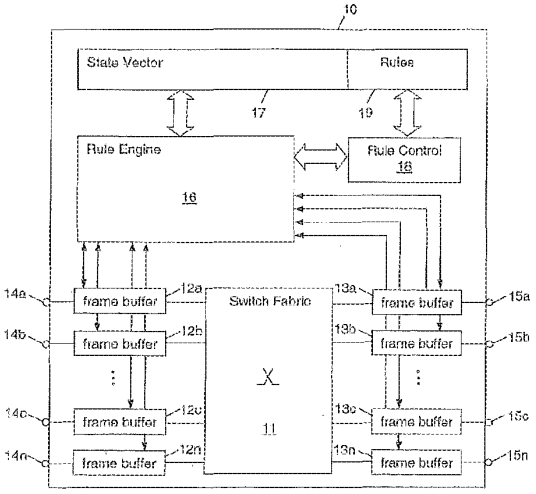
(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: ADAPTABLE NETWORK BRIDGE



(57) Abstract: An adaptable network bridge such as an Ethernet bridge (10) includes a Rule Engine (16) that processes data frames according to a set of switching rules. Each switching rule identifies a type of frame to which the rule applies, and how the type of frame is to be processed. The bridge also includes means (18) for dynamically adding, subtracting, or modifying the switching rules in response to changes in the bridge's state information, or changes in context information. If the bridge includes a plurality of input/output ports (14, 15), the Rule Engine (16) may include a plurality of sets of switching rules, with each set of switching rules being applicable to a different port in the bridge. In this way, different network providers can share the same equipment, but have different network behavior.

WO 2005/046145 A1

ADAPTABLE NETWORK BRIDGE

CROSS-REFERENCE TO RELATED APPLICATIONS

This nonprovisional application claims priority under 35 U.S.C. § 119(e) on U.S. Provisional Application No. 60/517,737 entitled, *Programmable Bridge*, filed November 6, 2003, the disclosure of which is incorporated herein in its entirety.

BACKGROUND OF THE INVENTION

Technical Field of the Invention

The present invention relates generally to digital communication systems. More particularly, and not by way of limitation, the invention is directed to an adaptable network bridge having a Rule Engine that simplifies adapting the bridge to dynamically changing conditions.

Description of Related Art

Ethernet is a layer-2 packet-based transmission protocol that is primarily used in local area networks (LANs). Ethernet is the common name for the Institute of Electrical and Electronics Engineers (IEEE) 802.3 industry specification. Data is transmitted in Ethernet frames. Each frame includes a preamble with 64 bits utilized for synchronization. A Start of Frame Delimiter (SFD), a destination address, a source address, and a length/type identifier follow the preamble. Media Access Control (MAC) client data, together with a Packet Assembler/Disassembler (PAD) may vary in length from 46 to 1500 bytes (octets). A Frame Check Sequence (FCS) adds four more octets. Higher-level protocols reside in the content part of the frame. The frame size is counted from the destination address to the FCS, inclusive, and thus may vary between 64 and 1518 octets, not including a Virtual Local Area Network (VLAN) tag, which adds 4 octets.

Today most packet-based networks are built on Ethernet technology, as it is a cheap and reliable technology with good performance. Ethernet has been used in office networks for a long time and is now used to build Wide Area Networks (WANs) as well as small networks in homes. The communications

industry is now expanding the use of Ethernet to what is called "Public Ethernet" where millions of users are connected in the same network. Unfortunately, Ethernet does not scale to such large networks due to flooding of broadcasted messages. Some solutions have been proposed, but these solutions require modifications to the existing standards if they are to be implemented on standard equipment.

Ethernet bridging is a way to connect networks together to form a larger network. The standard for bridging is ANSI/IEEE 802.1d, which is hereby incorporated by reference herein. A bridge is a way to connect two separate network segments together in a protocol-independent way. Packets are forwarded based on Ethernet address, rather than IP address. Since forwarding is done at Layer 2, all protocols can go transparently through a bridge.

There are basically two approaches to adding new functionality to Ethernet bridges (and other Ethernet equipment as well): standardization thru IEEE, or proprietary solutions, which make the equipment non-standard. Adding new functionality and behavior to IEEE 802.1d MAC bridges, better known as Ethernet switches (or other Ethernet equipment), is a difficult and time-consuming process without any guarantees of success. Each new function must be proposed to and scrutinized by an IEEE standardization group (an existing working group or a new group has to be accepted and established). If one is lucky, the proposed function is accepted and added to the standard. However, since each new function requires a change in the standard, there is reluctance to add new functions. If the proposal is rejected, one is limited to a proprietary solution on non-standard equipment. The members of the standardization groups come from different vendors and other organizations, and although they are supposed to act in the interest of IEEE and the entire community, they may also act on agendas from their own organization/company that might be in conflict with the proposed functionality, thereby turning it down. It should also be noted that if a new function is added to the standard, it is then up to the different vendors to add the standardized functionality. A feature may be standardized but not made mandatory.

The proprietary approach also has its drawbacks. For example,

EX1002
CISCO SYSTEMS, INC. / Page 164 of 1453

programmable network processors have been available for some time, and bridges may be purchased off the shelf containing programmable network processors. Proprietary solutions can be implemented on these. However, these network processors are vendor specific, and the solution will only work on that network processor or processor family. The solution will not be portable, and it will not be possible to run it on other vendors' equipment. Additionally, programming a network processor is done at a very low level, basically in assembly language, and the programming model is hard, requiring special skill. It should also be noted that a proprietary solution will make the equipment non-standard, and customers are more reluctant to buy non-standard equipment. There might also be inter-operational problems with other equipment.

SUMMARY OF THE INVENTION

The present invention is an adaptable network bridge having a Rule Engine that simplifies the adaptation of the bridge to dynamically changing conditions related, for example, to network conditions and user context. Simplicity is achieved by specifying how data frames should be processed and switched in terms of switching rules. Flexibility is achieved by enabling dynamic loading and updating of rules in the bridge via a protocol. In addition, one bridge may generate or modify rules for loading at another, neighboring, bridge. In a preferred embodiment, the bridge is an Ethernet bridge.

Thus, in one aspect, the invention is directed to an adaptable network bridge that includes a Rule Engine that processes data frames according to a set of switching rules. Each switching rule identifies a type of frame to which the rule applies, and how the type of frame is to be processed. The bridge also includes means for dynamically modifying the switching rules. In particular, the rules may be dynamically loaded and updated, for example, in response to changes in the bridge's state information, or changes in context information. In another embodiment, the bridge includes a plurality of input/output ports, and the Rule Engine includes a plurality of sets of switching rules, wherein each set of switching rules is applicable to a different port in the bridge.

In one aspect the rules are forced on the switch by external units such as a

EX1002
CISCO SYSTEMS, INC. / Page 165 of 1453

Network Management System (NMS).

In a further aspect, a switch generates or modifies rules that are forced on other switches.

In yet another aspect, the invention is directed to a method of processing and switching Ethernet frames in an adaptable Ethernet bridge. The method includes the steps of defining a set of switching rules for the adaptable Ethernet bridge; receiving a given frame in the bridge; determining whether any of the rules are applicable to the given frame; and upon determining that one of the rules is applicable to the given frame, processing and switching the frame according to the applicable rule. The switching rules may be dynamically added, subtracted, or modified, for example, in response to changes in state or context information.

An important aspect of the invention is how the extended state vector can be utilized in new ways in the switching process. The switching process can be controlled and adapted in new ways allowing completely new ways to control networks.

BRIEF DESCRIPTION OF THE DRAWINGS

In the following, the essential features of the invention will be described in detail by showing preferred embodiments, with reference to the figures of the attached drawings.

FIG. 1 is a simplified block diagram of a Rule Engine utilized in the adaptable network bridge of the present invention;

FIG. 2 is a sequence diagram illustrating the steps of a process performed by the Rule Engine; and

FIG. 3 is an illustration of a network of adaptable Ethernet bridges controlled by a Network Management System (NMS).

DETAILED DESCRIPTION OF THE INVENTION

In the following description, for purposes of explanation and not limitation, specific details are set forth, such as particular embodiments, circuits, signal formats etc. in order to provide a thorough understanding of the present invention. It will be apparent to one skilled in the art that the present invention may be

EX1002
CISCO SYSTEMS, INC. / Page 166 of 1453

practiced in other embodiments that depart from these specific details.

In existing Ethernet bridges, there are two identifiable phases in the switching process. In the first phase, parts of the frame header are checked for specific information. For example, the destination address of each frame may be checked against a forwarding table, priority bits, VLAN tags, and the like. In the second phase, different actions are taken within the bridge depending on the result of this check. For example, the frame may be sent to the port pointed to in the forwarding table, or the frame may be sent to all ports except the originating port, and so on. These steps characterize a process in which a frame is put through a filter that selects the action to take. Another important element is that the bridge stores and retrieves information in the form of a simple state vector in a forwarding table (i.e., memory), which the bridge is using in the process. However, the different parts of this process are fixed and may not be altered.

The present invention is based on a generalization of this switching process that adds several new key aspects to switching, enabling new ways of adapting and controlling the switching process as well as new ways to control Ethernet networks. The invention provides an adaptable Ethernet bridge having a Rule Engine that simplifies the addition or modification of functionality within the bridge. One of the purposes of the adaptable bridge is to provide a simple solution whereby anyone with reasonable skill can implement and add new functionality in a standardized way on standard equipment. Simplicity is achieved by specifying how Ethernet frames should be processed and switched in terms of switching rules. Flexibility is achieved by enabling dynamic loading and updating, inspection, and prioritization of rules in bridges via a protocol.

The generalized switching process consists of the Rule Engine processing Ethernet frames by applying the switching rules. A switching rule encapsulates a specific switching behavior that describes the filter and action processes together with the state vector. A switching rule thus consists of three parts:

1) A filter function that can filter any part or parts of a frame. The purpose of the filter is to decide if the rule is applicable to a given frame. In other words, the filter works as a predicate function on frames. In this decision process information in the state vector may be used.

EX1002
CISCO SYSTEMS, INC. / Page 167 of 1453

2) An action function that describes how a frame header (or the entire frame) should be transformed and how the frame should be switched, i.e. to which port or ports the frame should be sent. In this process the action function may alter the state vector.

3) A state vector that the filter function and the action function can use in the switching process.

The switching rule can also contain other information such as version, priority specification, vendor information, and the like.

The state vector is an abstraction of several parts:

1) A local memory for a rule or a set of rules where rule-specific data can be stored and altered. Specific "management rules" make it possible to access that data from, for example, a management system.

2) A global bridge memory where bridge-specific data applicable to and accessible by all rules can be stored and altered. One example is the port-forwarding table.

3) Access to a set of bridge resources that can be implemented as library functions. Some examples are a function to retrieve the source port of the frame processed, a function that provides timestamps, counters and timers, and functions that describe the traffic flows and load in the bridge. The invention is not limited to these examples; other functions may be identified by those skilled in the art.

A switching rule describes the types of frames that match the rule and how these frames should be processed (e.g., switched or transformed before switching). Each incoming frame is checked against the set of rules stored in the bridge. If a rule matches, the frame is processed and switched according to the specification in the rule. If no rule matches the frame, a default rule may be utilized, or the frame may be dropped.

With the concept of rules, the switching process is defined as a simple and understandable programming model. Standardizing rule language and making it possible to dynamically load new rules in a bridge also makes it possible to add new functionality, adapting standard equipment to the needs at hand. If some functionality becomes obsolete, that functionality can be removed by removing the

EX1002
CISCO SYSTEMS, INC. / Page 168 of 1453

rule or set of rules implementing it.

A powerful extension is to allow different rule sets to be valid for different ports enabling, for example, different network providers to share the same hardware but have different network behavior. Different embodiments of this extension include: a rules control mechanism that selects and prioritizes available rule sets based on port, time of day, load, and the like. Alternatively, this kind of information may be described in the filter functions, and the Rule Engine tries all rules until it finds a match.

Yet another powerful extension is to allow rules that monitor the state vector instead of being matched against Ethernet frames. That is, the filter function monitors the state vector, and when some condition is fulfilled, the action function is invoked. The monitoring process can be implemented by regularly processing these rules in the Rule Engine or in a separate Rule Engine.

Note that allowing the filter and action functions to have access to a state vector that goes beyond the forwarding table provides new and powerful ways to process and switch frames.

FIG. 1 is a simplified block diagram of an exemplary embodiment of the dynamically adaptable network bridge 10 of the present invention. The adaptable bridge includes many of the same components as existing bridges such as switch fabric 11, frame buffers 12a-12n and 13a-13n, and ports 14a-14n and 15a-15n. In addition, however, the adaptable bridge includes a Rule Engine 16, which replaces the implementation of some or all protocols. The adaptable bridge also includes a state vector memory 17 accessible by the Rule Engine, a rule control function 18, and a rules memory 19 accessible by the Rule Engine through the rule control function. Collectively, these new bridge components enable the adaptable bridge to receive and store rules from external units, store a state vector which may be dependent on external sources, and store rules that are imposed on other bridges.

Hybrid designs having both a Rule Engine and some of the protocols of existing bridges may also be implemented. The Rule Engine has processing capabilities, that is, the Rule Engine can (1) apply the filter function to a frame and calculate the result; (2) apply the action function if the rule matches; (3) access

EX1002
CISCO SYSTEMS, INC. / Page 169 of 1453

the state vector; and (4) access the other resources of the switch. A frame entering the adaptable bridge through an input port such as port 14a and frame buffer 12a is acted upon by switching rules in the Rule Engine 16, including the filter function, action function, and state vector. The result is a calculated result frame, which is outputted through switch fabric 11, and an appropriate frame buffer and output port such as frame buffer 13a and output port 15a.

The rule control function 18 adds and removes rules dynamically, and orders or prioritizes THE set of rules. The rule control function may be implemented as protocols and secured against unwanted manipulation by using well known techniques intended for that purpose, for example, using digital signatures and encryption. Additionally, the rule control function may include a mechanism to transform (or translate) switching rules in human-readable form to an efficient form understandable by the Rule Engine 16.

The mechanisms to access different bridge resources and state information (i.e., state vectors), mechanisms to access library functions, and a protocol for externally accessing the state information are important parts of the adaptable bridge. The bridge resources and state information may be accessed via, for example, an Application Programming Interface (API). The protocol for externally accessing the state information may be implemented as a set of rules. The state of the bridge can affect switching rules dynamically, that is, a rule can behave differently depending on the current state. For example, frames can be switched differently depending on time of day, traffic pattern, traffic load, and the like. This behavior can also be controlled externally by, for example, a network management system (NMS).

FIG. 2 is a sequence diagram illustrating the steps of a method of processing an Ethernet frame by the Rule Engine 16. The process starts at step 21 and moves to step 22 where, for each incoming Ethernet frame, the port-specific rules associated with the Source Port are merged with the rules shared among all ports of the bridge (this merge can be done in advance by the priority module as a ordered list). The rules in the list are then tested to determine whether the frame matches the rule. This process begins at step 23, where a determination is made whether there are any more rules left to test. If not, and all

EX1002
CISCO SYSTEMS, INC. / Page 170 of 1453

the rules have been tested, the frame is dropped at step 24. However, in the case of the first rule, there are rules left to test, so the method moves to step 25 where the filter function of the first rule in the list is applied to the frame. The filter function uses the information found in the frame together with the current state vector to determine whether the frame matches the rule. The filter function is a predicate, so the result at step 26 will be either true (the frame matches the rule) or false (the frame does not match the rule). If the result is false, the rule is discarded at step 27, and the method returns to step 23 where the test is performed on the next rule in the list.

The remainder of the rules are then tested until either no rules are left and the frame is dropped at step 24, or there is a match at step 26, and the method moves to step 28 where the action function of the rule is applied to the frame. The action function may use the library functions, the information in the frame, and the state vector to transform (or modify) the frame. In this process, the action function can use functions to modify the state vector. For example, a counter may be incremented, which counts the number of frames containing a specific high-level protocol coming from the port. At step 29, the action function determines the destination port or ports and sends the (possibly transformed) frame to the determined port or ports. The method then ends at step 30.

Another important aspect of the invention not shown in the sequence diagram is that other resources or modules in the bridge may continuously monitor and change the state vector in parallel. An extended Rule Engine, to the one described, may then invoke rules that, instead of being matched against Ethernet frames, monitor the state vector. When one or more predefined criteria are fulfilled (determined by the filter function), the action function generates new frames containing new rules to be sent to the bridge itself or to nearby bridges altering their behavior.

FIG. 3 is an illustration of a network 35 of adaptable Ethernet bridges controlled by a Network Management System (NMS) 36. The NMS monitors the state in the bridges and issues rules that adapt the behavior of certain bridges accordingly. For example, if $Bridge_{11}$ becomes heavily loaded with traffic, the NMS may issue a rule that will move some traffic from associated bridges (i.e.,

$Bridge_{21}$ – $Bridge_{23}$) to $Bridge_{12}$. For example, the rule may move every third frame or frames carrying a particular protocol to $Bridge_{12}$. Context information may also be added to the state vector, thereby allowing context to influence switching. Context information may contain, but is not limited to, information about traffic load in nearby bridges, forecasts or predictions of expected traffic, and the like. This feature is of particular interest in a mobile environment.

The NMS 36 is shown connected to the network by a dotted line because the adaptable bridges may automatically generate specific context rules and distribute them to nearby bridges as users move around in the network. When bridges automatically generate rules to other bridges (and to themselves), a self-managed network can be implemented in which bridges exchange rules dynamically. This capability can be used, for example, to setup a particular flow-path, distribute traffic during heavy load, or automatically redirect traffic in the case of network failures. For example, if Bridge11 receives a flow of high priority frames when it is already heavily loaded with traffic, it can issue a rule or set of rules to Bridge22 that move the flow to Bridge12 instead.

An Ethernet bridge is working in "wire-speed" and therefore it is desirable that the bridge introduce as little delay as possible. Adding a Rule Engine and basing the switching on rules may increase the delay. However, a number of techniques and mechanisms can be used to make the Rule Engine more efficient:

1) Filter functions can be tested in parallel, and a priority module can select the matching rule with highest priority. These computations can be performed because the filter functions are pure predicates, i.e. they contain no side effects.

2) Filter functions will in most cases be a conjunction (or disjunction) of comparisons. These can be directly mapped onto a pipelined matrix of comparison modules in hardware.

3) A similar pipelined hardware matrix realizing the language constructs used in the action functions can be implemented.

4) Some parts of the state vector, for example library functions reflecting bridge context and resources, can be implemented in hardware such as registers, thereby providing "instant" access to them.

In the preferred embodiment, the rule language used to describe the filter

and action functions is not a general purpose programming language. A programming language should only have the necessary constructs and mechanisms needed to express the solutions to the problems in the specified domain. If the language is too powerful, as a general-purpose language, it is possible to express an infinite loop (accidentally or on purpose) thereby increasing the delay to infinity. The preferred switching rule language, therefore, is a language primarily restricted to the domain of Ethernet switching (layer 2), with language constructs expressing the mechanisms used in the switching process. However, language constructs that are useful for other purposes like network management, constructs related to exchange of new rules, and so on, that are not in conflict with the basic requirements may also be included.

The present invention provides several advantages. The Ethernet standards can be implemented as switching rule sets, and as the standards evolve, the rule sets are updated. These updated rule sets can then easily be loaded into an adaptable network bridge. The rule sets can be vendor-independent and, for example, published by IEEE. Today, each vendor decides which protocols (standards) to support in a bridge, and unless the vendor issues an update whenever the standard is updated, users have to buy a new bridge if they need to follow the new standard.

In the present invention, the "programming language" of rules may be standardized thereby enabling anyone to add new functionality, as a switching rule, to any bridge with a Rule Engine. These rules can then be updated or removed if necessary. A proprietary solution can also be implemented as a rule or set of rules and loaded in any bridge with a Rule Engine. If a user later wants to use another solution, the rule set is simply replaced with a new rule set. It will be much less expensive to implement new functionality because, in most cases, the user only has to write some software in the form of a set of rules.

The present invention also greatly increases flexibility in networks because each bridge can be loaded with its own rule set down to the individual port level. The invention also provides the ability to adapt the functionality on each port based on time, user demands, service agreements, and the like. For example, different operators can share the same physical bridge (network) and provide

EX1002
CISCO SYSTEMS, INC. / Page 173 of 1453

different services to their respective users.

Some examples of functionality that can be implemented with switching rules include the following:

1) Broadcast tunnels. It is simple to implement broadcast tunnels necessary for building Public Ethernet Networks.

2) Distributed router functionality added to a set of bridges.

3) Simple firewall functionality.

4) User adapted services on the port level.

5) Authentication and security mechanisms on the port level that are transparent to users.

6) Self-managed networks or semi-self managed networks.

This list is not intended to be exhaustive, and other functions may also be implemented with switching rules and loaded into any adaptable bridge with a Rule Engine.

As shown by the above examples, the state of the dynamically adaptable bridge can be utilized in the switching process to enable entirely new functionality and to provide new ways to use bridges in networks.

Although preferred embodiments of the present invention have been illustrated in the accompanying drawings and described in the foregoing Detailed Description, it is understood that the invention is not limited to the embodiments disclosed, but is capable of numerous rearrangements, modifications, and substitutions without departing from the scope of the invention. The specification contemplates any all modifications that fall within the scope of the invention defined by the following claims.

WHAT IS CLAIMED IS:

1. A dynamically adaptable network bridge comprising:

a Rule Engine that processes data frames according to a set of switching rules, wherein each switching rule identifies a type of frame to which the rule applies, and how the type of frame is to be processed; and

means for dynamically modifying the switching rules.

2. The dynamically adaptable network bridge of claim 1 wherein the means for dynamically modifying the switching rules includes a protocol for dynamically loading and updating the switching rules.

3. The dynamically adaptable network bridge of claim 1, wherein each switching rule includes a filter function for determining whether a given rule is applicable to a given frame.

4. The dynamically adaptable network bridge of claim 3, wherein each switching rule also includes an action function for specifying changes to the given frame's header and how the given frame should be switched.

5. The dynamically adaptable network bridge of claim 1, wherein each switching rule includes a state vector utilized for processing the type of frames to which each rule applies.

6. The dynamically adaptable network bridge of claim 5, wherein the state vector includes an abstraction of a local memory for storing rule-specific data for each switching rule.

7. The dynamically adaptable network bridge of claim 6, wherein specific management rules enable the Rule Engine to access the rule-specific data for each switching rule.

EX1002
CISCO SYSTEMS, INC. / Page 175 of 1453

8. The dynamically adaptable network bridge of claim 6, wherein the state vector also includes an abstraction of a global bridge memory for storing bridge-specific data applicable to and accessible by all the switching rules.

9. The dynamically adaptable network bridge of claim 8, wherein the bridge-specific data includes a port-forwarding table.

10. The dynamically adaptable network bridge of claim 8, wherein the state vector also includes a set of library functions that implement bridge resources.

11. The dynamically adaptable network bridge of claim 10, wherein the set of library functions are selected from a group consisting of:

a function that retrieves a source port of a processed frame;
a function that provides timestamps;
a function that describes traffic flows in the bridge; and
a function that indicates the traffic load in the bridge.

12. The dynamically adaptable network bridge of claim 3, wherein the given frame is processed in accordance with the given rule if the filter function determines that the given rule is applicable to the given frame, and the given frame is dropped if the filter function determines that there is no rule applicable to the given frame.

13. The dynamically adaptable network bridge of claim 1, wherein the bridge includes a plurality of input/output ports, and the Rule Engine includes a plurality of sets of switching rules, wherein each set of switching rules is applicable to a different port in the bridge.

14. The dynamically adaptable network bridge of claim 1, wherein the bridge is an Ethernet bridge.

BNSDOCID: <WO_____2005046145A1_I_>

15. The dynamically adaptable network bridge of claim 1, wherein the means for dynamically modifying the switching rules includes a protocol that dynamically adds, subtracts, and modifies the switching rules.

16. The dynamically adaptable network bridge of claim 1, further comprising means for prioritizing rules within the set of switching rules.

17. The dynamically adaptable network bridge of claim 1, further comprising means for accessing state information for the bridge, wherein a given rule causes a given frame to be processed differently when the state information changes.

18. The dynamically adaptable network bridge of claim 17, wherein the given rule processes the given frame differently, depending on traffic load in the bridge.

19. The dynamically adaptable network bridge of claim 17, further comprising a port for receiving rules from a Network Management System (NMS), wherein the NMS monitors the state information for a plurality of adaptable bridges in a network, and issues rules that adapt the behavior of the bridge to optimize network performance.

20. The dynamically adaptable network bridge of claim 17, wherein the state information includes context information, wherein a given rule causes a given frame to be processed differently when the context information changes.

21. The dynamically adaptable network bridge of claim 1, wherein the bridge is one of a plurality of adaptable bridges in a network, and the bridge further comprises means for generating specific context rules and distributing the context rules to other adaptable bridges in the network.

BNSDOCID: <WO_____2005046145A1_I_>

22. A method of processing and switching data frames in an adaptable network bridge, said method comprising the steps of:

defining a set of switching rules for the adaptable bridge;

receiving a given frame in the bridge;

determining whether any of the rules are applicable to the given frame; and

upon determining that one of the rules is applicable to the given frame, processing and switching the frame according to the applicable rule.

23. The method of claim 22, further comprising dynamically adding, subtracting, and modifying the switching rules.

24. The method of claim 23, further comprising accessing state information for the bridge, wherein the step of dynamically adding, subtracting, and modifying the switching rules is performed in response to a change in the state information.

25. The method of claim 24, wherein the bridge is one of a plurality of adaptable bridges in a network, and the method further comprises the steps of:

receiving a new or modified switching rule from a Network Management System (NMS), wherein the NMS monitors the state information for a plurality of adaptable bridges in a network, and issues rules that adapt the behavior of the bridge to optimize network performance; and

processing and switching frames according to the new or modified switching rule received from the NMS.

26. The method of claim 24, further comprising adding context information to the state information, wherein the step of dynamically adding, subtracting, and modifying the switching rules is performed in response to a change in the context information.

27. The method of claim 22, wherein the bridge is one of a plurality of adaptable bridges in a network, and the method further comprises the steps of:

generating specific context rules; and

distributing the context rules to other adaptable bridges in the network.

28. The method of claim 22, wherein the bridge is an Ethernet bridge.

5

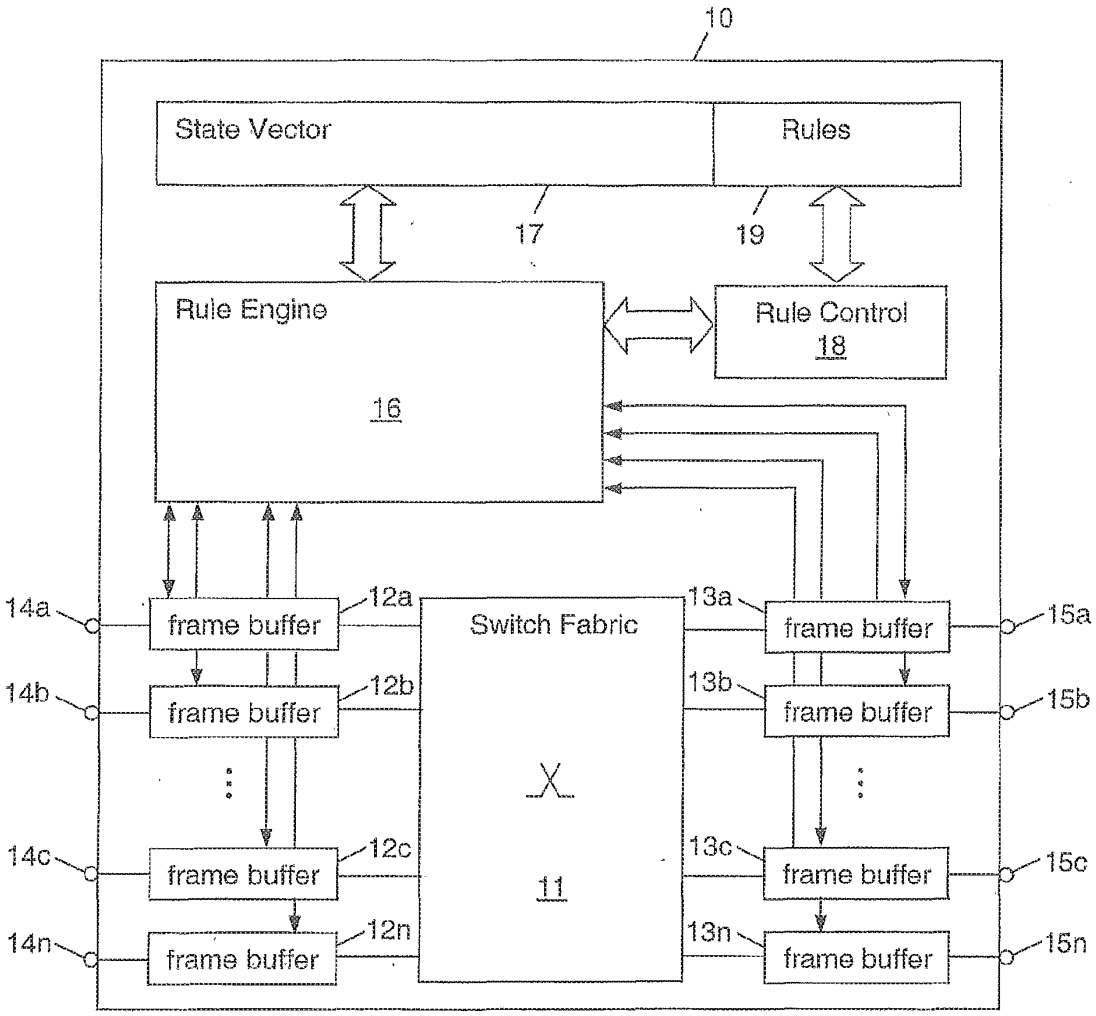


FIG. 1

BNSDOCID: <WO_____2005046145A1_I_>

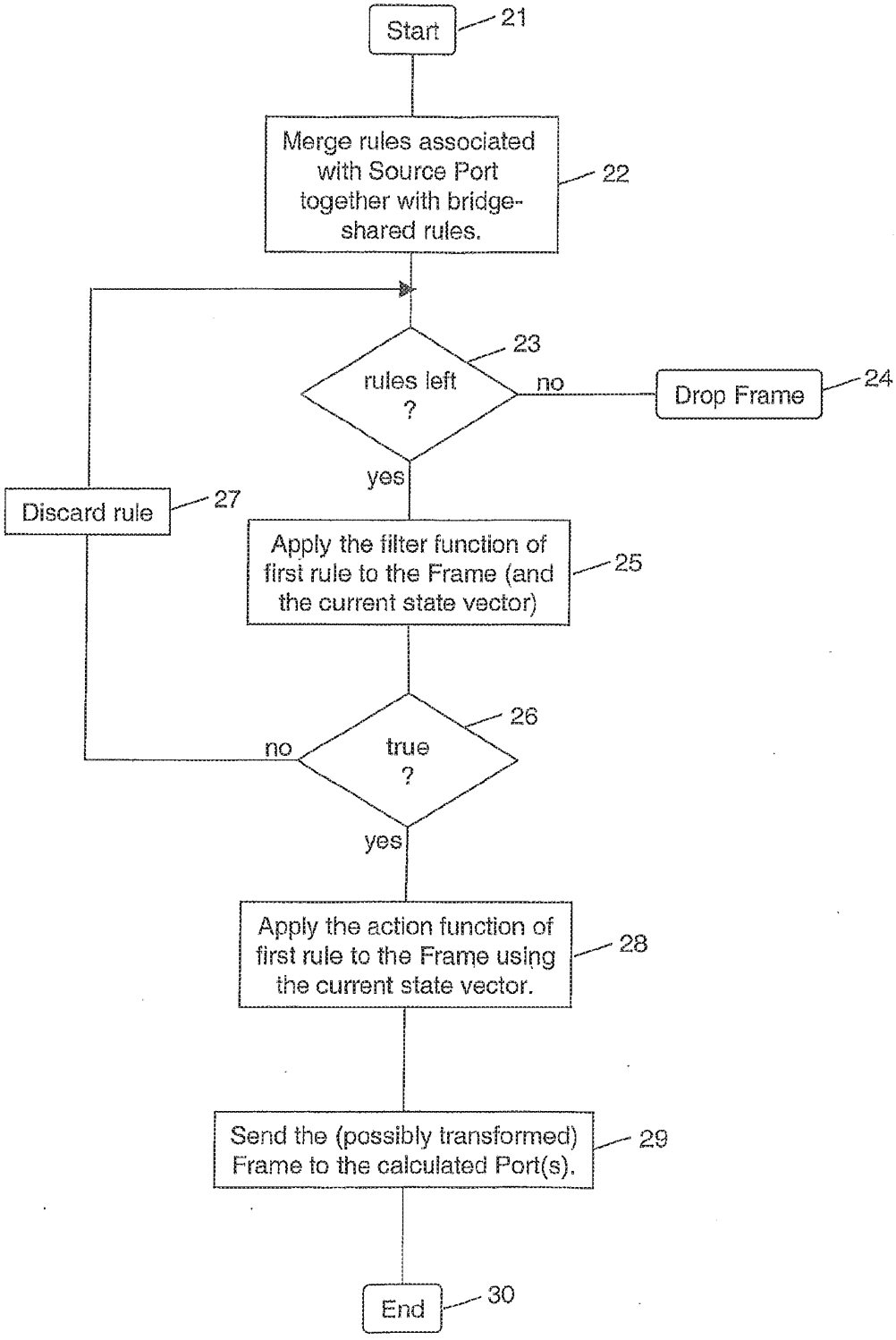


FIG. 2

BNSDOCID: <WO_____2005046145A1_I_>

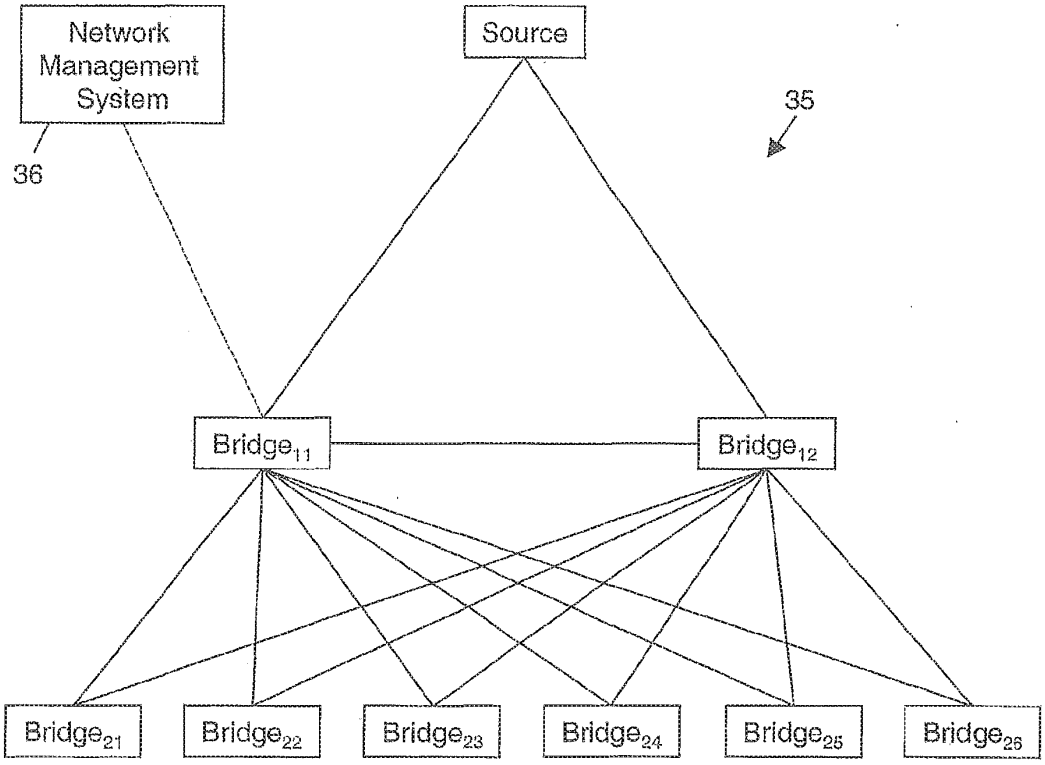


FIG. 3

BNSDOCID: <WO_____2005046145A1_I_>

INTERNATIONAL SEARCH REPORT

International Application No
[redacted]/SE2004/001611

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/56 H04L12/46

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 790 554 A (PITCHER ET AL) 4 August 1998 (1998-08-04) abstract column 1, line 15 - column 1, line 67 column 2, line 39 - column 3, line 25 column 3, line 48 - column 4, line 42 column 4, line 60 - column 8, line 4 column 8, line 24 - column 8, line 26; claims 1,2,14,22,28; figures 2,3 -/--	1-5, 12-20, 22-25, 27,28

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 March 2005	31/03/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Todorut, C

Form PCT/ISA/210 (second sheet) (January 2004)

BNSDOCID: <WO_____2005046145A1_I_>

INTERNATIONAL SEARCH REPORT

International Application No
T/SE2004/001611

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 396 493 A (SUGIYAMA ET AL) 7 March 1995 (1995-03-07) abstract column 1, line 63 - column 3, line 11 column 4, line 11 - column 4, line 51 column 5, line 67 - column 6, line 39; claims 1,17; figures 1-4	1-28
X	WO 00/56024 A (BROADCOM CORPORATION; KADAMBI, SHIRI; AMBE, SHEKHAR; KALKUNTE, MOHAN;) 21 September 2000 (2000-09-21) abstract	1-4,22, 23
A	page 53, line 12 - page 65, line 21; claims 1,2	5-21, 24-28
A	US 2003/123387 A1 (JACKSON ANDREW LLOYD 'GB!) 3 July 2003 (2003-07-03) abstract column 1, paragraph 2 - column 1, paragraph 9 column 2, paragraph 16 - column 3, paragraph 25; claims 1,6,9; figure 4	1-28
A	US 5 959 976 A (KUO ET AL) 28 September 1999 (1999-09-28) abstract column 1, line 5 - column 2, line 40 column 3, line 8 - column 3, line 18 column 5, line 56 - column 6, line 10; claim 1; figures 3-5	1-28
A	EP 0 508 886 A (DIGITAL EQUIPMENT CORPORATION) 14 October 1992 (1992-10-14) abstract column 1, line 40 - column 3, line 54 column 4, line 45 - column 5, line 16 column 5, line 55 - column 6, line 53; claims 1,23; figures 5-8	1-28
A	US 5 515 376 A (MURTHY ET AL) 7 May 1996 (1996-05-07) abstract column 6, line 1 - column 9, line 21	1-28

1

BNSDOCID: <WO_____2005046145A1_I_>

EX1002
CISCO SYSTEMS, INC. / Page 184 of 1453

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
/SE2004/001611

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5790554 A	04-08-1998	NONE	
US 5396493 A	07-03-1995	JP 6224918 A	12-08-1994
		KR 9614983 B1	23-10-1996
WO 0056024 A	21-09-2000	US 2001043611 A1	22-11-2001
		AU 3529500 A	04-10-2000
		AU 3752000 A	04-10-2000
		AU 4325800 A	04-10-2000
		EP 1161817 A2	12-12-2001
		EP 1169809 A2	09-01-2002
		EP 1159805 A2	05-12-2001
		WO 0056024 A2	21-09-2000
		WO 0056011 A2	21-09-2000
		WO 0056013 A2	21-09-2000
		US 6707817 B1	16-03-2004
		US 6810037 B1	26-10-2004
		US 6850521 B1	01-02-2005
		US 6707818 B1	16-03-2004
		US 2004174898 A1	09-09-2004
		US 2005047411 A1	03-03-2005
		US 2002039365 A1	04-04-2002
		AU 5442700 A	12-12-2000
		AU 5586400 A	12-12-2000
		AU 5737300 A	31-01-2001
		AU 6334400 A	22-01-2001
		EP 1181791 A1	27-02-2002
		EP 1181792 A1	27-02-2002
		EP 1212867 A2	12-06-2002
		EP 1192767 A2	03-04-2002
		WO 0072533 A1	30-11-2000
		WO 0102965 A2	11-01-2001
		WO 0072531 A1	30-11-2000
		WO 0101724 A2	04-01-2001
		US 2002093974 A1	18-07-2002
		US 2002186705 A1	12-12-2002
		US 6813268 B1	02-11-2004
		US 6735679 B1	11-05-2004
		US 6792500 B1	14-09-2004
		US 6842457 B1	11-01-2005
		US 6430188 B1	06-08-2002
		US 6859454 B1	22-02-2005
		US 2004170176 A1	02-09-2004
		US 2005036488 A1	17-02-2005
		US 2002031090 A1	14-03-2002
US 2003123387 A1	03-07-2003	NONE	
US 5959976 A	28-09-1999	NONE	
EP 0508886 A	14-10-1992	DE 69217103 D1	13-03-1997
		DE 69217103 T2	21-08-1997
		EP 0508886 A1	14-10-1992
		JP 5114905 A	07-05-1993
		US 5515513 A	07-05-1996
US 5515376 A	07-05-1996	EP 0710415 A1	08-05-1996
		JP 3335358 B2	15-10-2002

BNSDOCID: <WO_____2005046145A1_I_>

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
/SE2004/001611

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5515376 A		JP 9500774 T	21-01-1997
		WO 9503659 A1	02-02-1995
		US 5610905 A	11-03-1997
		US 6545982 B1	08-04-2003

BNSDOCID: <WO_____2005046146A1_I_>

US 20110055916A1

(19) United States

(12) Patent Application Publication

(10) Pub. No.: US 2011/0055916 A1

(43) Pub. Date: Mar. 3, 2011

Ahn

(54) METHODS, SYSTEMS, AND COMPUTER READABLE MEDIA FOR ADAPTIVE PACKET FILTERING

(76) Inventor: David K. Ahn, Winston-Salem, NC (US)

(21) Appl. No.: 12/871,806

(22) Filed: Aug. 30, 2010

Related U.S. Application Data

(60) Provisional application No. 61/237,974, filed on Aug. 28, 2009.

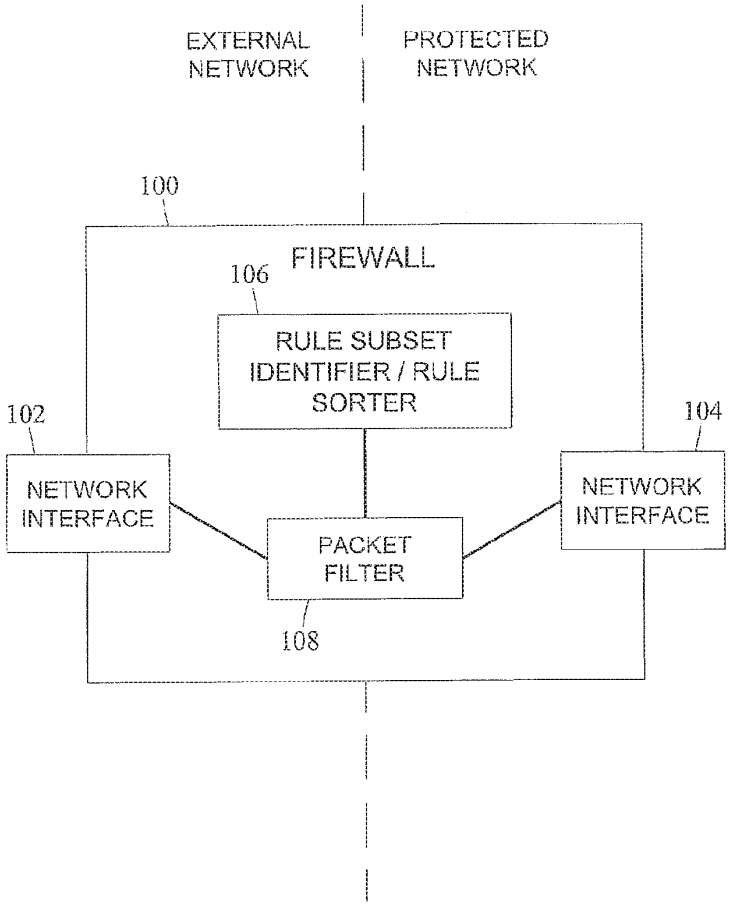
Publication Classification

(51) Int. Cl.
G06F 17/00 (2006.01)

(52) U.S. Cl. 726/13

(57) ABSTRACT

The subject matter described herein includes methods, systems, and computer readable media for adaptive packet filtering. One method includes identifying at least one subset of rules and an ordered set of firewall packet filtering rules that defines a firewall policy such that the subset contains disjoint rules. Disjoint rules are defined as rules whose order can be changed without changing integrity of the firewall policy. Rules in the subset are sorted to statistically decrease the number of comparisons that will be applied to each packet that a firewall encounters. Packets are filtered at the firewall using the sorted rules in the subset by comparing each packet to each of the sorted rules in the subset until the packet is allowed or denied and ceasing the comparing for the packet in response to the packet being allowed or denied and thereby achieving sub-linear searching for packets filtered using the sorted rules in the subset.



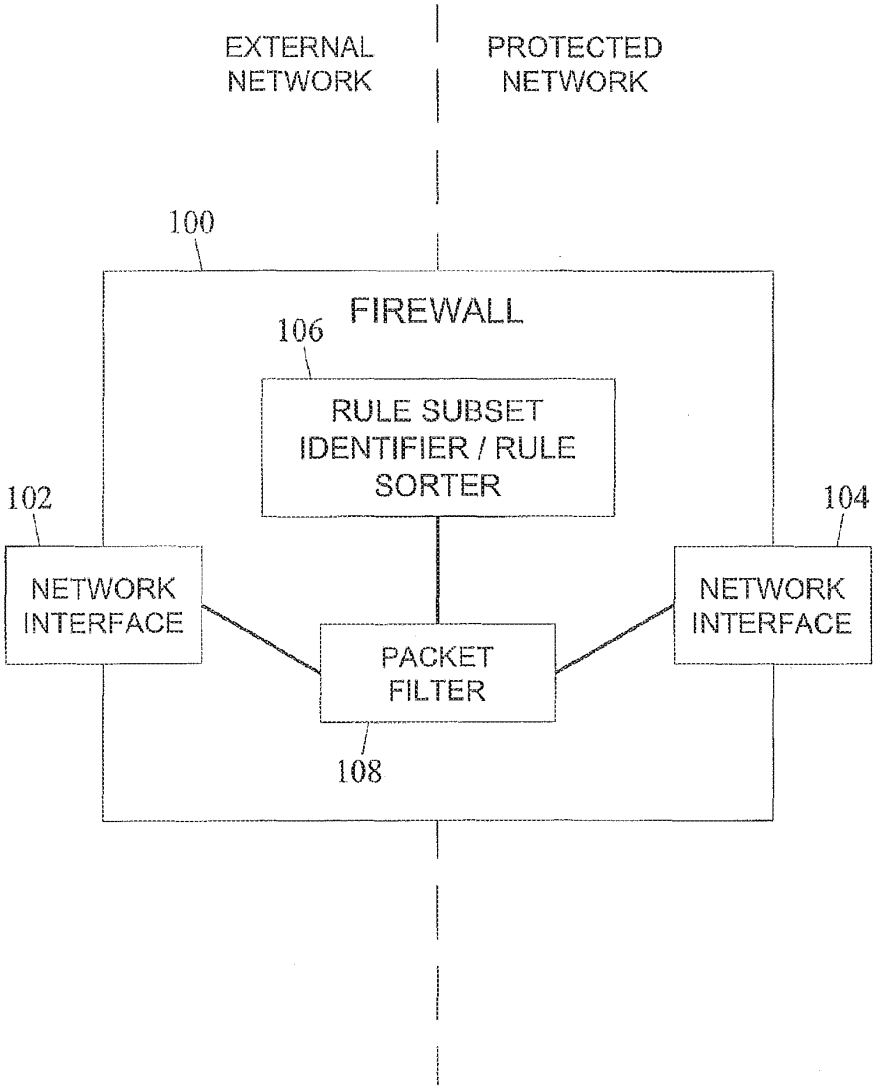


FIG. 1

BNSDOCID: <US____20110055916A1_I_>

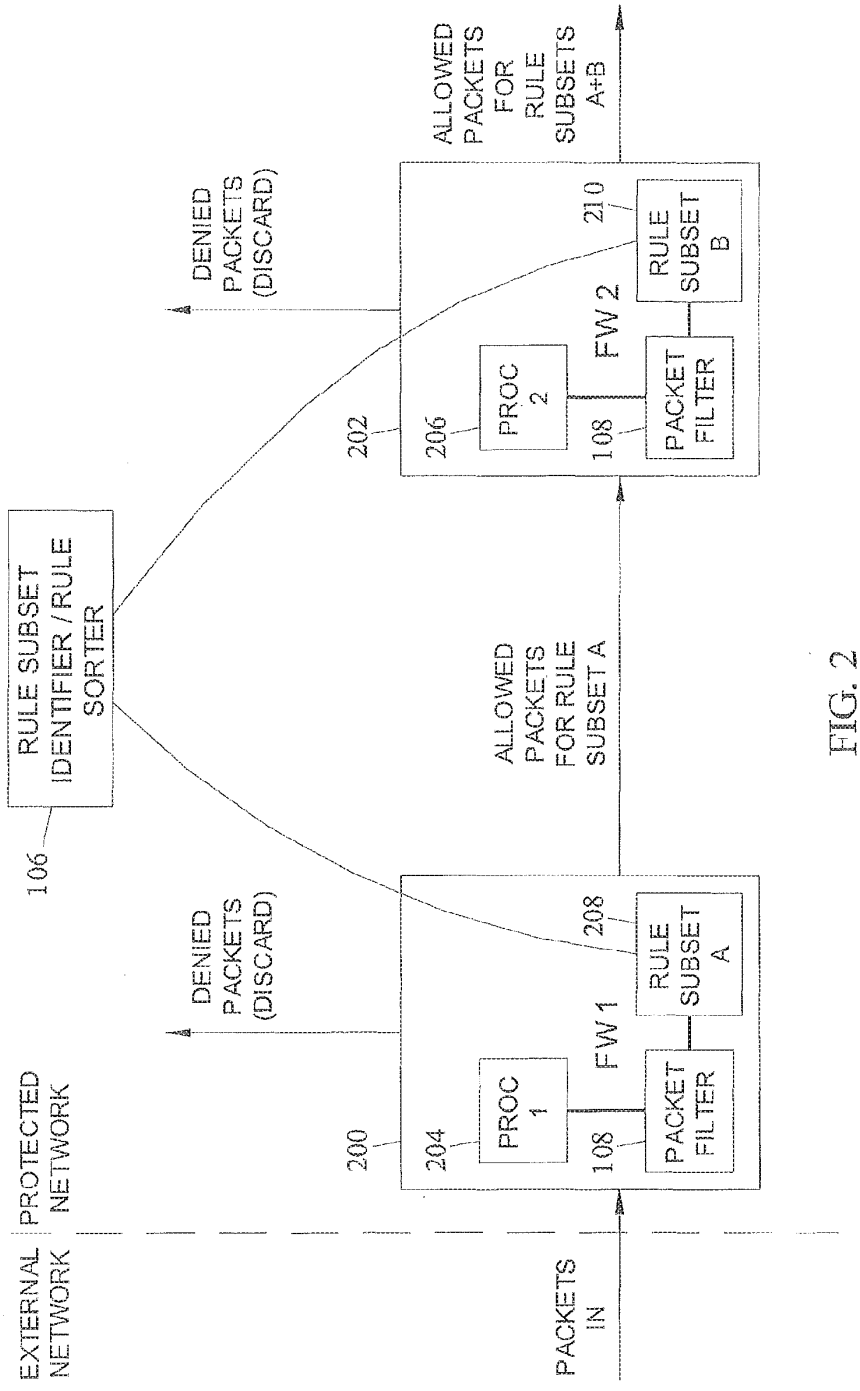


FIG. 2

BNSDOCID: <US____20110055916A1_I_>

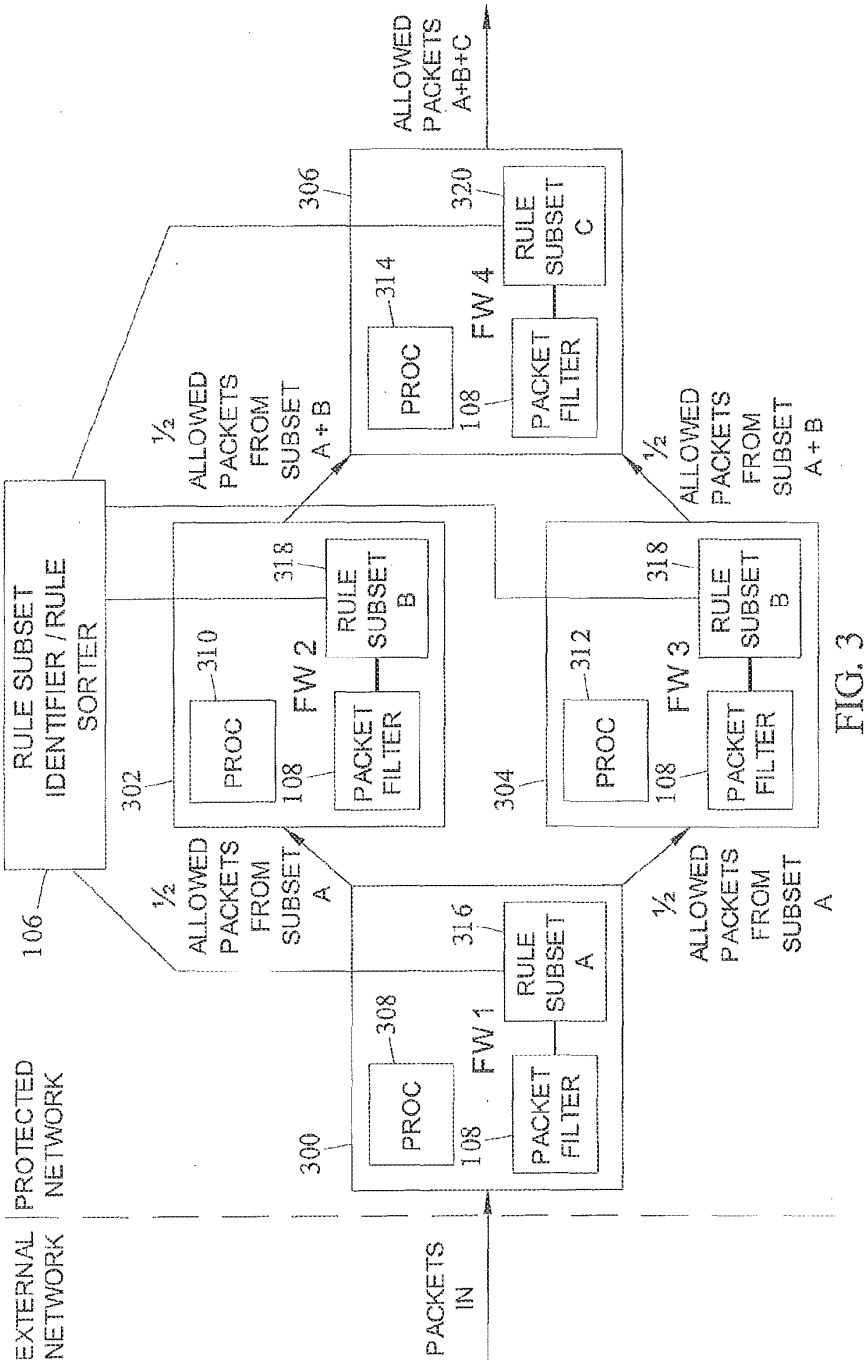


FIG. 3

BNSDOCID: <US____20110055916A1_|_>

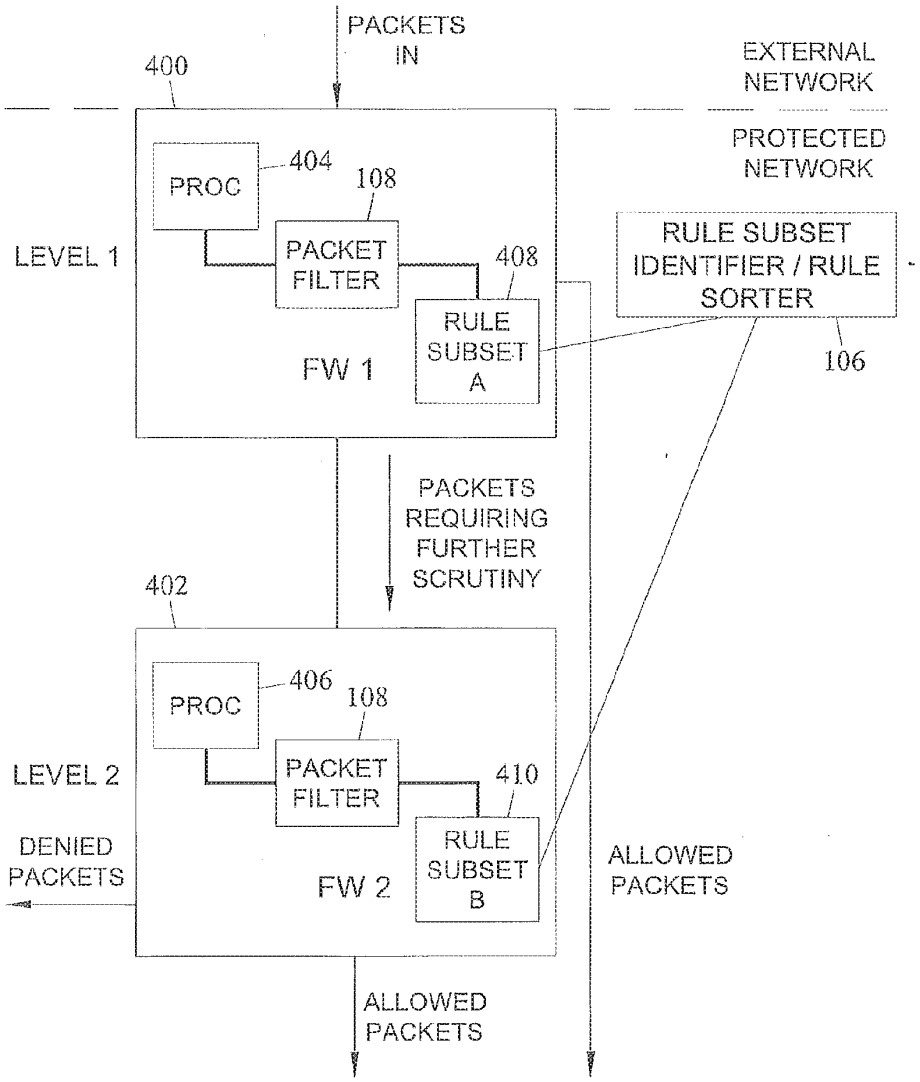


FIG. 4

BNSDOCID: <US____20110055916A1_I_>

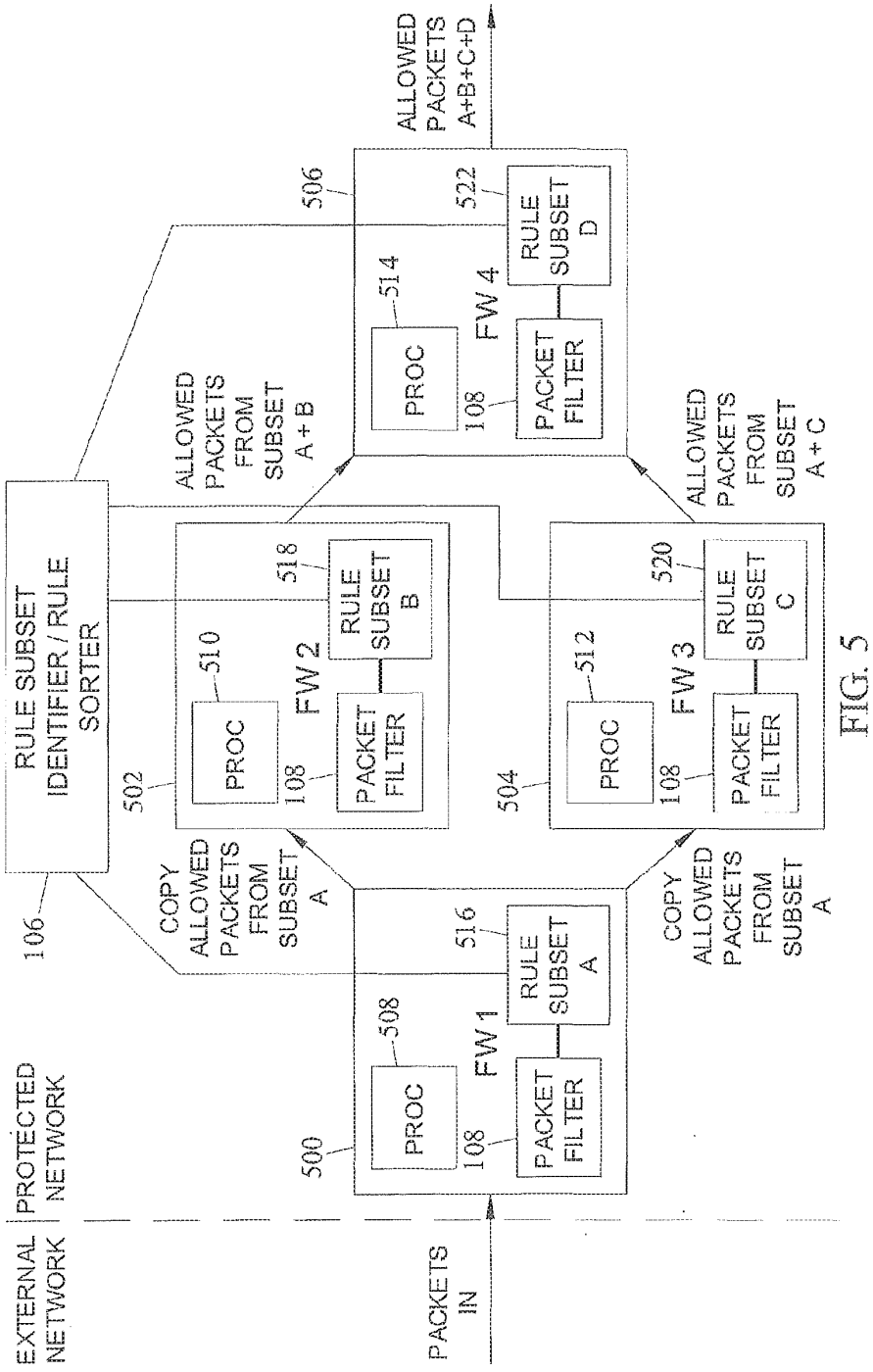


FIG. 5

BNSDOCID: <US____20110055916A1_I_>

METHODS, SYSTEMS, AND COMPUTER READABLE MEDIA FOR ADAPTIVE PACKET FILTERING

PRIORITY CLAIM

[0001] This application claims the benefit of U.S. Provisional Patent Application Ser. No. 61/237,974, filed Aug. 28, 2009; the disclosure of which is incorporated herein by reference in its entirety.

TECHNICAL FIELD

[0002] The subject matter described herein relates to network firewall filtering. More particularly, the subject matter described herein relates to methods, systems, and computer readable media for adaptive packet filtering.

BACKGROUND

[0003] A firewall generally processes a packet against a list of ordered rules to find the first rule match. The list of ordered rules represents an aggregate security policy, and arbitrarily changing the order of the rules can result in a violation of the aggregate security policy. The Wake Forest University (WFU) techniques described in U.S. patent application publication nos. 2006/0248580 and 2006/0195896 provide the methods to optimally reorder the list while preserving the aggregate security policy, thereby improving the performance of the firewall. The WFU techniques also include methods to break apart rules into functionally independent lists containing (groups of) dependent rules such that a function parallel firewall can simultaneously process one packet against multiple lists, which can substantially improve the performance of the firewall. However, these improvements provided by WFU techniques can be dwarfed by the performance degradation as the number of rules in the list becomes very large.

[0004] A key reason for the lack of scalability of most firewall implementations is due to the common use of linear search algorithms for comparing packets against a list of rules. In the worst case, a packet is matched at the last N^{th} rule in the list, so it must also be compared against all N−1 prior rules for a total of N comparisons. This poses a computational resource problem when the size of N is very large on a single processing node (including when such nodes are arranged in a data-, function-, hierarchical- or hybrid-parallel system), where the time required for processing each packet can quickly increase latency and reduce throughput to unacceptable levels. In fact, the WFU techniques provide good results in part because the reordering of, or the reduction in size of, rules on each processing node allows for a larger percentage of the total rules to reside in each processor's cache(s), which then substantially increases their performance relative to when only a small portion of those rules are cached.

[0005] The problem of searching firewall rule sets is well understood and highly researched, and there are some published techniques for sub-linear (substantially faster than linear) techniques applicable to firewall rules. However, these sub-linear techniques generally involve changing the underlying representation of rules. Examples of such an approach might be to use a graph, tric- or tree-like structure instead of a list to represent a set of rules, which would allow a match to be determined using tree search algorithms by traversing down the graph, trie or tree (see E. Fulp, Trie-Based Policy Representations for Network Firewalls, Proceedings of the IEEE International Symposium on Computer Communications, 2005 and Al-Shaer et al., Modeling and Management of Firewall Policies, IEEE Transactions on Network and Service Management, 2004). These approaches have potential but can add complexity or limitations that may reduce their practical usefulness in a commercial high performance firewall product.

SUMMARY

[0006] Adaptive packet filtering (APF), a set of techniques for processing firewall rules and packets, is described herein. APF offers improved processing performance compared to the WFU techniques in most cases, and can be combined with the WFU techniques or other parallel, pipelining and optimization techniques to achieve even greater performance.

[0007] The subject matter described herein includes methods, systems, and computer readable media for adaptive packet filtering. One method includes identifying at least one subset of rules in an ordered set of firewall packet filtering rules that defines a firewall policy such that the subset contains disjoint rules. Disjoint rules are defined as rules whose order can be changed without changing the integrity of the firewall policy. Rules in the subset are sorted to statistically decrease the number of comparisons that will be applied to each packet that a firewall encounters. Packets are filtered at the firewall using the sorted rules in the subset by using binary search, interpolated search, informed search, or hash lookup search algorithms to compare each packet to the sorted rules in the subset until the packet is allowed or denied and ceasing the comparing for the packet in response to the packet being allowed or denied and thereby achieving sub-linear searching for packets filtered using the sorted rules in the subset.

[0008] The subject matter described herein for adaptive packet filtering can be implemented in a non-transitory computer readable medium having stored thereon executable instructions that when executed by the processor of a computer control the computer to perform steps. Exemplary computer readable media suitable for implementing the subject matter described herein include chip memory devices, disk memory devices, programmable logic devices and application specific integrated circuits. In addition, a computer readable medium that implements a subject matter described herein may be located on a single device or computing platform or may be distributed across multiple devices or computing platforms.

[0009] Further, the subject matter described herein for adaptive packet filtering can be implemented on a particular machine, such as a network firewall including one or more network interfaces for receiving packets and packet filtering hardware and software for optimizing rules as described herein and for filtering packets using the optimized arrangement of rules.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] Preferred embodiments of the subject matter described herein will now be described with reference to the accompanying drawings of which:

[0011] FIG. 1 is a block diagram of a system for adaptive packet filtering according to an embodiment of the subject matter described herein;

[0012] FIG. **2** is a block diagram of application of the present subject matter to a pipelined processing approach according to an embodiment of the subject matter described herein;

[0013] FIG. **3** is a block diagram illustrating application of the present subject matter to a combination of pipelined and data parallel processing approaches according to an embodiment of the subject matter described herein; and

[0014] FIG. **4** is a block diagram illustrating application of the present subject matter to a short-circuiting pipelined processing approach according to an embodiment of the subject matter described herein; and

[0015] FIG. **5** is a block diagram illustrating application of the present subject matter to a combination of pipelined and function parallel processing approaches according to an embodiment of the subject matter described herein.

DETAILED DESCRIPTION

[0016] Methods, systems, and computer readable media for adaptive packet filtering are disclosed. FIG. **1** is a block diagram illustrating an exemplary system for adaptive packet filtering according to an embodiment of the subject matter described herein. Referring to FIG. **1**, a firewall **100** may function at the boundary between an external network and a protected network. Firewall **100** may include one or more network interfaces **102** for receiving packets from the external network. Firewall **100** may also include one or more network interfaces **104** for transmitting allowed packets to the protective network. In one implementation, firewall **100** may filter Internet protocol (IP) packets based on a combination of source and destination addresses in the IP headers of the packets. However, the subject matter described herein is not limited to filtering any particular protocol. Any packet network protocol with parameters for which firewall filtering rules can be defined is intended to be within the scope of the subject matter described herein.

[0017] As used herein, the term "firewall" includes any network security device or system of devices that inspects network traffic data that originates, terminates, or traverses the device system in any capacity and compares that traffic data (headers, payload, raw bits, etc.) to a set of one or more rules, signatures, or conditions, either inline (i.e., in real time) or offline (i.e., capture and replay of the traffic data). The term "firewall" is also intended to include an intrusion detection device that analyzes network traffic in real time or historically to detect the presence of intrusion events in a network. The term "firewall" is also intended to include a deep packet inspection device that analyzes network traffic in real time or historically to detect the presence of certain packet content in a network.

[0018] Firewall **100** includes a firewall rule subset identifier/rule sorter **106** for identifying at least one subset of rules in an ordered set of firewall packet filtering rules that defines a firewall policy such that the subset contains disjoint rules, where disjoint rules are defined as rules whose order can be changed without changing the firewall policy. Firewall rule subset identifier/rule sorter **106** may sort the rules in the subset or subsets to statistically decrease the number of comparison that will be applied to each packet that the firewall encounters. Exemplary methods for grouping and sorting rules will be described below.

[0019] Although in the example illustrated in FIG. **1** rule subset identifier/rule sorter **106** is illustrated as a component of firewall **100**, the subject matter described herein is not limited to such an implementation. Rule subset identifier/rule sorter **106** can be implemented on any computing platform capable of sorting firewall rules using the methods described herein, and the sorted rule set can be provided to firewall **100** through any suitable means, such as communication over a network. In one implementation, rule subset identifier/rule sorter **106** may be implemented on a management platform separate from firewall **100**.

[0020] Firewall **100** further includes a packet filter **108** for filtering packets at the firewall using the rules in the subset by using binary search, interpolated search, informed search, hash lookup search algorithms, or other sub-linear algorithms to compare each packet to each of the sorted rules in the subset until the packet is allowed or denied and ceasing the comparing for the packet in response to the packet being allowed or denied and thereby achieving sub-linear searching for the packets filtered using the sorted rules in the subset.

[0021] Once the subsets of disjoint rules have been identified by rule subset identifier/rule sorter **106**, the rule subsets can be distributed across plural firewall processors in order to improve packet filtering efficiency. FIG. **2** is a block diagram illustrating an exemplary pipelined approach where rules and different subsets are distributed across plural firewall processors for processing packets in a pipelined manner. Referring to FIG. **2**, firewalls **200** and **202** each include separate processors **204** and **206** for executing packet filters **108**. In this example, rule subset identifier/rule sorter **106** identifies two rule subsets, subset A **208** and subset B **210**. The rules within each subset **208** and **210** are disjoint and sorted to statistically decrease the number of comparisons that will be applied to each packet using the methods described herein. However, the rules in subset B **210** are dependent on the rules in rule subset A **208**. Accordingly, rule subset identifier/rule sorter **106** distributes the rule across firewall processors **204** such that the rules in rule subset A **208** are applied before the rules in rule subset B **210**. Because the rules in different subsets are distributed across plural processors in a pipeline manner, packet filtering efficiency is improved over a single-processor approach because the different processors can simultaneously apply rules to different packets. In the example illustrated in FIG. **2**, packets that pass the filtering of rule subset A **208** are processed by processor **206**, which applies rule subset B **210**, at the same time that processor **204** applies rule subset A to new incoming packets.

[0022] In yet another embodiment, rule subset identifier/rule sorter **106** may distribute the grouped, sorted rules across firewall processors such that a combination of pipelined and data parallel processing techniques are used. FIG. **3** illustrates an example where firewalls **300**, **302**, **304**, and **306** each include separate processors **308**, **310**, **312**, and **314** for applying their respective packet filters. In the illustrated example, rule subset identifier/rule sorter **106** distributes rule subset A **316** to firewall **300**, rule subset B **318** to firewalls **302** and **304**, and rule subset C **320** to firewall **306**. The rules within each subset A, B and C are disjoint. The rules in subset B are dependent upon the rules in subset A. The rules in subset C are dependent upon the rules in subsets A and B.

[0023] In operation, packets entering firewall **300** are filtered using rule subset A **316**. The packets that are allowed by rule subset A **316** are divided between firewalls **302** and **304** such that the application of the rules in rule subset B **318** to different packets is performed in parallel. This is referred to as a data parallel approach. The packets that pass the filtering by rule subset B **318** are passed to firewall **306** for application of

EX1002
CISCO SYSTEMS, INC. / Page 195 of 1453

the rules in rule subset C **320**. Accordingly, FIG. **3** illustrates an example where the rule subsets that are identified and sorted by rule subset identifier/rule sorter **106** are distributed across the firewall processors for a combination of pipelined and data parallel processing.

[0024] In yet another embodiment, the rules subsets that are identified and in which the rules are sorted using rule subset identifier/rule sorter **106** may be distributed across firewall processors in a short-circuiting pipelined manner. FIG. **4** is an example of short-circuiting pipelined filtering using rule subsets that are identified and sorted by rule subset identifier/rule sorter **106**. Referring to FIG. **4**, a first firewall **400** and a second firewall **402**, respectively including processors **404** and **406**, filter packets using packet filters **108**. In the illustrated example, packet filter **108** uses rule subset A **408** and packet filter **108** uses rule subset B **410**. Rule subsets A and B **408** and **410** may respectively implement different levels of a firewall hierarchy such that packets that pass the filtering by rule subset A **408** are allowed into the protected network. Packets that are identified by rule subset A **408** is requiring further filtering are distributed to rule subset B **410** for that filtering. Thus, rule subset identifier/rule sorter **106** can also be used with short-circuiting pipelined firewall techniques without departing from the scope of the subject matter described herein.

[0025] In yet another embodiment, rule subset identifier/rule sorter **106** may distribute the grouped, sorted rules across firewall processors such that a combination of pipelined and function parallel processing techniques are used. FIG. **5** illustrates an example where firewalls **500**, **502**, **504**, and **506** each include separate processors **508**, **510**, **512**, and **514** for applying their respective packet filters. In the illustrated example, rule subset identifier/rule sorter **106** distributes rule subset A **516** to firewall **500**, rule subset B **518** to firewalls **502**, and rule subset C **520** to firewall **504**, and rule subset D **522** to firewall **506**. The rules within each subset A, B, C and D are disjoint. The rules in subset B and C are dependent upon the rules in subset A. The rules in subset D are dependent upon the rules in subsets A, B and C.

[0026] In operation, packets entering firewall **500** are filtered using rule subset A **516**. The packets that are allowed by rule subset A **516** are copied to both firewalls **502** and **504** such that the application of the rules in rule subsets B **518** and C **520** to the packets is performed in parallel. This is referred to as a function parallel approach. The packets that pass the filtering by rule subsets B **518** and C **520** are passed to firewall **506** for application of the rules in rule subset D **522**. Accordingly, FIG. **5** illustrates an example where the rule subsets that are identified and sorted by rule subset identifier/rule sorter **106** are distributed across the firewall processors for a combination of pipelined and function parallel processing.

TECHNIQUE

[0027] APF analyzes and orders the list of firewall rules in-place to contain functionally dependent groups, where each group contains a subset of rules that are disjoint, dependent or both, without substantially changing the underlying representation of rules and while preserving the aggregate security policy. APF then uses varying criteria to sort each group containing disjoint rules, then uses sub-linear search algorithms when comparing packets against the rules within that group. APF uses linear search algorithms when comparing packets within a group containing dependent rules or when otherwise appropriate. A detailed computational complexity analysis of APF would need to be completed. However, on average, it is hypothesized that only O(log(N)) comparisons would be needed to process a rule list of size N. In the theoretical best case when all rules are disjoint, this translates to about 20 comparisons (instead of 1,000,000) for a list of N=1,000,000 rules and about 30 comparisons for a list of N=1,000,000,000 rules. In the worst case when all rules are dependent, APF performs the same as linear search firewall cores. In practice, APF should process a packet against a very large list of rules (N=millions) in the same amount of time that other techniques can process against a very small list (N=hundreds, or thousands). APF does not inherently use parallel techniques; therefore, it can be combined with WFU techniques or other parallel/pipelining techniques to increase performance.

[0028] The following table shows preliminary results comparing a single linear search firewall) with a single APF core as the number of rules is increased.

	linear firewall core		APF core	
N = # rules in the core	PPS = packets per second at max throughput with 0 loss	Latency in microseconds at max throughput with 0 loss	PPS = packets per second at max throughput with 0 loss	Latency in microseconds at max throughput with 0 loss
1	844,595	12.3	811,688	12.3
10	730,994	11.9	766,871	12.3
100	314,861	13.9	718,391	12.0
1,000	29,357	44.6	683,060	12.0
10,000	930	1,112.4	464,684	12.0
100,000	Fail	Fail	292,740	17.4
1,000,000			252,525	14.3
10,000,000			132,556	18.6

DETAILED TECHNIQUE

[0029] This section describes an exemplary algorithm for implementing the subject matter described herein.

[0030] A firewall rule is defined as an n-tuple criteria and an associated action for matching packets. For example, a 5-tuple rule that matches Internet Protocol version 4 (IPv4) packets might consist of 5 IPv4 header fields (source address, source port, destination address, destination port and protocol) and an action (allow, deny), and might specify the rule R1 as:

EX1002
CISCO SYSTEMS, INC. / Page 196 of 1453

Rule	Source Addr	Source Port	Dest Addr	Dest Port	Protocol	Action
R1	192.168.1.1	12345	10.1.1.1	80	TCP	DENY

[0031] A firewall rule set is defined as an ordered list of n rules R1, R2, R3, . . . , Rn where the i in Ri is the index of the rule in the list. Packets that traverse the firewall are checked against each rule in the rule set until the first matching rule is found and its associated action is applied. An example rule set is S1 which contains:

Rule	Source Addr	Source Port	Dest Addr	Dest Port	Protocol	Action
R1	192.168.1.1	12345	10.1.1.1	80	TCP	DENY
R2	192.168.2.2	ANY	10.2.2.2	25	TCP	ALLOW
R3	192.168.3.3	ANY	10.3.3.3	53	UDP	ALLOW
R4	ANY	ANY	10.1.1.1	ANY	ANY	ALLOW
R5	ANY	ANY	ANY	ANY	ANY	DENY

An example TCP packet from source 192.168.4.4 port 54321 to destination 10.1.1.1 port 80 would be checked against but not match R1, R2 and R3; would be checked against and match R4 and be allowed; and, would not be checked against R5 because R4 was the first matching rule.

[0032] A firewall security policy is defined as the set of all possible packets that can traverse the firewall along with their specified outcomes as defined by the rule set. Changing the rules in a rule set usually results in a change of its security policy.

[0033] Within a rule set, a firewall rule is dependent on another rule if swapping the order of the two rules results in a change in the security policy of the rule set. Otherwise, the two rules are disjoint if swapping the order does not result in a change the security policy. For example, in rule set S1 above, rules R1 and R4 are dependent because placing R4 ahead of R1 would render R1 ineffective, thereby changing the security policy. Rules R1 and R2 are disjoint because placing R2 ahead of R1 does not change the security policy.

[0034] A permutation of a rule set is defined as a new rule set which contains the same rules as the original rule set, but which lists a different ordering of the rules from the original rule set without changing the original security policy. For example, in the rule set S1 above, swapping the order of the disjoint rules R1 and R2 would result in a permutation rule set S1':

Rule	Source Addr	Source Port	Dest Addr	Dest Port	Protocol	Action
R2	192.168.2.2	ANY	10.2.2.2	25	TCP	ALLOW
R1	192.168.1.1	12345	10.1.1.1	80	TCP	DENY
R3	192.168.3.3	ANY	10.3.3.3	53	UDP	ALLOW
R4	ANY	ANY	10.1.1.1	ANY	ANY	ALLOW
R5	ANY	ANY	ANY	ANY	ANY	DENY

[0035] Two rules are spatially disjoint if they are disjoint and their corresponding tuples are either identical or do not overlap. For example, in the rule set S1 above, rules R1 and R2 are disjoint but not spatially disjoint because the source ports 12345 and ANY overlap. However, rules R2 and R3 are both disjoint and spatially disjoint because the source ports ANY and ANY are identical, and the other 4 tuples do not overlap. (Other examples follow.)

[0036] A transform function is an algorithm that can be applied to a rule to create a sortable key for that rule, which can then be used to sort the rules by their keys using a key comparison function. For example, the transform function Tfn could concatenate the tuples of a rule into a bit array that is interpreted as a large integer, and a corresponding comparison function Cfn could be a simple integer comparison function. (Other examples follow.)

[0037] A rule subset is defined as an ordered grouping of one or more rules within a rule set. For example, in rule set S1 above, the rule subsets might be:

Subset	Rules
T1	R1, R2, R3
T2	R4
T3	R5

[0038] A rule group is defined as a rule subset with a group type (dependent, disjoint), transform function, comparison function, and a search algorithm hint (linear, sub-linear). The group type can be dependent if the group contains dependent rules, or can be disjoint if the group strictly contains disjoint rules. For example, the rule set S1 above might contain the following disjoint rule group:

Group	Group Type	Rules	Transform Fn	Comparison Fn	Hint
G1	Disjoint	R1, R2, R3	Tfn	Cfn	Sub-linear

[0039] A rule set may be partitioned into a list of ordered rule groups such that the security policy of the rule set is not changed when each rule group is decomposed in the listed order. This partitioning is accomplished by applying a rule subset identification method to a given rule set. An example of such a method is:

[0040] 1. For a given rule set S containing n rules R1, R2, . . . , Rn:

[0041] a. Create a new empty disjoint rule group Gj (initially G1) in S.

[0042] b. Place the first ungrouped rule Ri (initially R1) into Gj.

[0043] c. For each remaining ungrouped rule Ri in S:

[0044] i. If Ri is disjoint from rules in Gj and placing Ri into Gj does not modify the security policy of S, then place Ri into Gj.

[0045] ii. Otherwise, leave Ri ungrouped.

[0046] d. If S contains ungrouped rules, then go to step 1.a.

[0047] 2. The rule set S now contains m disjoint rule groups G1, G2, G3, . . . , Gm which group together the n (possibly reordered) rules R1, R2, . . . , Rn.

Applying the above method to rule set S1 might result in its partitioning into the following list of disjoint ordered rule groups:

BNSDOCID: <US____20110055916A1_I_>

Group	Group Type	Rules	Transform Fn	Comparison Fn	Hint
G1	Disjoint	R1, R2, R3			Linear
G2	Disjoint	R4			Linear
G3	Disjoint	R5			Linear

Decomposing the disjoint rule groups would result in G1, G2, G3={R1, R2, R3}, {R4}, {R5}=R1, R2, R3, R4, R5=S1.

[0048] A partitioned rule set containing disjoint rule groups may then be sorted by applying a transform function to each rule within each disjoint group to derive a sortable key for each rule. Then, the rules may be reordered within their disjoint groups using their sortable keys. The resulting sorted groups may be searched using sub-linear searching algorithms. An example of the sorting method is:

[0049] 1. For each disjoint group Gj in rule set S:

[0050] a. For each rule Ri in Gj:

[0051] i. Apply Transform Tfn to Ri to derive a sortable key Ki.

[0052] b. Sort the rules in Gj using the comparison function Cfn on the sortable keys K.

[0053] 3. The rule set S now contains m sorted disjoint rule groups G1, G2, G3, . . . , Gm.

Applying the above method to the partitioned rule set S1 might result in a new permutation rule set S1' that contains the following list of sorted rule groups where the ordering of rules within G1 might change from R1, R2, R3 to R3, R1, R2:

Group	Group Type	Rules	Transform Fn	Comparison Fn	Hint
G1	Disjoint	R3, R1, R2	Tfn	Cfn	Sub-linear
G2	Disjoint	R4	Tfn	Cfn	Sub-linear
G3	Disjoint	R5	Tfn	Cfn	Sub-linear

[0054] The permutated rule set containing disjoint rule groups may be consolidated to reduce the number of groups that contain a rule count at or below a certain threshold, such as 1 rule, by merging two or more consecutive disjoint groups into a larger dependent group that may be searched using linear searching algorithms. An example of the consolidation method is:

[0055] 1. For each group Gj in rule set S:

[0056] a. If the sum of the number of rules in Gj and its subsequent group Gj+1 is less than or equal to a specified threshold (e.g. 1), then the two groups are merged, their rules are concatenated, and the group type is set to dependent.

[0057] 2. The rule set S now contains m or fewer rule groups of both dependent and disjoint types.

Applying the above method to the permuted rule set S1' might merge the disjoint group G3 into G2:

Group	Group Type	Rules	Transform Fn	Comparison Fn	Hint
G1	Disjoint	R3, R1, R2	Tfn	Cfn	Sub-linear
G2	Dependent	R4, R5	(none)	(none)	Linear

[0058] The APF packet filtering method matches packets against a given rule set by sequentially iterating over each of the ordered rule groups, then performing the specified sub-linear or linear search within each group. An example of a rule filtering method is:

[0059] 1. For each packet that traverses the firewall:

[0060] b. For each group Gj in rule set S:

[0061] i. If Gj is a dependent group, then perform linear search within that group until there is a first rule match.

[0062] ii. If Gj is a disjoint group:

[0063] 1. Apply transform T to the packet to derive a lookup key K.

[0064] 2. Use the comparison function C and sub-linear search within the group until there is a first rule match on key K.

[0065] iii. If there is a first rule match, then process the packet according to its specified action. Otherwise, continue to the next group Gj+1.

ADDITIONAL NOTES

[0066] The primary purpose of the partitioning of rules is to create rule groups that, in aggregate, enable the fastest possible searching of each packet against the rules in the rule set. In most cases, the optimal partitioning should be the grouping of maximal subsets of spatially disjoint rules. However, in some cases where these disjoint groups are small (e.g. less than 10 rules), consolidating the disjoint groups into a single larger group containing rules that are ordered using other criteria (such as hit probabilities or hardware cache friendliness) and employing linear or interpolated search algorithms may improve performance. A critical concept is the flexibility to organize the rules within the rule set in different ways that enable the use of the most efficient and applicable search algorithm that is available that accounts for the hardware capabilities, which is the motivation behind the term "adaptive" in Adaptive Packet Filtering.

[0067] Rule sets may be partitioned, sorted and consolidated in-place.

[0068] When partitioning a rule set into rule groups, each disjoint group should generally contain the maximal subsets of disjoint rules in order to reduce the number of disjoint groups in the rule set.

[0069] When partitioning a rule set into rule groups and/or sorting those groups, the transform and comparison functions may be different for each rule group.

[0070] When partitioning a rule set into rule groups and/or sorting those groups, the algorithms may account for the hit probabilities of each rule and the aggregate hit probabilities of each group.

[0071] When filtering packets, the search performed within any given rule group may employ the fastest available search algorithm applicable to that group even if it may be different from the specified search algorithm hint.

[0072] When filtering packets, a sub-linear binary search within a disjoint rule group may account for hit probabilities at each pivot so that each recursion could maximize the probability of a rule match.

[0073] When filtering packets, a constant-time search within a disjoint rule group is possible by defining a

hashing function as the transform function such that the hash values for all rules within a group are unique within that group.

Examples

[0074] This section provides examples of the following items described in the algorithm in the previous section.
1) Example of the rule breakup
2) Example of transform function
3) Definition of rule representation
4) Difference between sub-linear and linear
5) Explanation of disjoint rules

1) Examples of the Rule Breakup

[0075] Define
[0076] S1={R1, R2, R3, R4, R5)
and
[0077] R1=from 1.2.3.4 to 3.4.5.6 deny
[0078] R2=from 2.3.4.5 to 4.5.6.7 allow
[0079] R3=from 3.4.5.6 to 5.6.7.8 allow
[0080] R4=from *.*.*.* to 3.4.5.6 allow
[0081] R5=from *.*.*.* to *.*.*.* deny
[0082] Then S1' contains 3 groups of disjoint rules:
[0083] S1'={G1, G2, G3)
[0084] G1={R1, R2, R3)
[0085] G2={R4)
[0086] G3={R5)
[0087] Or, S1' can contain 2 groups of disjoint and dependent rules:
[0088] S1'={G1, G2)
[0089] G1={R1, R2, R3), disjoint, sub-linear
[0090] G2={R4, R5), dependent, linear
or
[0091] Define
[0092] S2={R1, R2, R3, R4, R5, R6, R7, R8, R9)
and
[0093] R1=from 1.2.3.4 to 3.4.5.6 deny
[0094] R2=from 2.3.4.5 to 4.5.6.7 allow
[0095] R3=from 1.2.3.4 to 4.5.6.7 deny
[0096] R4=from 1.*.*.* to *.*.*.* allow
[0097] R5=from 3.4.5.6 to 5.6.7.8 deny
[0098] R6=from 2.*.*.* to *.*.*.* deny
[0099] R7=from *.*.*.* to 3.4.5.6 allow
[0100] R8=from *.*.*.* to 5.6.7.8 allow
[0101] R9=from *.*.*.* to *.*.*.* deny
[0102] Then S2' contains 4 groups of "spatially disjoint" rules:
[0103] S2'={G1, G2, G3, G4)
[0104] G1={R1, R2, R3, R5)
[0105] G2={R4, R6)
[0106] G3={R7, R8)
[0107] G4={R9)
[0108] Or, S2' can contain 2 groups of disjoint and dependent rules:
[0109] S2'={G1, G2)
[0110] G1={R1, R2, R3, R5), disjoint, sub-linear
[0111] G2={R4, R6, R7, R8, R9), dependent, linear

2) Example of Transform Function

[0112] A rule R usually consists of an N-tuple, most basically a 3-tuple such as "from 1.2.3.4 to 3.4.5.6 deny"
[0113] tuple a=source IP address, e.g. "1.2.3.4"
[0114] tuple b=destination IP address, e.g. "3.4.5.6"
[0115] tuple c=action, e.g. "deny"
[0116] Each of these tuples have underlying scalar integer/bit vector representation, so in the above example:
[0117] source IP address="1.2.3.4"=32 bit integer 0016909060
[0118] destination IP address="3.4.5.6"=32 bit integer 0050595078
[0119] action="deny"=8 bit integer 000
[0120] One possible transform function is a transform to scalar key which concatenates the digits of each of the tuples into a large integer value:
[0121] T(a, b, c)=abc
[0122] T(1.2.3.4, 3.4.5.6, deny)=0016909060 0050595078 000=001690906000050595078000
[0123] Another possible transform function is a transform to scalar key which concatenates the bits of each of the tuples into a large integer/bit vector:
[0124] a=1.2.3.
4=00000001000000100000001100000100 (32 bits)
[0125] b=3.4.5.
6=00000011000000100000001010000110 (32 bits)
[0126] c=0=00000000 (8 bits)
T(a, b, c)=abc=00000001000000100000001100000100000000110000010000000101000011000000000
[0127] Another possible transform function is an identity function (i.e. transformation function that does not do anything), then defining a multi-dimensional comparison function for sorting purposes. An example of this is a comparison function that is radix-based for each tuple, which would essentially result in a rule set that is radix sorted by each tuple.
[0128] Note that the transform function must convert the rule into a sortable key, which does not necessarily have to be a scalar key (i.e. it can be a multi-dimensional key that uses a multi-dimensional comparison function for sorting).

3) Definition of Rule Representation.

[0129] Rule representation is the way a rule and a rule set are conceptually represented in software. The most common representation of a rule is as an N-tuple object or structure that simply holds all the tuples together:

```
struct rule {
    unsigned char ip_proto;
    unsigned int ip_src_addr;
    unsigned int ip_dst_addr;
    unsigned short ip_src_port;
    unsigned short ip_dst_port;
    ...
    unsigned char action;
};
```

[0130] The most common representation of a rule set is an array or linked list that hold the rules in a fixed order, and allows for iteration forwards and backwards in the array or list.
[0131] Example of Array:

memory location	0	1	2	3	4	5	6	7	8
value	R1	R2	R3	R4	R5	R6	R7	R8	R9

BNSDOCID: <US____20110055916A1_L>

[0132] Example of Linked List:

[0133] An alternate rule representation is to hold the rule and rule set in a trie or other graph structure. An example of this is described in "Balancing Trie-Based Policy Representations for Network Firewalls." Stephen J. Tarsa and Errin W. Fulp. Proceedings of the IEEE International Symposium on Computer Communications, 2006

[0134] Another alternate rule set representation is a hierarchical one as described in OPTWALL, described in Acharya et al., "OPTWALL: A Hierarchical Traffic-Ware Firewall," available at:
http://www.isoc.org/isoc/conferences/ndss/07/papers/OPTWALL.pdf,
where rule sets are broken down into mutually exclusive rule subsets which are arranged in a hierarchical order. Despite some similarities in terminology, OPTWALL and APF are different. For example, APF does not change the underlying rule or rule set representation. It simply reorders the rules in place and keeps track of the beginning and ending rules in each subset T externally from the rule or rule set. For example, say that a given rule is a standard structure and the rule set is an array form so that the rule set contains the following in the computer's memory:

[0135] Rule set S:

Location	0	1	2	3	4	5	6	7	8
value	R1	R2	R3	R4	R5	R6	R7	R8	R9

[0136] Suppose that the above rule set S can be divided into subsets containing disjoint rules:

[0137] T1=R2, R9, R1, R3

[0138] T2=R5, R7

[0139] T3=R2, R4, R8

so that

[0140] S'=T1, T2, T3=R2, R9, R1, R3, R5, R7, R2, R4, R8

[0141] Then the order of the rules in memory can be changed in place:

[0142] Rule set S':

location	0	1	2	3	4	5	6	7	8
value	R2	R9	R1	R3	R5	R7	R2	R4	R8
	|---------|				|---|		|-------|		
	T1				T2		T3		

[0143] The memory ranges for T1 (0-3), T2 (4-5) and T3 (6-8) are stored outside of the rule and rule set data structures.

4) Difference Between Linear and Sub-Linear.

[0144] A linear algorithm is one whose computational time increases linearly as the size of the set is increased. The best example of this is when looking up a word in a dictionary. If the dictionary is unsorted, then the order of the words would be arbitrary. Therefore, when looking up the word "zebra," one could start from the beginning and search until the end to find it. If the dictionary contains 1,000 entries, you would need to examine all 1,000 words in the worst case.

[0145] A sub-linear algorithm is one whose computational time increases sub-linearly as the size of the set is increased. In the above example, if the dictionary were sorted alphabetically, then one could still use a linear search by starting from the beginning and searching until the end to find "zebra." However, one could also use a sub-linear binary search algorithm by looking in the middle of the dictionary, then seeing if the middle entry comes alphabetically before or after (or is equal), then recursively selecting the middle of the appropriate half again and again to find the word "zebra." Since at each recursion ½ of the remaining words are eliminated, it would take about $\log_2$ (1,000) or about 10 examinations to find the entry in the worst case.

[0146] Another example of a sub-linear algorithm is hashing. Suppose that the above dictionary contains only 5 letter words. If we define a hash function that sums the alphabet order of each letter in the word (z=26, e=05, b=02, r=18, a=01), then hash("zebra")=26+05+02+18+01=52. The computer could have an array containing all the words in the dictionary where each word's position in the array is the hash value of the word (subject to collisions). In the above example, the array's 52nd position would have the word "zebra," so it would take only 1 comparison to determine a match without collision. This hash technique can be selectively used in APF.

5) Explanation of Disjoint Rules.

[0147] A rule R1 is "disjoint" from another rule R2 if their positions in the rule set S can be exchanged without altering the overall security policy. An example of this is rule set S containing:

[0148] R1=from 1.*.*.* to 2.3.4.5 deny

[0149] R2=from 1.2.3.4 to 1.2.3.4 allow

has the same security policy as rule set S' containing:

[0150] R2=from 1.2.3.4 to 1.2.3.4 allow

[0151] R1=from 1.*.*.* to 2.3.4.5 deny

because P=P'; therefore, R1 and R2 are disjoint.

[0152] The technique set forth above does not explain the concept of "spatially disjoint" rules. This is important if the transform function T cannot account for overlapping tuple values, which can be very common in practical settings.

[0153] A rule R1 is "spatially disjoint" from another rule R2 if they are "disjoint" and their corresponding tuples do not unevenly overlap (must be exactly equal, or do not overlap at all). In the above example, R1 and R2 are disjoint but not spatially disjoint because the first tuple of R1 (1.*.*.*) and R2 (1.2.3.4) are not equal but do overlap, i.e. the value of 1.2.3.4 would match the first tuple of both R1 and R2. An example of spatially disjoint rules are:

[0154] R3=from 1.2.3.4 to 3.4.5.6 deny

[0155] R4=from 2.3.4.5 to 3.4.5.6 allow

[0156] Here, the first tuple of R1 (1.2.3.4) and the first tuple of R2 (2.3.4.5) do not overlap, the second tuple of R1 (3.4.5.6) and R2 (3.4.5.6) are equal, and the >> third tuple of R1 (deny) and R2 (allow) do not overlap.

[0157] The importance of "spatially disjoint" rules is dependent upon the definition of a transform function T, so it may be possible to define T such that rules need not be "spatially disjoint" so long as rules are "disjoint."

[0158] The disclosure of each of the publications referenced herein is hereby incorporated by reference in its entirety.

[0159] It will be understood that various details of the presently disclosed subject matter may be changed without departing from the scope of the presently disclosed subject

EX1002
CISCO SYSTEMS, INC. / Page 200 of 1453

matter. Furthermore, the foregoing description is for the purpose of illustration only, and not for the purpose of limitation.

What is claimed is:

1. A method for adaptive packet filtering, the method comprising:

identifying at least one subset of rules in an ordered set of firewall packet filtering rules that defines a firewall policy such that the at least one subset contains disjoint rules, where disjoint rules are defined as rules whose order can be changed without changing the integrity of the firewall policy;

sorting the rules in the at least one subset to statistically decrease the number of comparisons that will be applied to each packet that a firewall encounters; and

filtering packets at the firewall using the sorted rules in the at least one subset by comparing each packet to each of the sorted rules in the at least one subset until the packet is allowed or denied and ceasing the comparing for the packet in response to the packet being allowed or denied and thereby achieving sub-linear searching for the packets filtered using the sorted rules in at least one subset.

2. The method of claim 1 comprising, for the disjoint rules within the at least one subset, identifying spatially disjoint rules and grouping the spatially disjoint rules together within the at least one subset and wherein sorting the rules includes sorting the rules within each of the spatially disjoint groupings.

3. The method of claim 1 comprising identifying at least another subset of rules in the ordered set of firewall rules that are non-disjoint and refraining from sorting the rules in the at least another subset and wherein filtering the packets includes filtering the packets using the sorted, disjoint rules and the non-sorted, non-disjoint rules, thereby achieving sub-linear searching for the sorted, disjoint rules and achieving linear searching for the non-sorted, non-disjoint rules.

4. The method of claim 1 wherein sorting the rules includes applying a transform function to each rule in the at least one subset to compute a sortable key for each of the rules and sorting the rules according to the keys.

5. The method of claim 1 wherein sorting the rules includes sorting the rules according to hit probabilities.

6. The method of claim 1 wherein sorting the rules includes sorting the rules in a binary search tree.

7. The method of claim 1 wherein filtering packets by comparing each packet to the sorted rules includes comparing each packet to the sorted rules using a binary search algorithm.

8. The method of claim 1 wherein filtering packets by comparing each packet to the sorted rules includes comparing each packet to the sorted rules using an interpolated search algorithm.

9. The method of claim 1 wherein filtering packets by comparing each packet to the sorted rules includes comparing each packet to the sorted rules using an informed search algorithm.

10. The method of claim 1 wherein filtering packets by comparing each packet to the sorted rules includes comparing each packet to the sorted rules using a hash lookup algorithm.

11. The method of claim 1 wherein each rule includes an IP source address and an IP destination address.

12. The method of claim 1 wherein the firewall includes a plurality of processors, the at least one subset comprises a plurality of subsets and further comprising distributing the subsets across the plurality of processors to implement at least one of pipelined processing, data parallel processing, and function parallel processing.

13. The method of claim 12 wherein the firewall implements a combination of pipelined and function parallel processing.

14. The method of claim 12 wherein the firewall implements a combination of pipelined and data parallel processing.

15. The method of claim 12 wherein the firewall implements a combination of pipelined, function parallel, and data parallel processing.

16. A system for adaptive packet filtering, the system comprising:

a firewall rule subset identifier/rule sorter for identifying at least one subset of rules in an ordered set of firewall packet filtering rules that defines a firewall policy such that the at least one subset contains disjoint rules, where disjoint rules are defined as rules whose order can be changed without changing integrity of the firewall policy, and for sorting the rules in the at least one subset to statistically decrease the number of comparisons that will be applied to each packet that a firewall encounters; and

a packet filter for filtering packets at the firewall using the sorted rules in the at least one subset by comparing each packet to each of the sorted rules in the at least one subset until the packet is allowed or denied and ceasing the comparing for the packet in response to the packet being allowed or denied and thereby achieving sub-linear searching for the packets filtered using the sorted rules in at least one subset.

17. The system of claim 16 comprising, for the disjoint rules within the at least one subset, the firewall rule subset identifier/rule sorter identifies spatially disjoint rules and groups the spatially disjoint rules together within the at least one subset and wherein the firewall rule subset identifier/rule sorter the rules within each of the spatially disjoint groupings.

18. The system of claim 16 wherein the firewall rule subset identifier/rule sorter identifies at least another subset of rules in the ordered set of firewall rules that are non-disjoint and refrains from sorting the rules in the at least another subset and wherein the firewall packet filter filters the packets using the sorted, disjoint rules and the non-sorted, non-disjoint rules, thereby achieving sub-linear searching for the sorted, disjoint rules and achieving linear searching for the non-sorted, non-disjoint rules.

19. The system of claim 16 wherein the firewall rule subset identifier/rule sorter applies a transform function to each rule in the at least one subset to compute a sortable key for each of the rules and sorting the rules according to the keys.

20. The system of claim 16 wherein the firewall rule subset identifier/rule sorter sorts the rules includes sorting the rules according to hit probabilities.

21. The system of claim 16 wherein the firewall rule subset identifier/rule sorter sorts the rules includes sorting the rules in a binary search tree.

22. The system of claim 16 wherein the packet filter compares each packet to the sorted rules using a binary search algorithm.

23. The system of claim 16 wherein the packet filter compares each packet to the sorted rules using an interpolated search algorithm.

BNSDOCID: <US____20110055916A1_I_>

24. The system of claim 16 wherein the packet filter compares each packet to the sorted rules using an informed search algorithm.

25. The system of claim 16 wherein the packet filter compares each packet to the sorted rules using a hash lookup algorithm.

26. The system of claim 16 wherein each rule includes an IP source address and an IP destination address.

27. The system of claim 16 wherein the firewall includes a plurality of processors, the at least one subset comprises a plurality of subsets and further comprising distributing the subsets across the plurality of processors to implement at least one of pipelined processing, data parallel processing, and function parallel processing.

28. The system of claim 27 wherein the firewall implements a combination of pipelined and function parallel processing.

29. The system of claim 27 wherein the firewall implements a combination of pipelined and data parallel processing.

30. The system of claim 27 wherein the firewall implements a combination of pipelined, data parallel, and function parallel processing.

31. A non-transitory computer readable medium having stored thereon on executable instructions that when implemented by a processor of a computer controls the computer to perform steps comprising:

identifying at least one subset of rules in an ordered set of firewall packet filtering rules that defines a firewall policy such that the at least one subset contains disjoint rules, where disjoint rules are defined as rules whose order can be changed without changing integrity of the firewall policy;

sorting the rules in the at least one subset to statistically decrease the number of comparisons that will be applied to each packet that a firewall encounters; and

filtering packets at the firewall using the sorted rules in the at least one subset by comparing each packet to each of the sorted rules in the at least one subset until the packet is allowed or denied and ceasing the comparing for the packet in response to the packet being allowed or denied and thereby achieving sub-linear searching for the packets filtered using the sorted rules in at least one subset.

* * * * *

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
Wright, Bradley C.
BANNER & WITCOFF, LTD.
1100 13th Street, N.W. Suite 1200
Washington, DC 20005-4051
ETATS-UNIS D'AMERIQUE

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

Applicant's or agent's file reference 007742.00031	Date of mailing *(day/month/year)* 26 June 2014 (26-06-2014)
International application No. PCT/US2014/027723	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
Applicant CENTRIPETAL NETWORKS, INC.	International filing date *(day/month/year)* 14 March 2014 (14-03-2014)

1. [X] The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the International Search Report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Fascimile No.: (41-22) 338.82.70

   For more detailed instructions, see *PCT Applicant's Guide*, International Phase, paragraphs 9.004 - 9.011.

2. [ ] The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. [ ] **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   [ ] the protest together with the decision thereon has been transmitted to the International Bureau together with any request to forward the texts of both the protest and the decision thereon to the designated Offices.

   [ ] no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.

Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before completion of the technical preparations for international publication (Rules 90*bis*.1 and 90*bis*.3).

Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the *PCT Applicant's Guide*, National Chapters.

Name and mailing address of the International Searching Authority European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040 Fax: (+31-70) 340-3016	Authorized officer GOTTAR, Chantal Tel: +49 (0)89 2399-3203

RECEIVED
JUL 01 2014
BANNER & WITCOFF LTD

Form PCT/ISA/220 (July 2010)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	FOR FURTHER ACTION	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
007742.00031		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2014/027723	14 March 2014 (14-03-2014)	15 March 2013 (15-03-2013)
Applicant		
CENTRIPETAL NETWORKS, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 4 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language,** the international search was carried out on the basis of:
      [X] the international application in the language in which it was filed
      [ ] a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. [ ] This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).
   c. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. [ ] **Certain claims were found unsearchable** (See Box No. II)

3. [ ] **Unity of invention is lacking** (see Box No III)

4. With regard to the **title,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings,**
   a. the figure of the **drawings** to be published with the abstract is Figure No. 1
      [X] as suggested by the applicant
      [ ] as selected by this Authority, because the applicant failed to suggest a figure
      [ ] as selected by this Authority, because this figure better characterizes the invention
   b. [ ] none of the figures is to be published with the abstract

RECEIVED
JUL 07 2014
BANNER & WITCOFF LTD

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2014/027723

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2006/048142 A1 (ROESE JOHN J [US] ET AL) 2 March 2006 (2006-03-02) figures 1-4 paragraph [0002] - paragraph [0027] paragraph [0037] - paragraph [0042] paragraph [0046] - paragraph [0058] ----- -/--	1-20

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 June 2014	26/06/2014

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Olaechea, Javier

1

Form PCT/ISA/210 (second sheet) (April 2005)

EX1002
CISCO SYSTEMS, INC. / Page 205 of 1453

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Sean Moore: "SBIR Case Study: Centripetal Networks Subtitle: How CNI Leveraged DHS S&T SBIR Funding to Launch a Successful Cyber Security Company Cyber Security Division 2012 Principal Investigators' Meeting 10-October-2012", , 10 October 2012 (2012-10-10), XP055122227, Retrieved from the Internet: URL:http://www.dhs.gov/sites/default/files/publications/csd-day-2-04-sbir-centripetal-price.pdf [retrieved on 2014-06-06] the whole document	1-20
A	EP 2 385 676 A1 (ALCATEL LUCENT [FR]; INST TELECOM TELECOM BRETAGNE [FR]) 9 November 2011 (2011-11-09) paragraph [0044] - paragraph [0059]	1-20
A	EP 2 498 442 A1 (OPENET TELECOM LTD [IE]) 12 September 2012 (2012-09-12) paragraph [0053] - paragraph [0079]	1-20
A	Cisco: "Control Plane Policing Implementation Best Practices", , 13 March 2013 (2013-03-13), XP002725728, Retrieved from the Internet: URL:https://web.archive.org/web/20130313135143/http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html [retrieved on 2014-06-12] the whole document	1-20
A	US 2010/011434 A1 (KAY RONY [US]) 14 January 2010 (2010-01-14) paragraph [0034] - paragraph [0045]	1-20

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2014/027723

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006048142 A1	02-03-2006	NONE	
EP 2385676 A1	09-11-2011	CN 102934122 A	13-02-2013
		EP 2385676 A1	09-11-2011
		JP 2013525927 A	20-06-2013
		KR 20130005301 A	15-01-2013
		US 2013111548 A1	02-05-2013
		WO 2011138417 A1	10-11-2011
EP 2498442 A1	12-09-2012	EP 2498442 A1	12-09-2012
		US 2012233656 A1	13-09-2012
US 2010011434 A1	14-01-2010	NONE	

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY
(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2014/027723	14.03.2014	15.03.2013

International Patent Classification (IPC) or both national classification and IPC
INV. H04L29/06

Applicant
CENTRIPETAL NETWORKS, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☒ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

RECEIVED
JUL 01 2014
BANNER & WITCOFF LTD

Name and mailing address of the ISA:
European Patent Office
D-80298 Munich
Tel. +49 89 2399 - 0
Fax: +49 89 2399 - 4465

Date of completion of this opinion
see form PCT/ISA/210

Authorized Officer
Olaechea, Javier
Telephone No. +49 89 2399-8233

Form PCT/ISA/237 (Cover Sheet) (July 2009)

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

   a. (means)

      ☐ on paper

      ☐ in electronic form

   b. (time)

      ☐ in the international application as filed

      ☐ together with the international application in electronic form

      ☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	
	No:	Claims	1-20
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-20
Industrial applicability (IA)	Yes:	Claims	1-20
	No:	Claims	

2. Citations and explanations

see separate sheet

Box No. VII Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1 Reference is made to the following document:

D1 US 2006/048142 A1 (ROESE JOHN J [US] ET AL) 2 March 2006 (2006-03-02)

D2 Sean Moore: "SBIR Case Study: Centripetal Networks Subtitle: How CNI Leveraged DHS S&T SBIR Funding to Launch a Successful Cyber Security Company Cyber Security Division 2012 Principal Investigators' Meeting 10-October-2012", , 10 October 2012 (2012-10-10), XP055122227, Retrieved from the Internet: URL:http://www.dhs.gov/sites/default/files/publications/csd-day-2-04-sbir-centripetal-price.pdf [retrieved on 2014-06-06]

D3 Cisco: "Control Plane Policing Implementation Best Practices", , 13 March 2013 (2013-03-13), XP002725728, Retrieved from the Internet: URL:https://web.archive.org/web/20130313135143/http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html [retrieved on 2014-06-12]

2 The present application does not meet the criteria of Article 33(1) PCT, because the subject-matter of claims 1, 11 and 16 is not new in the sense of Article 33(2) PCT.

2.1 The document D1 discloses (the references in parentheses applying to this document) in terms of claim 1:

A method, comprising:

at a computing platform comprising at least one processor, memory, and communication interface (*network device in Figures 1 and 2*):

receiving, via the communication interface, a plurality of packets (paragraph 55; *traffic is received by the network device*);
responsive to a determination that an overload condition has occurred in one or more networks associated with the computing platform, applying, by the processor and to at least some of the plurality of packets, a first group of packet-filtering rules that comprises at least one five-tuple indicating a first set of packets that should be allowed to continue toward their respective destinations, wherein applying the first group of packet-filtering rules includes allowing at least a first portion of the plurality of packets that fall within the first set of packets to continue toward their respective destinations (paragraphs 24, 56 and table in pages 9-10; *in response to an attack trigger, a rule set is activated by the network device, said rule set including disabling all traffic excluding the management traffic, RR1*); and

responsive to a determination that the overload condition has been mitigated to a first degree, applying, to at least some of the plurality of packets, a second group of packet-filtering rules that comprises at least one five-tuple indicating a second set of packets that should be allowed to continue toward their respective destinations, wherein applying the second group of packet-filtering rules includes allowing at least a second portion of the plurality of packets that fall within the second set of packets to continue toward their respective destinations, and wherein the second group of packet-filtering rules is less restrictive than the first group of packet-filtering rules (paragraph 24; *upon detection of a new triggering condition, a less restrictive set of filtering rules is implemented by the networking device*).

Since all the features of claim 1 are known in combination from document D1, the subject-matter of claim 1 is not new (Article 33(2) PCT). Therefore, claim 1 is not allowable (Article 33(1) PCT).

2.2 The same reasoning applies, mutatis mutandis, to the subject-matter of the corresponding independent claims 11 and 16, which therefore are also considered not new (Article 33(2) PCT).

2.3 Furthermore, it is noted that the disclosure of document D2 (see page 4) would also render the subject-matter of claims 1, 11 and 16 not new or at least not inventive.

3 None of the dependent claims 2-10, 12-15 and 17-20 contain additional features which lead the subject-matter to be both new and inventive (see documents D1-D3 and the corresponding passages cited in the search report).

Re Item VII

Certain defects in the international application

The independent claims are not in the two-part form in accordance with Rule 6.3(b) PCT, which in the present case would be appropriate, with those features known in combination from the prior art being placed in the preamble (Rule 6.3(b)(i) PCT) and with the remaining features being included in the characterising part (Rule 6.3(b)(ii) PCT).

The features of the claims are not provided with reference signs placed in parentheses (Rule 6.2(b) PCT).

The description is not in conformity with the claims as required by Rule 5.1(a)(iii) PCT.

Contrary to the requirements of Rule 5.1(a)(ii) PCT, the relevant background art disclosed in the documents D1-D3 is not mentioned in the description, nor are these documents identified therein.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
1743/2 PCT		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2010/054520	**28 OCTOBER 2010 (28.10.2010)**	28 AUGUST 2009 (28.08.2009)

Applicant

GREAT WALL SYSTEMS et al

This International search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of **3** sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language**, the international search was carried out on the basis of :
      ☒ the international application in the language in which it was filed
      ☐ a translation of the international application into _____ , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).
   c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.
2. ☐ **Certain claims were found unsearchable** (See Box No. II)
3. ☐ **Unity of invention is lacking** (See Box No. III)
4. With regard to the **title,**
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:
5. With regard to the **abstract,**
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.
6. With regard to the drawings,
   a. the figure of the **drawings** to be published with the abstract is Figure No. **1**
      ☒ as suggested by the applicant.
      ☐ as selected by this Authority, because the applicant failed to suggest a figure.
      ☐ as selected by this Authority, because this figure better characterizes the invention.
   b. ☐ none of the figure is to be published with the abstract.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2010/054520

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/22(2006.01)i, H04L 12/26(2006.01)i, H04L 12/56(2006.01)i, H04L 29/06(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 12/22; G06F 15/16; H04L 9/00; G06F 9/00; H04L 12/56

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords: firewall, filter, rule, policy

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6098172 A1 (MICHAEL JOHN COSS et al.) 01 August 2000 See figures 5A, 5B and their corresponding explanation.	1-31
A	US 2006-0070122 A1 (STEVEN MICHAEL BELLOVIN) 30 March 2006 See paragraphs [0007], [0049]-[0055].	1-31
A	US 2005-0010765 A1 (BRIAN D. SWANDER et al.) 13 January 2005 See figures 9, 10.	1-31
A	KR 10-2001-0079361 A (S.W. KIM) 22 August 2001 See abstract and figure 2.	1-31

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 APRIL 2011 (26.04.2011)	**27 APRIL 2011 (27.04.2011)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office Government Complex-Daejeon, 189 Cheongsa-ro, Seo-gu, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer CHUN, DAE NYUNG Telephone No. 82-42-481-5991

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2010/054520

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6098172 A1	01.08.2000	EP 0909073 A2	14.04.1999
		JP 03-298832 B2	19.04.2002
		JP 11-167537 A	22.06.1999
		JP 2002-215478 A	02.08.2002
		JP 2009-295187 A	17.12.2009
		JP 3298832 B2	08.07.2002
US 2006-0070122 A1	30.03.2006	US 7051365 B1	23.05.2006
US 2005-0010765 A1	13.01.2005	CN 1574791 A	02.02.2005
		EP 1484886 A2	08.12.2004
		JP 2004-364315 A	24.12.2004
		KR 10-2004-0110981 A	31.12.2004
		US 2007-0204154 A1	30.08.2007
		US 7308711 B2	11.12.2007
		US 7761708 B2	20.07.2010
KR 10-2001-0079361 A	22.08.2001	None	

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
GREGORY A. HUNT
JENKINS, WILSON, TAYLOR & HUNT, P.A.
SUITE 1200 UNIVERSITY TOWER
3100 TOWER BOULEVARD
DURHAM, NC 27707

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing (*day/month/year*)	03 JUL 2008
Applicant's or agent's file reference 1498/3/2 PCT	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date (*day/month/year*)	Priority date (*day/month/year*)
PCT/US06/11291	28 March 2006 (28.03.2006)	28 March 2005 (28.03.2005)

International Patent Classification (IPC) or both national classification and IPC

IPC: **H04L 9/00**(2006.01),**G06F 9/00,15/16/17/00,15/18**(2006.01)
USPC: 726/1,11,25;713/163,166

Applicant

WAKE FOREST UNIVERSITY

1. This opinion contains indications relating to the following items:

☒	Box No. I	Basis of the opinion
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(*b*) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US	Date of completion of this opinion	Authorized officer
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	24 June 2008 (24.06.2008)	Ayaz Sheikh DEBORAH A. THOMAS PARALEGAL SPECIALIST Telephone No. 571-272-3000

Form PCT/ISA/237 (cover sheet) (April 2007)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US06/11291

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

☒ the international application in the language in which it was filed

☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:

a. type of material

☐ a sequence listing

☐ table(s) related to the sequence listing

b. format of material

☐ on paper

☐ in electronic form

c. time of filing/furnishing

☐ contained in the international application as filed.

☐ filed together with the international application in electronic form.

☐ furnished subsequently to this Authority for the purposes of search.

4. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US06/11291

Box No. V Reasoned statement under Rule 43 *bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims 1-41	YES
	Claims NONE	NO
Inventive step (IS)	Claims 1-41	YES
	Claims NONE	NO
Industrial applicability (IA)	Claims 1-41	YES
	Claims NONE	NO

2. Citations and explanations:

Claims 1-41 meet the criteria set out in PCT Article 33(2)-(3), because the prior art does not teach or fairly suggest optimization of firewall policy management for intrusion detection and intrusion prevention while maintaining the integrity of the original policy. Prior art does not teach a heuristic to order firewall rules the reduces average number of comparison by calculating a probability indication a likelihood of receiving a packet matching the rule sorted in order of non-increasing probability while maintaining the integrity of firewall policy.

Claims 1-41 meet the criteria set out in PCT Article 33 (4) because the subject matter claimed can be made or used in industry.

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
GREGORY A. HUNT
JENKINS, WILSON & TAYLOR, P.A.
SUITE 1400 UNIVERSITY TOWER
3100 TOWER BOULEVARD
DURHAM, NC 27707

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	11 SEP 2006
Applicant's or agent's file reference 1498/3/3 PCT	FOR FURTHER ACTION See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US05/47008	22 December 2005 (22.12.2005)	22 December 2004 (22.12.2004)

International Patent Classification (IPC) or both national classification and IPC

IPC: **G06F 17/00**(2006.01) G06F 17/00(2006.01)
USPC: 726/14

Applicant

WAKE FOREST UNIVERSITY

1. This opinion contains indications relating to the following items:

- ☒ Box No. I — Basis of the opinion
- ☐ Box No. II — Priority
- ☐ Box No. III — Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV — Lack of unity of invention
- ☒ Box No. V — Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI — Certain documents cited
- ☐ Box No. VII — Certain defects in the international application
- ☐ Box No. VIII — Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis(b)* that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US	Date of completion of this opinion	Authorized officer
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	16 August 2006 (16.08.2006)	Nasser G Moazzami Telephone No. 571-272-2100

Form PCT/ISA/237 (cover sheet) (April 2005)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US05/47008

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

☒ the international application in the language in which it was filed

☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

a. type of material

☐ a sequence listing

☐ table(s) related to the sequence listing

b. format of material

☐ on paper

☐ in electronic form

c. time of filing/furnishing

☐ contained in the international application as filed.

☐ filed together with the international application in electronic form.

☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US05/47008

Box No. V Reasoned statement under Rule 43 *bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims NONE	YES
	Claims 1-52	NO
Inventive step (IS)	Claims NONE	YES
	Claims 1-52	NO
Industrial applicability (IA)	Claims 1-52	YES
	Claims NONE	NO

2. Citations and explanations:

Please See Continuation Sheet

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

V. 2. Citations and Explanations:
Claims 1-52 lack novelty under PCT Article 33(2) as being anticipated by Xu (U.S. Patent Pub. No. 2002/0038339 A1).

Regarding claims 1 and 31, Xu teaches a function-parallel firewall/system comprising:
a first firewall node for filtering received packets using a first portion of a rule set including a plurality of rules, the first portion including less than all of the rules in the rule set (figure 13, reference number 1361); and
at least one second firewall node for filtering packets using a second portion of the rule set, the second portion including at least one rule in the rule set that is not present in the first portion (figure 13, reference number 1362),
wherein the first and second portions together include all of the rules in the rule set (paragraph 0170).

Regarding claim 2, Xu teaches wherein the first and second portions respectively include rules present in first and second levels of a firewall hierarchy (figure 9E).

Regarding claim 3, Xu teaches wherein the first and second firewall nodes are connected to each other such that the rules in the first level are applied to received packets before the rules in the second level (paragraph 0092).

Regarding claim 4, Xu teaches wherein the first firewall node is adapted to forward packets that pass one of the rules in the first portion to an internal network in a manner that bypasses the second firewall node (paragraph 0122).

Regarding claim 5, Xu teaches wherein the first firewall node is adapted to discard packets that fail one of the rules in the first portion (paragraph 0171).

Regarding claim 6, Xu teaches wherein the rules in the second portion are more processor-intensive than the rules in the first portion (paragraph 0170).

Regarding claim 7, Xu teaches comprising:
a packet distributor for replicating each packet to the first and second firewall nodes (figure 13, reference number 1390); and
a gate machine for collecting results of applying the first and second portions of the rule set to each packet from the first and second firewall nodes and for making a forwarding decision based on the results (figure 13, reference number 1300).

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

Regarding claim 8, Xu teaches wherein each of the first and second firewall nodes is adapted to process the packets in a pipelined manner and wherein the gate machine is adapted to maintain state information for multiple packets simultaneously (paragraph 0168).

Regarding claim 9, Xu teaches wherein the gate machine is adapted to signal the second firewall node when processing of a packet is no longer needed due to matching of the packet with one of the rules used by the first firewall node (paragraph 0119).

Regarding claim 10, Xu teaches wherein the first and second firewall nodes implement rules of the same hierarchical level (figure 9E).

Regarding claim 11, Xu teaches wherein at least one of the rules in the first portion is present in the second portion to provide redundancy (paragraph 0177).

Regarding claims 12 and 22, Xu teaches wherein the first and second firewall nodes are configured to implement a gateless design wherein the rules are distributed among the first and second firewall nodes such that for any given packet, one of the first and second firewall nodes will accept the packet and the other of the first and second firewall nodes will deny the packet (paragraph 0201).

Regarding claim 13, Xu teaches wherein the first and second firewall nodes are implemented on different physical machines (figure 13, reference number 1361, 1362, and 1363).

Regarding claim 14, Xu teaches wherein the first and second firewall nodes are implemented on different processors in the same machine (paragraph 0244).

Regarding claims 15 and 28, Xu teaches wherein the first and second firewall nodes are adapted to simultaneously process copies of the same packets (figure 12, reference number 1261-1263).

Regarding claims 16, 24, 32, and 36, Xu teaches wherein the rule set includes firewall rules for filtering packets based on packet headers (paragraph 0091).

Regarding claims 17, 25, 33, and 37, Xu teaches wherein the rule set includes intrusion detection rules for filtering packets based on packet payloads (paragraph 0091).

Regarding claims 18, 26, 34, and 38, Xu teaches wherein the rule set includes intrusion protection rules for filtering packets based on a combination of packet headers and packet payloads (paragraph 0091).

Regarding claim 19, Xu teaches a stateful function-parallel firewall system comprising:
a first function-parallel firewall subsystem including a plurality of firewall nodes implementing a first rule set for filtering packets arriving in a network, wherein the first function-parallel firewall subsystem includes at least first and second firewall nodes respectively implementing first and second portions of the first rule set, the first portion including at least one rule that is not present in the second portion (figure 13, reference number 1361 and figure 8, INBOUND PACKETS); and
a second function-parallel firewall sub-system including a second set of firewall nodes implementing a second rule set for filtering packets departing from the network, wherein the second function-parallel firewall subsystem includes at least third and fourth firewall nodes, the third and fourth firewall nodes implementing first and second portions of the second rule set, the first portion of the second rule set including at least one rule that is not present in the second portion of the second rule set, wherein the first and second function-parallel firewall subsystems share state information regarding connections established through the first and second sets of firewall nodes (figure 13, reference number 1362 and figure 8, OUTBOUND PACKETS).

Regarding claim 20, Xu teaches comprising a database node coupled to the first and second function-parallel firewall subsystems, wherein the database node stores the state information, wherein the first set of firewall nodes obtains state information regarding connections established through the second set of firewall nodes from the database node, and wherein the second set of firewall nodes obtains state information regarding connections established through the first set of firewall nodes from the database node (figure 14, reference number 1471-1473).

Regarding claim 21, Xu teaches wherein the first and second sets of firewall nodes store copies of the state information maintained by the database node (paragraph 0014).

Regarding claim 23, Xu teaches wherein the firewall nodes of the first subsystem are adapted to simultaneously process copies of the same packets arriving in the network and wherein the firewall nodes in the second subsystem are adapted to simultaneously process copies of packets departing from the network (figure 12, reference number 1261-1263).

Regarding claim 27, Xu teaches a firewall grid comprising:
a plurality of firewall nodes being physically connected to each other via a network for filtering packets (figure 12, reference

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient.**

number 1261, 1262, and 1263); and
a controller for controlling logical connections between the firewall nodes, wherein the controller is adapted to configure the firewall nodes in a logical firewall hierarchy without changing physical connections between the firewall nodes (paragraph 0165-0167).

Regarding claim 29, Xu teaches wherein the logical firewall hierarchy comprises a function-parallel hierarchy where individual firewall nodes implement different portions of a rule set (figure 13, reference number 1361-1363).

Regarding claim 30, Xu teaches wherein the controller is adapted to detect congestion at a first level in the firewall hierarchy and is adapted to reconfigure the logical connections between the firewall nodes to add a firewall node from another level in the firewall hierarchy to the level at which congestion was detected (figure 17).

Regarding claims 35 and 50, Xu teaches a method/computer program product for controlling access to a network based on a set of packet filtering rules distributed in a function-parallel manner, the method comprising:
distributing packet filtering rules of a rule set among a plurality of different nodes in a function-parallel manner so that at least some of the different nodes implement different portions of the rule set (figure 13, reference number 1361-1363);
replicating packets to each of the nodes (paragraph 0168); and
applying the rules to filter the packets (paragraph 0170).

Regarding claim 39, Xu teaches comprising, receiving a first packet at a first node, determining whether the packet matches a first rule implemented by the first node, and, in response to determining that a match occurs, notifying the other nodes of the match (paragraph 0119).

Regarding claim 40, Xu teaches comprising, at the other nodes, ceasing processing of the first packet (paragraph 0119).

Regarding claims 41 and 51, Xu teaches a method/computer program product for distributing rules in a function-parallel firewall, the method comprising:
defining a rule set for a function-parallel firewall (paragraph 0168);
assigning rules in the rule set to nodes and branches in a trie data structure, wherein each node in the trie data structure corresponds to a data field and each branch represents a value for each data field to be compared to values in corresponding fields in received packets (figure 13, reference number 1361-1363 and paragraph 0170); and
pruning the trie data structure in a manner that preserves ordering of the rules in the rule set (figure 20, deleting certain entries in 2091, 2092, and 2093).

Regarding claim 42, Xu teaches wherein pruning the trie data structure includes pushing a rule to its descendants and deleting the original rule (figure 20, deleting entries in 2091-2093).

Regarding claim 43, Xu teaches comprising reducing the depth of the trie using level reordering (paragraph 0246).

Regarding claim 44, Xu teaches wherein assigning rules in the rule set to nodes and branches in the trie data structure includes assigning rules requiring longer processing time to lower levels in the trie (paragraph 0170).

Regarding claims 45 and 52, Xu teaches a method/computer program product for assigning rules to a plurality of firewall nodes, the method comprising:
assigning packet filtering rules to nodes in a directed acyclical graph (DAG) (paragraph 0168);
representing relationships between rules by edges in the DAG (figure 9E); and
distributing the rules among a plurality of firewall nodes using the DAG such that different firewall nodes implement different rules and such that relationships between the rules specified in the DAG are preserved (figure 13, reference number 1361-1363 and paragraph 0170).

Regarding claim 46, Xu teaches wherein distributing the rules among a plurality of firewall nodes using the DAG includes distributing the rules such that intersecting accept rules are not present in more than one firewall node (figure 9E, rules that overlap are blacked out).

Regarding claim 47, Xu teaches wherein distributing the rules among a plurality of firewall nodes using the DAG includes distributing the rules such that the edges to not span multiple firewall nodes (figure 9E, rules that overlap are blacked out).

Regarding claim 48, Xu teaches wherein distributing the rules among a plurality of firewall nodes using the DAG includes replicating deny rules in each of the firewall nodes (paragraph 0177).

Regarding claim 49, Xu teaches comprising eliminating a deny rule implemented by a first firewall node in response to determining that the deny rule for the first firewall node includes no inbound edges and outbound edges from the first deny rule terminate only in a superset deny rule (paragraph 0177).

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14757638
Filing Date	2015-12-23
First Named Inventor	David K. Ahn
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	007742.00059\US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

	1	J. Xu et al., "Design and Evaluation of a High-Performance ATM Firewall Switch and Its Applications", IEEE Journal on Selected Areas in Communications, 17(6): 1190-1200, June 1999	
	2	C. Benecke, "A Parallel Packet Screen for High Speed Networks", Proceedings of the 15th Annual Computer Security Applications Conference, 1999	
	3	R. Funke et al., "Performance Evaluation of Firewalls in Gigabit-Networks", Proceedings of the Symposium on Performance Evaluation of Computer and Telecommunication Systems, 1999	
	4	S. Suri et al., "Packet Filtering in High Speed Networks", Proceedings of the Symposium on Discrete Algorithms, 969-970, 1999	
	5	J. Ellermann et al., "Firewalls for ATM Networks", Proceedings of INFOSEC'COM, 1998	
	6	V. Srinivasan et al., "Fast and Scalable Layer Four Switching", Proceedings of ACM SIGCOMM, 191-202, 1998	
	7	M. Degermark et al., "Small Forwarding Tables for Fast Routing Lookups", Proceedings of ACM SIGCOMM, 4-13, 1997	
	8	S,M. Bellovin et al., "Network Firewalls", IEEE Communications Magazine, 50-57, 1994	
	9	W.E. Leland et al., "On the Self-Similar Nature of Ethernet Traffic", IEEE Transactions on Networking, 2(1); 15, 1994	
	10	G. Brightwell et al., "Counting Linear Extensions is #P-Complete", Proceedings of the Twenty-Third Annual ACM Symposium on Theory of Computing, 1991	
	11	M. Al-Suwaiyel et al., "Algorithms for Trie Compaction", ACM Transactions on Database Systems, 9(2): 243-263, June 1984	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

	12	D. Comer, "Analysis of a Heuristic for Full Trie Minimization", ACM Transactions on Database Systems, 6(3): 513-537, Sept. 1981	
	13	R.L. Graham et al., "Optimization and Approximation in Deterministic Sequencing and Scheduling: A Survey", Annals of Discrete Mathematics, 5: 287-326, 1979	
	14	E.L. Lawler, "Sequencing Jobs to Minimize Total Weighted Completion oTime Subject to Precedence Constraints", Annals of Discrete Mathematics, 2: 75-90, 1978	
	15	J.K. Lenstra et al., "Complexity of Scheduling Under Precedence Constraints", Operations Research, 26(1): 22-35,1978	
	16	R. Rivest, "On Self-Organizing Sequential Search Heuristics", Communications of the ACM, 19(2): 1976	
	17	W.E. Smith, "Various Optimizers for Single-Stage Productions", Naval Research Logistics Quarterly, 3: 59-66, 1956	
	18	Bellion, "HIgh Performance Packet Classification", http://www.hipac.org (Publication Date Unknown)	
	19	2011 Oct 18 - (EP) Communication Pursuant to Article 94(3) - App 06 758 213.0	
	20	2011 Jun 09 - (US) Notice of Allowance - App 11/390,976	
	21	2012 Jun 26 - (EP) Extended Search Report - App 05857614.1	
	22	2012 Jun 09 - (AU) Notice of Acceptance - App 2006230171	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

	23	2011 Nov 11 - (AU) Second Office Action - App 2006230171	
	24	2013 Jan 17 - (CA) Office Action - App 2,600,236	
	25	2013 Jan 16 - (CA) Office Action - App 2,594,020	
	26	2012 Nov 20 - (EP) Communication under rule 71(3) - App 06 758 213.0	
	27	2013 Apr 18 - (EP) Decision to Grant a European Patent - App 06758212.0	
	28	2011 Aug 25 - (US) Non Final Rejection - App 12/871,806	
	29	2012 Feb 06 - (US) Final Rejection - App 12/871,806	
	30	2012 Aug 07 - (US) Non Final Rejection - App 12/871,806	
	31	2012 Nov 26 - (US) Final Rejection - App 12/871,806	
	32	2013 Apr 04 - (US) Notice of Allowance - App 12/871,806	
	33	2015 Jan 14 - (EP) Extended Search Report - App 10819667.6	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

	34	2014 May 26 - (CA) Office Action - App 2010297968	
	35	2015 May 25 - (AU) Notice of Acceptance - App 2010297968	
	36	2015 May 14 - (US) Non Final Rejection - App 13/940,240	
	37	2015 Nov 27 - (US) Final Rejection - App 13/940,240	
	38	2015 Jul 10 - (WO) Communication Relating to the Results of the Partial International Search for International App - PCT/US2015/024691	
	39	2015 Jul 23 - (WO) International Preliminary Report on Patentability - App PCT/US2013/072566	
	40	2016 Jan 28 - (WO) International Search Report and Written Opinion - App PCT/US2015/062691	
	41	International Search Report and Written Opinion for International App. No. PCT/US2015/024691, dated September 16, 2015.	
	42	International Preliminary Report on Patentability for International App. No. PCT/US2013/057502, dated April 28, 2015	
	43	International Preliminary Report on Patentability for International App. No. PCT/US2014/023286, dated September 15, 2015.	
	44	International Preliminary Report on Patentability for International App. No. PCT/US2014/027723, dated September 15, 2015.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

	45	Statement RE: Related Application, dated July 24, 2015	
	46	2015 Dec 22 - (US) Final Office Action - App 14/714,207	
	47	2016 Feb 26 - (US) Non Final Office Action - App 14/253,992	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Bradley C. Wright/	Date (YYYY-MM-DD)	2016-03-30
Name/Print	Bradley C. Wright	Registration Number	38061

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

PCT

To:
Wright, Bradley C.
BANNER & WITCOFF, LTD.
1100 13th Street, N.W. Suite 1200
Washington, DC 20005-4051
ETATS-UNIS D'AMERIQUE

INVITATION TO PAY ADDITIONAL FEES AND, WHERE APPLICABLE, PROTEST FEE

(PCT Article 17(3)(a) and Rule 40.1 and 40.2(e))

Applicant's or agent's file reference 007742.00043	Date of mailing *(day/month/year)* 10 July 2015 (10-07-2015)
International application No. PCT/US2015/024691	**PAYMENT DUE** within **ONE MONTH** from the above date of mailing
Applicant CENTRIPETAL NETWORKS, INC.	International filing date *(day/month/year)* 7 April 2015 (07-04-2015)

1. This International Searching Authority

(i) considers that there are 3 *(number of)* inventions claimed in the international application covered by the claims indicated on an extra sheet:

(ii) therefore considers that **the international application does not comply with the requirements of unity of invention** (Rules 13.1, 13.2 and 13.3) for the reasons indicated on an extra sheet:

(iii) [X] has carried out a partial international search (see Annex) [ ] will establish the international search report on those parts of the international application which relate to the invention first mentioned in claims Nos.:

see extra sheet

(iv) will establish the international search report on the other parts of the international application only if, and to the extent to which, additional fees are paid.

2. Consequently, the applicant is hereby **invited to pay,** within the time limit indicated above, the amount indicated below:

EUR 1.875,00	x	2	=	EUR 3.750,00
Fee per additional invention		number of additional inventions		currency/total amount of additional fees

3. The applicant is informed that, according to Rule 40.2(c), **the payment of any additional fee may be made under protest,** i.e., a reasoned statement to the effect that the international application complies with the requirement of unity of invention or that the amount of the required additional fee is excessive, where applicable, subject to the payment of a protest fee.

Where the applicant pays additional fees under protest, the applicant is hereby invited, within the time limit indicated above, to pay a protest fee (Rule 40.2(e)) in the amount of EUR 865,00 *(currency/amount)*

Where the applicant has not, within the time limit indicated above, paid the required protest fee, the protest will be considered not to have been made and the International Searching Authority will so declare.

4. [ ] Claim(s) Nos. _____ have been found to be unsearchable under Article 17(2)(b) because of defects under Article 17(2)(a) and therefore have not been included with any invention.

Name and mailing address of the International Searching Authority	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040 Fax: (+31-70) 340-3016	BARRIO BARANANO, Ainhoa Tel: +49 (0)89 2399-8621

RECEIVED
JUL 21 2015
BANNER & WITCOFF LTD

Form PCT/ISA/206 (April 2005)
Registered Mail

INVITATION TO PAY ADDITIONAL FEES

International application No.
PCT/US2015/024691

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-9

A method for packet filtering based on application-layer packet header information

---

2. claims: 10-18

A method for selective packet digest logging

---

3. claims: 19, 20

A method for security policy update and management

The lack of unity becomes apparent a posteriori, i.e. for the following reasoning document D1 (US20060136987) is taken into account. From this prior art document what is known is a method comprising a security policy management server ("the controller 13 provides the identifying rule and the processing rule" in paragraph [0093]; "the controller may delete from the identifying rule/processing rule setting table the identifying rule and the processing rule which have not been accessed for a predetermined time." in paragraph [0036]) as claimed in claim 1. These features are the only features common to all the groups of inventions.
With the reference to the prior art document D1:
The third group yields the potential special technical feature of receiving, by a security policy management server and from a computing device, a security update comprising a set of network addresses; updating, one or more rules; receiving, from a different computing device, a security update comprising a different set of network addresses; determining that the different set of network addresses includes at least a portion of network addresses included in the set of network addresses; and responsive to that identifying the at least a portion of network addresses included in the set of network addresses, at least one of the one or more rules stored in the memory that specifies a range of network addresses comprising the at least a portion of network addresses; and updating the at least one of the one or more rules to include one or more other network addresses included in the different set of network addresses, hence solving the objective problem of how to manage security policies based on information received from different sources comprising overlapping network addresses.
Moreover, the first and second invention have further common features, which are also disclosed in document D1 as shown in the following. From document D1 what is further known is:
receiving ("receive the identifying rule and the processing rule from another communication apparatus" in paragraph [0040]), by each of a plurality of packet security gateways associated with a security policy management server and from the security policy management server ("the controller 13 provides the identifying rule and the processing rule" in paragraph [0093]; "while the notifying destination of the notifying

message (identifying rule and the processing rule) 740 is made the router 100C in FIG. 8, the gateway apparatus, a switch, and a management system (not shown) may be made a notifying destination." in paragraph [0095]), a dynamic security policy ("receive the identifying rule and the processing rule from another communication apparatus" in paragraph [0040]; "the controller may delete from the identifying rule/processing rule setting table the identifying rule and the processing rule which have not been accessed for a predetermined time." in paragraph [0036]) that includes at least one rule specifying a packet transformation function to be performed on packets

receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway ("received packet" in the abstract);

identifying, by the packet security gateway, from amongst the packets associated with the network protected by the packet security gateway, and on a packet-by-packet basis, one or more packets ("identify a protocol type of a communication packet transmitted/received by a device" in paragraph [0028]); and

performing, by the packet security gateway and on a packet-by-packet basis, the packet transformation function on each of the one or more packets ("to automatically set the processing rule of the packet" in paragraph [0028]; "the processing policy may include a policy concerning at least one of a service quality class, filtering, and routing of the packet." in paragraph [0029]) as claimed in claim 1. These features are the only features common to the first two groups of inventions.

With the reference to the prior art document D1:

The first group yields the potential special technical feature of using application-layer packet-header information as the packet identification at the gateway, hence solving the objective problem of how to improve the scalability issues in high resolution filtering.

The second group yields the potential special technical feature of using a packet digest logging function to the identified packets, hence solving the objective problem of how to enable security awareness information in a network.

Consequently, neither the objective problems underlying the subjects of the three claimed inventions, nor the solutions as defined by the special technical features described allow for the link of a common inventive concept to be established between said inventions in the meaning of Rule 13.2 PCT. In conclusion, the three groups of claims are not linked by a single general inventive concept. The application hence does not meet the requirements of unity of invention as defined in Rule 13.1 PCT.

Annex to Form PCT/ISA/206
COMMUNICATION RELATING TO THE RESULTS OF THE PARTIAL INTERNATIONAL SEARCH

International Application No
PCT/US2015/024691

1. The present communication is an Annex to the invitation to pay additional fees (Form PCT/ISA/206). It shows the results of the international search established on the parts of the international application which relate to the invention first mentioned in claims Nos.:
see 'Invitation to pay additional fees'
2. This communication is not the international search report which will be established according to Article 18 and Rule 43.

3. If the applicant does not pay any additional search fees, the information appearing in this communication will be considered as the result of the international search and will be included as such in the international search report.

4. If the applicant pays additional fees, the international search report will contain both the information appearing in this communication and the results of the international search on other parts of the international application for which such fees will have been paid.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2006/136987 A1 (OKUDA MASATO [JP]) 22 June 2006 (2006-06-22) paragraph [0028] - paragraph [0030]; figures 1,21 paragraphs [0033], [0036], [0040], [0093], [0095], [0135]	1-9
X	US 2007/240208 A1 (YU MING-CHE [TW] ET AL) 11 October 2007 (2007-10-11) abstract paragraphs [0021], [0024] - paragraph [0026] paragraph [0033] - paragraph [0036] paragraph [0039] - paragraph [0040]	1-9
A	US 2006/146879 A1 (ANTHIAS TEFCROS [US] ET AL) 6 July 2006 (2006-07-06) paragraph [0074] - paragraph [0076] paragraph [0112] - paragraph [0119] paragraphs [0207], [0208], [0240]	1-9
A	US 8 306 994 B2 (KENWORTHY STACY [US]) 6 November 2012 (2012-11-06) abstract; figures 4,6 column 2 - column 4 column 6 - column 9	1-9

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Form PCT/ISA/206 (Annex, first sheet) (July 1992, reprint January 2004)

Patent Family Annex

Information on patent family members

International Application No
PCT/US2015/024691

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006136987 A1	22-06-2006	JP 2006174350 A	29-06-2006
		US 2006136987 A1	22-06-2006
US 2007240208 A1	11-10-2007	NONE	
US 2006146879 A1	06-07-2006	CN 101099345 A	02-01-2008
		EP 1834453 A2	19-09-2007
		US 2006146879 A1	06-07-2006
		WO 2006073740 A2	13-07-2006
US 8306994 B2	06-11-2012	US 6317837 B1	13-11-2001
		US 2002049899 A1	25-04-2002
		US 2010242098 A1	23-09-2010
		US 2013061294 A1	07-03-2013

European Patent Organisation

Account details

N° 3 338 800 00 (BLZ 700 800 00)
Commerzbank
Promenadeplatz 7
D-80273 München
SWIFT Code: DRESDEFF700
IBAN: DE20 7008 0000 0333 880000
BIC: DRESDEFF

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY
(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44*bis*)

Applicant's or agent's file reference 007742.00031	**FOR FURTHER ACTION**	See item 4 below
International application No. PCT/US2014/027723	International filing date *(day/month/year)* 14 March 2014 (14.03.2014)	Priority date *(day/month/year)* 15 March 2013 (15.03.2013)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant CENTRIPETAL NETWORKS, INC.		

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 *bis*.1(a).

2. This REPORT consists of a total of 7 sheets, including this cover sheet.

   In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☒	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44*bis*.3(c) and 93*bis*.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44*bis* .2).

	Date of issuance of this report 15 September 2015 (15.09.2015)
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	Authorized officer Nora Lindner e-mail: pt05.pct@wipo.int

Form PCT/IB/373 (January 2004)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY
(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2014/027723	14.03.2014	15.03.2013

International Patent Classification (IPC) or both national classification and IPC
INV. H04L29/06

Applicant
CENTRIPETAL NETWORKS, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☒ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Fax: +49 89 2399 - 4465	see form PCT/ISA/210	Olaechea, Javier Telephone No. +49 89 2399-8233

Form PCT/ISA/237 (Cover Sheet) (July 2009)

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

   a. (means)

      ☐ on paper

      ☐ in electronic form

   b. (time)

      ☐ in the international application as filed

      ☐ together with the international application in electronic form

      ☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	
	No:	Claims	1-20
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-20
Industrial applicability (IA)	Yes:	Claims	1-20
	No:	Claims	

2. Citations and explanations

see separate sheet

Box No. VII Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1 Reference is made to the following document:

D1 US 2006/048142 A1 (ROESE JOHN J [US] ET AL) 2 March 2006 (2006-03-02)

D2 Sean Moore: "SBIR Case Study: Centripetal Networks Subtitle: How CNI Leveraged DHS S&T SBIR Funding to Launch a Successful Cyber Security Company Cyber Security Division 2012 Principal Investigators' Meeting 10-October-2012", , 10 October 2012 (2012-10-10), XP055122227, Retrieved from the Internet: URL:http://www.dhs.gov/sites/default/files/publications/csd-day-2-04-sbir-centripetal-price.pdf [retrieved on 2014-06-06]

D3 Cisco: "Control Plane Policing Implementation Best Practices", , 13 March 2013 (2013-03-13), XP002725728, Retrieved from the Internet: URL:https://web.archive.org/web/20130313135143/http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html [retrieved on 2014-06-12]

2 The present application does not meet the criteria of Article 33(1) PCT, because the subject-matter of claims 1, 11 and 16 is not new in the sense of Article 33(2) PCT.

2.1 The document D1 discloses (the references in parentheses applying to this document) in terms of claim 1:

A method, comprising:

at a computing platform comprising at least one processor, memory, and communication interface (*network device in Figures 1 and 2*):

receiving, via the communication interface, a plurality of packets (paragraph 55; *traffic is received by the network device*);
responsive to a determination that an overload condition has occurred in one or more networks associated with the computing platform, applying, by the processor and to at least some of the plurality of packets, a first group of packet-filtering rules that comprises at least one five-tuple indicating a first set of packets that should be allowed to continue toward their respective destinations, wherein applying the first group of packet-filtering rules includes allowing at least a first portion of the plurality of packets that fall within the first set of packets to continue toward their respective destinations (paragraphs 24, 56 and table in pages 9-10; *in response to an attack trigger, a rule set is activated by the network device, said rule set including disabling all traffic excluding the management traffic, RR1*); and

responsive to a determination that the overload condition has been mitigated to a first degree, applying, to at least some of the plurality of packets, a second group of packet-filtering rules that comprises at least one five-tuple indicating a second set of packets that should be allowed to continue toward their respective destinations, wherein applying the second group of packet-filtering rules includes allowing at least a second portion of the plurality of packets that fall within the second set of packets to continue toward their respective destinations, and wherein the second group of packet-filtering rules is less restrictive than the first group of packet-filtering rules (paragraph 24; *upon detection of a new triggering condition, a less restrictive set of filtering rules is implemented by the networking device*).

Since all the features of claim 1 are known in combination from document D1, the subject-matter of claim 1 is not new (Article 33(2) PCT). Therefore, claim 1 is not allowable (Article 33(1) PCT).

2.2 The same reasoning applies, mutatis mutandis, to the subject-matter of the corresponding independent claims 11 and 16, which therefore are also considered not new (Article 33(2) PCT).

2.3 Furthermore, it is noted that the disclosure of document D2 (see page 4) would also render the subject-matter of claims 1, 11 and 16 not new or at least not inventive.

3 None of the dependent claims 2-10, 12-15 and 17-20 contain additional features which lead the subject-matter to be both new and inventive (see documents D1-D3 and the corresponding passages cited in the search report).

Re Item VII

Certain defects in the international application

The independent claims are not in the two-part form in accordance with Rule 6.3(b) PCT, which in the present case would be appropriate, with those features known in combination from the prior art being placed in the preamble (Rule 6.3(b)(i) PCT) and with the remaining features being included in the characterising part (Rule 6.3(b)(ii) PCT).

The features of the claims are not provided with reference signs placed in parentheses (Rule 6.2(b) PCT).

The description is not in conformity with the claims as required by Rule 5.1(a)(iii) PCT.

Contrary to the requirements of Rule 5.1(a)(ii) PCT, the relevant background art disclosed in the documents D1-D3 is not mentioned in the description, nor are these documents identified therein.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY
(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44*bis*)

Applicant's or agent's file reference 007742.00030	**FOR FURTHER ACTION**	See item 4 below
International application No. PCT/US2014/023286	International filing date *(day/month/year)* 11 March 2014 (11.03.2014)	Priority date *(day/month/year)* 12 March 2013 (12.03.2013)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant CENTRIPETAL NETWORKS, INC.		

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 *bis*.1(a).

2. This REPORT consists of a total of 6 sheets, including this cover sheet.

   In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☒	Box No. VIII	Certain observations on the international application

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44*bis*.3(c) and 93*bis*.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44*bis* .2).

	Date of issuance of this report 15 September 2015 (15.09.2015)
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	Authorized officer Philippe Bécamel e-mail: pt03.pct@wipo.int

Form PCT/IB/373 (January 2004)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2014/023286	11.03.2014	12.03.2013

International Patent Classification (IPC) or both national classification and IPC
INV. H04L29/06

Applicant
CENTRIPETAL NETWORKS, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☒ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Fax: +31 70 340 - 3016	see form PCT/ISA/210	Veen, Gerardus Telephone No. +31 70 340-3811

Form PCT/ISA/237 (Cover Sheet) (July 2009)

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

   a. (means)

      ☐ on paper

      ☐ in electronic form

   b. (time)

      ☐ in the international application as filed

      ☐ together with the international application in electronic form

      ☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	
	No:	Claims	1-20
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-20
Industrial applicability (IA)	Yes:	Claims	1-20
	No:	Claims	

2. Citations and explanations

see separate sheet

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

The following documents are referred to:

D1 US 2003/123456 A1 (DENZ PETER R [US] ET AL) 3 July 2003 (2003-07-03)

D2 US 2007/083924 A1 (LU HONGQIAN K [US]) 12 April 2007 (2007-04-12)

1 The present application does not meet the criteria of Article 33(2) PCT, because the subject-matter of claims 1-20 is not new.

1.1 Independent claim 1 (as far as it is clear, see **Item VIII**) defines a method for filtering a packet, the method having two stages:

1) in the first stage, a first operation ('operator') is performed upon the packet, based on a first header field value;

2) in the second stage, a second operation ('transformation') is performed upon the packet, based on a second header field value.

Moreover, these two steps are interrelated in the sense that the criteria, with which the second header field value is compared during the second stage, are determined during the first stage.

Such a method is also disclosed in D1 (see the passages cited in the search report).

Present claim 1 is thus not new according to Art. 33(2) PCT.

1.2 The same reasoning applies, mutatis mutandis, to independent claims 11 and 20 which are, therefore, also not new.

1.3 Dependent claims 2-10 and 12-19 do not appear to contain any features which, in combination with the features of the claims to which they refer, meet the requirements of the PCT in respect of novelty and inventive step, see D1, D2 and the corresponding references cited in the search report.

1.4 It is further noted that a reasoning based on D2 would lead to very similar conclusions.

Re Item VIII

Certain observations on the international application

2 Claims 1-20 do not meet the requirements of Article 6 PCT for, at least, the following reasons:

- in claim 1, the expressions 'header field' and 'application header field', and especially how they differ from each other, are not clear;

- a similar remark applies to the expressions 'operator' and 'packet transformation function', respectively.

Similar observations apply to independent claims 11 and 20.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY
(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44*bis*)

Applicant's or agent's file reference 007742.00023	**FOR FURTHER ACTION**	See item 4 below
International application No. PCT/US2013/057502	International filing date *(day/month/year)* 30 August 2013 (30.08.2013)	Priority date *(day/month/year)* 22 October 2012 (22.10.2012)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant CENTRIPETAL NETWORKS, INC.		

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 *bis*.1(a).

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44*bis*.3(c) and 93*bis*.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44*bis* .2).

	Date of issuance of this report 28 April 2015 (28.04.2015)
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	Authorized officer Kihwan Moon e-mail: pt01.pct@wipo.int

Form PCT/IB/373 (January 2004)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2013/057502	30.08.2013	22.10.2012

International Patent Classification (IPC) or both national classification and IPC
INV. H04L29/06

Applicant
CENTRIPETAL NETWORKS, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Fax: +31 70 340 - 3016	see form PCT/ISA/210	Veen, Gerardus Telephone No. +31 70 340-3811

Form PCT/ISA/237 (Cover Sheet) (July 2009)

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

   a. (means)

      ☐ on paper

      ☐ in electronic form

   b. (time)

      ☐ in the international application as filed

      ☐ together with the international application in electronic form

      ☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	
	No:	Claims	1-20
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-20
Industrial applicability (IA)	Yes:	Claims	1-20
	No:	Claims	

2. Citations and explanations

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1 The following documents are referred to:

D1 EP 1 677 484 A2 (MICROSOFT CORP [US]) 5 July 2006 (2006-07-05)

D2 US 6 226 372 B1 (BEEBE TODD [US] ET AL) 1 May 2001 (2001-05-01)

2 The present application does not meet the criteria of Article 33(2) PCT, because the subject-matter of claims 1-20 is not new.

2.1 In the words of independent claim 1, D1 discloses:

'A method (column 4, line 13), comprising:

at each of one or more packet security gateways (c.4, l.16, 'enforcement engine') associated with a security policy management server (c.4, l.15, 'policy server'):

receiving a dynamic security policy from the security policy management server (c.4, l.16-19);

receiving packets associated with a network protected by each respective packet security gateway; and

performing, on a packet by packet basis, at least one of multiple packet transformation functions specified by the dynamic security policy on the packets (c.4, l.19-20, 'enforcing the security policies'), wherein performing the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets comprises performing at least one packet transformation function other than forwarding or dropping the packets (c.5, l.30-36)'.

Claim 1 is thus not new (Art. 33(2) PCT).

2.2 The same reasoning applies, mutatis mutandis, to independent claims 19 and 20 which are, therefore, also not new.

2.3 Dependent claims 2-18 do not contain any features which, in combination with the features of the claims to which they refer, meet the requirements of the PCT in respect of novelty and inventive step, see D1, D2 and the corresponding citations in the search report.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY
(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44*bis*)

Applicant's or agent's file reference 007742.00025	**FOR FURTHER ACTION**	See item 4 below
International application No. PCT/US2013/072566	International filing date *(day/month/year)* 02 December 2013 (02.12.2013)	Priority date *(day/month/year)* 11 January 2013 (11.01.2013)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant CENTRIPETAL NETWORKS, INC.		

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 *bis*.1(a).

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44*bis*.3(c) and 93*bis*.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44*bis* .2).

	Date of issuance of this report 14 July 2015 (14.07.2015)
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	Authorized officer Simin Baharlou e-mail: pt09.pct@wipo.int

Form PCT/IB/373 (January 2004)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY
(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2013/072566	02.12.2013	11.01.2013

International Patent Classification (IPC) or both national classification and IPC
INV. H04L29/06

Applicant
CENTRIPETAL NETWORKS, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Fax: +31 70 340 - 3016	see form PCT/ISA/210	Oliveira, Joel Telephone No. +31 70 340-3334

Form PCT/ISA/237 (Cover Sheet) (July 2009)

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

   a. (means)

      ☐ on paper

      ☐ in electronic form

   b. (time)

      ☐ in the international application as filed

      ☐ together with the international application in electronic form

      ☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	2, 3, 6-9, 11, 13, 14, 17-22, 24
	No:	Claims	1, 4, 5, 10, 12, 15, 16, 23
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-24
Industrial applicability (IA)	Yes:	Claims	1-24
	No:	Claims	

2. Citations and explanations

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

Reference is made to the following documents:

D1 EP 1 313 290 A1 (STONESOFT CORP [FI]) 21 May 2003 (2003-05-21)

D2 WO 2005/046145 A1 (ERICSSON TELEFON AB L M [SE]) 19 May 2005 (2005-05-19)

D3 US 2011/055916 A1 (AHN DAVID K [US]) 3 March 2011 (2011-03-03)

1 The present application does not meet the criteria of Article 33(2) PCT, because the subject-matter of claims **1, 12 and 23** is not new.

1.1 **D1** discloses a method comprising, at a network protection device **(abstract)**:

receiving a first rule set **(paragraph [0010], column3 lines 4-7)**;

receiving a second rule set **(paragraph [0010], column3 lines 4-7)**;

preprocessing the first rule set and the second rule set **(considered to be implicit from paragraphs [0010], [0013], [0040]: when a new set of rules is made available it must be made certain that they do not contain errors which could stop the filtering of the firewall)**;

configuring the network protection device to process packets in accordance with the first rule set **(paragraph [0010], column3 lines 13-18)**;

receiving packets **(column 6 lines 23-26)**;

processing a first portion of the packets in accordance with the first rule set **(paragraphs [0010], [0020])**;

reconfiguring the network protection device to process packets in accordance with the second rule set **(paragraphs [0010], [0024])**; and

processing a second portion of the packets in accordance with the second rule set **(paragraphs [0010], [0024])**.

1.2 The same reasoning applies, mutatis mutandis, to the subject-matter of the corresponding independent apparatus and computer-readable media claims **12 and 23**, which therefore are also considered not new.

1.3 Dependent claims **2-11, 13-22 and 24** do not contain any features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT in respect of novelty (for claims **4, 5, 10, 15, 16**) and/or inventive step (for claims **2, 3, 6, 7, 8, 9, 11, 13, 14, 17, 18, 19, 20, 21, 22, 24)** see passages cited in the Search Report.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
007742.00043		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2015/024691	7 April 2015 (07-04-2015)	16 April 2014 (16-04-2014)
Applicant		
CENTRIPETAL NETWORKS, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 6 sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language,** the international search was carried out on the basis of:
      ☒ the international application in the language in which it was filed
      ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).
   c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. ☐ **Certain claims were found unsearchable** (See Box No. II)

3. ☒ **Unity of invention is lacking** (see Box No III)

4. With regard to the **title,**
   ☒ the text is approved as submitted by the applicant
   ☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**
   ☒ the text is approved as submitted by the applicant
   ☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings,**
   a. the figure of the **drawings** to be published with the abstract is Figure No. 11
      ☐ as suggested by the applicant
      ☐ as selected by this Authority, because the applicant failed to suggest a figure
      ☒ as selected by this Authority, because this figure better characterizes the invention
   b. ☐ none of the figures is to be published with the abstract

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2015/024691

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-9

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/024691

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
ADD. H04L29/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2006/136987 A1 (OKUDA MASATO [JP]) 22 June 2006 (2006-06-22) paragraph [0028] - paragraph [0030]; figures 1,21 paragraphs [0033], [0036], [0040], [0093], [0095], [0135] -----	1-9
X	US 2007/240208 A1 (YU MING-CHE [TW] ET AL) 11 October 2007 (2007-10-11) abstract paragraphs [0021], [0024] - paragraph [0026] paragraph [0033] - paragraph [0036] paragraph [0039] - paragraph [0040] ----- -/--	1-9

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
3 July 2015	16/09/2015

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Barla Harter, I

1

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2006/146879 A1 (ANTHIAS TEFCROS [US] ET AL) 6 July 2006 (2006-07-06) paragraph [0074] - paragraph [0076] paragraph [0112] - paragraph [0119] paragraphs [0207], [0208], [0240] -----	1-9
A	US 8 306 994 B2 (KENWORTHY STACY [US]) 6 November 2012 (2012-11-06) abstract; figures 4,6 column 2 - column 4 column 6 - column 9 -----	1-9

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2015/024691

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006136987 A1	22-06-2006	JP 2006174350 A	29-06-2006
		US 2006136987 A1	22-06-2006
US 2007240208 A1	11-10-2007	NONE	
US 2006146879 A1	06-07-2006	CN 101099345 A	02-01-2008
		EP 1834453 A2	19-09-2007
		US 2006146879 A1	06-07-2006
		WO 2006073740 A2	13-07-2006
US 8306994 B2	06-11-2012	US 6317837 B1	13-11-2001
		US 2002049899 A1	25-04-2002
		US 2010242098 A1	23-09-2010
		US 2013061294 A1	07-03-2013

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-9

   A method for packet filtering based on application-layer packet header information

   ---

2. claims: 10-18

   A method for selective packet digest logging

   ---

3. claims: 19, 20

   A method for security policy update and management

Espacenet

Bibliographic data: EP1677484 (A2) — 2006-07-05

Method and system for distributing security policies

No documents available for this priority number.

Inventor(s): PALEOLOGU EMANUEL [US]; YOUNGBLUT ERIC E [US]; IVANOV MAXIM A [US]; NAGAMPALLI NARASIMHA RAO S S [US]; SHETH SACHIN C [US]; KOTI SHIRISH R [US]; LIN YUN [US] ± (PALEOLOGU, EMANUEL, ; YOUNGBLUT, ERIC E, ; IVANOV, MAXIM A, ; NAGAMPALLI, NARASIMHA RAO, ; SHETH, SACHIN C, ; KOTI, SHIRISH R, ; LIN, YUN, ; NAGAMPALLI, NARASIMHA RAO S.S)

Applicant(s): MICROSOFT CORP [US] ± (MICROSOFT CORPORATION)

Classification: - international: ***H04L29/06***
- cooperative: **H04L63/0218**; **H04L63/0263**; **H04L63/20**

Application number: EP20050110420 20051107

Priority number(s): US20040993688 20041119

Also published as: EP1677484 (A3) US2006129808 (A1) US7509493 (B2) US2009172774 (A1) US7831826 (B2) more

Abstract of EP1677484 (A2)

A method and system for distributing and enforcing security policies is provided. A firewall agent executing at a host computer system that is to be protected receives security policies for the enforcement engines responsible for enforcing the security policies on the host computer system. A security policy has rules that each provide a condition and action to be performed when the condition is satisfied. A rule also has a rule type that is used by the distribution system to identify the security components that are responsible for enforcing the rules. To distribute the security policies that have been received at a host computer system, the firewall agent identifies to which enforcement engine a rule applies based in part on rule type. The firewall agent then distributes the rule to the identified enforcement engine, which then enforces the rule.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 677 484 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
05.07.2006 Bulletin 2006/27

(51) Int Cl.:
H04L 29/06 *(2006.01)*

(21) Application number: **05110420.6**

(22) Date of filing: **07.11.2005**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR MK YU

(30) Priority: **19.11.2004 US 993688**

(71) Applicant: **MICROSOFT CORPORATION**
Redmond, Washington 98052-6399 (US)

(72) Inventors:
- **Paleologu, Emanuel,**
  cO Microsoft Corporation
  Redmond,
  WA 98052 (US)
- **Youngblut, Eric E.,**
  c/o Microsoft Corporation
  Redmond,
  WA 98052 (US)
- **Ivanov, Maxim A.,**
  c/o Microsoft Corporation
  Redmond,
  WA 98052 (US)
- **Nagampalli, Narasimha Rao S.S.,**
  c/o Microsoft Corp
  Redmond,
  WA 98052 (US)
- **Sheth, Sachin C.,**
  c/o Microsoft Corporation
  Redmond,
  WA 98052 (US)
- **Koti, Shirish R.,**
  c/o Microsoft Corporation
  Redmond,
  WA 98052 (US)
- **Lin, Yun,**
  c/o Microsoft Corporation
  Redmond,
  WA 98052 (US)

(74) Representative: **Schuster, Thomas**
Grünecker, Kinkeldey,
Stockmair & Schwanhäusser
Anwaltssozietät
Maximilianstrasse 58
D-80538 München (DE)

(54) Method and system for distributing security policies

(57) A method and system for distributing and enforcing security policies is provided. A firewall agent executing at a host computer system that is to be protected receives security policies for the enforcement engines responsible for enforcing the security policies on the host computer system. A security policy has rules that each provide a condition and action to be performed when the condition is satisfied. A rule also has a rule type that is used by the distribution system to identify the security components that are responsible for enforcing the rules. To distribute the security policies that have been received at a host computer system, the firewall agent identifies to which enforcement engine a rule applies based in part on rule type. The firewall agent then distributes the rule to the identified enforcement engine, which then enforces the rule.

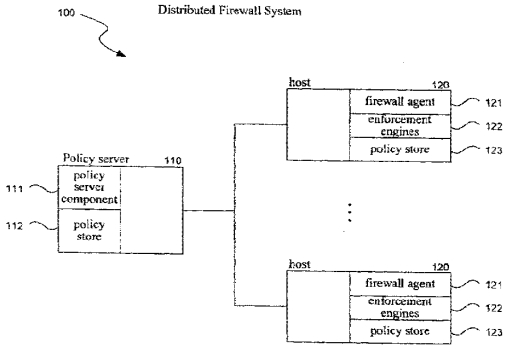


FIG. 1

EP 1 677 484 A2

Printed by Jouve, 75001 PARIS (FR)

Description

TECHNICAL FIELD

[0001] The described technology relates generally to systems that prevent the exploitation of vulnerabilities of computer systems.

BACKGROUND

[0002] Although the Internet has had great successes in facilitating communications between computer systems and enabling electronic commerce, the computer systems connected to the Internet have been under almost constant attack by hackers seeking to disrupt their operation. Many of the attacks seek to exploit vulnerabilities of software systems including application programs or other computer programs executing on those computer systems. Developers of software systems and administrators of computer systems of an enterprise go to great effort and expense to identify and remove vulnerabilities. Because of the complexity of software systems, however, it is virtually impossible to identify and remove all vulnerabilities before software systems are released. After a software system is released, developers can become aware of vulnerabilities in various ways. A party with no malicious intent may identify a vulnerability and may secretly notify the developer so the vulnerability can be removed before a hacker identifies and exploits it. If a hacker identifies a vulnerability first, the developer may not learn of the vulnerability until it is exploited—sometimes with disastrous consequences.

[0003] Regardless of how a developer finds out about a vulnerability, the developer typically develops and distributes to system administrators "patches" or updates to the software system that remove the vulnerability. If the vulnerability has not yet been exploited (e.g., might not be known to hackers), then a developer can design, implement, test, and distribute a patch in a disciplined way. If the vulnerability has already been widely exposed, then the developer may rush to distribute a patch without the same care that is used under normal circumstances. When patches are distributed to the administrators of the computer systems, they are responsible for scheduling and installing the patches to remove the vulnerabilities.

[0004] Unfortunately, administrators often delay the installation of patches to remove vulnerabilities for various reasons. When a patch is installed, the software system and possibly the computer system on which it is executing may need to be shut down and restarted. If the vulnerability is in a software system that is critical to the success of an organization, then the administrator needs to analyze the tradeoffs of keeping the software system up and running with its associated risk of being attacked and of shutting down a critical resource of the enterprise to install the patch. Some administrators may delay the installation of the patch because they fear that, because of a hasty distribution, it might not be properly tested and have unintended side effects. If the patch has an unintended side effect, then the software system, the computer system, or some other software component that is impacted by the patch may be shut down by the patch itself. Administrators need to factor in the possibility of an unintended side effect when deciding whether to install a patch. These administrators may delay installing a patch until experience by others indicates that there are no serious unintended side effects.

[0005] Intrusion detection systems have been developed that can be used to identify whether an attempt is being made to exploit a known vulnerability that has not yet been patched. These intrusion detection systems can be used to prevent exploitations of newly discovered vulnerabilities for which patches have not yet been developed or installed. These intrusion detection systems may define a "signature" for each way a vulnerability can be exploited. For example, if a vulnerability can be exploited by sending a certain type of message with a certain attribute, then the signature for that exploitation would specify that type and attribute. When a security enforcement event occurs, such as the receipt of a message, the intrusion detection system checks its signatures to determine whether any match the security enforcement event. If so, the intrusion detection system may take action to prevent the exploitation, such as dropping the message.

[0006] Signatures for newly discovered exploitations of vulnerabilities can be created in different ways. Developers of intrusion detection systems may create and distribute new signatures when they become aware of new exploitations. An administrator can then install the new signatures to prevent the exploitation. A developer may not, however, provide signatures for all known exploitations. For example, the vulnerability may be in a special-purpose application program that the developer does not support. To prevent exploitation of such a vulnerability, intrusion detection systems may allow administrators to create their own signatures.

[0007] A set of one or more signatures may be considered a security policy. Developers of intrusion detection systems may provide various security policies. For example, a developer may provide one security policy that defines signatures of vulnerabilities of an operating system and many other security policies that are specific to an application or a class of applications. Similarly, an administrator may define a security policy that is specific to custom applications used by the enterprise.

[0008] Because intrusions can occur at various points within an operating system or an application, intrusion detection systems have been developed to detect and prevent exploitation of vulnerabilities at each of these points. For example, an intrusion detection system may be developed to prevent exploitation of vulnerabilities that can be detected at the network layer of a communication protocol, and another intrusion detection system may be developed to prevent exploitation of vulnerabilities that can be detected when a file is accessed. Each

EX1002
CISCO SYSTEMS, INC. / Page 272 of 1453

developer of an intrusion detection system can provide their own implementation and security policies that need to be distributed to each computer system to be protected. In addition, any updates to the implementation or security policies also need to be distributed to the computer systems to be protected.

[0009] The distribution and updating of security policies for an enterprise with a large number of computer systems can be a complex and time-consuming task. Each security policy needs to be provided to each computer system and then to the appropriate intrusion detection system that is installed on the computer system. Since the developers of intrusion detection systems typically develop their systems independent of each other, each intrusion detection system may have a proprietary mechanism for defining and distributing security policies. A system administrator of an enterprise may need to be aware of each of these mechanisms to use the intrusion detection system effectively.

[0010] It would be desirable to have a mechanism that would provide a uniform way to distribute security policies received at a computer system to components responsible for enforcing the security policies.

SUMMARY

[0011] A method and system for distributing and enforcing security policies is provided. A distributed firewall system includes a policy server component, firewall agents, and enforcement engines. A firewall agent executing at a host computer system that is to be protected receives from the policy server component security policies for the enforcement engines responsible for enforcing the security policies on the host computer system. A security policy has rules that each provide a condition and action to be performed when the condition is satisfied. A rule also has a rule type (also referred to as a security type) that is used by the firewall agent to identify the enforcement engines that are responsible for enforcing the rules. The firewall agent may distribute the security policies to enforcement engines executing in user mode and in kernel mode. The enforcement engines may provide a layered approach to security enforcement. To distribute the security policies that have been received at a host computer system, the firewall agent identifies to which enforcement engine a rule applies based in part on rule type. The firewall agent then distributes the rule to the identified enforcement engine, which then enforces the rule.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] Figure 1 is a block diagram that illustrates the distributed firewall system in one embodiment.

[0013] Figure 2 is a block diagram that illustrates the components of the portions of the distributed firewall system executing on a host computer system in one embodiment.

[0014] Figure 3 is a flow diagram that illustrates the processing of the distribute policy component of the firewall agent in one embodiment.

[0015] Figure 4 is a flow diagram that illustrates the processing of the flow manager component in one embodiment.

[0016] Figure 5 is a flow diagram that illustrates the processing of an enforcement engine for a specific layer in one embodiment.

DETAILED DESCRIPTION

[0017] A method and system for distributing and enforcing security policies is provided. A distributed firewall system includes a policy server component, firewall agents, and enforcement engines. A firewall agent executing at a host computer system that is to be protected receives from a policy server security policies for the enforcement engines responsible for enforcing the security policies on the host computer system. A security policy has an execution scope and associated rules. An execution scope defines the attributes of a process or application to which the associated rules are to be applied. A rule provides a condition and action to be performed when the condition is satisfied. A rule also has a rule type (also referred to as a security type) that is used by the firewall agent to identify the enforcement engines that are responsible for enforcing the rules. The firewall agent may distribute the security policies to enforcement engines executing in user mode and in kernel mode. The enforcement engines may provide a layered approach to a distributed firewall. For example, enforcement engines may be installed on a host computer system to prevent intrusions at various layers of the ISO 7-layer reference model. The network layer, the transport layer, and the session layer may each have an enforcement engine that is developed to detect attempted intrusions at that layer. To distribute the security policies that have been received at a host computer system, the firewall agent identifies to which enforcement engine a rule applies based in part on rule type. The firewall agent then distributes the rule to the identified enforcement engine, which then enforces the rule. Upon receiving a rule, an enforcement engine may distribute the rule to its subcomponents as appropriate. For example, the firewall agent may distribute all rules destined for kernel-mode enforcement engines to a single kernel-mode security component that then distributes the rules to the enforcement engines. In this way, the distributed firewall system provides a single mechanism for distributing rules of security policies to the enforcement engines providing different layers of protection for a host computer system.

[0018] In one embodiment, a security policy includes rules that specify conditions, actions, and optionally exceptions. For example, a rule may indicate that an application may not receive messages on any network port other than port 80. The condition of the rule may be satisfied when a message is received on a network port

EX1002
CISCO SYSTEMS, INC. / Page 273 of 1453

other than port 80, and the action may result in the message being discarded. As another example, a rule may indicate that when an application attempts to send a message on network port 80, authorization is to be solicited from a user of the computing system on which the rule is enforced. The rules may be categorized into rule or security types based on their behavior. For example, rules with a network security type may be directed to security enforcement for network traffic. Each security type may have its own security component for enforcing rules of that security type. Languages for specifying security policies is described in U.S. Patent Application No. 10/882,438, entitled "Languages for Expressing Security Policies" and filed on July 1, 2004, which is hereby incorporated by reference.

[0019] The condition, action, and exception of the rules may be specified as expressions. A rule may be semantically expressed as "IF conditions THEN actions EXCEPT exceptions." Conditions of a rule are expressions of circumstances under which security enforcement actions of the rule are to be performed. An action is an expression of activity to be performed when the condition is satisfied. A rule may have multiple actions. An exception is an expression of when the actions may not be performed even though the condition is satisfied. A condition may be either static or dynamic. A static condition is one which refers, for example, to a hard-coded list of files. A dynamic condition is one which, for example, performs a query to determine a list of files matching a provided criterion. Security enforcement actions may include allowing a request that caused the security enforcement event, denying the request, soliciting input from a user, notifying the user, and so on. Other rule constructs are also possible. As an example, an "else" construct could be added to perform alternate actions when a condition is false.

[0020] Figure 1 is a block diagram that illustrates the distributed firewall system in one embodiment. An enterprise may have a network system 100 that includes a policy server computer system 110 and host computer systems 120. A system administrator uses a policy server component 111 of the policy server computer system to prepare and distribute security policies stored in a security policy store 112 to the host computer systems. Each host computer system includes a firewall agent 121, enforcement engines 122, and a policy store 123. The firewall agent provides a central mechanism through which a host computer system receives and distributes security policies to the enforcement engines of that host computer system. Upon receiving a security policy from the policy server computer system, the firewall agent of a host computer system stores the security policy in the policy store. The firewall agent then processes the security policies on a rule-by-rule basis and provides the rules to the appropriate enforcement engine. The firewall agent may combine various security policies, order the rules of the security policies, and dynamically notify the enforcement engines of changes to security policies or system configurations that will affect the enforcement of the security policies. Such combining, ordering, and notifying is described in U.S. Patent Application No. 10/966,800, entitled "Method and System for Merging Security Policies" and filed on October 14, 2004, which is hereby incorporated by reference. The enforcement engines then enforce the rules by applying them to network events. The enforcement engines may provide various type of security enforcement. An enforcement engine may detect an attempt to perform a certain behavior and block the attempt. For example, an application that is infected with a virus may attempt to delete certain files of the operating system. A security engine executing in the same process space as the application may detect and block the attempt to delete the file. A security engine for performing behavior blocking is described in U.S. Patent Application No. 10/832,798, entitled "A Method and System for Enforcing a Security Policy via a Security Virtual Machine" and filed on April 27, 2004, which is hereby incorporated by reference. The enforcement engines may be adapted to apply rules to network events of various protocols, such as IP, ICMP, TCP, FTP, DNS, HTTP, RPC, and so on. Techniques preventing exploitation of vulnerabilities are described in U.S. Patent Application No. 10/955,963, entitled "Method and System for Filtering Communications to Prevent Exploitation of a Software Vulnerability" and filed on September 30, 2004, which is hereby incorporated by reference.

[0021] Figure 2 is a block diagram that illustrates the components of the distributed firewall system executing on a host computer system in one embodiment. The host computer system includes firewall agent components 220, kernel-mode components 230, and application user-mode components 240. The firewall agent components include a receive policy component 221, a parse policy component 222, and a distribute policy component 223. The firewall agent components also include a policy store 224 and a configuration manager 225. The receive policy component receives security policies provided by the policy server computer system and stores the policies in the policy store. The parse policy component retrieves the policies from the policy store and converts them to a lower-level language for processing by the enforcement engines. The distribute policy component receives the parsed security policies and distributes the rules of the security policies to the appropriate enforcement engines. The configuration manager provides configuration information for use in determining which rules should be distributed to which enforcement engines based on the current configuration of the host computer system.

[0022] The kernel-mode components include enforcement engines 231, flow manager components 233, and protocol hooks 234. The components may be layered from layer 0 to layer N, which may correspond to various layers of the ISO 7-layer reference model. Each layer may have an associated protocol hook, flow manager, and enforcement engine that is specific to the layer, parses network events specific to that layer, and enforces the

EX1002
CISCO SYSTEMS, INC. / Page 274 of 1453

rules provided by the firewall agent to that layer. The rules for each layer are stored in a rule store 232 that may be specific for that layer. The flow manager components are responsible for intercepting network events and invoking the corresponding enforcement engine to enforce the rules. Each flow manager component receives network events from the corresponding protocol hook that is responsible for detecting network events at the corresponding layer. The application user-mode components may be provided as a dynamic link library that links into an application for providing layered security in a manner that is similar in overall architecture to the kernel-mode components.

[0023] The computing device on which the distribution system is implemented may include a central processing unit, memory, input devices (e.g., keyboard and pointing devices), output devices (e.g., display devices), and storage devices (e.g., disk drives). The memory and storage devices are computer-readable media that may contain instructions that implement the distribution system. In addition, the data structures and message structures may be stored or transmitted via a data transmission medium, such as a signal on a communications link. Various communication links may be used, such as the Internet, a local area network, a wide area network, a point-to-point dial-up connection, a cell phone network, and so on.

[0024] The distribution system may be implemented in various operating environments that include personal computers, server computers, hand-held or laptop devices, multiprocessor systems, microprocessor-based systems, programmable consumer electronics, digital cameras, network PCs, minicomputers, mainframe computers, distributed computing environments that include any of the above systems or devices, and so on. The host computer systems may be cell phones, personal digital assistants, smart phones, personal computers, programmable consumer electronics, digital cameras, and so on.

[0025] The distribution system may be described in the general context of computer-executable instructions, such as program modules, executed by one or more computers or other devices. Generally, program modules include routines, programs, objects, components, data structures, and so on that perform particular tasks or implement particular abstract data types. Typically, the functionality of the program modules may be combined or distributed as desired in various embodiments.

[0026] Figure 3 is a flow diagram that illustrates the processing of the distribute policy component of the firewall agent in one embodiment. Upon receiving policies from the parse policy component, the component identifies the enforcement engines to which the rules apply and distributes the rules to the identified enforcement engines. In blocks 301-307, the component loops selecting the security policies. In block 301, the component selects the next security policy. In decision block 302, if all the security policies have already been selected, then the component completes, else the component continues at block 303. In blocks 303-307, the component loops processing each rule within the selected security policy. In block 303, the component selects the next rule of the selected security policy. In decision block 304, if all the rules of the selected security policy have already been selected, then the component loops to block 301 to select the next security policy, else the component continues at block 305. In block 305, the component identifies the rule type (or security type) of the selected security rule. In block 306, the component identifies the enforcement engine that is responsible for enforcing the rules of the identified rule type. In block 307, the component provides the selected rule to the identified component and then loops to block 303 to select the next rule of the selected security policy.

[0027] Figure 4 is a flow diagram that illustrates the processing of the flow manager component in one embodiment. The flow manager component is passed a network event and invokes the appropriate enforcement engine for processing the network event. The flow manager component may be implemented as a separate flow manager for each layer that processes network events only for that layer or may be implemented as a single flow manager component that process network events for all layers. In this illustrated embodiment, the flow manager component processes all network events for all layers. In decision blocks 401-403, the component identifies the layer to which a network event applies. The component then invokes the associated enforcement engine for that layer in blocks 411-413. The component then completes. The flow manager may maintain a separate flow for each network connection. The enforcement engines and flow managers may be specific to the layer and the protocol implemented by the layer. For example, when a connection uses the Transmission Control Protocol ("TCP") or the User Datagram Protocol ("UDP") at the packet layer, the flow manager invokes the enforcement engine that is appropriate for the protocol. The invoked enforcement engines may instantiate data structures for tracking state information from one invocation to the next. Each application that is protected by user-mode enforcement engine may also have a flow manager with a separate flow for each connection.

[0028] Figure 5 is a flow diagram that illustrates the processing of an enforcement engine for a specific layer in one embodiment. The enforcement engine, which is a component of the distributed firewall system, is provided a network event, identifies the rules to apply to the event, determines whether the conditions of the rules are satisfied, and if so, performs the action associated with the rule. In blocks 501-504, the component loops selecting each rule associated with the layer of the enforcement engine. In block 501, the component selects the next rule. In decision block 502, if all the rules have already been selected, then the component completes, else the component continues at block 503. In decision block 503, if the condition of the rule is satisfied, then the component continues at block 504, else the component loops to block

EX1002
CISCO SYSTEMS, INC. / Page 275 of 1453

501 to select the next rule. In block 504, the component performs the action associated with the rule and then loops to block 501 to select the next rule. Each enforcement engine may be adapted to process the network events and rules that are appropriate to its layer. For example, an enforcement engine for the network layer may parse network packets and enforce rules related to the network packets. An enforcement engine for the application layer may detect unauthorized attempts to access or modify files relating to that application.

[0029] From the foregoing, it will be appreciated that specific embodiments of the distributed firewall system have been described herein for purposes of illustration, but that various modifications may be made without deviating from the spirit and scope of the invention. Accordingly, the invention is not limited except as by the appended claims.

Claims

1. A method in a computer system for distributing rules of security policies to enforcement engines for enforcing the security policies, the method comprising:

   providing at the computer system enforcement engines that implement different layers of security enforcement;
   receiving and storing at the computer system security policies having rules, each rule having a rule type;
   under control of a firewall agent executing on the computer system,
   retrieving the stored security policies; and
   for rules of a retrieved security policy,
   identifying an enforcement engine to which a rule applies based on the rule type of the rule; and
   providing the rule to the identified enforcement engine; and under control of the enforcement engines, enforcing the rules provided to the enforcement engine by the firewall agent,
   wherein the firewall agent provides a mechanism for distributing the rules to multiple enforcement engines of the computer system.

2. The method of claim 1 wherein the security policies are received from policy computer system that distributes the security policies for multiple computer systems.

3. The method of claim 1 wherein the enforcement engines provide a layered firewall.

4. The method of claim 1 wherein the enforcement engines include a behavior blocking security component.

5. The method of claim 1 wherein an enforcement engine includes subcomponents and wherein upon being provided with a rule, the enforcement engine provides the rule to a subcomponent.

6. The method of claim 1 wherein at least one enforcement engine executes in kernel mode and at least one enforcement engine executes in user mode.

7. The method of claim 1 wherein the firewall agent includes a user-mode subcomponent and a kernel-mode subcomponent, and the user-mode subcomponent distributes rules to the kernel-mode subcomponent for providing the rules to enforcement engines that execute in kernel mode.

8. The method of claim 1 wherein a flow manager component intercepts network events at the various layers and invokes an enforcement engine associated with a layer to enforce the rules for that layer.

9. The method of claim 8 wherein a single flow manager component handles network events from multiple layers,

10. The method of claim 8 wherein a flow manager component handles network events from only one layer.

11. The method of claim 1 wherein enforcement engines provide for security at various layers of a network protocol stack.

12. The method of claim 11 wherein layers of different enforcement engines are used for different connections.

13. A computer system architecture for distributing security policies, the architecture comprising:

   a policy server computer system for establishing security policies, the security policies having rules with rule types, and for providing the security policies to host computer systems for enforcement of the security policies at the host computer systems; and
   multiple host computer systems that include:

      enforcement engines for enforcing a type of security at the host computer system; and
      a firewall agent that receives the security policies from the policy server computer system, identifies the enforcement engine to which the rules apply based on rule type and enforcement engine type, and provides the rules to the identified enforcement engines for enforcement of the security policies.

EX1002
CISCO SYSTEMS, INC. / Page 276 of 1453

14. The computer system architecture of claim 13 wherein the enforcement engines are layered so that when one enforcement engine determines that the rules provided to it do not to apply to a network event, another enforcement engine determines whether the rules provided to it apply to the network event.

15. The computer system architecture of claim 14 wherein the layers include a protocol interception hook and an enforcement engine.

16. The computer system architecture of claim 13 wherein the firewall agent distributes rules to enforcement engines executing in user mode.

17. The computer system architecture of claim 13 wherein the firewall agent distributes rules to enforcement engines executing in kernel mode.

18. The computer system architecture of claim 13 wherein the enforcement engines are layered and including a flow manager component that handles network events at each layer and invokes an enforcement engine of the layer to enforce the rules of that layer on the network event.

19. The computer system architecture of claim 18 wherein the flow manager component handles network events for multiple layers.

20. The computer system architecture of claim 18 wherein the flow manager component handles network events for a single layer.

21. A host computer system for distributing rules of security policies to enforcement engines for enforcing the security policies of the host computer system, comprising:

multiple enforcement engines that implement different layers of firewall security enforcement at the host computer system by receiving and enforcing rules of security policies;
a component that receives at the host computer system security policies having rules, each rule having a rule type; and
a component that identifies enforcement engines to which a rule applies based on the rule type of the rule and that provides the rule to the identified security component;
wherein a mechanism is provided for distributing the rules to the layered enforcement engines of the host computer system.

22. The computer system of claim 21 wherein the security policies are received from a policy computer system that distributes the security policies for multiple host computer systems.

23. The computer system of claim 21 wherein the enforcement engine includes a behavior blocking security component.

24. The computer system of claim 21 wherein an enforcement engine includes subcomponents and wherein upon being provided with a rule, the enforcement engine provides the rule to a subcomponent.

25. The computer system of claim 21 wherein at least one enforcement engine executes in kernel mode and at least one enforcement engine executes in user mode.

26. The computer system of claim 21 wherein the component that provides the rules to the enforcement engines includes a user-mode subcomponent and a kernel-mode subcomponent, and the user-mode subcomponent distributes rules to the kernel-mode subcomponent for providing the rules to enforcement engine that execute in kernel mode.

27. The computer system of claim 21 including a flow manager component that intercepts network events at the various layers and invokes an enforcement engine associated with a layer to enforce the rules for that layer.

28. The computer system of claim 27 wherein a single flow manager component handles network events from multiple layers.

29. The computer system of claim 27 wherein a flow manager component handles network events from only one layer.

30. A computer-readable medium containing instructions for controlling a host computer system to distribute security policies to enforcement engines for enforcing the security policies, by a method comprising:

receiving and storing at the host computer system security policies having rules, each rule having a rule type;
under control of a firewall agent executing on the host computer system,
retrieving the stored security policies; and
for rules of a retrieved security policy,
identifying an enforcement engine to which a rule applies based on the rule type of the rule; and
providing the rule to the identified enforcement engine; and under control of the enforcement engines, enforcing the rules provided to the enforcement engines by the distribution component.

EX1002
CISCO SYSTEMS, INC. / Page 277 of 1453

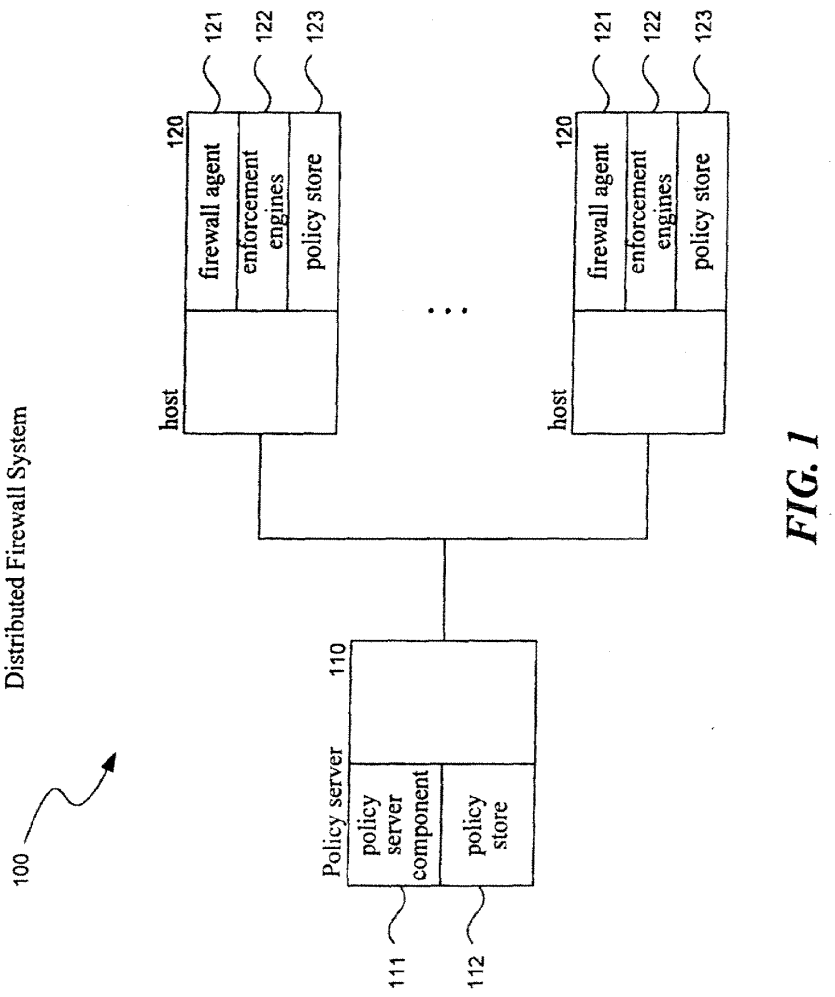

Distributed Firewall System
100
Policy server
110
policy server component
policy store
111
112
host
120
firewall agent
enforcement engines
policy store
121
122
123

FIG. 1

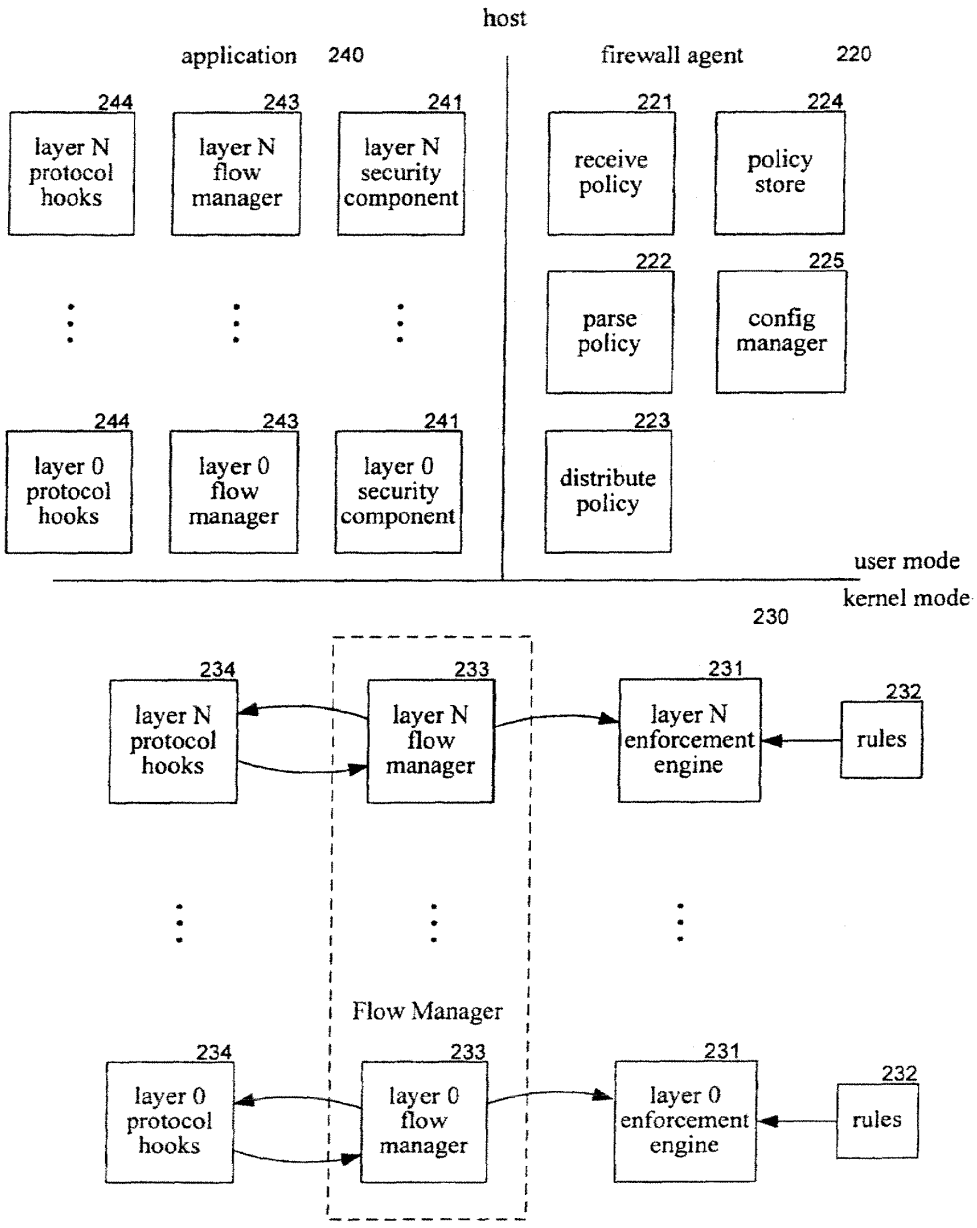

host
application 240
firewall agent 220
244
layer N protocol hooks
243
layer N flow manager
241
layer N security component
221
receive policy
224
policy store
222
parse policy
225
config manager
244
layer 0 protocol hooks
243
layer 0 flow manager
241
layer 0 security component
223
distribute policy
user mode
kernel mode
230
234
layer N protocol hooks
233
layer N flow manager
231
layer N enforcement engine
232
rules
Flow Manager
234
layer 0 protocol hooks
233
layer 0 flow manager
231
layer 0 enforcement engine
232
rules

FIG. 2

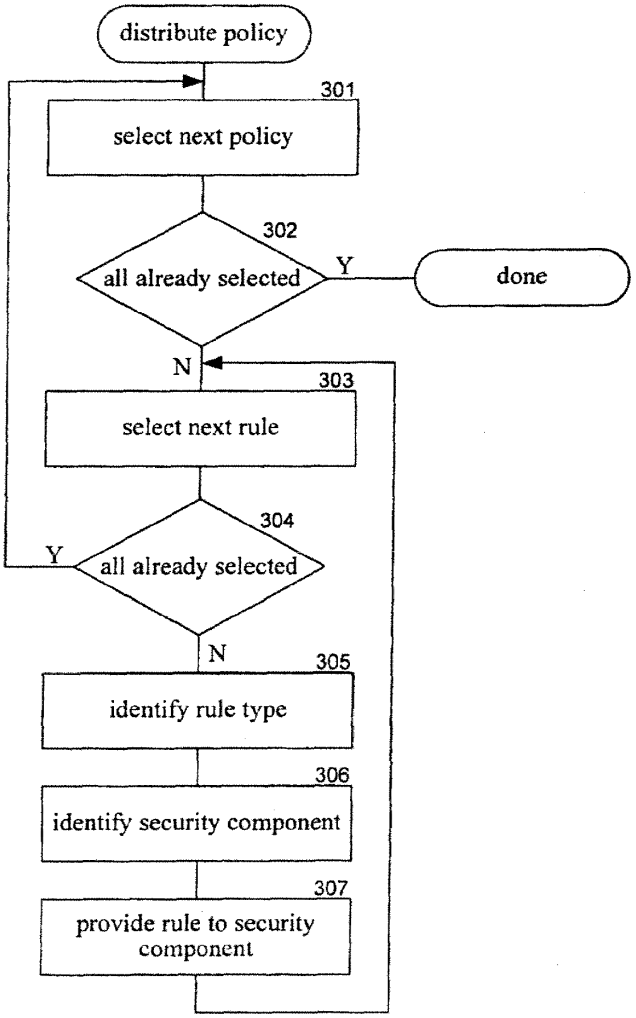


FIG. 3

EX1002
CISCO SYSTEMS, INC. / Page 280 of 1453

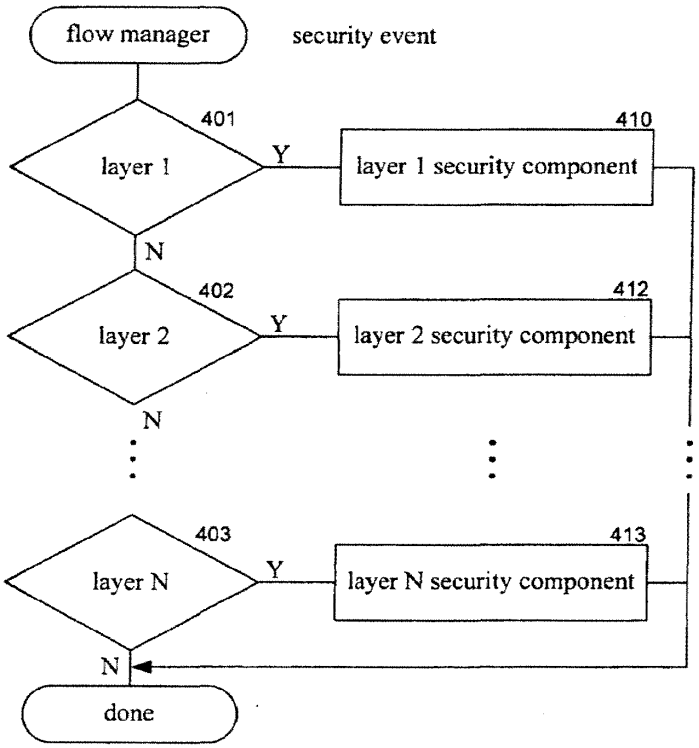


FIG. 4

EX1002
CISCO SYSTEMS, INC. / Page 281 of 1453

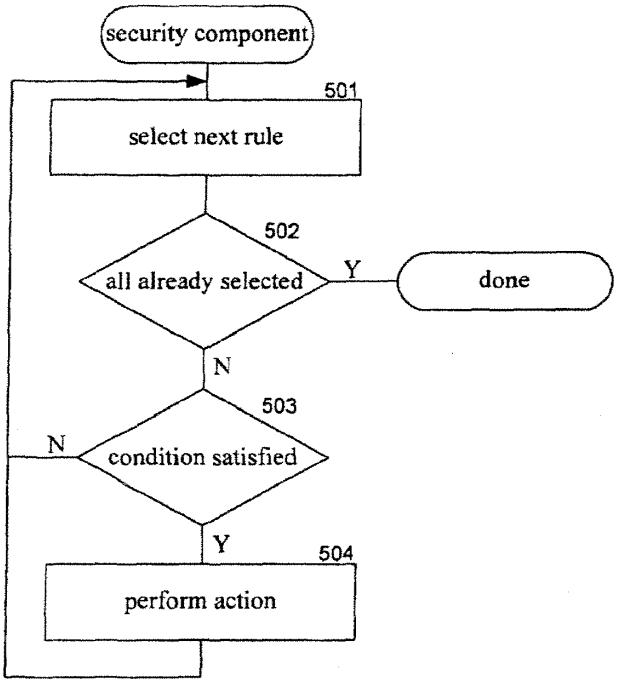


FIG. 5

EX1002
CISCO SYSTEMS, INC. / Page 282 of 1453

Espacenet

Bibliographic data: EP1313290 (A1) — 2003-05-21

A personal firewall with location dependent functionality

No documents available for this priority number.

Inventor(s): SYVAENNE TUOMO [FI] ± (SYVAENNE, TUOMO)

Applicant(s): STONESOFT CORP [FI] ± (STONESOFT CORPORATION)

Classification: **- international:** ***H04L29/06;*** (IPC1-7): H04L29/06
- cooperative: **H04L63/0227**; **H04L63/0263**; **H04L63/107**

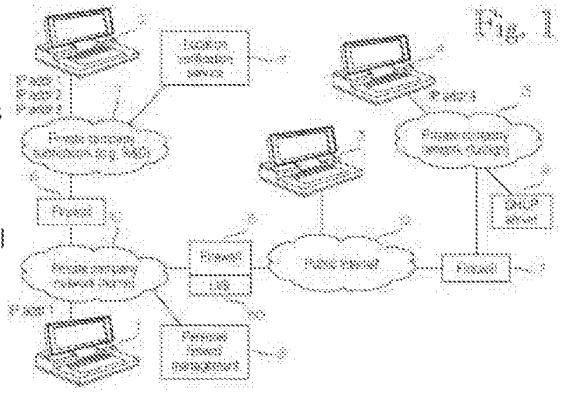
Application number: EP20020102581 20021114

Priority number (s): US20010988356 20011119

Also published as: EP1313290 (B1) US2003097590 (A1) US7325248 (B2) DE60216218 (T2) AT346446 (T)

Abstract of EP1313290 (A1)

A computer device is provided with a local security mechanism, a personal firewall, for protecting the computer device from attacks from a foreign network, in addition to or instead of a firewall in the internal network which protects the computer when connected to a home network. The personal firewall is provided with different sets of security rules for the home network and foreign networks. The personal firewall is arranged to detect its current location, i.e. determine to which network it is connected to at each particular moment. The personal firewall activates one of the given sets of security rules according to the detected current location of the computer device, i.e. the personal firewall automatically uses the security rules predefined for the network to which the computer device is connected at each particular moment.; Upon detecting a change in the location, the personal firewall immediately adapts to use security rules predefined for the new location.



(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 313 290 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
21.05.2003 Bulletin 2003/21

(51) Int Cl.[7]: **H04L 29/06**

(21) Application number: **02102581.2**

(22) Date of filing: **14.11.2002**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **19.11.2001 US 988356**

(71) Applicant: **Stonesoft Corporation**
00210 Helsinki (FI)

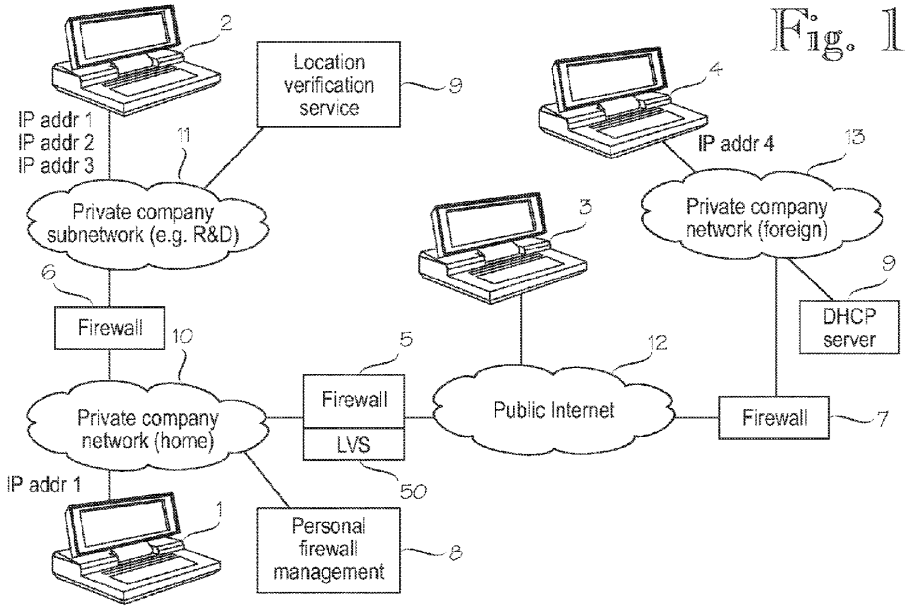
(72) Inventor: **Syvänne, Tuomo**
Fin-01450, Vantaa (FI)

(74) Representative: **Äkräs, Tapio Juhani**
Kolster Oy Ab,P.O. Box 148,
Iso Roobertinkatu 23
00121 Helsinki (FI)

(54) A personal firewall with location dependent functionality

(57) A computer device is provided with a local security mechanism, a personal firewall, for protecting the computer device from attacks from a foreign network, in addition to or instead of a firewall in the internal network which protects the computer when connected to a home network. The personal firewall is provided with different sets of security rules for the home network and foreign networks. The personal firewall is arranged to detect its current location, i.e. determine to which network it is connected to at each particular moment. The personal firewall activates one of the given sets of security rules according to the detected current location of the computer device, i.e. the personal firewall automatically uses the security rules predefined for the network to which the computer device is connected at each particular moment. Upon detecting a change in the location, the personal firewall immediately adapts to use security rules predefined for the new location.

Fig. 1



EP 1 313 290 A1

Printed by Jouve, 75001 PARIS (FR)

Description

Field of the Invention

[0001] The present invention relates to network security and, more particularly, to personal firewalls.

Background of the Invention

[0002] Traditionally, a firewall is considered as a set of components forming a gateway between two or more networks. Thus, a firewall has been a gateway which operates at the same time as a connector and a separator between the networks in a sense that the firewall keeps track of the traffic that passes through it from one network to another and restricts connections and packets that are defined as unwanted by the administrator of the system. Physically a firewall is a machine with appropriate software to do the tasks assigned to it. It can be a router, a personal computer (PC), or any other device that can be used for such purposes. Although firewalls are mostly used to connect Local Area Networks (LANs), i.e. internal networks, to the Internet and to protect against attackers or undesired traffic in general, they may also be used to separate and connect different segments of internal network for security purposes. The advantages of having a firewall are numerous. A firewall secures the network and can be used as a tool for monitoring the traffic especially from the outside to the inside of the network guarded by a firewall. Because all traffic intended for the internal network must pass through the firewall, most of the network security actions and policies can be concentrated in this particular point. This is of course a cost and administrative advantage.

[0003] Nowadays, laptop computers and other portable computer devices are widely used. While outside the internal network, the laptop cannot make benefit of the protection provided by the conventional "gateway-type" firewall. Therefore, approaches to improve security of a client located in a foreign network (a public network or an internal network of a foreign organisation) have been proposed. These approaches are based on protecting the laptop itself by means of a local security mechanism, called a personal firewall herein, installed in the laptop (in addition to or instead of a firewall in an internal network, which protects the computers connected to the internal network). The personal firewall may be implemented as software installed in the computer device, or as a separate electronic device connected to the computer device.

[0004] European patent application EP 0 952 715 discloses a firewall security device connected to an external communication port of a computer device. The incoming communications stream to the computer device from e.g. public networks is passed through the firewall security device. The firewall device applies standard security measures, thereby protecting the computer device.

[0005] There is a particular need for such protection by means of a personal firewall if the laptop is allowed to have a remote access, e.g. make a VPN (Virtual Private Network) connection to company network while being connected to a foreign network. In order to improve security of the VPN connections, one prior art solution is to enforce a protection level of a laptop, when a VPN tunnel to a company network is created. This means for example that, during a VPN connection, the IP address forwarding is not allowed, or that any connection attempts to the laptop are denied.

[0006] Clearly this is not enough, since the laptop must be protected as soon as it is connected to a foreign network, not only during a VPN connection. The laptops are often used by non-technical people, which increases the risk of overlooking security aspects. Laptops contain sensitive material, such as customer emails. If a laptop is unprotected, when connected to a foreign network, even for a short period of time, there is a risk of getting infected by a hostile application. Such application can be activated later, when the laptop is connected to an internal network and offer inside help for attacks.

[0007] Thus, there is a need to protect the laptop by means of a personal firewall always when the laptop is connected to a foreign network. However, when the laptop is connected to a company internal network, such personal firewall may unduly prevent some essential traffic. For example, the personal firewall should allow use of a laptop at home (internal) network and access to all services, such as disk-share. In a home network even non-IP protocols are sometimes used. Therefore, it is not feasible to have a personal firewall running at all times, at least not with the same configuration, since the protection needs in an internal network are different from those in a foreign network.

[0008] Some of the current solutions allow changing the set of rules used in the personal firewall, that is, they allow the user of the laptop to use different rule sets when connected to the internal network and when connected to a foreign network. However this is a manual operation. Since manual action is required, there is a high risk that operation is not done. Risk is even higher if the end user does not fully understand the need of a firewall.

Summary of the Invention

[0009] An object of the invention is to improve the security and flexibility of a personal firewall. The object is achieved by the invention disclosed in the attached independent claims. Preferred embodiments are disclosed in the attached dependent claims.

[0010] A computer device which can be connected to a home network (such as an internal network of a company or other organisation where the user is employed) and to a foreign network (such as a public network or an internal network of a foreign organisation) is provided with a local security mechanism, called a personal fire-

EX1002
CISCO SYSTEMS, INC. / Page 286 of 1453

wall herein, for protecting the computer device from attacks from a foreign network, in addition to or instead of a firewall in the internal network which protects the computer when connected to the internal network. The personal firewall is provided with different sets of security rules, at least one set of rules for the home network and at least one set of rules for foreign networks. In its simplest form, the set of rules for the home network contains no restrictions for the communication or use of service in the home network. The personal firewall is arranged to detect its current location, i.e. to determine the network to which it is connected at each particular moment. The personal firewall activates one of the given sets of security rules according to the detected current location of the computer device, i.e. the personal firewall automatically uses the security rules predefined for the network to which the computer device is connected at each particular moment. Upon detecting a change in the location, the personal firewall immediately adapts to use security rules predefined for the new location. A benefit of the invention is that the protection of a personal firewall is always enabled at the correct level, depending on the current location. On the other hand, when the computer device is located in the home network, a lower level of protection, or no protection at all, can be automatically provided by the personal firewall, so that the communication and services are not unduly restricted in the home network. Thus, the automated location-dependent management of different sets of rules offers optimal protection in different networks, while not unduly restricting operation in the home network.

[0011] The current location of the computer device is preferably determined on the basis of a currently used IP address of the computer device. This is based on the common practice that a computer device has a different IP address, either a fixed address or a dynamic address, in different networks. The IP address can thereby be utilized for identifying the current network and the location of the computer device.

[0012] However, there are situations where the IP address fails to indicate current location of the computer device. Therefore, in an embodiment of the invention, the current location determined on the basis of the current IP address of the computer device is verified by carrying out an additional location verification procedure with a predetermined network element. In a still further embodiment of the invention, availability of said predetermined network element related to the current IP address is checked. The predetermined network element is such that it responses only if the computer device is located in the network in which it is assumed to be on the basis of the current IP address. If the predetermined network element responses and identifies itself properly, the current location determined based on the current IP address is considered to be verified. Otherwise the computer device determines that the current IP address fails to indicate current location of the computer device. The additional verification process makes it even possible to automatically create a secured tunnel, such as a VPN tunnel to a home network even if the computer device uses the same IP address in the current location as in the internal (home) network. The present invention offers benefits even with stand alone personal firewalls wherein the security rules can be defined locally by the user, although the use of these rules is automated and location-dependent. However, more advantages are achieved when the basic invention is used with a central management of personal firewalls.

[0013] According to an aspect of the invention, security rules are defined, updated and distributed centrally by a centralized rule-based server. Especially the updating of the rules is challenging, because the rule updates must be applied as soon as possible, and therefore the process of updating rules in the personal firewalls must be automated. Updating of rules by push method from the centralized rule base server is not a sufficient option in this case. Use of DHCP (Dynamic Host Configuration Protocol), frequent travelling and the fact that at times the laptop may not be connected to any network makes it next to impossible for the centralized management to initiate contacts with the personal firewalls in the computer devices, because there is no way for the centralized management to know the IP address the computer device is using at a given moment. Therefore, according to an aspect of the invention, the personal firewall is configured to periodically query the availability of updated security rules from the centralized management. The queries should only be made, while the computer device is located in the home network, or optionally, when the computer device has a remote access (e.g. VPN connection) to the home network while being located in a foreign network. In other words, also the updating process is dependent on the current location of the computer device in a similar manner as the selection of the active rules, and similar methods can be utilized for determining the current location.

[0014] According to another aspect of the invention, log files containing information of a status and usage of resources of the computer device are handled in a centralized management location. This enables personnel aware of security aspects to verify whether there have been any attacks against the computer device or not. To that end, the personal firewall sends the log files to the central management, such as to a centralized log server, when the computer device is located in the home network. However, when the computer device is disconnected from the home network, the log files are collected and stored locally in the firewall. In order to enable central handling of the log files, the personal firewall transfers the collected log files to the central log server when such is available. This is performed automatically, whenever the computer device is located in, or optionally, connected to the home network. Again, the handling of the log files in the personal firewall is automated and location dependent in a way similar to the selection of active rules, and similar methods can be used for de-

EX1002
CISCO SYSTEMS, INC. / Page 287 of 1453

termining the current location of the computer device.

[0015] The present invention allows use of a computer device in a home (internal) network and access to all services, such as disc-share, and even use of non-IP protocols, which are often denied in foreign networks.

Brief description of the drawings

[0016] Preferred embodiments of the invention will now be described with reference to the attached drawings, in which

Figure 1 is a schematic block diagram of an exemplary network configuration where the present invention can be applied;

Figure 2 shows an exemplary protocol stack of a computer device containing a personal firewall according to the present invention,

Figure 3 illustrates exemplary selection rules and a security rule basis, and the association therebetween,

Figure 4 is a flow diagram illustrating a location-dependent rule base selection according to an embodiment of the invention;

Figures 5 and 6 are flow diagrams illustrating the location verification procedure according to an embodiment of the invention;

Figures 7 and 8 are flow diagrams illustrating the rule base updating according to an embodiment of the invention; and

Figure 9 is a flow diagram illustrating the handling of log files according to an embodiment of the invention.

Preferred embodiments of the invention

[0017] The present invention can be applied in personal firewalls in any computer device which can be moved and connected to different networks. Typically such devices are portable computer devices, such as laptop computers, PDAs, communicators, smart phones, intelligent telecommunication devices, etc. In the following illustrative embodiments of the invention, a laptop computer is used as an example of suitable computer devices.

[0018] Figure 1 shows a schematic block diagram of an exemplary network configuration. The configuration is shown only to facilitate the understanding and description of the present invention. The present invention is not intended to be restricted to any particular network configuration. Further, in order to improve clarity, only network elements which are somehow involved with the present invention are shown in Figure 1.

[0019] As illustrated in Figure 1, private local networks 10 and 13 are coupled to a public network, such as the Internet 12 via firewalls 5 and 7, respectively. Naturally, the coupling between the private networks and the public Internet 12 may include also routers and Internet service providers (ISPs not shown in Figure 1). As is well known in the art, private networks 10 and 13 may be, for example, company networks, such as local area networks (LANs) which connect users and resources, such as workstations, servers, printers and the like of the company. A private internal network may also consist of several sub-networks separated by internal firewalls. In the exemplary network configuration shown in Figure 1, the private company sub-network 11 is connected via a firewall 6 to the private local network 10. Such a sub-network 11 may be, for example, a dedicated network for a specific department of the organisation, such as the research and development (R&D) department which must have a restrictive access and higher protection level compared with other part of the company network. Sub-networks of the company, such as the local networks of organisation headquarters and branch offices may be interconnected by secure connections, such as virtual private network (VPN).

[0020] As already described above, the firewalls 5, 6 and 7 are gateways which operate at the same time as connectors and separators between the networks in a sense that the firewall keeps track of the traffic that passes through it from one network to another and restricts connections and packets that are defined as unwanted by the administrator of the system. Physically a firewall is a machine with appropriate software to perform the task assigned to it. It can be a router, a personal computer (PC), or whatever that can be used for such purposes.

[0021] However, the firewalls between the networks, or the implementations thereof, are not relevant to the present invention.

[0022] The present invention relates to protecting of the computer device, e.g. laptop itself, by means of a local security mechanism, called a personal firewall herein, installed on the laptop in addition to or instead of a firewall in a private network. The personal firewall may be implemented as software installed and run in the computer device, which is a preferred embodiment, or as a separate electronic device connected to the computer device. In Figure 1, the laptops 1, 2, 3 and 4 illustrate laptops provided with a personal firewall.

[0023] Figure 2 illustrates the basic principle of a personal firewall installed in a laptop. Physical and network layers 200 refer to all protocols and physical connections required for transferring protocol data units (PDUs) of the upper layers. The upper layers 200 include applications and any transmission protocols employed, such as Internet protocol (IP) transmission control protocol (TCP), NetPEUI, IPX, etc. Basically the personal firewall protection layer 201 operates in a manner analogue to a firewall between networks. More particularly, the personal firewall protection layer 201 operates at the same time as a connector and a separator between the underlying layers and the upper layer in a sense that the personal firewall keeps track of the traffic that passes through it from underlying layers to the upper layers, and

EX1002
CISCO SYSTEMS, INC. / Page 288 of 1453

vice versa, and restricts connections and packets that are defined as unwanted according to the security rules used. The personal firewall protection layer 201 is implemented or controlled by a personal firewall application 203 run in the laptop. In a preferred embodiment of the invention, the personal firewall application 203 carries out the location detection and the location-dependent functions described below, such as the selection of the active rule base according to the current location of the laptop. However, it should be appreciated that the present invention is not intended to be restricted to any specific practical implementation of the personal firewall.

[0024] In accordance with the principles of the present invention, the personal firewall has different sets of rules for the home network (such as the private company network 10) and foreign network, such as the public Internet 12, or the foreign private network 13, or a network of another department of the company. It is not relevant to the present invention what kind of security rules are applied, but some examples are given in Figure 3. For example, a rule base 301 for the foreign company network may list as allowed connections of protocols: hypertext transfer protocol (http), secured http (Https), domain name service (DNS), single message transfer protocol (SMTP) and a VPN connection with IPsec. In the preferred embodiment of the invention these rules are exclusive, in other words, other protocols and connections are denied and blocked by the personal firewall. For a default network, which may be the public Internet 12, the rule base 302 is similar to the rule base 301, except that the SMTP protocol is no longer allowed. For the home network 10, a rule base 300 is defined. The allowed protocols include, in addition to the http, https and the SMTP, also other transmission protocols, such as NetBEUI and IPX. The rule base 300 also allows a disc-share for predefined servers using NetBIOS. Other protocols and connections are denied. It is also possible that the rule base 300 allows all protocols and connections in the home network. Since the home network is protected by a company firewall, the use of a personal firewall in the home network may be regarded as unnecessary. However, the company firewall gives protection only against attacks from the outside of the home network, and the use of a personal firewall protection may be necessary for protecting against attacks from within the home network.

[0025] The different rule bases could be activated manually by a user. However, according to the basic principle of the present invention, the personal firewall automatically selects and activates the proper rule base according to the current location of the laptop.

[0026] Figure 4 is a flow diagram illustrating the selection of the rule base according to one embodiment of the present invention. The simplest way to determine the current location of the laptop is to do it on the basis of the currently used IP address only. This is possible in the cases where the laptop has a different IP address, either a fixed or a dynamic address, in different networks. As is well known in the art, a part of the IP address identifies the network, and can thus be used for detecting the current network of the laptop. The personal firewall may, for example, contain information on the IP address space of home network, and optionally, foreign networks, or a list of addresses available for the laptop in the home network.

[0027] When the current IP address of the laptop matches to a given address space or a list of addresses of the home network 10, for example, it can be assumed that the laptop is located in the home network 10 and the rule base 300 of the home network 10 is used. Thus, the current IP address is used as a selection rule for activating the rule base 300. However, there is some uncertainty in determining the location based on the current IP address only, and some approaches to overcome this problem are described with reference to further embodiments of the invention below.

[0028] Referring again to the generic flow diagram shown in Figure 4, the current IP address of the laptop is firstly determined in the step 401. The current IP address may be obtained simply by asking for it from the operating system of the laptop by means of using IP configuration routine. The current location of the laptop is monitored constantly, and therefore the personal firewall may be configured to periodically query the current IP address from the operating system. More preferably, the operating system of the laptop may be configured to inform any changes in the IP address to the personal firewall, and therefore a need for query the IP address time-to-time can be avoided. The step 401 may also include verification of the location determined based on the IP address by a verification procedure described below. In step 402, the personal firewall compares the current IP address with the current IP address stored in the personal firewall. If the IP address has not changed, the present active rule base can be maintained. However, if the IP address has changed, the personal firewall checks whether the new IP address matches to any IP address space or IP address belonging to one of the networks on the selection rule list in the personal firewall (step 403). If the new IP address does not belong to any of the networks on the selection rule list, the personal firewall considers the current network an unidentified network, and a default rule base 302 is selected (step 404). If the network cannot be identified and the default rule base must be used, it is normally assumed that the laptop is in a potentially hostile environment, most likely in the public Internet 12. Therefore, the default rule base is typically defined to provide the maximum protection needed. If the new IP address belongs to one of the networks defined on the selection rule list in step 403, it means that the network has been identified and a rule base linked to the identified network (or the corresponding selection rule) is selected and activated (step 405). In the simplest implementation, the selection rules include only the home network of the laptop and the cor-

EX1002
CISCO SYSTEMS, INC. / Page 289 of 1453

responding IP address space or list of addresses . If the current IP address belongs to the home network, the rule base 300 of the home network 10 is used. Otherwise the rule base 310 for foreign network or the default rule base 302 is used. In a more complicated implementation, there are selection rules (i.e. IP addresses and associated rule bases) also for at least one foreign network and/or different segments of the home network 10.

[0029] In the examples described above there are two or more rule bases which are enabled or disabled on the basis of the current location of the laptop. However, there are also alternative ways to implement different rule bases. One alternative is to provide only one rule base in which the rules are enabled and disabled in different combinations on the basis of the current location of the laptop.

[0030] As noted above, there are situations where the location (the current network) determined on the basis of the current IP address is uncertain, i.e. the IP address fails to indicate the current location of the laptop. If the IP address does not match the current network, use of the Internet protocol (IP) to attack against the laptop is not likely, and one may reason that in that case a personal firewall does not need to be used. However, there is still a possibility that there is an attack using other protocols, such NetBEUI or IPX. By detecting the situation where the IP address of the laptop is not an IP address of the current network, it is possible to block such protocols while in foreign networks. Further, NAT (network address translation) and private IP addresses are frequently used. This means that the same IP address is in use in several networks. In that case it is not enough to trust IP address information only when determining the location of the laptop. It is even possible that while being connected to a hostile network, the DHCP (dynamic host configuration protocol) gives familiar IP address to make it easier to attack the laptop. Basically, the DHCP enables individual computers on a network to connect to a DHCP server, such as the server 9 in Figure 1, and be assigned a dynamic IP address of the current network.

[0031] Thus, according to an aspect of the invention, in addition to the detection of location based on the current IP address described above, a further location verification procedure is carried out with a predetermined network element, which is preferably reachable only from the location to be verified. More generally, the network element is selected in such a way that it responses to the verification request only if the request originates from the location (i.e. the network) to be verified. Preferably, the specific network element is provided with a location verification service supporting the verification according to the invention. The verification procedure requires that the verification method be specified for the personal firewall, preferably at the same time as the different locations are specified. In other words, the methods to verify the location are specified for the personal firewall in the initial configuration, for example. It is also possible that the verification methods are updated or changed by means of the updating procedure described below, in a manner similar to other security rules.

[0032] A generic location verification procedure according to one embodiment of the invention is described with reference to Figures 5 and 6. Firstly, the current location is determined on the basis of the currently used IP address as described above (step 501). Next, the personal firewall selects a predetermined network element that should be available for verification from the determined current location (step 502). Then the personal firewall sends to the selected network element a request to send a response with some data proving the identity of the network element (step 503). Referring now to Figure 6, the verifying network element receives the verification request (step 601) from a personal firewall. Then, either always in response to the verification request or only if predetermined requirements are met, the network element sends the response with the required identity data to the personal firewall (step 602). Referring again to Figure 5, the personal firewall waits for a response (step 504), and if no response is received (preferably within a predetermined period of time), the location determined on the basis of the current IP address is rejected, and the location is determined to be unknown (step 505). In that case, a default location and an associated rule base, such as the rule base 302, can be used.

[0033] However, if the response is received from the network element in the step 504, the personal firewall verifies the identity of the network element on the basis of the received identity data, e.g. by comparing the received identity data with identity data stored in the personal firewall (step 506). If the verification of the identity is unsuccessful (step 507), the procedure proceeds to the step 505 described above. However, if the verification of the identity of the network element is successful, also the location of the laptop determined on the basis of the current IP address has been successfully verified and can be accepted.

[0034] Additionally, it is possible that one IP address is included in more than one selection rule in the personal firewall. In that case, if the verification of the laptop being located in a first network indicated by the current IP address fails, it is checked if the laptop is located in a second network indicated by the current IP address. There are various ways to implement the generic location verification procedure described above. The simplest way to implement the location verification service is to probe some known (known to the personal firewall) element. For example, it is possible to ask the MAC address of the known network element located in the home network and having a known IP address. The network element returns the MAC address in response, and if the AMC address is the one that it is assumed to be (e. g. matches with a MAC address stored in the personal firewall), it is verified that the laptop is located in the home network. If the MAC address is not the correct one, the laptop is determined to be outside the internal

EX1002
CISCO SYSTEMS, INC. / Page 290 of 1453

network.

[0035] One possible implementation is that the location verification service is implemented in such network element in an internal network which can be reached only from inside the internal network. For example, the firewall protecting the internal network, such as firewall 5 in Figure 1, may be configured to discard all connections from outside the internal network to this network element. If the personal firewall is able to reach this specific network element, it is verified that the personal firewall resides inside the internal network. Otherwise the personal firewall resides outside the internal network. There may be a plurality of such location verification services in a plurality of internal networks or sub-networks, and if the personal firewall cannot reach any of them, then it is assumed to be outside this plurality of internal networks or sub-networks.

[0036] The location verification service may be incorporated into the network firewall, such as the location verification service 50 in the firewall 5 in Figure 1. For example, verification requests only from the direction of the internal network (such as home network 10) may be responded by the location verification service 50. This implementation is rather straightforward, since the present firewalls are readily capable of detecting from which direction, that is, from which interface, a data packet is coming from.

[0037] In any case it is preferred that the personal firewall communicates with the location verification service by using some cryptographically strong method, such as public key encryption. For example SSL can be used. The certainty of the location verification can be further improved by setting the TTL (time-to-live) field in the location verification request to a relatively low value, so that the request is capable of reaching only a nearby location verification service. The TTL value is decremented each time the verification request passes through a router connecting different networks or network segments. If the TTL value is set to, for example, a zero value the verification request is not able to pass through a router to a different network or a network segment.

[0038] The use of additional location verification makes it even possible to automatically create a VPN tunnel to the home network even if the current location (a foreign network) is using the same IP address as in the internal network.

[0039] All the embodiments described above are effective both in standalone computers and in centrally managed computers. The central management of personal firewalls enables a uniform protection level in all computer devices using the private network. One feature of the central management is that preferably all of the personal firewalls have essentially similar security rules. It should also be possible to update these. It is preferable that rule updates are applied in the personal firewalls as soon as possible after they have been made in the central management. Because it is not sufficient to rely on the manual updating by the user, the process of updating the rules must be automated. However, distribution of the updated rules by a push transmission from the central management is not a sufficient option in a case where the personal firewalls can move from one network to another. Therefore, according to an aspect of the invention, the personal firewalls are arranged to periodically query the availability of updated rules from the central management. An updating procedure according to one embodiment of the invention is described with reference to Figures 7 and 8.

[0040] Firstly, a personal firewall measures a predetermined updating period, which can be any period of time, preferably one day or a few days (step 701). In step 702, the personal firewall checks whether the updating period has expired, and if not, the procedure returns to the step 701. When the updating period has expired, the personal firewall checks whether the current location of the laptop is in the home network (step 703) or in another subnetwork of the same company. The location determination is preferably based on the methods described above. If the current location is in the home network, the process proceeds directly to the step 705. However, if the current location is not in the home network, the personal firewall waits for the laptop to return to or establish a connection (e.g. VPN) to the home network (step 704), before proceeding to the step 705. In the step 705, the personal firewall sends a rule update query to the central management, such as the personal firewall management server 8 in Figure 1. Referring now to Figure 8, the personal firewall management 8 receives the rule update query from the personal firewall (step 801) and sends updated rules, if there are any, to the personal firewall (step 802). Referring again to Figure 7, the personal firewall checks whether the reply received from the personal firewall management 8 contains rule updatings (step 706), and if not, the process returns to the step 701 to measure the next updating period. However, if rule updatings have been received, the personal firewall updates the relevant rule bases stored in the laptop (step 707).

[0041] It is also preferable that the logs relating to the communication transactions of the laptop are handled in a central location. Since the laptops are frequently disconnected from the home network, logs must be collected locally. In order to enable central handling, the logs must be transferred to a central log server, such as the personal firewall management 8, when such is available. This should take place automatically when the computer device provided with a personal firewall is connected to the home network. Figure 9 illustrates log handling according to one embodiment of the invention.

[0042] Firstly, the personal firewall creates a log file each time the laptop is involved with a communication transaction, such as an Internet session (step 91). Then the personal firewall determines the current location of the laptop, preferably based on the location determining methods described above (steps 92 and 93). If the lo-

EX1002
CISCO SYSTEMS, INC. / Page 291 of 1453

cation of the laptop is in the home network or in another subnetwork of the same company, the personal firewall sends the log file to the central log server 8 immediately (step 94). However, if the current location of the laptop is not in the home network, the process proceeds to the step 95, where the log file is stored locally. Similarly, a number of log files is collected locally while the laptop is disconnected from the home network. When the personal firewall next time detects that the computer device is relocated in the home network, it sends the collected log files to the central log server 8. Optionally, the personal firewall may also send the collected log files to the personal firewall management 8 when the laptop has established a (e.g. VPN) connection to the home network.

[0043] It is apparent for those skilled in the art that the illustrative embodiments described are only examples and that various modifications can be made within the scope and spirit of the invention as defined in the appended claims.

Claims

1. A method of controlling a personal firewall in a client computer, said method comprising
   providing said personal firewall with at least one set of security rules to be used when said client computer is connected to a home network of said client computer, and at least one set of security rules to be used when said client computer is connected to foreign networks,
   monitoring the current location of said client computer based on an Internet Protocol (IP) address currently used by said client computer, and
   automatically selecting one of said sets of security rules by said personal firewall according to said current location of said client computer.

2. A method according to claim 1, wherein
   said step of providing comprises providing said client computer with said set of security rules in form of at least two rule bases,
   said step of selecting comprises enabling one of said rule bases at a time according to the current location of said client computer.

3. A method according to claim 1, wherein
   said step of providing comprises providing said client computer with said set of security rules in form of one rule base, and
   said step of selecting comprises enabling and disabling rules in said one rule base in different combinations according to the current location of said client computer.

4. A method according to claim 1, wherein said step of monitoring comprises
   storing in said client computer an IP address space of said home network,
   comparing the current IP address of said client computer with said IP address space, and
   if the current IP address of said client computer matches said IP address space, determining said personal firewall to be located in said home network.

5. A method according to any one of claims 1, 2 or 3, wherein said step of monitoring comprises
   storing in said client computer a list of IP addresses of said home network,
   comparing the current IP address of said client computer with said list of IP addresses, and
   if the current IP address of said client computer matches one of said addresses on said list, determining said client computer to be located in said home network.

6. A method according to any one of claims 1, 2 or 3, comprising
   verifying the current location determined on the basis of the current IP address of said client computer by carrying out a location verification procedure with a predetermined network element.

7. A method according to claim 6, wherein said step of verifying comprises
   checking availability of said predetermined network element related to the current IP address, said predetermined network element responding only if said client computer is located in the network in which it is assumed to be on the basis of the current IP address,
   verifying the current location determined based on said current IP address, if said predetermined network element responses with a specific identity data.

8. A method according to claim 7, wherein said specific identity data is a Media Access Control (MAC) address of said predetermined network element.

9. A method of managing a personal firewall in a client computer, comprising
   storing in said personal firewall at least one set of security rules to be used when said client computer is connected to a home network of said client computer, and at least one set of security rules to be used when said client computer is connected to foreign networks,
   storing updated sets of security rules, if any, in a centralized unit in said home network of said client computer,
   configuring said personal firewall to periodically query the availability of said updated sets of security rules from said centralized rule base server

EX1002
CISCO SYSTEMS, INC. / Page 292 of 1453

when being located in said home network, or when having a remote access to said home network while being located in a foreign network, and

loading said updated sets of security rules from said centralized rule base server to said personal firewall in response to said query, if such updated sets of security rules are available.

10. A method according to claim 9, comprising

monitoring the current location of said client computer based on an Internet Protocol (IP) address currently used by said client computer, and

automatically activating said periodical query, when the current location of said client computer is in said home network.

11. A method according to claim 9, comprising

monitoring the current location of said client computer based on an Internet Protocol (IP) address currently used by said client computer,

sending log files to a centralized log server from said personal firewall, when the current location of said client computer is in said home network, said log files containing information on communication transactions in said client computer,

collecting log files locally at said personal firewall, when the current location of said client computer is not in said home network, and

transferring said locally collected log files from said personal firewall to said centralized log server, when said client computer is connected to said home network.

12. A computer terminal, comprising

a personal firewall provided with at least one set of security rules to be used when said computer terminal is connected to a home network of said computer terminal, and at least one set of security rules to be used when said computer terminal is connected to foreign networks,

said personal firewall having a mechanism monitoring the current location of said computer terminal based on an Internet Protocol (IP) address currently used by said computer terminal, and

said personal firewall having a mechanism automatically selecting one of said sets of security rules by said personal firewall according to said current location of said computer terminal.

13. A computer terminal according to claim 12, further comprising

a mechanism verifying the current location determined on the basis of the current IP address of said computer terminal by carrying out a location verification procedure with a predetermined network element.

14. A computer-readable medium, containing a computer software which, when executed in a computer device, causes the computer device to provide a personal firewall routine comprising

storing at least one set of security rules to be used when said computer device is connected to a home network of said computer device, and at least one set of security rules to be used when said computer device is connected to foreign networks,

monitoring the current location of said computer device based on an Internet Protocol (IP) address currently used by said computer device, and

automatically selecting one of said sets of security rules by said personal firewall according to said current location of said computer device.

15. A computer-readable medium according to claim 14, said personal firewall routine further comprising

verifying the current location determined on the basis of the current IP address of said client computer by carrying out a location verification procedure with a predetermined network element

16. A computer device, comprising a personal firewall routine configured to store security rules for a home network of said computer device, and for foreign networks,

periodically query the availability of updated security rules from a centralized rule base server in said home network of said computer device when said computer device is located in said home network, and

download said updated security rules from said centralized rule base server, if such updated security rules are available in said centralized rule base server.

17. A computer device according to claim 16, said personal firewall routine being further configured to

activate said periodical query also when said computer device has a remote access to said home network while being located in a foreign network.

18. A computer device, comprising a personal firewall routine configured to

send log files to a centralized log server, when a current location of said computer device is in a home network of said computer device, said log files containing information on communication transactions in said computer device,

collect log files locally in said computer device, when the current location of said client device is not in said home network,

transfer said locally collected log files to said centralized log server, when said computer device is reconnected to said home network.

19. A computer-readable medium, containing computer software which, when executed in a computer de-

EX1002
CISCO SYSTEMS, INC. / Page 293 of 1453

vice, causes the computer device to provide a personal firewall routine comprising

storing security rules for a home network of said computer device, and for foreign networks,

periodically querying the availability of updated security rules from a centralized rule base server in said home network of said computer device when said computer device is located in said home network, and

downloading said updated security rules from said centralized rule base server, if such updated security rules are available in said centralized rule base server.

20. A computer-readable medium, containing computer software which, when executed in a computer device, causes the computer device to provide a personal firewall routine comprising

sending log files to a centralized log server, when a current location of said computer device is in a home network of said computer device, said log files containing information on communication transactions in said computer device,

collecting log files locally in said computer device, when the current location of said client device is not in said home network,

transferring said locally collected log files to said centralized log server, when said computer device is reconnected to said home network.

21. A computer program comprising program code means for performing all the steps of any one of claims 1 to 11 when the program is run on a computer.

EX1002
CISCO SYSTEMS, INC. / Page 294 of 1453

Fig. 1

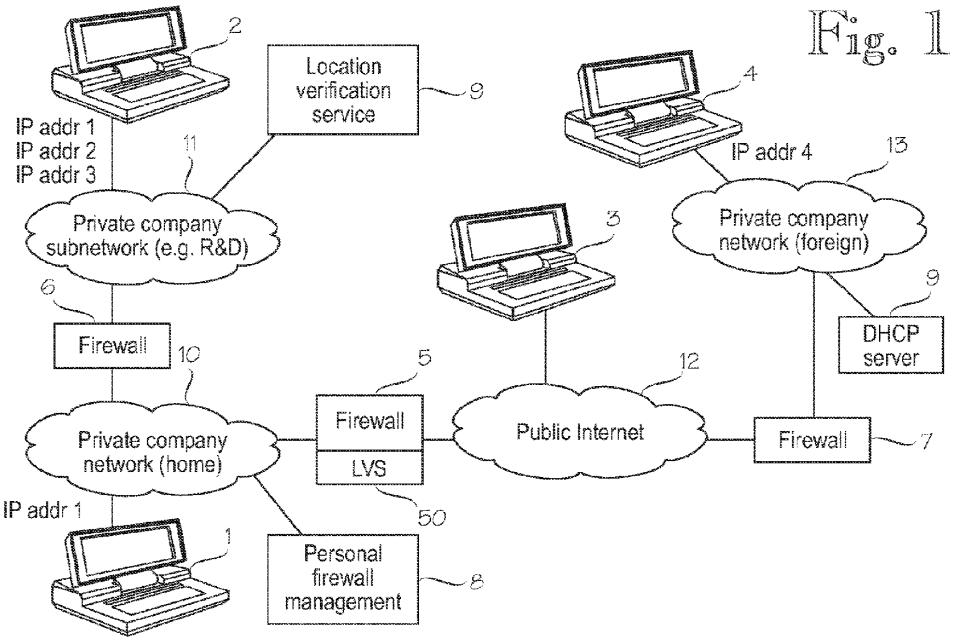


Fig. 2

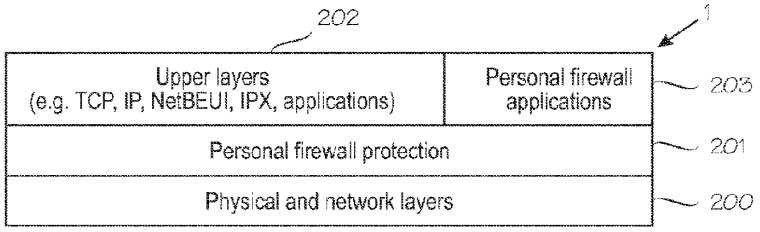
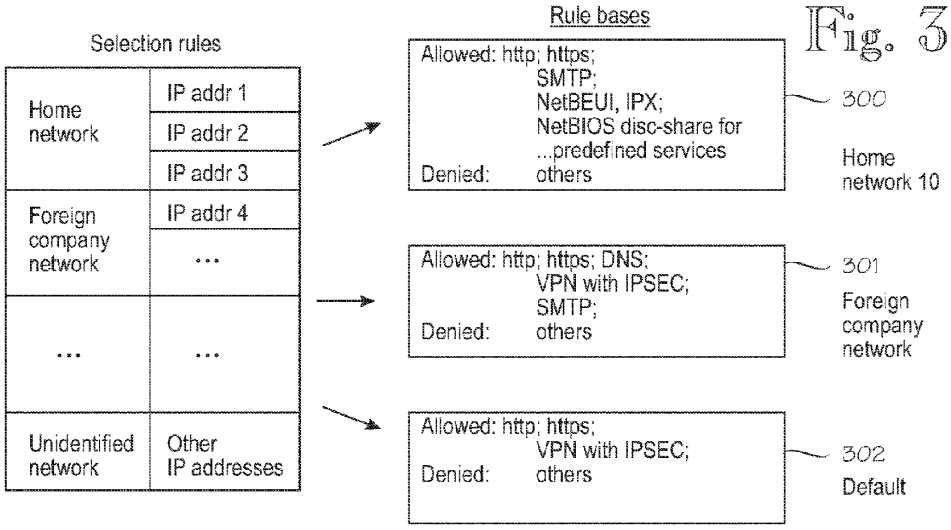


Fig. 3



EX1002
CISCO SYSTEMS, INC. / Page 295 of 1453

Fig. 4

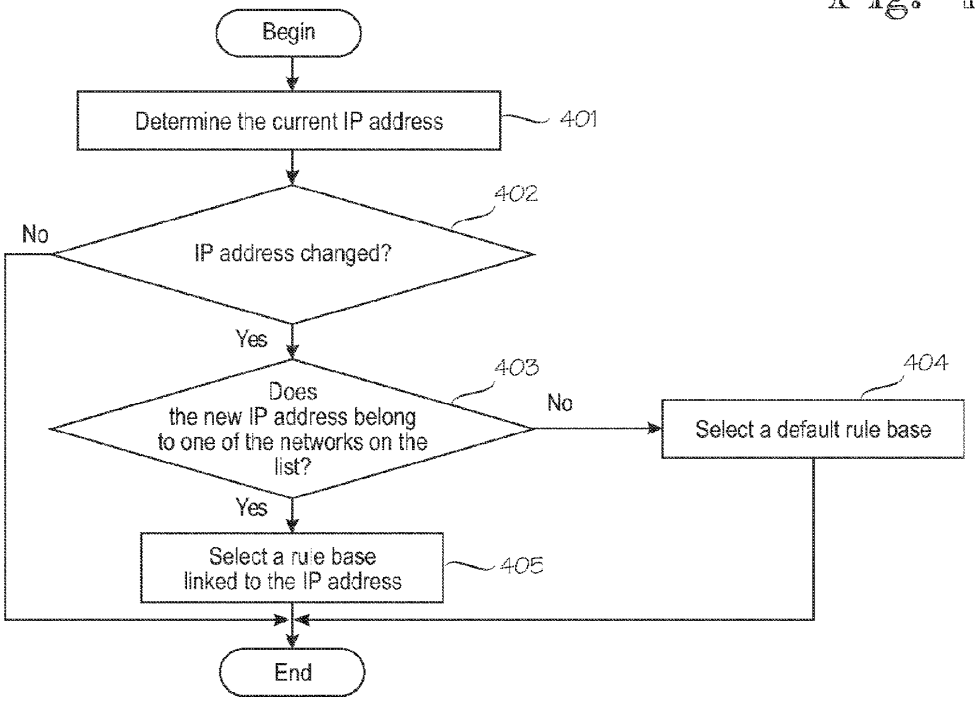
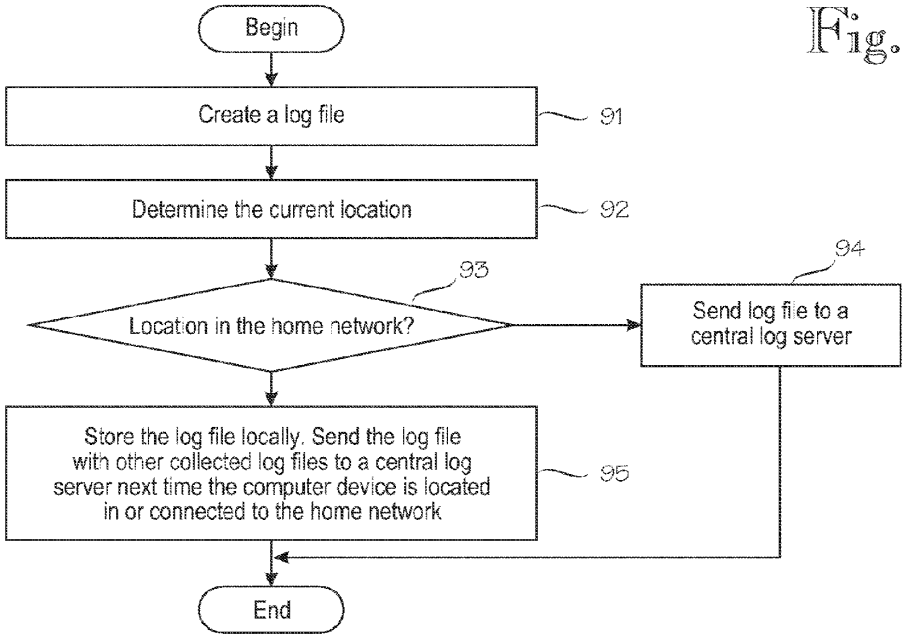


Fig. 9



EX1002
CISCO SYSTEMS, INC. / Page 296 of 1453

Fig. 5

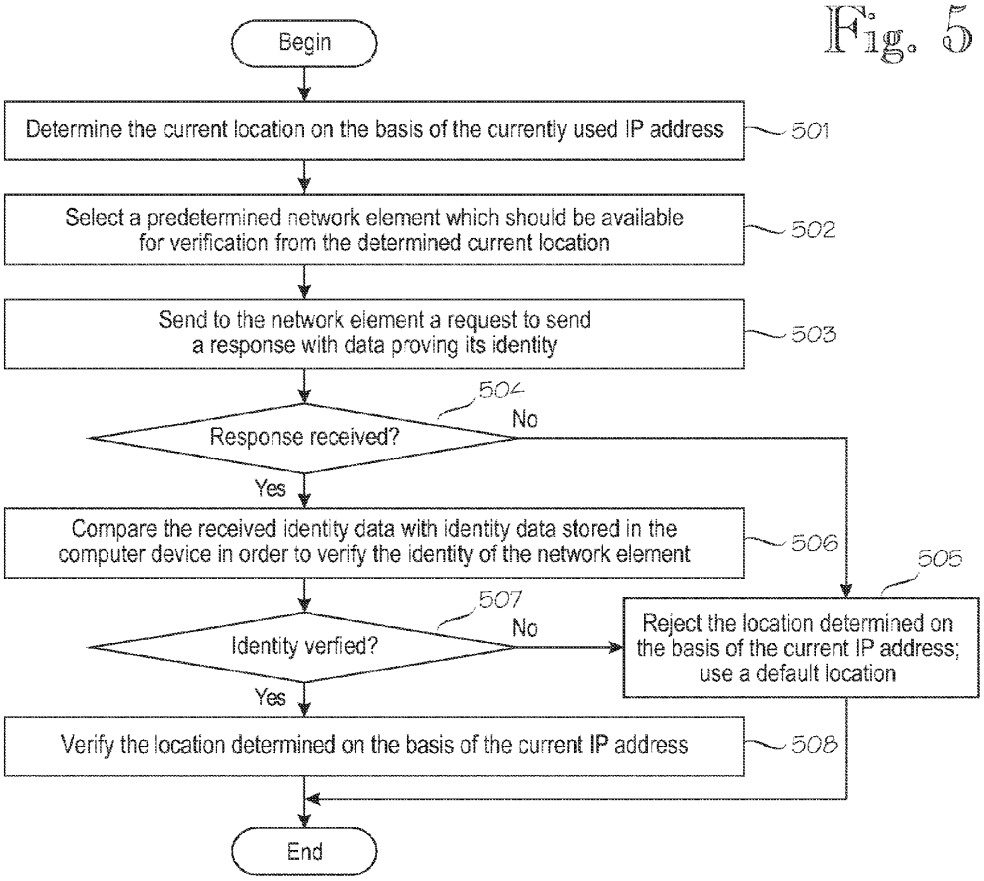


Fig. 6

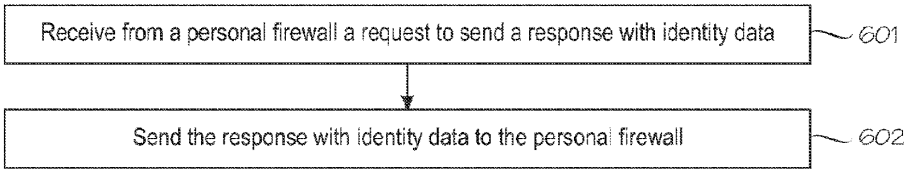
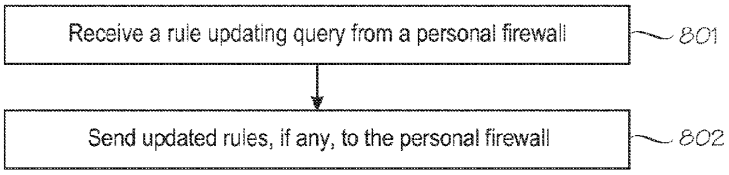
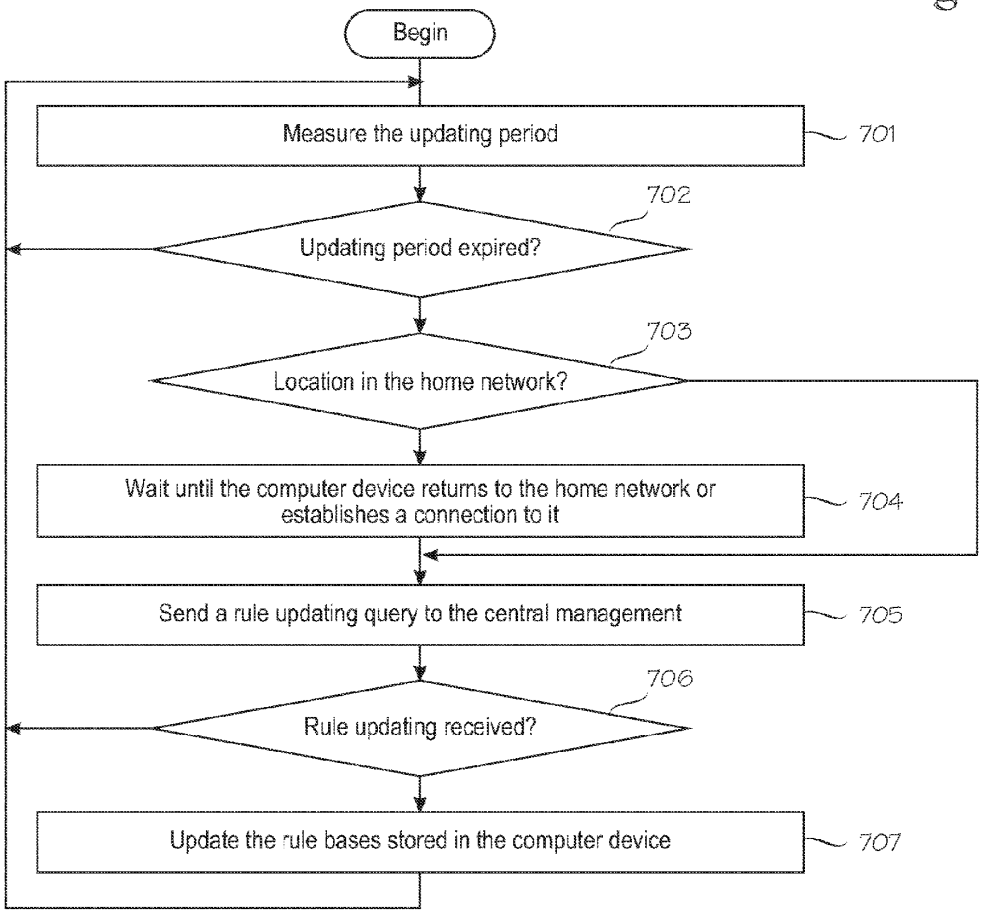


Fig. 8



EX1002
CISCO SYSTEMS, INC. / Page 297 of 1453

Fig. 7



EX1002
CISCO SYSTEMS, INC. / Page 298 of 1453

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 02 10 2581

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	EP 0 854 621 A (AT & T CORP) 22 July 1998 (1998-07-22) * page 4, line 28 - line 47 * ---	1-21	H04L29/06
A	US 6 158 008 A (OWENS LESLIE DALE ET AL) 5 December 2000 (2000-12-05) * claim 1 * -----	1-21	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)

H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	14 March 2003	Veen, G

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

EX1002
CISCO SYSTEMS, INC. / Page 299 of 1453

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 02 10 2581

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

14-03-2003

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0854621 A	22-07-1998	US 6233686 B1	15-05-2001
		CA 2226814 A1	17-07-1998
		EP 0854621 A1	22-07-1998
		JP 10229418 A	25-08-1998
US 6158008 A	05-12-2000	WO 9921339 A1	29-04-1999

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

Espacenet

Bibliographic data: WO2005046145 (A1) — 2005-05-19

ADAPTABLE NETWORK BRIDGE

No documents available for this priority number.

Inventor(s): HALEN JOACIM ± (HALEN, JOACIM)

Applicant(s): ERICSSON TELEFON AB L M [SE] ± (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL))

Classification: **- international:*H04L12/24; H04L12/46; H04L12/56;***
(IPC1-7): H04L12/46; H04L12/56
- cooperative: H04L12/4625; H04L41/0893; H04L41/0896; H04L45/04; H04L45/56; H04L45/66; H04L49/351

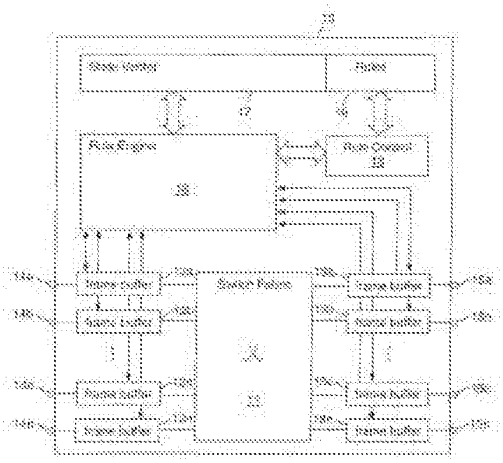
Application number: WO2004SE01611 20041105

Priority number (s): US20030517737P 20031106 ; US20040977724 20041029

Also published as: US2005111434 (A1) US7672318 (B2) JP2007534219 (A) JP4323523 (B2) EP1683313 (A1) more

Abstract of WO2005046145 (A1)

An adaptable network bridge such as an Ethernet bridge (10) includes a Rule Engine (16) that processes data frames according to a set of switching rules. Each switching rule identifies a type of frame to which the rule applies, and how the type of frame is to be processed. The bridge also includes means (18) for dynamically adding, subtracting, or modifying the switching rules in response to changes in the bridge's state information, or changes in context information. If the bridge includes a plurality of input/output ports (14, 15), the Rule Engine (16) may include a plurality of sets of switching rules, with each set of switching rules being applicable to a different port in the bridge. In this way, different network providers can share the same equipment, but have different network behavior.



(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 May 2005 (19.05.2005)

PCT

(10) International Publication Number
WO 2005/046145 A1

(51) International Patent Classification[7]: H04L 12/56, 12/46

(21) International Application Number:
PCT/SE2004/001611

(22) International Filing Date:
5 November 2004 (05.11.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/517,737	6 November 2003 (06.11.2003)	US
10/977,724	29 October 2004 (29.10.2004)	US

(71) Applicant: **TELEFONAKTIEBOLAGET LM ERICSSON (publ)** [SE/SE]; S-164 83 Stockholm (SE).

(72) Inventor: **HALEN, Joacim**; Anhaltsvägen 8, S-191 40 Sollentuna (SE).

(74) Agent: **KARIN BOESTAD et al.**; Ericsson AB, Patent Unit Core Networks Kista, S-164 80 Stockholm (SE).

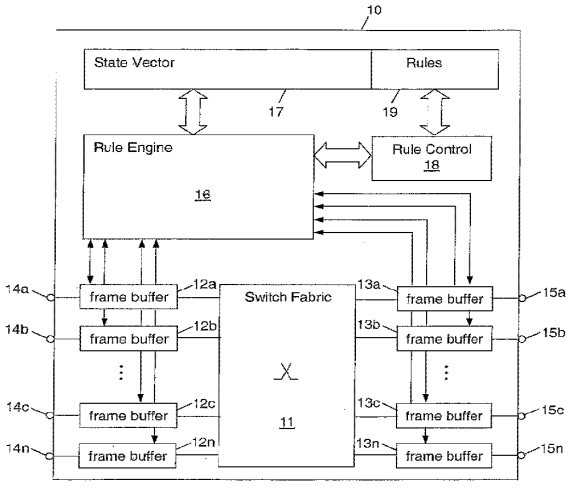
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: ADAPTABLE NETWORK BRIDGE



(57) Abstract: An adaptable network bridge such as an Ethernet bridge (10) includes a Rule Engine (16) that processes data frames according to a set of switching rules. Each switching rule identifies a type of frame to which the rule applies, and how the type of frame is to be processed. The bridge also includes means (18) for dynamically adding, subtracting, or modifying the switching rules in response to changes in the bridge's state information, or changes in context information. If the bridge includes a plurality of input/output ports (14, 15), the Rule Engine (16) may include a plurality of sets of switching rules, with each set of switching rules being applicable to a different port in the bridge. In this way, different network providers can share the same equipment, but have different network behavior.

WO 2005/046145 A1

ADAPTABLE NETWORK BRIDGE

CROSS-REFERENCE TO RELATED APPLICATIONS

This nonprovisional application claims priority under 35 U.S.C. § 119(e) on U.S. Provisional Application No. 60/517,737 entitled, *Programmable Bridge*, filed November 6, 2003, the disclosure of which is incorporated herein in its entirety.

BACKGROUND OF THE INVENTION

Technical Field of the Invention

The present invention relates generally to digital communication systems. More particularly, and not by way of limitation, the invention is directed to an adaptable network bridge having a Rule Engine that simplifies adapting the bridge to dynamically changing conditions.

Description of Related Art

Ethernet is a layer-2 packet-based transmission protocol that is primarily used in local area networks (LANs). Ethernet is the common name for the Institute of Electrical and Electronics Engineers (IEEE) 802.3 industry specification. Data is transmitted in Ethernet frames. Each frame includes a preamble with 64 bits utilized for synchronization. A Start of Frame Delimiter (SFD), a destination address, a source address, and a length/type identifier follow the preamble. Media Access Control (MAC) client data, together with a Packet Assembler/Disassembler (PAD) may vary in length from 46 to 1500 bytes (octets). A Frame Check Sequence (FCS) adds four more octets. Higher-level protocols reside in the content part of the frame. The frame size is counted from the destination address to the FCS, inclusive, and thus may vary between 64 and 1518 octets, not including a Virtual Local Area Network (VLAN) tag, which adds 4 octets.

Today most packet-based networks are built on Ethernet technology, as it is a cheap and reliable technology with good performance. Ethernet has been used in office networks for a long time and is now used to build Wide Area Networks (WANs) as well as small networks in homes. The communications

industry is now expanding the use of Ethernet to what is called "Public Ethernet" where millions of users are connected in the same network. Unfortunately, Ethernet does not scale to such large networks due to flooding of broadcasted messages. Some solutions have been proposed, but these solutions require modifications to the existing standards if they are to be implemented on standard equipment.

Ethernet bridging is a way to connect networks together to form a larger network. The standard for bridging is ANSI/IEEE 802.1d, which is hereby incorporated by reference herein. A bridge is a way to connect two separate network segments together in a protocol-independent way. Packets are forwarded based on Ethernet address, rather than IP address. Since forwarding is done at Layer 2, all protocols can go transparently through a bridge.

There are basically two approaches to adding new functionality to Ethernet bridges (and other Ethernet equipment as well): standardization thru IEEE, or proprietary solutions, which make the equipment non-standard. Adding new functionality and behavior to IEEE 802.1d MAC bridges, better known as Ethernet switches (or other Ethernet equipment), is a difficult and time-consuming process without any guarantees of success. Each new function must be proposed to and scrutinized by an IEEE standardization group (an existing working group or a new group has to be accepted and established). If one is lucky, the proposed function is accepted and added to the standard. However, since each new function requires a change in the standard, there is reluctance to add new functions. If the proposal is rejected, one is limited to a proprietary solution on non-standard equipment. The members of the standardization groups come from different vendors and other organizations, and although they are supposed to act in the interest of IEEE and the entire community, they may also act on agendas from their own organization/company that might be in conflict with the proposed functionality, thereby turning it down. It should also be noted that if a new function is added to the standard, it is then up to the different vendors to add the standardized functionality. A feature may be standardized but not made mandatory.

The proprietary approach also has its drawbacks. For example,

programmable network processors have been available for some time, and bridges may be purchased off the shelf containing programmable network processors. Proprietary solutions can be implemented on these. However, these network processors are vendor specific, and the solution will only work on that network processor or processor family. The solution will not be portable, and it will not be possible to run it on other vendors' equipment. Additionally, programming a network processor is done at a very low level, basically in assembly language, and the programming model is hard, requiring special skill. It should also be noted that a proprietary solution will make the equipment non-standard, and customers are more reluctant to buy non-standard equipment. There might also be inter-operational problems with other equipment.

SUMMARY OF THE INVENTION

The present invention is an adaptable network bridge having a Rule Engine that simplifies the adaptation of the bridge to dynamically changing conditions related, for example, to network conditions and user context. Simplicity is achieved by specifying how data frames should be processed and switched in terms of switching rules. Flexibility is achieved by enabling dynamic loading and updating of rules in the bridge via a protocol. In addition, one bridge may generate or modify rules for loading at another, neighboring, bridge. In a preferred embodiment, the bridge is an Ethernet bridge.

Thus, in one aspect, the invention is directed to an adaptable network bridge that includes a Rule Engine that processes data frames according to a set of switching rules. Each switching rule identifies a type of frame to which the rule applies, and how the type of frame is to be processed. The bridge also includes means for dynamically modifying the switching rules. In particular, the rules may be dynamically loaded and updated, for example, in response to changes in the bridge's state information, or changes in context information. In another embodiment, the bridge includes a plurality of input/output ports, and the Rule Engine includes a plurality of sets of switching rules, wherein each set of switching rules is applicable to a different port in the bridge.

In one aspect the rules are forced on the switch by external units such as a

Network Management System (NMS).

In a further aspect, a switch generates or modifies rules that are forced on other switches.

In yet another aspect, the invention is directed to a method of processing and switching Ethernet frames in an adaptable Ethernet bridge. The method includes the steps of defining a set of switching rules for the adaptable Ethernet bridge; receiving a given frame in the bridge; determining whether any of the rules are applicable to the given frame; and upon determining that one of the rules is applicable to the given frame, processing and switching the frame according to the applicable rule. The switching rules may be dynamically added, subtracted, or modified, for example, in response to changes in state or context information.

An important aspect of the invention is how the extended state vector can be utilized in new ways in the switching process. The switching process can be controlled and adapted in new ways allowing completely new ways to control networks.

BRIEF DESCRIPTION OF THE DRAWINGS

In the following, the essential features of the invention will be described in detail by showing preferred embodiments, with reference to the figures of the attached drawings.

FIG. 1 is a simplified block diagram of a Rule Engine utilized in the adaptable network bridge of the present invention;

FIG. 2 is a sequence diagram illustrating the steps of a process performed by the Rule Engine; and

FIG. 3 is an illustration of a network of adaptable Ethernet bridges controlled by a Network Management System (NMS).

DETAILED DESCRIPTION OF THE INVENTION

In the following description, for purposes of explanation and not limitation, specific details are set forth, such as particular embodiments, circuits, signal formats etc. in order to provide a thorough understanding of the present invention. It will be apparent to one skilled in the art that the present invention may be

practiced in other embodiments that depart from these specific details.

In existing Ethernet bridges, there are two identifiable phases in the switching process. In the first phase, parts of the frame header are checked for specific information. For example, the destination address of each frame may be checked against a forwarding table, priority bits, VLAN tags, and the like. In the second phase, different actions are taken within the bridge depending on the result of this check. For example, the frame may be sent to the port pointed to in the forwarding table, or the frame may be sent to all ports except the originating port, and so on. These steps characterize a process in which a frame is put through a filter that selects the action to take. Another important element is that the bridge stores and retrieves information in the form of a simple state vector in a forwarding table (i.e., memory), which the bridge is using in the process. However, the different parts of this process are fixed and may not be altered.

The present invention is based on a generalization of this switching process that adds several new key aspects to switching, enabling new ways of adapting and controlling the switching process as well as new ways to control Ethernet networks. The invention provides an adaptable Ethernet bridge having a Rule Engine that simplifies the addition or modification of functionality within the bridge. One of the purposes of the adaptable bridge is to provide a simple solution whereby anyone with reasonable skill can implement and add new functionality in a standardized way on standard equipment. Simplicity is achieved by specifying how Ethernet frames should be processed and switched in terms of switching rules. Flexibility is achieved by enabling dynamic loading and updating, inspection, and prioritization of rules in bridges via a protocol.

The generalized switching process consists of the Rule Engine processing Ethernet frames by applying the switching rules. A switching rule encapsulates a specific switching behavior that describes the filter and action processes together with the state vector. A switching rule thus consists of three parts:

1) A filter function that can filter any part or parts of a frame. The purpose of the filter is to decide if the rule is applicable to a given frame. In other words, the filter works as a predicate function on frames. In this decision process information in the state vector may be used.

2) An action function that describes how a frame header (or the entire frame) should be transformed and how the frame should be switched, i.e. to which port or ports the frame should be sent. In this process the action function may alter the state vector.

3) A state vector that the filter function and the action function can use in the switching process.

The switching rule can also contain other information such as version, priority specification, vendor information, and the like.

The state vector is an abstraction of several parts:

1) A local memory for a rule or a set of rules where rule-specific data can be stored and altered. Specific "management rules" make it possible to access that data from, for example, a management system.

2) A global bridge memory where bridge-specific data applicable to and accessible by all rules can be stored and altered. One example is the port-forwarding table.

3) Access to a set of bridge resources that can be implemented as library functions. Some examples are a function to retrieve the source port of the frame processed, a function that provides timestamps, counters and timers, and functions that describe the traffic flows and load in the bridge. The invention is not limited to these examples; other functions may be identified by those skilled in the art.

A switching rule describes the types of frames that match the rule and how these frames should be processed (e.g., switched or transformed before switching). Each incoming frame is checked against the set of rules stored in the bridge. If a rule matches, the frame is processed and switched according to the specification in the rule. If no rule matches the frame, a default rule may be utilized, or the frame may be dropped.

With the concept of rules, the switching process is defined as a simple and understandable programming model. Standardizing rule language and making it possible to dynamically load new rules in a bridge also makes it possible to add new functionality, adapting standard equipment to the needs at hand. If some functionality becomes obsolete, that functionality can be removed by removing the

rule or set of rules implementing it.

A powerful extension is to allow different rule sets to be valid for different ports enabling, for example, different network providers to share the same hardware but have different network behavior. Different embodiments of this extension include: a rules control mechanism that selects and prioritizes available rule sets based on port, time of day, load, and the like. Alternatively, this kind of information may be described in the filter functions, and the Rule Engine tries all rules until it finds a match.

Yet another powerful extension is to allow rules that monitor the state vector instead of being matched against Ethernet frames. That is, the filter function monitors the state vector, and when some condition is fulfilled, the action function is invoked. The monitoring process can be implemented by regularly processing these rules in the Rule Engine or in a separate Rule Engine.

Note that allowing the filter and action functions to have access to a state vector that goes beyond the forwarding table provides new and powerful ways to process and switch frames.

FIG. 1 is a simplified block diagram of an exemplary embodiment of the dynamically adaptable network bridge 10 of the present invention. The adaptable bridge includes many of the same components as existing bridges such as switch fabric 11, frame buffers 12a-12n and 13a-13n, and ports 14a-14n and 15a-15n. In addition, however, the adaptable bridge includes a Rule Engine 16, which replaces the implementation of some or all protocols. The adaptable bridge also includes a state vector memory 17 accessible by the Rule Engine, a rule control function 18, and a rules memory 19 accessible by the Rule Engine through the rule control function. Collectively, these new bridge components enable the adaptable bridge to receive and store rules from external units, store a state vector which may be dependent on external sources, and store rules that are imposed on other bridges.

Hybrid designs having both a Rule Engine and some of the protocols of existing bridges may also be implemented. The Rule Engine has processing capabilities, that is, the Rule Engine can (1) apply the filter function to a frame and calculate the result; (2) apply the action function if the rule matches; (3) access

the state vector; and (4) access the other resources of the switch. A frame entering the adaptable bridge through an input port such as port 14a and frame buffer 12a is acted upon by switching rules in the Rule Engine 16, including the filter function, action function, and state vector. The result is a calculated result frame, which is outputted through switch fabric 11, and an appropriate frame buffer and output port such as frame buffer 13a and output port 15a.

The rule control function 18 adds and removes rules dynamically, and orders or prioritizes THE set of rules. The rule control function may be implemented as protocols and secured against unwanted manipulation by using well known techniques intended for that purpose, for example, using digital signatures and encryption. Additionally, the rule control function may include a mechanism to transform (or translate) switching rules in human-readable form to an efficient form understandable by the Rule Engine 16.

The mechanisms to access different bridge resources and state information (i.e., state vectors), mechanisms to access library functions, and a protocol for externally accessing the state information are important parts of the adaptable bridge. The bridge resources and state information may be accessed via, for example, an Application Programming Interface (API). The protocol for externally accessing the state information may be implemented as a set of rules. The state of the bridge can affect switching rules dynamically, that is, a rule can behave differently depending on the current state. For example, frames can be switched differently depending on time of day, traffic pattern, traffic load, and the like. This behavior can also be controlled externally by, for example, a network management system (NMS).

FIG. 2 is a sequence diagram illustrating the steps of a method of processing an Ethernet frame by the Rule Engine 16. The process starts at step 21 and moves to step 22 where, for each incoming Ethernet frame, the port-specific rules associated with the Source Port are merged with the rules shared among all ports of the bridge (this merge can be done in advance by the priority module as a ordered list). The rules in the list are then tested to determine whether the frame matches the rule. This process begins at step 23, where a determination is made whether there are any more rules left to test. If not, and all

the rules have been tested, the frame is dropped at step 24. However, in the case of the first rule, there are rules left to test, so the method moves to step 25 where the filter function of the first rule in the list is applied to the frame. The filter function uses the information found in the frame together with the current state vector to determine whether the frame matches the rule. The filter function is a predicate, so the result at step 26 will be either true (the frame matches the rule) or false (the frame does not match the rule). If the result is false, the rule is discarded at step 27, and the method returns to step 23 where the test is performed on the next rule in the list.

The remainder of the rules are then tested until either no rules are left and the frame is dropped at step 24, or there is a match at step 26, and the method moves to step 28 where the action function of the rule is applied to the frame. The action function may use the library functions, the information in the frame, and the state vector to transform (or modify) the frame. In this process, the action function can use functions to modify the state vector. For example, a counter may be incremented, which counts the number of frames containing a specific high-level protocol coming from the port. At step 29, the action function determines the destination port or ports and sends the (possibly transformed) frame to the determined port or ports. The method then ends at step 30.

Another important aspect of the invention not shown in the sequence diagram is that other resources or modules in the bridge may continuously monitor and change the state vector in parallel. An extended Rule Engine, to the one described, may then invoke rules that, instead of being matched against Ethernet frames, monitor the state vector. When one or more predefined criteria are fulfilled (determined by the filter function), the action function generates new frames containing new rules to be sent to the bridge itself or to nearby bridges altering their behavior.

FIG. 3 is an illustration of a network 35 of adaptable Ethernet bridges controlled by a Network Management System (NMS) 36. The NMS monitors the state in the bridges and issues rules that adapt the behavior of certain bridges accordingly. For example, if $Bridge_{11}$ becomes heavily loaded with traffic, the NMS may issue a rule that will move some traffic from associated bridges (i.e.,

$Bridge_{21}$ – $Bridge_{23}$) to $Bridge_{12}$. For example, the rule may move every third frame or frames carrying a particular protocol to $Bridge_{12}$. Context information may also be added to the state vector, thereby allowing context to influence switching. Context information may contain, but is not limited to, information about traffic load in nearby bridges, forecasts or predictions of expected traffic, and the like. This feature is of particular interest in a mobile environment.

The NMS 36 is shown connected to the network by a dotted line because the adaptable bridges may automatically generate specific context rules and distribute them to nearby bridges as users move around in the network. When bridges automatically generate rules to other bridges (and to themselves), a self-managed network can be implemented in which bridges exchange rules dynamically. This capability can be used, for example, to setup a particular flow-path, distribute traffic during heavy load, or automatically redirect traffic in the case of network failures. For example, if Bridge11 receives a flow of high priority frames when it is already heavily loaded with traffic, it can issue a rule or set of rules to Bridge22 that move the flow to Bridge12 instead.

An Ethernet bridge is working in "wire-speed" and therefore it is desirable that the bridge introduce as little delay as possible. Adding a Rule Engine and basing the switching on rules may increase the delay. However, a number of techniques and mechanisms can be used to make the Rule Engine more efficient:

1) Filter functions can be tested in parallel, and a priority module can select the matching rule with highest priority. These computations can be performed because the filter functions are pure predicates, i.e. they contain no side effects.

2) Filter functions will in most cases be a conjunction (or disjunction) of comparisons. These can be directly mapped onto a pipelined matrix of comparison modules in hardware.

3) A similar pipelined hardware matrix realizing the language constructs used in the action functions can be implemented.

4) Some parts of the state vector, for example library functions reflecting bridge context and resources, can be implemented in hardware such as registers, thereby providing "instant" access to them.

In the preferred embodiment, the rule language used to describe the filter

and action functions is not a general purpose programming language. A programming language should only have the necessary constructs and mechanisms needed to express the solutions to the problems in the specified domain. If the language is too powerful, as a general-purpose language, it is possible to express an infinite loop (accidentally or on purpose) thereby increasing the delay to infinity. The preferred switching rule language, therefore, is a language primarily restricted to the domain of Ethernet switching (layer 2), with language constructs expressing the mechanisms used in the switching process. However, language constructs that are useful for other purposes like network management, constructs related to exchange of new rules, and so on, that are not in conflict with the basic requirements may also be included.

The present invention provides several advantages. The Ethernet standards can be implemented as switching rule sets, and as the standards evolve, the rule sets are updated. These updated rule sets can then easily be loaded into an adaptable network bridge. The rule sets can be vendor-independent and, for example, published by IEEE. Today, each vendor decides which protocols (standards) to support in a bridge, and unless the vendor issues an update whenever the standard is updated, users have to buy a new bridge if they need to follow the new standard.

In the present invention, the "programming language" of rules may be standardized thereby enabling anyone to add new functionality, as a switching rule, to any bridge with a Rule Engine. These rules can then be updated or removed if necessary. A proprietary solution can also be implemented as a rule or set of rules and loaded in any bridge with a Rule Engine. If a user later wants to use another solution, the rule set is simply replaced with a new rule set. It will be much less expensive to implement new functionality because, in most cases, the user only has to write some software in the form of a set of rules.

The present invention also greatly increases flexibility in networks because each bridge can be loaded with its own rule set down to the individual port level. The invention also provides the ability to adapt the functionality on each port based on time, user demands, service agreements, and the like. For example, different operators can share the same physical bridge (network) and provide

different services to their respective users.

Some examples of functionality that can be implemented with switching rules include the following:

1) Broadcast tunnels. It is simple to implement broadcast tunnels necessary for building Public Ethernet Networks.

2) Distributed router functionality added to a set of bridges.

3) Simple firewall functionality.

4) User adapted services on the port level.

5) Authentication and security mechanisms on the port level that are transparent to users.

6) Self-managed networks or semi-self managed networks.

This list is not intended to be exhaustive, and other functions may also be implemented with switching rules and loaded into any adaptable bridge with a Rule Engine.

As shown by the above examples, the state of the dynamically adaptable bridge can be utilized in the switching process to enable entirely new functionality and to provide new ways to use bridges in networks.

Although preferred embodiments of the present invention have been illustrated in the accompanying drawings and described in the foregoing Detailed Description, it is understood that the invention is not limited to the embodiments disclosed, but is capable of numerous rearrangements, modifications, and substitutions without departing from the scope of the invention. The specification contemplates any all modifications that fall within the scope of the invention defined by the following claims.

WHAT IS CLAIMED IS:

1. A dynamically adaptable network bridge comprising:

a Rule Engine that processes data frames according to a set of switching rules, wherein each switching rule identifies a type of frame to which the rule applies, and how the type of frame is to be processed; and

means for dynamically modifying the switching rules.

2. The dynamically adaptable network bridge of claim 1 wherein the means for dynamically modifying the switching rules includes a protocol for dynamically loading and updating the switching rules.

3. The dynamically adaptable network bridge of claim 1, wherein each switching rule includes a filter function for determining whether a given rule is applicable to a given frame.

4. The dynamically adaptable network bridge of claim 3, wherein each switching rule also includes an action function for specifying changes to the given frame's header and how the given frame should be switched.

5. The dynamically adaptable network bridge of claim 1, wherein each switching rule includes a state vector utilized for processing the type of frames to which each rule applies.

6. The dynamically adaptable network bridge of claim 5, wherein the state vector includes an abstraction of a local memory for storing rule-specific data for each switching rule.

7. The dynamically adaptable network bridge of claim 6, wherein specific management rules enable the Rule Engine to access the rule-specific data for each switching rule.

8. The dynamically adaptable network bridge of claim 6, wherein the state vector also includes an abstraction of a global bridge memory for storing bridge-specific data applicable to and accessible by all the switching rules.

9. The dynamically adaptable network bridge of claim 8, wherein the bridge-specific data includes a port-forwarding table.

10. The dynamically adaptable network bridge of claim 8, wherein the state vector also includes a set of library functions that implement bridge resources.

11. The dynamically adaptable network bridge of claim 10, wherein the set of library functions are selected from a group consisting of:

a function that retrieves a source port of a processed frame;

a function that provides timestamps;

a function that describes traffic flows in the bridge; and

a function that indicates the traffic load in the bridge.

12. The dynamically adaptable network bridge of claim 3, wherein the given frame is processed in accordance with the given rule if the filter function determines that the given rule is applicable to the given frame, and the given frame is dropped if the filter function determines that there is no rule applicable to the given frame.

13. The dynamically adaptable network bridge of claim 1, wherein the bridge includes a plurality of input/output ports, and the Rule Engine includes a plurality of sets of switching rules, wherein each set of switching rules is applicable to a different port in the bridge.

14. The dynamically adaptable network bridge of claim 1, wherein the bridge is an Ethernet bridge.

15. The dynamically adaptable network bridge of claim 1, wherein the means for dynamically modifying the switching rules includes a protocol that dynamically adds, subtracts, and modifies the switching rules.

16. The dynamically adaptable network bridge of claim 1, further comprising means for prioritizing rules within the set of switching rules.

17. The dynamically adaptable network bridge of claim 1, further comprising means for accessing state information for the bridge, wherein a given rule causes a given frame to be processed differently when the state information changes.

18. The dynamically adaptable network bridge of claim 17, wherein the given rule processes the given frame differently, depending on traffic load in the bridge.

19. The dynamically adaptable network bridge of claim 17, further comprising a port for receiving rules from a Network Management System (NMS), wherein the NMS monitors the state information for a plurality of adaptable bridges in a network, and issues rules that adapt the behavior of the bridge to optimize network performance.

20. The dynamically adaptable network bridge of claim 17, wherein the state information includes context information, wherein a given rule causes a given frame to be processed differently when the context information changes.

21. The dynamically adaptable network bridge of claim 1, wherein the bridge is one of a plurality of adaptable bridges in a network, and the bridge further comprises means for generating specific context rules and distributing the context rules to other adaptable bridges in the network.

22. A method of processing and switching data frames in an adaptable network bridge, said method comprising the steps of:

defining a set of switching rules for the adaptable bridge;

receiving a given frame in the bridge;

determining whether any of the rules are applicable to the given frame; and

upon determining that one of the rules is applicable to the given frame, processing and switching the frame according to the applicable rule.

23. The method of claim 22, further comprising dynamically adding, subtracting, and modifying the switching rules.

24. The method of claim 23, further comprising accessing state information for the bridge, wherein the step of dynamically adding, subtracting, and modifying the switching rules is performed in response to a change in the state information.

25. The method of claim 24, wherein the bridge is one of a plurality of adaptable bridges in a network, and the method further comprises the steps of:

receiving a new or modified switching rule from a Network Management System (NMS), wherein the NMS monitors the state information for a plurality of adaptable bridges in a network, and issues rules that adapt the behavior of the bridge to optimize network performance; and

processing and switching frames according to the new or modified switching rule received from the NMS.

26. The method of claim 24, further comprising adding context information to the state information, wherein the step of dynamically adding, subtracting, and modifying the switching rules is performed in response to a change in the context information.

27. The method of claim 22, wherein the bridge is one of a plurality of adaptable bridges in a network, and the method further comprises the steps of:

generating specific context rules; and

distributing the context rules to other adaptable bridges in the network.

28. The method of claim 22, wherein the bridge is an Ethernet bridge.

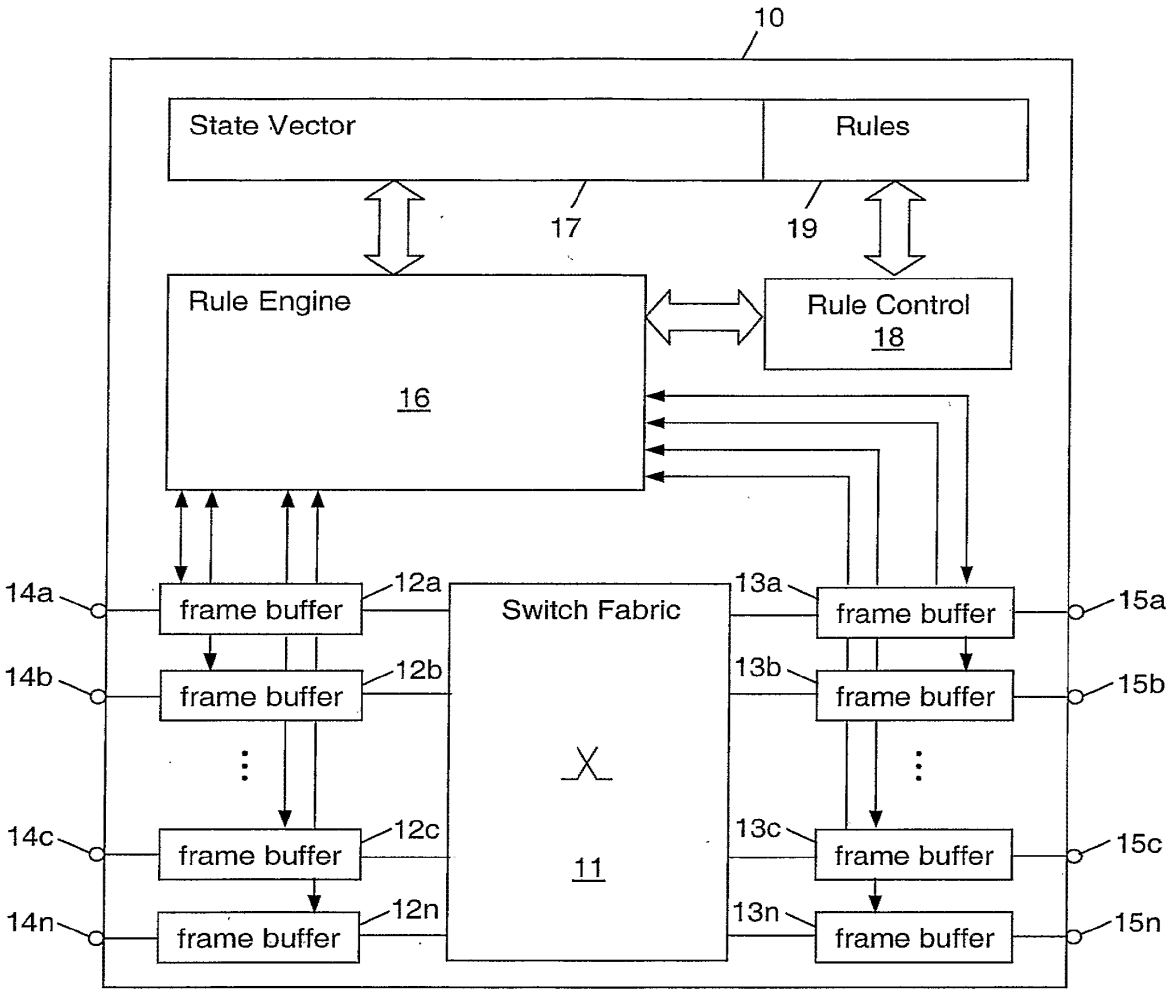

10
State Vector
Rules
17
19
Rule Engine
16
Rule Control
18
14a
frame buffer
12a
Switch Fabric
13a
frame buffer
15a
14b
frame buffer
12b
13b
frame buffer
15b
14c
frame buffer
12c
11
13c
frame buffer
15c
14n
frame buffer
12n
13n
frame buffer
15n

FIG. 1

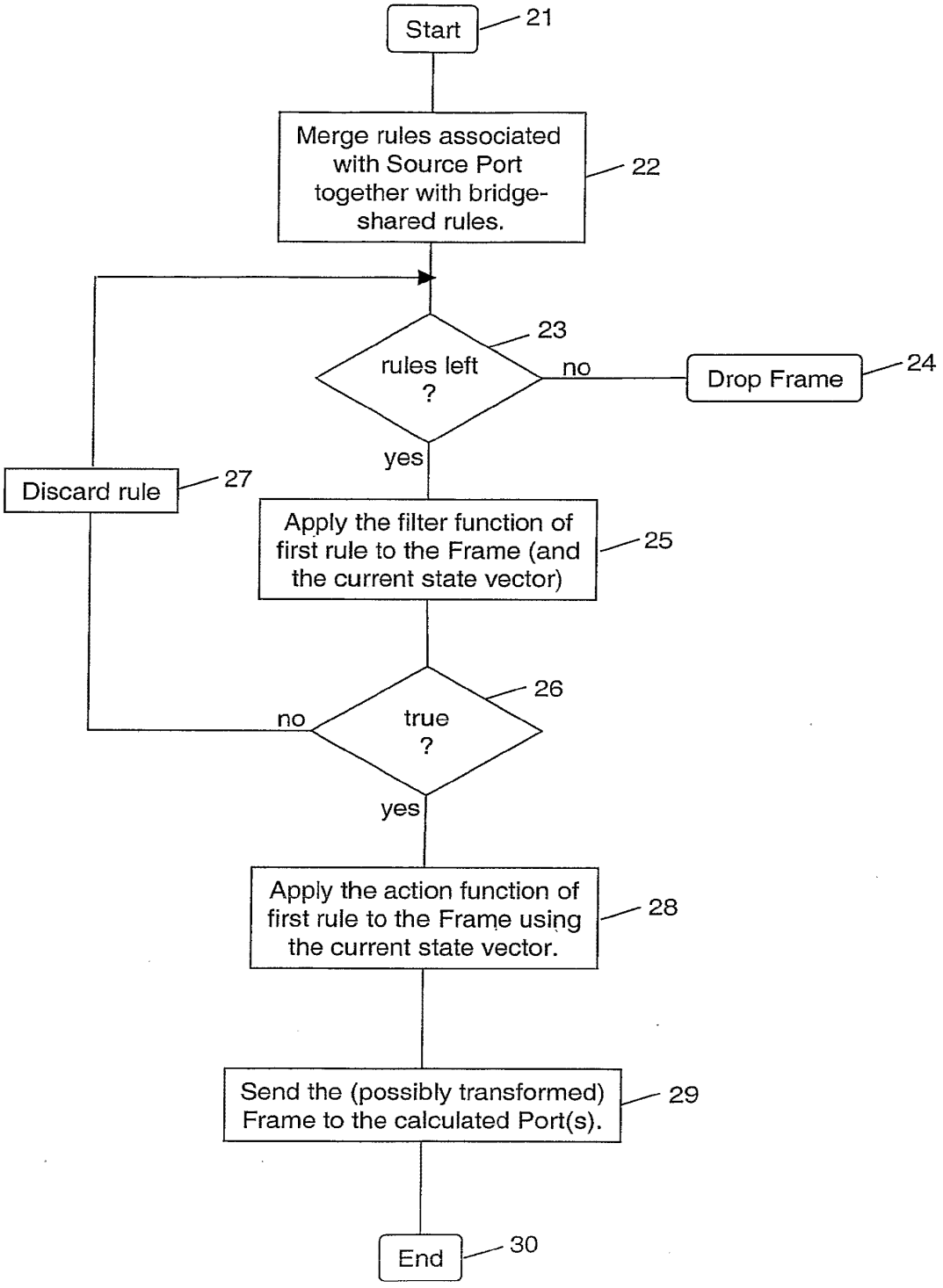

Start
21
Merge rules associated with Source Port together with bridge-shared rules.
22
rules left ?
23
no
Drop Frame
24
yes
Discard rule
27
Apply the filter function of first rule to the Frame (and the current state vector)
25
true ?
26
no
yes
Apply the action function of first rule to the Frame using the current state vector.
28
Send the (possibly transformed) Frame to the calculated Port(s).
29
End
30

FIG. 2

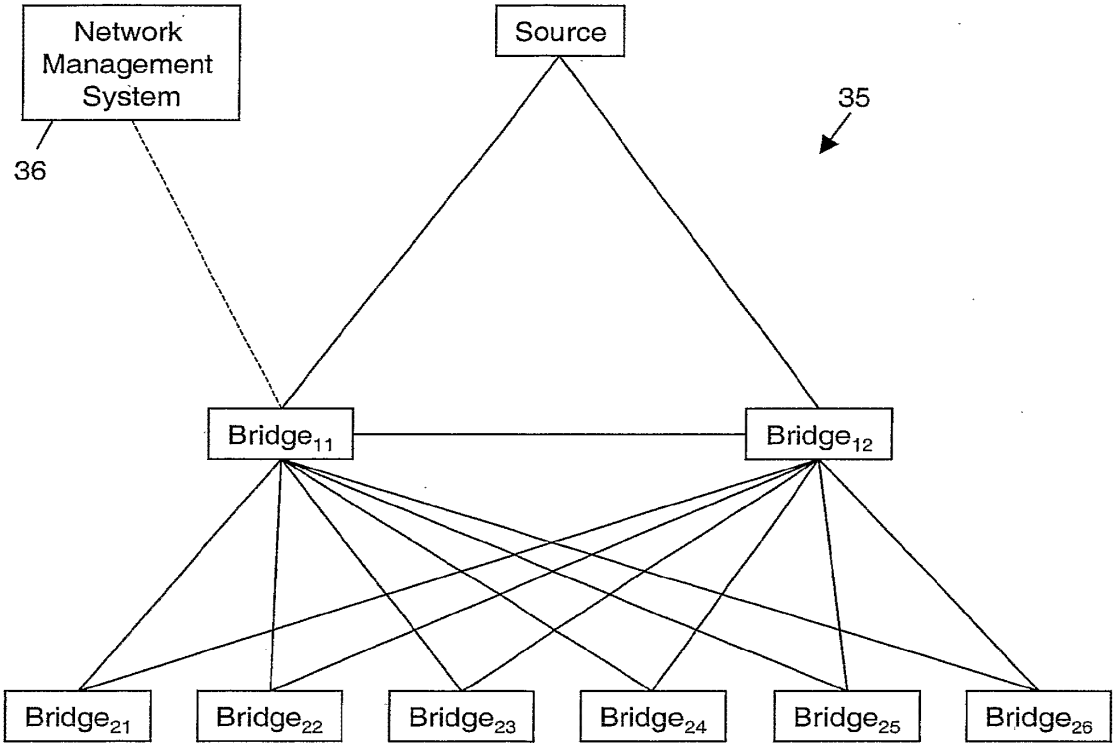

Network Management System
36
Source
35
Bridge11
Bridge12
Bridge21
Bridge22
Bridge23
Bridge24
Bridge25
Bridge26

FIG. 3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/SE2004/001611

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/56 H04L12/46

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 790 554 A (PITCHER ET AL) 4 August 1998 (1998-08-04) abstract column 1, line 15 - column 1, line 67 column 2, line 39 - column 3, line 25 column 3, line 48 - column 4, line 42 column 4, line 60 - column 8, line 4 column 8, line 24 - column 8, line 26; claims 1,2,14,22,28; figures 2,3 ----- -/--	1-5, 12-20, 22-25, 27,28

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 March 2005	31/03/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Todorut, C

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
T/SE2004/001611

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 396 493 A (SUGIYAMA ET AL) 7 March 1995 (1995-03-07) abstract column 1, line 63 - column 3, line 11 column 4, line 11 - column 4, line 51 column 5, line 67 - column 6, line 39; claims 1,17; figures 1-4	1-28
X	WO 00/56024 A (BROADCOM CORPORATION; KADAMBI, SHIRI; AMBE, SHEKHAR; KALKUNTE, MOHAN;) 21 September 2000 (2000-09-21) abstract	1-4,22, 23
A	page 53, line 12 - page 65, line 21; claims 1,2	5-21, 24-28
A	US 2003/123387 A1 (JACKSON ANDREW LLOYD 'GB!) 3 July 2003 (2003-07-03) abstract column 1, paragraph 2 - column 1, paragraph 9 column 2, paragraph 16 - column 3, paragraph 25; claims 1,6,9; figure 4	1-28
A	US 5 959 976 A (KUO ET AL) 28 September 1999 (1999-09-28) abstract column 1, line 5 - column 2, line 40 column 3, line 8 - column 3, line 18 column 5, line 56 - column 6, line 10; claim 1; figures 3-5	1-28
A	EP 0 508 886 A (DIGITAL EQUIPMENT CORPORATION) 14 October 1992 (1992-10-14) abstract column 1, line 40 - column 3, line 54 column 4, line 45 - column 5, line 16 column 5, line 55 - column 6, line 53; claims 1,23; figures 5-8	1-28
A	US 5 515 376 A (MURTHY ET AL) 7 May 1996 (1996-05-07) abstract column 6, line 1 - column 9, line 21	1-28

1

Form PCT/ISA/210 (continuation of second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
/SE2004/001611

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5790554 A	04-08-1998	NONE	
US 5396493 A	07-03-1995	JP 6224918 A	12-08-1994
		KR 9614983 B1	23-10-1996
WO 0056024 A	21-09-2000	US 2001043611 A1	22-11-2001
		AU 3529500 A	04-10-2000
		AU 3752000 A	04-10-2000
		AU 4325800 A	04-10-2000
		EP 1161817 A2	12-12-2001
		EP 1169809 A2	09-01-2002
		EP 1159805 A2	05-12-2001
		WO 0056024 A2	21-09-2000
		WO 0056011 A2	21-09-2000
		WO 0056013 A2	21-09-2000
		US 6707817 B1	16-03-2004
		US 6810037 B1	26-10-2004
		US 6850521 B1	01-02-2005
		US 6707818 B1	16-03-2004
		US 2004174898 A1	09-09-2004
		US 2005047411 A1	03-03-2005
		US 2002039365 A1	04-04-2002
		AU 5442700 A	12-12-2000
		AU 5586400 A	12-12-2000
		AU 5737300 A	31-01-2001
		AU 6334400 A	22-01-2001
		EP 1181791 A1	27-02-2002
		EP 1181792 A1	27-02-2002
		EP 1212867 A2	12-06-2002
		EP 1192767 A2	03-04-2002
		WO 0072533 A1	30-11-2000
		WO 0102965 A2	11-01-2001
		WO 0072531 A1	30-11-2000
		WO 0101724 A2	04-01-2001
		US 2002093974 A1	18-07-2002
		US 2002186705 A1	12-12-2002
		US 6813268 B1	02-11-2004
		US 6735679 B1	11-05-2004
		US 6792500 B1	14-09-2004
		US 6842457 B1	11-01-2005
		US 6430188 B1	06-08-2002
		US 6859454 B1	22-02-2005
		US 2004170176 A1	02-09-2004
		US 2005036488 A1	17-02-2005
		US 2002031090 A1	14-03-2002
US 2003123387 A1	03-07-2003	NONE	
US 5959976 A	28-09-1999	NONE	
EP 0508886 A	14-10-1992	DE 69217103 D1	13-03-1997
		DE 69217103 T2	21-08-1997
		EP 0508886 A1	14-10-1992
		JP 5114905 A	07-05-1993
		US 5515513 A	07-05-1996
US 5515376 A	07-05-1996	EP 0710415 A1	08-05-1996
		JP 3335358 B2	15-10-2002

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
/SE2004/001611

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5515376 A		JP 9500774 T	21-01-1997
		WO 9503659 A1	02-02-1995
		US 5610905 A	11-03-1997
		US 6545982 B1	08-04-2003

Espacenet

Bibliographic data: EP2385676 (A1) — 2011-11-09

Method for adapting security policies of an information system infrastructure

Inventor(s): CUPPENS FREDERIC [FR]; CUPPENS NORA [FR]; DUBUS SAMUEL [FR]; KANOUN WAEL [FR] ± (CUPPENS, FREDERIC, ; CUPPENS, NORA, ; DUBUS, SAMUEL, ; KANOUN, WAEL)

Applicant(s): ALCATEL LUCENT [FR]; INST TELECOM TELECOM BRETAGNE [FR] ± (ALCATEL LUCENT, ; INSTITUT TELECOM - TELECOM BRETAGNE)

Classification: **- international:** ***G06F21/57; H04L29/06***
- cooperative: **G06F21/577**; **H04L63/1408**; **H04L63/1433**; **H04L63/20**; H04L63/1441

Application number: EP20100290250 20100507

Priority number (s): EP20100290250 20100507

Also published as: US2013111548 (A1) KR20130005301 (A) JP2013525927 (A) WO2011138417 (A1) CN102934122 (A)

Abstract of EP2385676 (A1)

The present invention refers to a method for adapting security policies of an information system infrastructure in function of attacks wherein it comprises the steps of: - storing potential attacks and their associated risks in a data repository (125); - storing curative security policies (128) in response of the potential attacks in a data repository; - monitoring (101) entering contents representing data streams of the information system; - detecting (129) at least one attack in the information system; - assessing a success probability parameter (132) of the at least one detected attack and its associated cost impact parameter (133); -

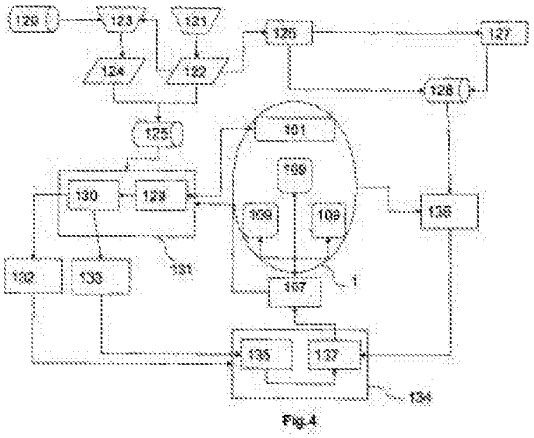


Fig.4

assessing an activation impact parameter (136) of at least one curative security policy in response to the at least one detected attack and its associated cost impact parameter; - deciding of the activation or deactivation (134) of a curative security policy in function of the success probability parameter of the, at least one, detected attack, of the activation impact parameter of at least one curative security policy and of the cost impact parameters of both the detected at least one attack and the at least one curative security policy.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 385 676 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
09.11.2011 Bulletin 2011/45

(51) Int Cl.:
H04L 29/06 *(2006.01)* ***G06F 21/00*** *(2006.01)*

(21) Application number: **10290250.9**

(22) Date of filing: **07.05.2010**

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK SM TR
Designated Extension States:
BA ME RS

(71) Applicants:
- **Alcatel Lucent**
  75008 Paris (FR)
- **Institut Télécom - Télécom Bretagne**
  29238 BREST cedex 3 (FR)

(72) Inventors:
- **Cuppens, Frédéric**
  29238 Brest Cedex 3 (FR)
- **Cuppens, Nora**
  29238 Brest Cedex 3 (FR)
- **Dubus, Samuel**
  91620 Nozay (FR)
- **Kanoun, Wael**
  91620 Nozay (FR)

(74) Representative: **Croonenbroek, Thomas Jakob et al**
Cabinet Innovincia
11, avenue des Tilleuls
74200 Thonon-les-Bains (FR)

(54) Method for adapting security policies of an information system infrastructure

(57) The present invention refers to a method for adapting security policies of an information system infrastructure in function of attacks wherein it comprises the steps of:
- storing potential attacks and their associated risks in a data repository (125);
- storing curative security policies (128) in response of the potential attacks in a data repository;
- monitoring (101) entering contents representing data streams of the information system;
- detecting (129) at least one attack in the information system;
- assessing a success probability parameter (132) of the at least one detected attack and its associated cost impact parameter (133);
- assessing an activation impact parameter (136) of at least one curative security policy in response to the at least one detected attack and its associated cost impact parameter;
- deciding of the activation or deactivation (134) of a curative security policy in function of the success probability parameter of the, at least one, detected attack, of the activation impact parameter of at least one curative security policy and of the cost impact parameters of both the detected at least one attack and the at least one curative security policy.

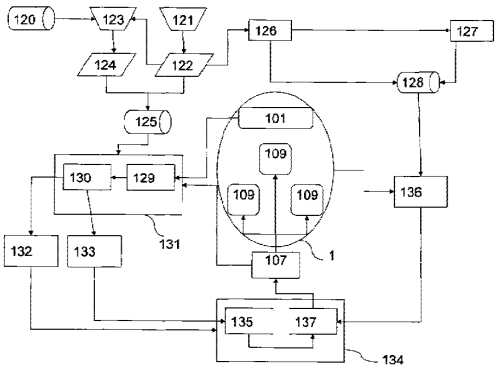


Fig.4

EP 2 385 676 A1

Description

[0001] The present invention relates to the field of information system protection and more precisely to the management of security policy in function of attacks undergone or being undergone by the information system.

[0002] Infrastructures of information systems need to be protected from harmful attacks leading to malicious events such as intrusions, data thefts, viruses or worms...

[0003] Due to the potential number of alerts generated by the existing attack detection systems with large information system infrastructures, it becomes impossible for operators to assess in real-time the risk of an attack and to decide of the suitable response to apply in response to the attack. Thus, automatic deployment of formally defined operational security policies starts to be considered in the protection of telecommunication and information infrastructures.

[0004] Fig.1 represents an example of such automatic protection of the state of the art.

[0005] The first step 101 corresponds to the detection of attacks toward the monitored information system which leads to the creation of elementary alerts (102). An alert correlation is then processed (103) to define correlated alerts (104) that are sent to a policy instantiation engine (105) to activate the appropriate security rules (106). These rules are sent to a policy decision point (107) which generates the configuration scripts (108) which are then used to configure policy enforcement points (109). Said policy enforcement points (109) are located in the information system 1 and apply the security rules in response to the detected attacks.

[0006] Such configuration of automatic policy activation suffers from drawbacks. Indeed, it is based only on correlated alerts and the number of correlated alerts may reach a very large number (up to thousands within a single day with large system) which would lead to thousands of security policy activations. Moreover, the deactivation of said security policies is not taken into account in the configurations of the state of the art such that a security policy may remain activated even if its impact on the users of the information system 1 is worth than the impact of the attack.

SUMMARY OF THE INVENTION

[0007] One object of the present invention is therefore to overcome the precited drawbacks of the state of the art and offer a method that allow to dynamically trig security policy activations only when it is necessary by taking into account a plurality of parameters influencing the activation decision and by defining a method that allow the deactivation of a security policy when it is necessary.

[0008] This is achieved by a method for adapting security policies of an information system infrastructure in function of attacks wherein it comprises the steps of:

- storing potential attacks and their associated risks in a data repository;
- storing curative security policies in response of the potential attacks in a data repository;
- monitoring entering contents representing data streams of the information system;
- detecting at least one attack in the information system;
- assessing a success probability parameter of the at least one detected attack and its associated cost impact parameter;
- assessing an activation impact parameter of at least one curative security policy in response to the at least one detected attack and its associated cost impact parameter;
- deciding of the activation or deactivation of a curative security policy in function of the success probability parameter of the, at least one, detected attack, of the activation impact parameter of at least one curative security policy and of the cost impact parameters of both the detected at least one attack and the at least one curative security policy.

[0009] According to another aspect of the invention, the step of storing potential attacks and their associated risks in a data repository comprises the steps of:

- defining the information system topology and attack detection signatures;
- defining a risk analysis of the information system that identifies potential attack objectives;
- specifying attack models to reach the identified attack objectives;
- storing said attack models in a data repository.

[0010] According to a further aspect of the invention, the step of storing curative security policies in response of the potential attacks in a data repository comprises:

- specifying at least one attack context;
- specifying curative security policies corresponding to the specified at least one attack context;
- storing said curative security policies in a data repository.

[0011] According to an additional aspect of the present invention, the step of assessing a success probability parameter of the at least one detected attack and its associated cost impact parameter comprises:

- generating attack strategy graphs based on the stored attack models and the detected at least one attack;
- assessing the probability for the attack to reach its objective;
- assessing the impact of the attack objective on the system security level and on the system quality of service (QoS) level;
- assessing the associated cost impact parameter of

EX1002
CISCO SYSTEMS, INC. / Page 331 of 1453

the attack objective;

[0012] According to another aspect of the present invention, the step of assessing an activation impact parameter of at least one curative security policy in response to the at least one detected attack and its associated cost impact parameter is based on the stored curative security policies and the state of the monitored information system.

[0013] According to a further aspect of the invention, the step of deciding of the activation or deactivation of a curative security policy in function of the success probability parameter of the, at least one, detected attack, of the activation impact parameter of at least one curative security policy and of the cost impact parameters of both the detected at least one attack and the at least one curative security policy is applied dynamically based on the evolution of the state of the monitored system.

[0014] According to an additional aspect of the invention, the cost impact parameters comprise:

- a quality of service (QoS) impact and,
- a security level degradation impact.

[0015] The present invention also refers to a monitoring and protecting equipment comprising:

- at least one data repository for:
  - storing potential attacks and their associated risks;
  - storing curative security policies in response of the potential attacks;
- processing means for:
  - monitoring entering contents representing data streams of the information system;
  - detecting at least one attack in the information system;
  - assessing a success probability parameter of the detected at least one attack and its associated cost impact parameter;
  - assessing at least one activation impact parameter of at least one curative security policy in response to the at least one detected attack and its associated cost impact parameter;
  - deciding of the activation of a curative security policy in function of the success probability parameter of the at least one detected attack, of the activation impact parameter of at least one curative security policy and of the cost impact parameters of both the at least oneattack and the at least one curative policy,
  - activating at least one curative security policy.

[0016] The present invention also refers to a monitoring and protecting equipment comprising:

- at least one data repository for:
  - storing potential attacks and their associated risks;
  - storing curative security policies in response of the potential attacks;
- processing means for:
  - monitoring entering contents representing data streams of the information system;
  - detecting at least one attack in the information system;
  - assessing a success probability parameter of the detected at least one attack and its associated cost impact parameter;
  - assessing at least one activation impact parameter of at least one curative security policy in response to the at least one detected attack and its associated cost impact parameter;
  - deciding of the deactivation of a curative security policy in function of the success probability parameter of the at least one detected attack, of the activation impact parameter of at least one curative security policy and of the cost impact parameters of both the at least one attack and the at least one curative policy,
  - deactivating at least one curative security policy.

BRIEF DESCRIPTION OF THE DRAWINGS

[0017]

FIG.**1** is a synoptic diagram of the different steps of a protective method for launching security policies against attacks of an information system according to the state of the art;

FIG.**2** is a synoptic diagram of the different steps of a protective method for adapting security policies of an information system infrastructure against attacks according to the present invention;

FIG.**3** is a diagram of an example of attack graph comprising the different attack steps and the objectives associated with these attacks;

FIG.4 is a synoptic diagram of the different steps of a detailed protective method for adapting security policies of an information system infrastructure against attacks according to the present invention;

DETAILED DESCRIPTION OF THE INVENTION

[0018] As used herein, the term "attack" refers to an event in a system that transgress the normal authorized usage of the system or exploits deliberately or accidentally a vulnerability in the system as for example a network scanning, a password cracking, a sending of malicious email (also called spam), a sending of a malformed internet protocol (IP) packet... Moreover, the expression

EX1002
CISCO SYSTEMS, INC. / Page 332 of 1453

attack with respect to an information system refers to attacks initiated from outside or inside of the information system (usually from an attacker machine) and directed toward said information system in order to produce dysfunctionings in said system.

[0019] As used herein, the term "SIP" refers to the acronym session Internet protocol.

[0020] As used herein, the term "IP" refers to the acronym Internet protocol.

[0021] As used herein, the term "QoS" refers to the acronym quality of service.

[0022] The embodiments of the present invention refer to a method for activating and deactivating security policies in order to protect an information system against malicious attacks wherein not only impacts of the attacks but also the success likelihood for the attack to reach its objective and impacts of security policies are taken into account in the activation/deactivation decision in order to minimize the impact, and in particular the cost, of attacks on the users of the information system.

[0023] Fig.2 represents the general steps of the method for adapting the protection of the information system 1.

[0024] Step 110 refers to the specification and the storing in a data repository of potential attacks and their associated risks. This first step allows to provide attack models that define the strategy and the objectives of the possible attacks.

[0025] Step 111 refers to specification and storing in a data repository of the foreseen security policies to apply in response to the possible attacks defined in the previous step.

[0026] Step 112 refers to the monitoring of entering content of the information system 1 corresponding to data streams and the attacks detection.

[0027] Step 113 refers to the assessment of a success probability of detected attacks and the cost impact associated with these attacks. Such assessment is achieved based on the attack models stored in step 110 and the attacks detected in step 112.

[0028] Step 114 refers to the assessment of the impact of an activation of a curative security policy in response to a detected attack and the cost impact associated with this activation. Such assessment is achieved based on the security policies stored in step 111 and the state of the monitored information system 1.

[0029] Step 115 refers to the decision of activating or deactivating a curative security policy in function of the assessments achieved in steps 113 and 114. Such decision corresponds to the comparison of the cumulative impacts of both the attack and the curative security policy on the information system 1.

[0030] The activation or deactivation decided in step 115 is then applied in step 116.

[0031] Moreover, it has to be noted that the steps 110 and 111 are preliminary steps which can be achieved offline whereas the steps 112, 113, 114, 115, 116 are dynamic steps which are achieved online such that any modification of the information system is taken into account in real time to decide of the activation or the deactivation of security policies.

[0032] Thus, the present invention, thanks to the assessments of both the attack consequences and the consequences of the activation of a security policy allows to determine if it is worthy to activate a curative security policy and when said policy is activated to determine if it is worthy to keep this policy activated in function of the evolution of the information system and the impact of this policy on said information system.

[0033] As described above, an attack is an event occurring in a system. In practice, an attack comprises different levels (or steps) that lead to the objective of the attack as described in fig.3 where an example of attack graph aimed at hacking a voice over internet protocol (VoIP) system is described.

[0034] The first level 201 corresponds to the sending of an email (malicious email or spam) toward a victim machine. Then the below (or next) levels represent the different steps to reach the objectives (213, 214, 215 and 216). The second level 202 refers to the gain of a remote shell in the victim machine (corresponding to the opening by the user of the malicious link or attachment of the email). The third level 203 corresponds to a bot (robot) infection which is the installation of a malicious software bot capable of simulating human activity that uses the remote shell. The bot can wait for future orders from the attacker to execute. As represented in fig.3, several remote shells and several corresponding bot infections may be develop in parallel in the information system.

[0035] The next level 204 corresponds to the discovery of the session initial protocol (SIP) discovery which is a scanning of the system (or network) to discover machines (computers in general) or servers using SIP protocol. Such attack may be done by a bot.

[0036] From this step, the attack may use two different ways depending on its objective.

[0037] The first way leads to step 205 which refers to the SIP fingerprinting which consists of identifying the type and the version of the software (operating systems, softphones, servers, etc...) installed on the SIP entities discovered at the previous level (204). This level may also be performed by a bot.

[0038] From step 205, the attack may have two different ways again, one leading to the objective of spam over IP (SPIT) 213 and comprising two levels, a discovery of the active users which is a scanning to determine the users of the VoIP system and which may be performed by a bot and a direct call 209 referring to a call to the victim user (by a bot) to perform spam over IP (SPIT).

[0039] The other possibility from level 205 is the discovery of the media access control (MAC) address of potential victim machines 207 (which may be performed by a bot).

[0040] The next step 208 is then the address resolution protocol (ARP) poisoning which forces the traffic (e.g. the established calls) between two victim users to pass through one bot. The attacker may then have access to

EX1002
CISCO SYSTEMS, INC. / Page 333 of 1453

all the traffic between both victim users. This leads either to a step of sniff audio 211 to sniff the audio packets transmitted between both users or a step of inject audio 212 to inject audio packets in the transmission between both users for altering the established call. The corresponding respective objectives being the conversation tapping 214 and the conversation injection 215.

[0041] From level 204 the second attack solution consists in a server flooding 210 wherein the bots flood the main server of the VoIP system to cause a denial of service (DoS) which is the objective 216.

[0042] It has to be noted that the closer to the objective is the attack, the higher the probability to reach the objective. Thus, when a spam (level 201) is detected, it is generally not worth activating a security policy as the probability for the attack to reach one of the objectives (213, 214, 215 or 216) is still low whereas if the server is flooded (level 210) for example, then the probability of reaching the objective 216 is very high.

[0043] The graphs such as presented in fig.3 are achieved automatically based on attack models stored in data repository and are used in the assessment of the impact of an attack and its probability to reach its objective as described previously.

[0044] In order to better understand the different steps of the invention, a detailed configuration of a possible embodiment of the invention will now be described based on fig.4, it refers to a more detailed presentation of the organization presented in fig.2.

[0045] Step 120 corresponds to the storing in a data repository of the information system topology and the attack or intrusion detection signatures (IDS). Step 121 is a risk analysis for the monitored system which is conducted by an expert to identify potential attack objectives 122. Based on these attack objectives and the system topology (stored in step 120), attack models are specified (by an expert) 123 as well as an attack context specification 126. Attack models such as presented in fig.4 are then set up 124 and stored as elementary models in a data repository 125.

[0046] On the other hand, the specification of attack contexts 126 allows to specify response contexts 127. For each identified attack context an appropriate response context is specified with the associated security rules. Said security rules and attack contexts are stored as security policies in a data repository 128. Said security policies refer, for example, to firewall activation, authentication request activation or user account blocking or any actions allowing to cure the information system or reduce the impact of the attack. Based on the stored attack models and security policies to apply in response to each attack, the automatic and dynamic part of the invention may be implemented.

[0047] The information system 1 is monitored by intrusion detection systems (IDS) 101 which correspond to any types of sensors capable of detecting an attack and of generating and sending alerts. Said sensors may be made of specific electronic devices (micro-controllers, application specific integrated systems (ASICs)...) or in an information technology (IT) environment, it may simply be a software run by a computer, a server or a router.

[0048] The alerts sent by the IDS are then aggregated 129 in an online correlation engine 131 which uses these aggregated alerts and the attack models stored in a data repository to generate attack graphs such as presented in fig.3. The generated graphs are used, on one hand, for the assessment of the probability for the attack to reach its objective 132 and, on the other hand, for the assessment of the impact of the attack 133.

[0049] The determination of the probability to reach the objective corresponds to the success likelihood for an attack to reach an objective. Thus, the success likelihood level of each attainable objective (predefined in the attack graph) of the attack is calculated. This level shows how close the attack is with respect to its objective.

[0050] The attack impact assessment corresponds to the determination of the impact of the attack on the security and the quality of service (QoS) of the information system 1. This gathers the impact on the confidentiality, the integrity and the availability and any parameters influencing the using of the information system 1. Such assessment is also based on the state of the information system 1.

[0051] The results of both assessments are then sent to a policy instantiation engine (PIE) 134 where the cumulative impact of the attacks is determined.

[0052] Besides, in the same way as the assessment of the impact of the attacks, an assessment of the impact of the curative security policies which can be used in response of the attacks 136 is done based on the stored security policies. Again, impact on both the security and the QoS of the information system as well as as the state of said system are taken into account in the assessment. The results of the assessment are also transmitted to the PIE 134 where the cumulative impact of the curative security policies is determined.

[0053] The policy instantiation engine 134 receives the assessments corresponding on one side of the attack impact and on the other side of the curative security policy impact which are processed respectively by an attack handler module 135 and a response handler module 137. For each type of impact, at least one metric is defined, and in the general case, a plurality of metrics corresponding to different aspects of the impact (on security, on QoS...) are defined and the assessed value of all these impact contributions are added (practically by integrated their value over time).

[0054] Based on both cumulative impacts computed by the attack handler module and the response handler module as well as the probability for the attack to reach its objective (also called success likelihood) and the state of the monitored information system 1, the PIE 134 determines if curative security policies have to be activated or deactivated.

[0055] Different activation/deactivation rules may be used, for example, a security policy may be activated if

EX1002
CISCO SYSTEMS, INC. / Page 334 of 1453

the success likelihood reached a given threshold, or if the attack impact reach a predetermined threshold. It can also be a combination of both (activation if the attack impact and the success likelihood reach given thresholds).

[0056] In general, a response policy must be activated when:

- the detected threat violated the security and operational policies and,
- the success likelihood (calculated dynamically, considering the attack progress and the state of the monitored system) of the threat exceeds a predefined threshold and,
- the impact of the threat exceeds a predefined threshold, and is greater than the cost of the associated response policy.

[0057] In the same way, if the success likelihood goes below a given threshold or the response impact goes over a predefined threshold or a combination of both, an activated security policy have to be deactivated. Such case may occur if the impact of a response policy induced more drawbacks than advantages with respect to the initial attack or if the risks associated with the attack have been dismissed or eradicated.

[0058] The order or command of activating or deactivating a security policy is then sent to response policy deployment point (PDP) 107 (also called policy decision point) wherein each security rule of a response policy is converted into scripts to configure the policy enforcement points (PEP) 109 which are located within the information system 1 and which are used to enforce the security policies (firewall activation or configuration, intrusion prevention systems activations, account permissions or access modifications...). The online steps (comprising the online correlation engine 131, the attack objective probability assessment 132, the attack impact assessment, the attack response assessment 136, the policy instantiation engine 134, the policy deployment point and the policy enforcement point) may be achieved by programs or software run by a computer or a server. Said online steps use the stored elements of the data repositories (attack model data repository 125 and response policy data repository 128) to determine dynamically the necessity of activation/deactivation of response security policy in function of the detected attacks and of the state of the monitored information system 1.

[0059] Thus, the present invention allows to provide a dynamic assessment of the impact of an attack as well as the impact of the security policy to apply in response to the attack providing therefore an optimized efficiency of the use of a security policy. Moreover, the idea of determining conditions for deactivating a security policy allows to improve the reactivity of the information system protection and to avoid an unnecessary degraded use of the information system. Indeed, security policy usually correspond to a degraded mode that limits the effects of the attack but also reduces the capacity of said information system and may disturb and affect the users of the information system leading to a loss of productivity or a reduction of quality of service (QoS) for the company using the information system.

Claims

1. Method for adapting security policies of an information system infrastructure in function of attacks wherein it comprises the steps of:

   - storing potential attacks and their associated risks in a data repository;
   - storing curative security policies in response of the potential attacks in a data repository;
   - monitoring entering contents representing data streams of the information system;
   - detecting at least one attack in the information system;
   - assessing a success probability parameter of the at least one detected attack and its associated cost impact parameter;
   - assessing an activation impact parameter of at least one curative security policy in response to the at least one detected attack and its associated cost impact parameter;
   - deciding of the activation or deactivation of a curative security policy in function of the success probability parameter of the, at least one, detected attack, of the activation impact parameter of at least one curative security policy and of the cost impact parameters of both the detected at least one attack and the at least one curative security policy.

2. Method for adapting security policies of an information system infrastructure in accordance with claim 1 wherein the step of storing potential attacks and their associated risks in a data repository comprises the steps of:

   - defining the information system topology and attack detection signatures;
   - defining a risk analysis of the information system that identifies potential attack objectives;
   - specifying attack models to reach the identified attack objectives;
   - storing said attack models in a data repository.

3. Method for adapting security policies of an information system infrastructure in accordance with claim 1 or 2 wherein the step of storing curative security policies in response of the potential attacks in a data repository comprises:

   - specifying at least one attack context;

EX1002
CISCO SYSTEMS, INC. / Page 335 of 1453

- specifying curative security policies corresponding to the specified at least one attack context;
- storing said curative security policies in a data repository.

4. Method for adapting security policies of an information system infrastructure in accordance with one of the previous claims wherein the step of assessing a success probability parameter of the at least one detected attack and its associated cost impact parameter comprises:

- generating attack strategy graphs based on the stored attack models and the detected at least one attack;
- assessing the probability for the attack to reach its objective;
- assessing the impact of the attack objective on the system security level and on the system quality of service (QoS) level;
- assessing the associated cost impact parameter of the attack objective;

5. Method for adapting security policies of an information system infrastructure in accordance with one of the previous claims wherein the step of assessing an activation impact parameter of at least one curative security policy in response to the at least one detected attack and its associated cost impact parameter is based on the stored curative security policies and the state of the monitored information system.

6. Method for adapting security policies of an information system infrastructure in accordance with one of the previous claims wherein the step of deciding of the activation or deactivation of a curative security policy in function of the success probability parameter of the, at least one, detected attack, of the activation impact parameter of at least one curative security policy and of the cost impact parameters of both the detected at least one attack and the at least one curative security policy is applied dynamically based on the evolution of the state of the monitored system.

7. Method for adapting security policies of an information system infrastructure in accordance with one of the previous claims wherein the cost impact parameters comprise:

- a quality of service (QoS) impact and,
- a security level degradation impact.

8. Monitoring and protecting equipment comprising:

- at least one data repository for:

- storing potential attacks and their associated risks;
- storing curative security policies in response of the potential attacks;

- processing means for:

- monitoring entering contents representing data streams of the information system;
- detecting at least one attack in the information system;
- assessing a success probability parameter of the detected at least one attack and its associated cost impact parameter;
- assessing at least one activation impact parameter of at least one curative security policy in response to the at least one detected attack and its associated cost impact parameter;
- deciding of the activation of a curative security policy in function of the success probability parameter of the at least one detected attack, of the activation impact parameter of at least one curative security policy and of the cost impact parameters of both the at least one attack and the at least one curative policy,
- activating at least one curative security policy.

9. Monitoring and protecting equipment comprising:

- at least one data repository for:

- storing potential attacks and their associated risks;
- storing curative security policies in response of the potential attacks;

- processing means for:

- monitoring entering contents representing data streams of the information system;
- detecting at least one attack in the information system;
- assessing a success probability parameter of the detected at least one attack and its associated cost impact parameter;
- assessing at least one activation impact parameter of at least one curative security policy in response to the at least one detected attack and its associated cost impact parameter;
- deciding of the deactivation of a curative security policy in function of the success probability parameter of the at least one detected attack, of the activation impact parameter of at least one curative security pol-

EX1002
CISCO SYSTEMS, INC. / Page 336 of 1453

icy and of the cost impact parameters of both the at least one attack and the at least one curative policy
- deactivating at least one curative security policy.

EX1002
CISCO SYSTEMS, INC. / Page 337 of 1453

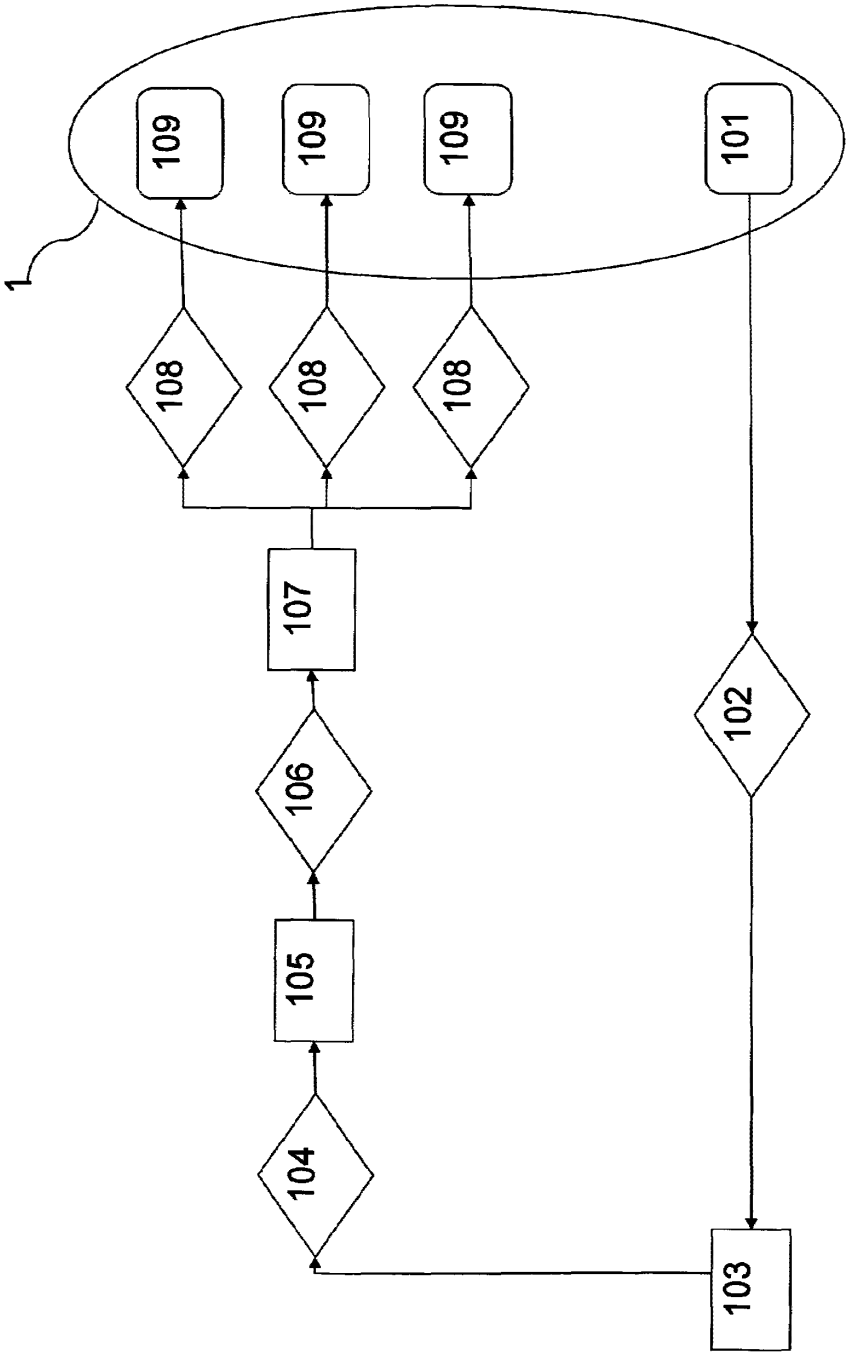


Fig.1

EX1002
CISCO SYSTEMS, INC. / Page 338 of 1453

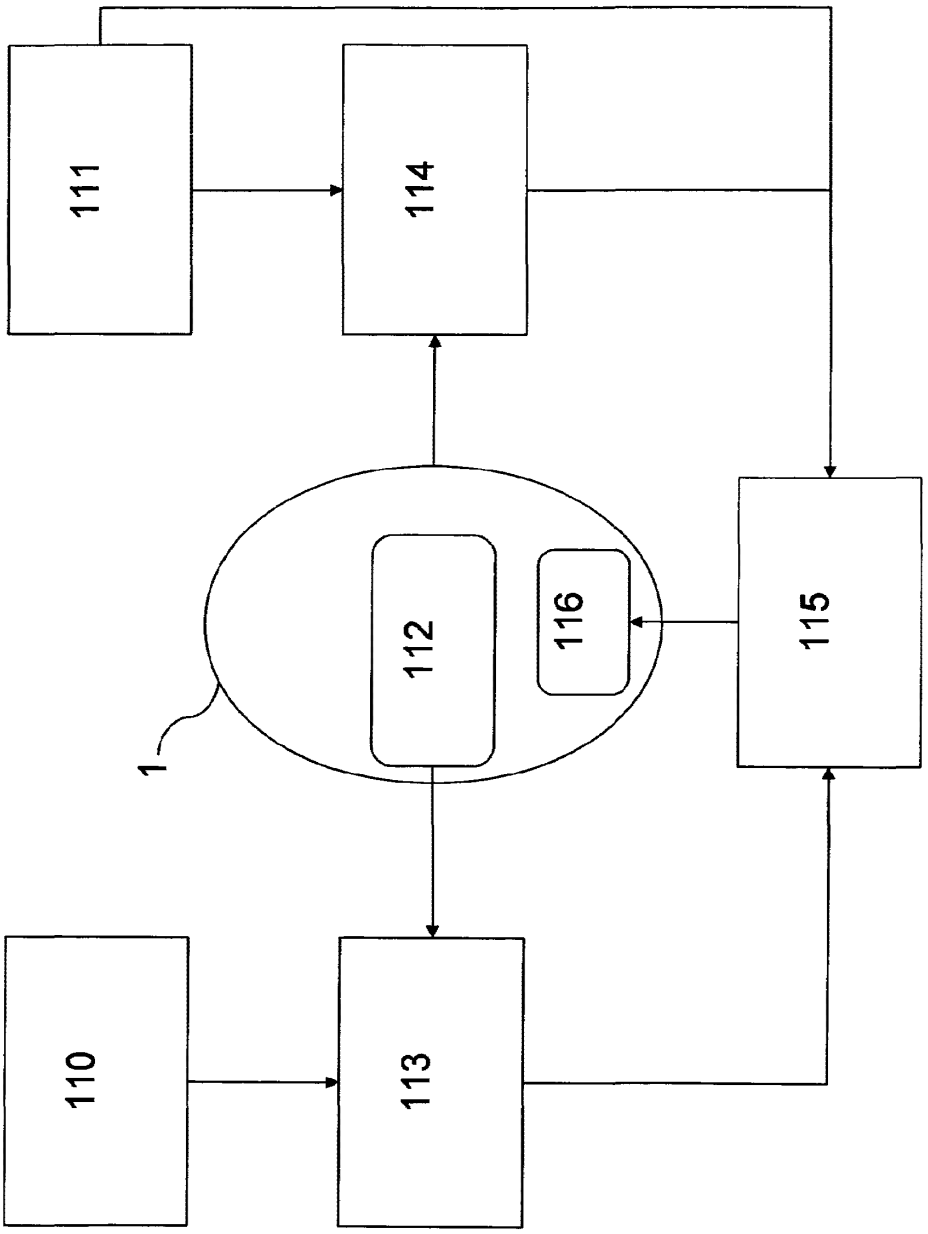


Fig.2

EX1002
CISCO SYSTEMS, INC. / Page 339 of 1453

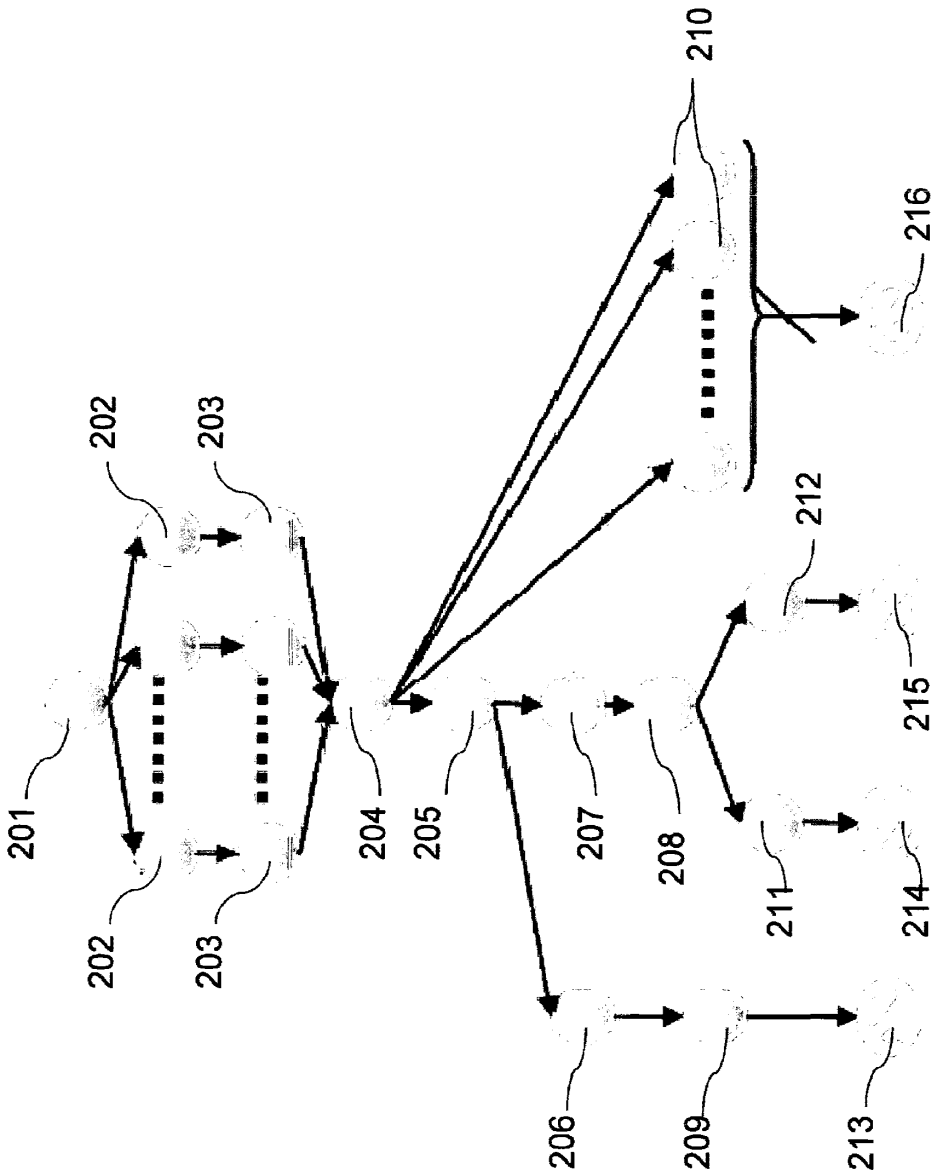


Fig.3

EX1002
CISCO SYSTEMS, INC. / Page 340 of 1453

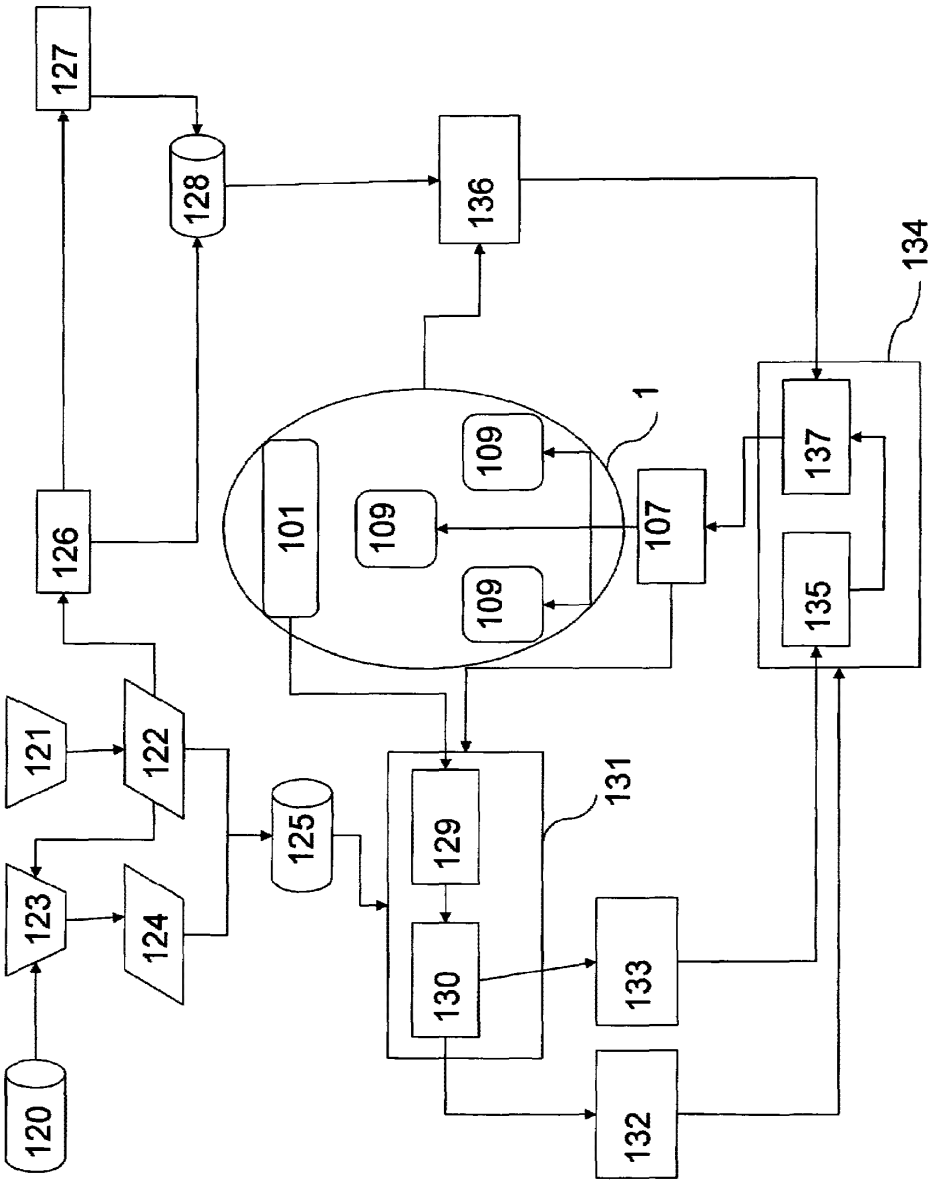


Fig.4

EX1002
CISCO SYSTEMS, INC. / Page 341 of 1453

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 10 29 0250

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	WO 2004/015908 A2 (ALPHATECH INC [US]; KREIDL O PATRICK [US]; FRAZIER TIFFANY [US]) 19 February 2004 (2004-02-19) * abstract; figures 1-6; tables I, II * * paragraphs [0006], [0008], [0013] * * paragraphs [0021] - [0023] * * paragraphs [0037] - [0039] * * paragraphs [0052], [0053], [0062] * * paragraphs [0067], [0069], [0072] * * paragraphs [0073], [0076] * * paragraphs [0088] - [0110] * -----	1-9	INV. H04L29/06 G06F21/00
X	KANOUN W ET AL: "Success Likelihood of Ongoing Attacks for Intrusion Detection and Response Systems" COMPUTATIONAL SCIENCE AND ENGINEERING, 2009. CSE '09. INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 29 August 2009 (2009-08-29), pages 83-91, XP031543989 ISBN: 978-1-4244-5334-4 * abstract; figures 3,6,7 * * page 83, left-hand column, line 1 - right-hand column, line 37 * * page 84, left-hand column, line 42 - right-hand column, line 2 * * page 84, right-hand column, line 44 - page 85, left-hand column, line 15 * * page 87, left-hand column, line 35 - right-hand column, line 19 * -----	1-9	TECHNICAL FIELDS SEARCHED (IPC) H04L G06F G06N
A	WO 2007/027131 A2 (TELIASONERA AB [SE]; ENDERSZ VIKTOR [SE]) 8 March 2007 (2007-03-08) * figure 1 * * page 4, line 29 - page 8, line 34 * -----	1-9	

-/--

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	21 October 2010	Schossmaier, Klaus

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

4

EX1002
CISCO SYSTEMS, INC. / Page 342 of 1453

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 10 29 0250

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
A	MIGUEL JOHN: "COMPOSITE COST/BENEFIT/RISK ANALYSIS METHODOLOGY" COMPUTER SECURITY: A GLOBAL CHALLENGE; PROCEEDINGS / PROCEEDINGS OF THE IFIP INTERNATIONAL CONFERENCE ON COMPUTER SECURITY,, 1 January 1984 (1984-01-01), pages 307-311, XP009139953 ISBN: 978-0-444-87618-8 * the whole document * -----	1-9	

TECHNICAL FIELDS SEARCHED (IPC)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	21 October 2010	Schossmaier, Klaus

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

4

EX1002
CISCO SYSTEMS, INC. / Page 343 of 1453

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 10 29 0250

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

21-10-2010

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2004015908 A2	19-02-2004	AU 2003278706 A1	25-02-2004
		CA 2495147 A1	19-02-2004
		EP 1535422 A2	01-06-2005
WO 2007027131 A2	08-03-2007	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

Espacenet

Bibliographic data: EP2498442 (A1) — 2012-09-12

Methods, systems and devices for the detection and prevention of malware within a network

Inventor(s): RIESCHICK GARY [US]; DUNNE CAMERON ROSS [IE]; MCNAMEE ALAN [IE]; HOGAN JOE [IE] ± (RIESCHICK, GARY, ; DUNNE, CAMERON ROSS, ; MCNAMEE, ALAN, ; HOGAN, JOE)

Applicant(s): OPENET TELECOM LTD [IE] ± (OPENET TELECOM LTD)

Classification: **- international:** ***H04L12/24; H04L29/06; H04W12/08; H04W12/12;*** *H04W24/00; H04W88/16*
- cooperative: **H04L63/1441**; **H04W12/08**; **H04W12/12**; H04L63/1408; H04W88/16

Application number: EP20120158921 20120309

Priority number (s): US201161451775P 20110311 ; US201113159710 20110614

Also published as: US2012233656 (A1) US8726376 (B2)

Abstract of EP2498442 (A1)

Methods, systems and devices examine data flows in a communication system control network for known malware threats and suspicious properties typically associated with malware threats. A policy management system inside the control network accesses a user repository and a charging network, and performs pattern matching and/or observed behavior detection methods to determine if the data flows carry content (e.g., malware) that poses a security risk to network or wireless devices. The policy management system generates policy rules based on user preferences and risk-level. The policy management system sends the generated policy rules to a gateway/PCEF, which blocks the data flows, allows the data flows, or restricts the data flow based on the policy rules.

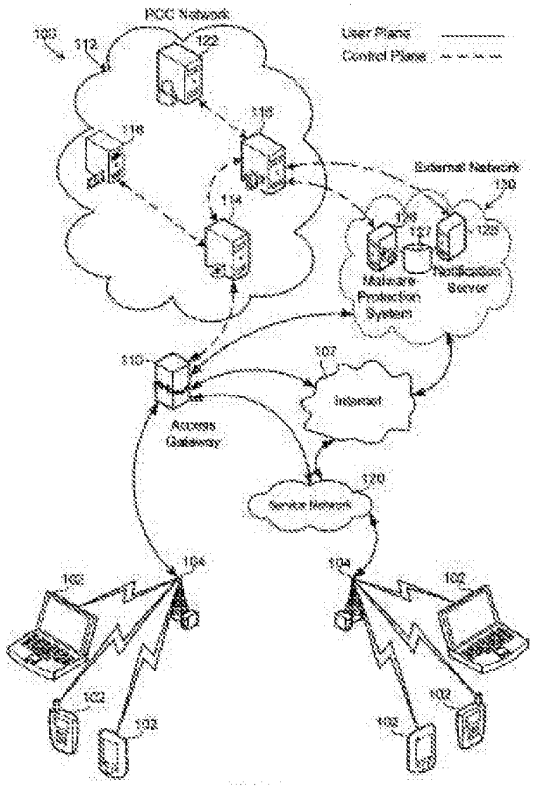

PCC Network
User Plane
Control Plane
External Network
Malware Protection System
Notification Server
Access Gateway
Internet
Service Network

FIG. 2

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 498 442 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
12.09.2012 Bulletin 2012/37

(21) Application number: **12158921.2**

(22) Date of filing: **09.03.2012**

(51) Int Cl.:
H04L 12/24 *(2006.01)* ***H04L 29/06*** *(2006.01)*
H04W 12/08 *(2009.01)* ***H04W 12/12*** *(2009.01)*
H04W 24/00 (2009.01) *H04W 88/16 (2009.01)*

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME

(30) Priority: **11.03.2011 US 201161451775 P**
14.06.2011 US 201113159710

(71) Applicant: **Openet Telecom Ltd.**
12 Dublin (IE)

(72) Inventors:
- **Rieschick, Gary**
  Louisburg, KS Kansas KS 66053 (US)
- **Dunne, Cameron Ross**
  County Kildare (IE)
- **McNamee, Alan**
  Dublin, 9 (IE)
- **Hogan, Joe**
  County Dublin (IE)

(74) Representative: **Kelly, Madeleine**
FRKelly
27 Clyde Road
Ballsbridge
Dublin 4 (IE)

(54) Methods, systems and devices for the detection and prevention of malware within a network

(57) Methods, systems and devices examine data flows in a communication system control network for known malware threats and suspicious properties typically associated with malware threats. A policy management system inside the control network accesses a user repository and a charging network, and performs pattern matching and/or observed behavior detection methods to determine if the data flows carry content (e.g., malware) that poses a security risk to network or wireless devices. The policy management system generates policy rules based on user preferences and risk-level. The policy management system sends the generated policy rules to a gateway/PCEF, which blocks the data flows, allows the data flows, or restricts the data flow based on the policy rules.

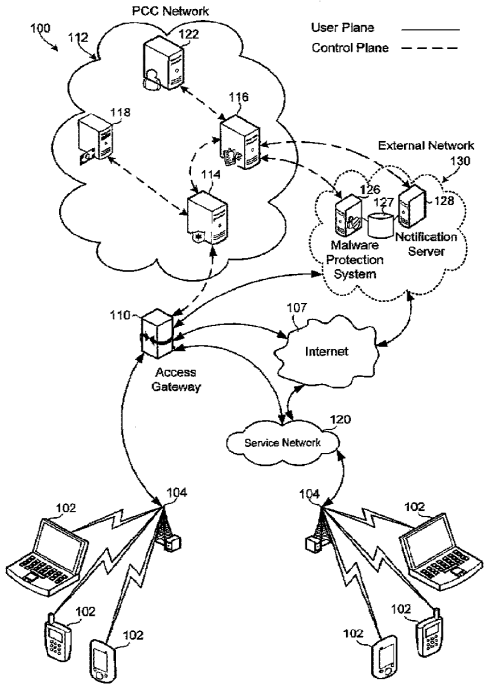


FIG. 2

EP 2 498 442 A1

Printed by Jouve, 75001 PARIS (FR)

Description

BACKGROUND

[0001] Recent advances in wireless and mobile technologies enable mobile-device users to access the Internet at any time and in any place. Internet usage habits are changing and many new types of Internet-enabled devices are emerging to meet the evolving user demands and changing Internet-usage habits. Many of these new and emerging Internet-enabled wireless devices use custom and/or non-traditional operating systems and access the Internet through mobile data networks. Further, many of these devices include powerful processors capable of executing third-party application software downloaded from digital application distribution platforms (e.g., Apple Inc.'s App Store, etc.). The emergence these new technologies and wireless devices presents additional security challenges for the telecommunications networks, mobile data networks and to the new wireless devices themselves.

[0002] Today, malicious software (herein "malware") may be used by thieves and hackers to steal confidential information, launch attacks on web servers and to flood networks with spam. Recently, there have been many high-profile cases of confidential customer information being stolen from businesses, and private wireless device users being subjected to online financial and identity thefts. Perhaps even more significantly, there has recently been an increase in wireless devices being infected by malware that forces the wireless device to participate in malicious activities without the user's knowledge or consent, causing users to incur higher usage-charges and leaving them vulnerable to potential legal actions. Recent press reports indicate this problem is increasing at an alarming rate. The emergence of these new types of Internet-enabled devices is likely to exacerbate these problems, as current malware detection and prevention techniques are ineffective at preventing or removing malware from wireless devices, especially the new breed of Internet-enabled wireless devices that have custom and/or non-traditional operating systems.

[0003] Further, the growth in popularity of application distribution platforms (herein "app ecosystems") allows wireless device users to more readily download third party software and execute the downloaded software with full administrative privileges on the mobile device. Such downloaded applications may be sourced from many different sources, such as email attachments, instant messaging systems, and device-to-device transfers. The emergence of app ecosystems presents additional security challenges that are distinct from the traditional security challenges presented by a malicious page being displayed within web browsers which could be managed by implementing a sandbox model.

[0004] Current malware detection and prevention techniques typically involve installing a protective software client application onto a traditional Internet-enabled device, such as a desktop computer or a laptop computer. Thus, current techniques aim to prevent malware by protecting user-level devices (e.g., laptops) rather than providing a comprehensive solution that can eliminate malware from within the network. Further, since many of the new and emerging Internet-enabled wireless devices do not have traditional operating systems, they cannot effectively employ existing malware detection and prevention techniques. As these new Internet-enabled devices grow in popularity, so will the importance of detecting and preventing malware from within the network.

SUMMARY

[0005] The various embodiments provide methods, systems and devices for receiving from one or more communication system control network components data flow parameters identifying characteristics of a data flow, performing a detection method to determine if the data flow carries malicious content, generating restrictive policy rules in response to determining the data flow carries malicious content, generating non-restrictive policy rules in response to determining the data flow does not carry malicious content, and pushing the generated policy rules to a communication system gateway configured to control the flow of packet-based data between a wireless device and an external network. In various embodiments, generating restrictive policy rules in response to determining the data flow carries malicious content includes generating restrictive policy rules that instruct the gateway to block the data flow and/or to block future data flows originating from the wireless device. The data flow may originate from a wireless device or an Internet server.

[0006] Various embodiment methods, systems and devices may perform charging operations that charge subscriber accounts for data flows allowed by the gateway and not charge subscriber accounts for the data flows blocked by the gateway.

[0007] Pattern matching detection methods may be performed in embodiment methods, systems and devices to determine if the data flow carries content that is a security risk. In an embodiment, pattern matching detection methods may be performed by comparing identified binary-file characteristic information with a binary-file characteristic of a known malware type to determine if the data flow carries content having binary-file characteristics of known malware, which may include comparing the identified binary-file characteristic information with a binary-file characteristic of a spam-sending Internet bot.

[0008] The embodiments include servers configured to implement the various methods through software programming, systems implementing such servers, and non-transitory computer-readable storage media on which are stored server-executable instructions implementing the various methods.

EX1002
CISCO SYSTEMS, INC. / Page 348 of 1453

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] The accompanying drawings, which are incorporated herein and constitute part of this specification, illustrate exemplary aspects of the invention, and, together with the general description given above and the detailed description given below, serve to explain features of the invention.

[0010] FIG. 1 is a communication system block diagram illustrating network components of a communication system having a third generation partnership project (3GPP), evolved packet core (EPC) architecture suitable for use in the various embodiments.

[0011] FIG. 2 is a communication system block diagram illustrating network components and of an example communication-system having a policy and charging control (PCC) network in accordance with the various embodiments.

[0012] FIG. 3A is a communication system block diagram illustrating example communications between logical components in an example control network and an external network.

[0013] FIG. 3B is an communication system block diagram illustrating example communications between a malware protection system and external networks in accordance with various embodiments.

[0014] FIG. 4A is a process flow diagram illustrating an example method for receiving signaling flows and enforcing policy rules on the signaling flows in accordance with various embodiments.

[0015] FIG. 4B is a process flow diagram illustrating an example policy management system method for receiving parameters from a gateway and generating rules in accordance with the various embodiments.

[0016] FIG. 5 is a process flow diagram illustrating an example pattern matching detection method in accordance with an embodiment.

[0017] FIGs. 6A and 6B are process flow diagrams illustrating example observed behavior detection methods in accordance with various embodiments.

[0018] FIG. 7 is a component block diagram of a server suitable for use with an embodiment.

DETAILED DESCRIPTION

[0019] The various embodiments will be described in detail with reference to the accompanying drawings. Wherever possible, the same reference numbers will be used throughout the drawings to refer to the same or like parts. References made to particular examples and implementations are for illustrative purposes, and are not intended to limit the scope of the invention or the claims.

[0020] The word "exemplary" is used herein to mean "serving as an example, instance, or illustration." Any implementation described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other implementations.

[0021] As used herein, the terms "mobile device," "wireless device" and "user equipment (UE)" may be used interchangeably and refer to any one of various cellular telephones, smart-phones (e.g., iPhone®), personal data assistants (PDA's), palm-top computers, laptop computers, wireless electronic mail receivers (e.g., the Blackberry® and Treo® devices), VoIP phones, multimedia/Internet enabled cellular telephones, and similar electronic devices capable of sending and receiving wireless communication signals. A wireless device may include a programmable processor and memory.

[0022] As used herein, the term "bot" is used to refer to software applications that emulate human online-activity by automatically performing tasks typically performed by human computer users.

[0023] As used herein, the phrase "malware protection system" is used to refer to any system configured to detect, prevent and/or remove malware such as computer viruses, computer worms, Trojan horses, bots, spyware, adware, etc. Thus, a malware protection system may include a malware prevention system, a malware detection system, a malware removal system, or any other system that assists the detection, prevention and/or removal of malware, as well as combinations of such systems.

[0024] A number of different cellular and mobile communication services and standards are available or contemplated in the future, all of which may implement and benefit from the various embodiments. Such services and standards include, e.g., 3rd generation partnership project (3GPP), long term evolution (LTE) systems, 3rd generation wireless mobile communication technology (3G), 4th generation wireless mobile communication technology (4G), global system for mobile communications (GSM), universal mobile telecommunications system (UMTS), 3GSM, general packet radio service (GPRS), code division multiple access (CDMA) systems (e.g., cdmaone, CDMA2000TM), worldwide interoperability for microwave access (WiMAX), enhanced data rates for GSM evolution (EDGE), advanced mobile phone system (AMPS), digital AMPS (IS-136/TDMA), evolution-data optimized (EV-DO), digital enhanced cordless telecommunications (DECT), and integrated digital enhanced network (iden). Each of these technologies involves the transmission and reception of signaling and content messages. It should be understood that any references to terminology and/or technical details related to an individual standard or technology are for illustrative purposes only and are not intended to limit the scope of the claims to a particular broadcast communication system or technology unless specifically recited in the claim language.

[0025] As discussed above, Internet usage habits are changing and many new types of Internet-enabled devices are emerging to meet evolving user demands. The emergence of these devices presents new security challenges that cannot be addressed by existing antivirus/malware detection and removal systems. For example, current malware detection and prevention techniques attempt to prevent malware by protecting user-level devic-

EX1002
CISCO SYSTEMS, INC. / Page 349 of 1453

es (e.g., laptops) rather than from within the network. Since many new and emerging Internet-enabled devices do not having traditional operating systems, current malware detection and prevention techniques cannot efficiently detect or prevent malware.

[0026] The various embodiments provide a comprehensive security solution for detecting and preventing malware from within a mobile data network. The various embodiments protect mobile devices from becoming infected with malicious software (malware) and protect Internet servers and network components from attacks (e.g., denial of service attacks) and inconveniences (e.g., spam) caused by malware. The various embodiments detect both known and yet-to-be identified security threats by performing pattern matching and observed behavior detection methods. Various embodiments monitor network traffic for suspicious content or activities to detect malware and block suspicious data flows from within the network.

[0027] Various embodiments provide methods for detecting and preventing malware from within a data network by combining a policy management component, which has a global or near global view of network traffic and transactions, with a malware system detection component configured to recognize malware based upon patterns within the network traffic and transactions. The various embodiments may operate exclusively within the network and support any type of Internet device.

[0028] The various embodiments may detect transmissions of known and unknown malware in real time as the network patterns emerge. Various embodiments may enable defensive and ameliorative actions, such as modifying the transmissions of the malware or transmission generated by malware, which may include throttling malware transmissions. Various embodiments may prevent the transmission of malware once it has been detected. Various embodiments may alert wireless device users of detected malware. Various embodiments may alert telecommunications network operators of detected malware so they can take corrective actions and/or warn targets of an attack.

The various embodiments may include machine learning mechanisms to enable the malware protection system to learn about malware-generated transmissions and recognize malware patterns as they develop. Such machine learning capabilities may include tracking or correlating network activity levels of recognized threats as well as details of suspicious activities not yet recognized as threatening. Various embodiments may store user-specific malware detection (e.g., patterns in network traffic that occurred while a malware event was underway) and prevention information (e.g., countermeasures that proved effective in responding to a malware event), which may be used by the malware protection system for the detection and prevention of future malware events. Various embodiments may map specific malware threats identified to users of the network. Malware threats may be identified using any suitable mechanism, including the use of IP addresses.

[0029] The various embodiments may push client software capable of exchanging malware and security information with a control network to wireless devices. The malware and security information may include report details generated by the client, alerts generated by the system, instructions from the system to the client that relate to a specific threat to the client, and/or instructions that instruct the wireless device to change its behavior. In an embodiment, the malware and security information may include instructions that instruct a first application executing on the wireless device to cause a second application executing on the wireless device to change its behavior.

[0030] The various embodiments may detect spam by recognizing network traffic with certain characteristics, which may include destination information, protocols, and/or payload content. The various embodiments may protect networks by preventing wireless devices from being used as a source of malware attacks. Various embodiments may detect denial of service attacks by recognizing rapid increases in traffic addressed to a single or related destination from multiple sources. Various embodiments may prevent spam and denial of service attacks by throttling or blocking suspected malicious traffic.

[0031] The various embodiments may reduce the need for network operators to augment capacity and provide network congestion relief. The various embodiments may send detection and prevention information to telecommunications network operators, wireless devices and/or malware systems in real time.

[0032] The various embodiments may be implemented within a variety of mobile communication systems, an example of which is illustrated in FIG. 1. Wireless devices 102 may be configured to send and receive voice, data and control signals to and from a service network 36 (and ultimately the Internet) using a variety of communication systems/technologies (e.g., GPRS, UMTS, LTE, cdmaOne, CDMA2000™, etc). For example, general packet radio service (GPRS) data transmitted from a wireless device 102 is received by a base transceiver station (BTS) 12 and sent to a base station controller (BSC) and/or packet control unit (PCU) component (BSC/PCU) 18. Code division multiple access (CDMA) data transmitted from a wireless device 102 is received by a base transceiver station 12 and sent to a base station controller (BSC) and/or point coordination function (PCF) component (BSC/PCF) 22. Universal mobile telecommunications system (UMTS) data transmitted from a wireless device 102 is received by a NodeB 14 and sent to a radio network controller (RNC) 20. Long term evolution (LTE) data transmitted from a wireless device 102 is received by an eNodeB 16 and sent directly to a serving gateway (SGW) 28 located within the EPC 40.

[0033] The BSC/PCU 18, RNC 20 and BSC/PCF 22 components process the GPRS, UMTS and CDMS data, respectively, and send the processed data to a node within the EPC 40. More specifically, the BSC/PCU 18 and

EX1002
CISCO SYSTEMS, INC. / Page 350 of 1453

RNC 20 units send the processed data to a serving GPRS support node (SGSN) 24 and the BSC/PCF 22 sends the processed data to a packet data serving node (PDSN) and/or high rate packet data serving gateway (HSGW) component (PDSN/HSGW) 30. The PDSN/HSGW 30 may act as a connection point between the radio access network and the IP based PCEF/PGW 32. The SGSN 24 is responsible for routing the data within a particular geographical service area and may send signaling (control plane) information (e.g., information pertaining to call set-up, security, authentication, etc.) to a mobility management entity (MME) 26. The MME may request user and subscription information from a home subscriber server (HSS) 42, perform various administrative tasks (e.g., user authentication, enforcement of roaming restrictions, etc), select a SGW 28 and send administrative and/or authorization information to the SGSN 24.

[0034] Upon receiving the authorization information from the MME 26 (e.g., authentication complete, identifier of a selected SGW, etc.), the SGSN 24 sends the GPRS/ UMTS data to a selected SGW 28. The SGW 28 stores information about the data (e.g., parameters of the IP bearer service, network internal routing information, etc.) and forwards user data packets to a policy control enforcement function (PCEF) and/or packet data network gateway (PGW) 32. The PCEF/ PGW 32 sends signaling information (control plane) to a policy control rules function 34. The PCRF 34 accesses subscriber databases, creates a set of intelligent policy rules and performs other specialized functions (e.g., interacts with online/offline charging systems, application functions, etc.) and sends the intelligent policy rules to the PCEF/ PGW 32 for enforcement. The PCEF/ PGW 32 implements the policy rules to control the bandwidth, the quality of service and the characteristics of the data, services and flows being communicated between the service network 36 and the end users.

[0035] FIG. 2 illustrates various logical components in an example communication system 100 suitable for implementing the various embodiments. Wireless devices 102 may be configured to communicate via cellular telephone network, a radio access network (e.g., UTRAN, RAN, etc.), WiFi network, WiMAX network, and/or other well known technologies (e.g., GPRS, UMTS, LTE, cdmaOne, CDMA2000TM). Wireless devices 102 may be configured to transmit and receive voice, data and control signals to and from a base station (e.g., base transceiver station, NodeB, eNodeB, etc.) 104, which may be coupled to a controller (e.g., cellular base station, radio network controller, service gateway, etc.) operable to communicate the voice, data, and control signals between mobile devices and to other network destinations. The base station 104 may communicate with an access gateway 110, which serves as the primary point of entry and exit of wireless device traffic and connects the wireless devices 102 to their immediate service provider and/or packet data networks (PDNs). The access gateway 110 may be a part of the policy control and charging network 112 or external to the policy control and charging network 112, and may include one or more of a controller, a gateway, a serving gateway (SGW), a packet data network gateway (PGW), an evolved packet data gateway (ePDG), a packet data serving node (PDSN), a serving general packet radio service support node (SGSN), a policy and charging enforcement function (PCEF), or any combination of the features/functions provided thereof. The access gateway 110 may be implemented in a single computing device or in many computing devices, either within a single network or across a wide area network, such as the Internet.

[0036] The access gateway 110 may forward the voice, data, and control signals to other network components as user data packets, provide connectivity to external packet data networks, manage and store contexts (e.g. network internal routing information, etc.) and act as an anchor between different technologies (e.g., 3GPP and non-3GPP systems). The access gateway 110 may also coordinate the transmission and reception of data to and from the Internet 107, and the transmission and reception of voice, data and control information to and from an external service network 120 connected to the Internet 107 and other base stations 104 and wireless devices 102. The access gateway 110 may also route control/signaling information to a policy and charging control (PCC) network 112, which may be a part of an implementation of an evolved packet core (EPC)/long term evolution (LTE) architecture.

[0037] The PCC network 112 may include a gateway and/or policy and charging enforcement function (PCEF) 114 component for controlling the flow of Internet protocol (IP) data between mobile devices 102 and external networks (e.g., Internet 107, service network 120, etc.). The gateway/PCEF 114 may contain a deep packet inspection (DPI) component (not illustrated) configured to obtain additional application-level information about a particular IP data flow and provide the information to other components in the PCC network 112. In various embodiments, the gateway/PCEF 114 may be integrated with, or a part of, the access gateway 110, either within the PCC network 112 or outside of the PCC network 112.

[0038] The policy and charging control network 112 may also include a policy management system 116, a charging system 118 and a user repository 122. The policy management system 116 may communicate with a malware protection system 126 and a notification server 128 in a network (External Network) 130 outside the telecommunications provider network. The notification server 128 may be configured to receive requests from the policy management system 116 (e.g., PCRF) and send messages to mobile devices 102 using various technologies/mechanisms, such as email, short message service (SMS) texts, instant messaging (IM) systems, interactive voice response (IVR) systems. The notification server 128 may also send messages in a mobile device-specific format, which may be unique to each mobile device type. The notification server 128 may choose

EX1002
CISCO SYSTEMS, INC. / Page 351 of 1453

a communications technology/mechanism on a case-by-case basis. For example, the notification server 128 may choose a communications technology/mechanism depending on the user's preferences and/or mobile device type. Messages may be sent through the Internet 107 or the access gateway 110. In an embodiment, the notification server 128 may send messages to a client application running on the mobile devices 102 (e.g., via the Internet 107, access gateway 110, etc.), which may send a response to the notification server 128 for forwarding to the policy management system 116.

[0039] In an embodiment, the notification server 128 may be configured to send messages to mobile devices 102 "in-band" or "out-of-band." The in-band notifications may use the same communication mechanism used for receiving message and the out-of-band notifications may use a different communication mechanism than that used for receiving message. For example, if a user is browsing web pages and receives an in-band notification, then the notification may appear as a new web page.

[0040] The malware protection system 126 may be a dedicated malware system or server, which is sometime referred to herein as a "malware expert system." The malware protection system 126 may be implemented within one or a number of dedicated servers located within the communication network 100, or within one or a number of dedicated servers located external from but with communication links to the communication network 100 (as illustrated). In a further embodiment, some or all elements of the malware protection system 126 functionality may be implemented within a server performing another network function, such as the policy management system 116, a charging system 118 or a user repository 122.

[0041] The malware protection system 126 may maintain a repository of known security risks, gather real-time information regarding emerging security/malware threats, identify security/malware threats by monitoring traffic within the communication network 100, and generate security/malware threat counter-measures. Such security/malware threat counter-measures may include malware removal software and/or malware repair software. In an embodiment, the malware protection system 126 may be configured to generate security/malware threat counter-measures, malware removal software and/or malware repair software in a format specific to each mobile device 102 type. The mobile device formats may be defined by configuration or determined in real time by the policy control system 116, or by the malware protection system 126 based on information received in real time from the policy control system 116.

[0042] The malware protection system 126 may also include a local malware prevention memory or database 127 for each policy management system 116. Likewise, the policy management system 116 may include a local policy management memory (not illustrated), which may be populated by the policy management system 116, the malware protection system 126, or both. In an embodiment, the malware protection system 126 may push data to the policy management memory of the policy management system 116. In an embodiment, the policy management system 116 may periodically request information from the malware protection system 126 and populate the policy management memory with the received information.

[0043] FIG. 3 A is a system architecture diagram illustrating communications between logical components in an example control network 150 (e.g., PCC network) and an external network 155. FIG. 3 illustrates that the control network 150 may include one or more components for providing a policy and charging enforcement function (PCEF) 114, a policy management system 116, a charging system 118, and a user repository 122. The gateway/PCEF 114 may be a part of, or perform operations typically associated with, a gateway GPRS support node (GGSN), a packet data network gateway (PGW), an access gateway 110, or other similar components. In an embodiment, the policy management system 116 may include a policy and charging rules function (PCRF). In an embodiment, the charging system 118 may include an off-line charging system (OFCS) and an on-line charging system (OCS). In an embodiment, the user repository 122 may include a subscriber profile repository (SPR).

[0044] The gateway/PCEF 114 may serve as the primary enforcement point, as a gateway and as a router providing a routing mechanism between the Internet and the radio infrastructure/radio access network. The gateway/PCEF 114 may receive signaling flows and use information contained therein to select an optimal route for a particular type of communication, session, or quality of service (QoS). The gateway/PCEF 114 may also enforce various policies on the received flows, which may include querying, coordinating and/or adjusting various network resources based on a set of policy rules provided by the policy management system 116.

[0045] The policy management system 116 may identify appropriate policy rules for a given situation and send the identified policy rules to the gateway/PCEF 114 for enforcement. Each policy rule may govern the services, quality of service (QoS) and/or bandwidth that are made available to a particular subscriber in a particular data call and/or session. The policy rules may also govern when certain services are made accessible to the subscriber (e.g. weekdays from 9AM to 5PM, etc.) and how long the subscriber may access to those services (e.g., 15 minutes at a time, a total of two hours, etc.). The policy rules may further govern whether specific IP data flows should be "blocked," "allowed" or "allowed with constraints," based on current and potential security risks/malware threats, as discussed in further detail below.

[0046] In an embodiment, the policy management system 116 may generate, compile and select a set of business, technology and security rules that define the policies that are to be enforced. In doing so, the policy management system 116 may communicate with the user repository 122 and/or the charging system 118. The user

EX1002
CISCO SYSTEMS, INC. / Page 352 of 1453

repository 112 may store subscriber information (e.g., customer IDs, preferences, subscription levels, etc.) and user-specific information, such as details of a user's subscription to malware prevention services and historical details of a user's exposure to specific malware threats. The charging system 118 may store information pertaining to how much wireless data is being used by a wireless subscriber and information pertaining to whether the subscriber has sufficient funds/credits/access units to receive a requested service/flow. The policy management system 116 may use the information stored by the user repository 122 and charging system 118 to identify potential security risks/malware threats and user preferences for responding to identified security risks/malware threats and make rule decisions based on a combination of the risk/threat and user preference. The policy management system 116 may make the rule decisions on a per-subscriber, per-session and/or per-service basis. For example, the policy management system 116 may use subscriber information (e.g., subscriber's city of residence), the current usage parameters (e.g., day of week, time of day, peak hours, etc.) and the subscriber's service level (e.g., Gold, Bronze, etc.) in conjunction with identified security risks (e.g., known virus, irregular usage patterns, etc.) and user preferences to generate and/or select one or more rules or rule groups, which are pushed to the gateway/PCEF 114 for enforcement.

[0047] The policy management system 116 may also communicate with external systems 155, such as a malware protection system 126 and a notification server 128. As mentioned above, the malware protection system 126 may maintain a repository of known malware threats, gather information regarding emerging malware threats, identify current and potential malware threats and generate malware threat counter-measures, malware removal software and/or malware repair software to neutralize the security threats. The policy management system 116 may send information to the malware protection system 126 to aid in the malware prevention operations. Likewise, the malware protection system 126 may send security related information to the policy management system 116 to aid in the rule making decisions/operations.

[0048] FIG. 3B is a system architecture diagram illustrating communications between policy management systems and malware protection systems. Specifically, FIG. 3B illustrates that the malware protection system 126 may receive information from the policy management system 116, and share information with other policy management systems (e.g., policy management systems 166) or external antivirus/malware protection systems (e.g., malware detection system 162).

[0049] In an embodiment, the policy management system 116 may provide malware detection feedback to the malware protection system 126. In an embodiment, the malware detection feedback may include detection rate information extracted from the IP data flows. The detection rate information may identify the detection rates of known malware threats and include additional parameters (e.g., wireless device type, location of a wireless device, etc.) readily accessible to components within the control network (e.g., policy management system 116, gateway/PCEF 114, etc.). These communication system control network components are generally unavailable to external services and servers (e.g., antivirus servers, malware detection systems, etc.). Such additional parameters may be carried by the IP data flows, extracted by the gateway/PCEF 114 and/or the policy management system 116 and sent to the malware protection system 126. The malware protection system 126 may then use this information to update its malware protection services (e.g., to update lists, generate new prevention software, etc.).

[0050] In an embodiment, the policy management system 116 may send the malware protection system 126 information relating to IP data flows with suspicious characteristics. This information may be used by the malware protection system 126 to identify emerging and unidentified malware threats that are not yet prevalent enough to be known to the malware protection system 126. The malware protection system 126 may also use this information to develop preemptive or preventative countermeasures for the identified malware threats.

[0051] In an embodiment, the policy management system 116 may send malware protection system sample data extracted from IP traffic flows within the detection feedback, which the malware protection system 126 may use for analyzing the malware threats.

[0052] In an embodiment, the malware protection system 126 can subsequently share information received from the policy management system 116 with other policy management systems (e.g., policy management systems 166) in other mobile data networks (e.g., roaming/home networks, external networks, etc.) and/or with independent malware protection systems (e.g., malware detection system 162) operating in private data networks, such as corporate networks, etc.

[0053] FIG. 4A illustrates an example gateway/PCEF method 400 for receiving signaling flows and enforcing policy rules on the signaling flows in accordance with the various embodiments. This embodiment method 400 may be implemented in a server configured with server-executable instructions configured to cause the server to perform the operations of the method steps. In step 402, the gateway/PCEF may receive a data flow originating from, or destined for, a wireless device. In step 406, the gateway/PCEF may examine the data flows and/or the network traffic, identify key characteristics of the data flows and/or network traffic, generate parameters based on the key characteristics and send the generated parameters to a policy managements system for analysis. In step 408, the gateway/PCEF may receive one or more policy rules from the policy management system. In step 410, the gateway/PCEF may use the received policy rules to enforce the various policies discussed above, such as blocking, restricting, or allowing

EX1002
CISCO SYSTEMS, INC. / Page 353 of 1453

the data flow to be sent to, or received from, a wireless device.

[0054] FIG. 4B illustrates an example policy management system method 450 for receiving parameters from a gateway/PCEF and generating/selecting rules in accordance with the various embodiments. In step 452, the policy management system may receive parameters generated by the gateway/PCEF. In step 454, the policy management system may use the received parameters to determine if the data flows carry content (e.g., malware) that poses a security risk to network and/or wireless devices. For example, the policy management system may use the parameters to perform pattern matching detection methods or observed behavior detection methods to determine if the data flow carries malicious content or is otherwise a security risk. The policy management system may retrieve information from a local memory and/or request/receive information from external memories/systems/servers (e.g., user repository, charging system, a malware protection system, etc.) that may be used to determine if the data flows carry content (e.g., malware) associated with a potential or known security risk. In step 456, the policy management system may generate/select policy rules based on determining the data flows carry content that poses a "known risk," a "potential risk," or "no risk." In step 458, the policy management system may send the generated/selected policy rules to the gateway/PCEF for enforcement.

[0055] As mentioned above, the policy management system may retrieve information from a local memory as well as from external memories/systems/servers. In an embodiment, the policy management system may first access the local memory before requesting information from the external memories/systems/servers to reduce latency and improve efficiency. In an embodiment, if the local memory identifies the data flow as carrying a potential security risk, the policy management system may forgo accessing the external memories/systems/servers and generate rules based on the information in the local memory. This reduces latency and improves efficiency because fewer operations and external communications are required to make intelligent policy rule decisions.

[0056] FIG. 5 illustrates an example pattern matching detection method 500, which may be performed by the policy management system to determine if an IP data flow carries content (e.g., malware) that poses a security risk. In step 502, the policy management system may receive parameters identifying certain key characteristics of the IP data flows and/or network traffic. In step 504, the policy management system may examine the parameters to identify/extract information that may be used to determine if the data flow carries content that poses an unacceptable security risk to a wireless device, the network, or both. For example, in step 504, the policy management system may extract binary-file characteristic information, uniform resource locator (URL) information (e.g., from the HTTP-headers of IP packets), IP address information and/or simple mail transfer protocol (SMTP) information (e.g., from SMTP headers/bodies of outgoing emails) from the received parameters.

[0057] In determination step 506, the policy management system may compare the extracted binary-file characteristic information with binary-file characteristics of known malware types (e.g., bots, viruses, worms, Trojan Horses, etc.) to determine if the data flow carries content having binary-file characteristics of known malware (e.g., bots, viruses, worms, Trojan Horses, etc). If the policy management system determines that the data flow carries content that has binary-file characteristics in common with known malware (i.e., determination step 506 = "Yes"), in step 550, the policy management system may generate restrictive policies rules (e.g., "block content," "allow with constraints," etc.) based on the severity of the risk and push the generated rules to the gateway/PCEF. In an embodiment, the policy management system may generate restrictive policy rules that instruct the gateway/PCEF to block the IP data flow upon determining that an IP data flow carries content having binary-file characteristics of known malware threats (e.g., viruses, Trojan Horses, etc.).

[0058] If the policy management system determines that the data flow does not carry content having binary-file characteristics of known malware types (i.e., determination step 506 = "No"), in determination step 510, the policy management system may compare extracted URL information against a list of URLs known to be under attack (e.g., denial-of-service attack, etc.) to determine if the destination of data flow content is a server under attack. If the policy management system determines that the data flow carries or is likely to carry content destined for a server under attack (i.e., determination step 510 = "Yes"), in step 550, the policy management system may generate policy rules (e.g., "block content," "allow with constraints," etc.) based on various factors (e.g., severity of the risk, subscriber's usage history, subscription level, likelihood request is genuine, etc.) and push the generated rules to the gateway/PCEF. In an embodiment, the policy management system may generate an "allow with constraints" rule upon determining that the IP data flow represents a malware threat (e.g., carries content destined for a server under attack), but does not contain a binary that is a malware threat (e.g., carries content having binary-file characteristics of known malware). In an embodiment, the policy management system may generate rules that include constraints that set an upper threshold on the rate of IP data flows and/or introduce an artificial latency to the IP data flow. In this manner, the policy management system may generate intelligent policy rules to prevent attacks on servers, in real time and from within the network, without shutting off all communications to a particular Internet site.

[0059] If the policy management system determines that the data flow does not carry content destined for a server under attack (i.e., determination step 510 = "No"), in determination step 512, the policy management system may compare SMTP information of emails carried

EX1002
CISCO SYSTEMS, INC. / Page 354 of 1453

by a data-flow with known spam heuristics (e.g., incorrect SMTP headers, origin IP address blacklisting, email not relayed, message body contains blacklisted keywords, message attachment scanning using Optical Character Recognition (OCR) techniques, Artificial Intelligence (AI) based methods such as Bayesian filtering, or any combination of these) to determine if the emails originate from a spam-sending bot. If the policy management system determines that the data-flow carries an email that originates from a spam-sending bot (i.e., determination step 512 = "Yes"), in step 550, the policy management system may generate restrictive policy rules that block or restrict the data flow and push the generated rules to the gateway/PCEF for enforcement. In an embodiment, the policy management system may generate an "allow with constraints" rule upon determining that the IP data flow carries content from a known spam bot. In this manner, the policy management system may generate intelligent policy rules to reduce spam, in real time and from within the network, without filtering desired emails/communications.

[0060] If the policy management system determines that the IP data flow does not carry an email that originates from a spam-sending bot (i.e., determination step 512 = "No"), in determination step 514, the policy management system may compare the IP address information with a list of known offender IP addresses to determine if the IP data flow originates from, or is destined for, a mobile device that is compromised (e.g., infected with malware, a virus, etc.) or blacklisted (e.g., known to intentionally engage in malicious activities). If the policy management system determines that the IP address information is associated with an IP address in the list of known offender IP addresses (i.e., determination step 514 = "Yes"), in step 550, the policy management system may generate policy rules that block or restrict the data flow and push the generated rules to the gateway/PCEF for enforcement. In an embodiment, the policy management system may generate an "allow with constraints" rule upon determining that the IP data flow carries content originating from, or destined for, a mobile device that is compromised or blacklisted. In this manner, the policy management system may generate intelligent policy rules to prevent the wireless device, a network server, or both from engaging in malicious activities, without blocking all the services/communications between a wireless device and a network component.

[0061] If the policy management system determines that the IP address information is not associated with an IP address in the list of known offender IP addresses (i.e., determination step 514 = "No"), in determination step 516, the policy management system may compare the URL information to a list of known offender network addresses (e.g., URLs) to determine if the data flow is destined for a website/server known to engage in malicious activities. If the policy management system determines that the URL information is associated with a URL in the list of known offender URLs (i.e., determination step 516 = "Yes"), in step 550, the policy management system may generate restrictive policy rules and push the generated rules to the gateway/PCEF for enforcement. In an embodiment, the policy management system may generate an "allow with constraints" rule upon determining that the IP data flow carries content destined for a website/server known to engage in malicious activities, without blocking all access to the website/server.

[0062] If the policy management system determines that the URL information is not associated with a URL in the list of known offender URLs (i.e., determination step 516 = "No"), in step 560, the policy management system may generate rules to allow the flow, or perform additional operations (e.g., observed behavior detection methods) to determine if the data flow carries content (e.g., malware) that poses a security risk to a wireless device, network server, or both.

[0063] In an embodiment, the policy management system may perform observed behavior detection methods to determine if the data flow carries content (e.g., malware) that may be harmful or a security risk to the network/wireless devices. The policy management system may perform the observed behavior detection methods instead of, or in addition to, the pattern matching detection methods discussed above. Observed behavior detection methods allow the policy management system to detect emerging and yet-unidentified security risks (e.g., malware threats) that are not yet prevalent enough to be known to the malware protection system or third party antivirus/security systems. The observed behavior detection methods may exploit the policy management system's access to the control network information to monitor IP data flows for suspicious characteristics and to identify security risks. For example, the policy management system may access information stored in a user repository and/or charging system in a control network to identify and neutralize security risks that cannot be identified or neutralized by systems that do not have access to user/charging information (e.g., components outside the control network).

[0064] FIGs. 6A-6B illustrate example observed behavior detection methods that may be performed by the policy management system to determine if an IP data flow is a security risk/malware threat. Performing the observed behavior oriented detection methods may include monitoring a number of data flows matching a specific behavior and/or detecting an unexpected rise in a number of requests matching a defined behavior from a specific wireless device. The specific and defined behaviors may include any of the behaviors described below, including unexpected rise in requests, requests to a specific port 80 of a specific IP address, increases in HTTP requests to a specific URL, unexpected rise in requests to a single destination, unexpected rise in outbound emails and/or DNS queries, etc.

[0065] FIG. 6A illustrates an example observed behavior detection method 600 for determining if an IP data flow carries content that may contribute to a denial of

EX1002
CISCO SYSTEMS, INC. / Page 355 of 1453

service attack. In step 602, the policy management system may receive parameters identifying certain key characteristics of the IP data flows and/or network traffic. In step 604, the policy management system may analyze the parameters and update memories, counters and/or threshold values used to monitor sudden and unexpected rises in requests to a single destination. These counters may be used to store running totals, averages, and/or maximum values for one or more different time periods (e.g., the total number of requests to a destination IP address in the last 24 hours, or the average number of requests to a destination IP address per month). Therefore, the counters can be used to store or derive request rates. The counters may be specific to the user, or they may be generalized across groups of users. Therefore, a sudden and unexpected rise in requests to a single destination can be defined in terms of a counter value surpassing a pre-defined rate. This predefined rate can be expressed in terms of the counters (e.g., a sudden and unexpected rise can be defined as the current rate being greater than a tripling of the maximum hourly rate ever experienced). The associated thresholds may be defined as constants, or in terms of the counters (e.g., a threshold can be defined as a quadrupling of the maximum hourly rate ever experienced). Thus, there can be a sudden and unexpected rise in the number of requests to a single destination, but it may not exceed a threshold. In step 606, the policy management system may monitor the number of requests by performing IP level and application level monitoring operations. IP level monitoring operations may include monitoring requests to a specific port 80 of a specific IP address. Application level monitoring operations may include monitoring increases in HTTP requests to a specific URL. In determination step 608, the policy management system may determine if there has been a sudden and unexpected rise in requests to a single destination. This determination may be based upon a counter value surpassing a pre-defined rate, as described previously. If the policy management system determines that there has not been a sudden and unexpected rise in requests to a particular address (i.e., determination step 608 = "No"), in step 612, the policy management system may generate policy rules and push the generated rules to the gateway/PCEF. If the policy management system determines that there has been a sudden and unexpected rise in requests to a single destination (i.e., determination step 608 = "Yes"), in determination step 610, the policy management system may determine if the rise in requests exceeds a predetermined threshold. If the rise in requests does not exceed the predetermined threshold (i.e., determination step 610 = "No"), in step 612, the policy management system may generate policy rules and push the generated rules to the gateway/PCEF. If the rise in requests exceeds the predetermined threshold (i.e., determination step 610 = "Yes"), the policy management system may conclude that a denial of service attack is emerging, and in step 614, register the destination as being under attack, generate restrictive policy rules to block or limit current and future flows from accessing the registered destination, and push the generated rules to the gateway/PCEF for implementation.

[0066] FIG. 6B illustrates an example observed behavior detection method 650 for determining if an IP data flow carries content from spam engines. In step 652, the policy management system may receive parameters identifying certain key characteristics of the IP data flows and/or network traffic from a gateway/PCEF. In step 654, the policy management system may analyze the parameters and update local databases and/or counters with information that may be used to monitor sudden rises in outbound emails and/or sudden rises in domain name system (DNS) queries for mail exchanger (MX) records by a single mobile device. In step 656, the policy management system may monitor the number of outbound emails and/or DNS queries by performing IP-level and application-level monitoring operations. IP-level monitoring operations performed by the policy management system may include monitoring/counting the number of requests by a specific mobile device to port 25 of different IP addresses. Application-level monitoring operations may include monitoring the number of SMTP requests being sent directly to an email recipient's SMTP server from a single mobile device. The IP-level and application-level monitoring operations may be used to identify data flows carrying content originating from a spam engine because "well-behaved" email clients generally send all their outbound email via a single SMTP server, whereas spam engines typically send outbound emails directly to the email recipient's SMTP server.

[0067] In determination step 658, the policy management system may determine if there has been a sudden and unexpected rise in outbound emails and/or in domain name system (DNS) queries for mail exchanger (MX) records by a single mobile device. This determination may be based upon a counter value surpassing a pre-defined rate, as described previously. If the policy management system determines that there has not been a sudden and unexpected rise in outbound emails/queries (i.e., determination step 658 = "No"), in step 662, the policy management system may generate policy rules and push the rules to the gateway/PCEF. If the policy management system determines that there has been a sudden and unexpected rise in outbound emails and/or in domain name system (DNS) queries (i.e., determination step 658 = "Yes"), in determination step 660, the policy management system may determine if the rise in requests exceeds a predetermined threshold. If the rise exceeds the predetermined threshold (i.e., determination step 660 = "Yes"), in step 664, the policy management system may identify the data flow as carrying content from a spam engine, register the spam engine (e.g., update a spam engine list in memory, etc.), generate restrictive policy rules to block or limit data flows originating from the spam engine, and push the rules to the gateway/PCEF for enforcement. If the rise does not exceed the

EX1002
CISCO SYSTEMS, INC. / Page 356 of 1453

predetermined threshold (i.e., determination step 660 = "No"), in step 664, the policy management system may generate policy rules (e.g., allow, allow with constraints, etc.) and push the rules to the gateway/PCEF.

[0068] As mentioned above, the policy management system may perform detection methods (e.g., pattern matching, observed behavior, etc.) and generate restrictive policy rules based on the type of malware detected. For example, the policy management system may generate a "block" rule if an IP data flow carries content having binary-file characteristics of known malware threats (e.g., viruses, Trojan Horses, etc.) and an "allow with constraints" rule if the IP data flow represents a malware threat, but does not contain a binary that is a malware threat (e.g., the IP data flow is part of a denial of service attack, the IP data flow originates from a spam bot, etc.). The "allow with constraints" rule may define requirements (i.e., constraints) for allowing certain IP data flows to pass through the gateway/PCEF. For example, the constraints may require the gateway/PCEF to introduce an artificial latency to certain IP data flows or to set an upper threshold on certain IP data flow rates.

[0069] The "allow with constraints" type rules, and the constraints they impose, allow the policy management system to customize each rule to the preferences of a particular subscriber, wireless device type or type value, network component or network client. For example, the policy management system may access user preference parameters that define which constraints are to be used in various situations, as well as the actions, conditions and variables (e.g., risk levels, thresholds, data usage levels, costs, etc.) associated with each constraint. In an embodiment, a unique/separate set of user preference parameters may be maintained for each wireless subscriber, device, device type, network component, or client. In this manner telecommunications network operators and their customers may customize responses to malware events, which may be implemented automatically and in real time, consistent with the type of threat and how the network operator and/or customer prefers to respond. For example, some organizations cannot to afford to shut off all requests for service during a denial of service attack, and thus would prefer constraints on the volume or data rates imposed on incoming service requests.

[0070] In an embodiment, the constraints imposed by the policy management system may be proportional to a malware threat or threat-level as determined by the malware protection system or specified by an operator. Methods for determining a malware threat-level within malware protection system are disclosed herein. In an embodiment, the constraints imposed by the policy management system may become progressively more restrictive or constrained, in real-time, as a malware threat or threat-level rises as determined by malware protection system, an operator or other systems configured to identify the threat level.

[0071] User preference parameters may define the actions and conditions associated with each constraint in "allow with constraints" type rules. Thus, the user preference parameters may be used by the policy management system to generate policy rules that instruct the gateway/PCEF to perform several different types of operations (i.e., actions) as well as set conditions for performing those actions. For example, the policy management system may access the user preference parameters to determine that the correct course of action (i.e., the correct rule) for the gateway/PCEF upon the detection of low-risk malware is to send an alert message to the wireless device without blocking the IP data flow. Likewise, the user preference parameters may be used by the policy management system to generate rules that instruct the gateway/PCEF to block the current IP data flow and all future IP data flows until the malware has been manually removed from the mobile device.

[0072] In an embodiment, the policy management system may perform quarantining operations by storing details of IP data flows, aggregated details of the IP data flows, or sequestering the actual content of the IP data flows, that were allowed, constrained, or blocked. The policy management system may store source information, destination information and time information for each IP data flow that is constrained. For example, the policy management system may track the number of IP data flows containing infected binaries within a predetermined time period (e.g., within the last month) and store the number value in a memory. The policy management system may also store emails deemed to be spam. This information may be stored such that a wireless device user whose mobile device is associated with these IP data flows may subsequently view the quarantining details. In an embodiment, the policy management system may be configured to receive messages from the wireless device user that trigger further quarantining actions (e.g., removing a stored IP data flow, un-quarantining stored IP data flow, etc.). For example, the user may send the policy management system a message to reclassify an email as not spam, in which case the email may be pushed to the mobile device by the policy management system. In an embodiment, the user may classify the IP data flow in a manner that causes the policy management system to allow delivery of future similar IP data flows.

[0073] In the various embodiments, user preference parameters may be generated from information from a subscriber account in the user repository, by interacting with the user (e.g., via SMS messages sent through the notification server 126, etc.) to determine his/her preferences in real-time, by using contextual information (e.g., roaming in third party network, home network, etc.), or any combination thereof. For example, a wireless device user may upload user preference parameters to the user repository that instructs the policy management system to send an alert to the user's wireless device warning of potential risks if the wireless device is not roaming in a third-party mobile data network and to block the current IP data flow and all future IP data flows if the wireless

EX1002
CISCO SYSTEMS, INC. / Page 357 of 1453

device is roaming in a third-party mobile data network. In this manner, cost conscientious users may prevent a potential malware program from accessing online services while roaming in an expensive third-party mobile data network.

[0074] In an embodiment, the user preference parameters may be based on a malware threat model. The malware threat model may be defined in terms of multiple independent factors, such as the probability of infection, the type of infection, the severity of the threat posed by the infection, and the difficulty associated with removing the infection. These factors may be weighted and combined to produce an overall threat level. The user may then specify his/her preference in terms of this overall threat level. Alternatively, the user may specify his/her preference in terms of one of the factors within the threat model (e.g., a user may be willing to be exposed to a type of infection that installs Adware, whereas he/she may not be willing to be exposed to a type of infection that corrupts or destroys data stored on the wireless device).

[0075] In an embodiment, the policy management system and/or gateway/PCEF may be configured to charge users/subscribers differently for the IP data flows depending on the actions. For example, a user/subscriber may not be charged for any IP data flows that were blocked by the gateway.

[0076] In an embodiment, a malware prevention and removal client (MPRC) software application may be pushed to the wireless devices. The policy management system may, upon determining that an IP data flow is associated with a malware threat, notify the malware protection system of the wireless device's identity and the detected malware. The malware protection system may then update, or instruct, the MPRC to take preventative, recovery, or removal actions specific to the wireless device type or type value and the detected malware threat. For example, the malware protection system may instruct the MPRC to disable the wireless device's data capabilities and/or isolate the mobile device from the mobile data network until the malware is removed or is otherwise no longer a threat. In an embodiment, the policy management system may send a notification based on the status of the user's subscription to the malware prevention service.

[0077] As discussed above with reference to FIG. 3, the policy management system may exchange information with both a user repository and a charging system. In an embodiment, the policy management system may directly charge the subscription accounts of beneficiaries (e.g., wireless device users, web servers, telecommunication clients, etc.) of the above mentioned malware detection/prevention services by sending a charging message to deduct funds from each subscriber's service account. For example, the policy management system may send a charge message to charge a wireless device user's wireless subscription account each time malware is detected and/or removed from the user's wireless device.

[0078] The policy management system may support multiple different charging models to support any required business models. The charging models may include providing the above mentioned services free-of-charge, charging on an annual basis, on a pay-as-you-consume basis, or any combination thereof. If the services are charged on an annual basis, the policy management system may determine the status of the users' annual subscriptions (e.g., last time payment was made, account status, subscription level, etc.) by accessing the user repository and sending charging messages to the charging system to charge the customers as required. If the services are charged on a pay-as-you-consume basis, the policy management system may send a charging request to the charging system each time the service is provided (e.g., each time a message is send waning of potential malware). In an embodiment, each service may be charged separately. For example, the policy management system may send charging messages to the charging system annually for the detection services and send charging messages to the charging system each time malware is removed.

[0079] In an embodiment, the policy management system may be configured to automatically adapt to a network wide stance if the detection of malware indicates that the network is under attack. The adaption of the network wide stance may be in stages, such that the network-wide protections are progressive. In an embodiment, the policy management system may change and/or bulk push policies/rules into the network if the network the detection of malware indicates that the network is under attack. Policies/rules may be pushed to network elements upon detection of a new malware threat or upon a malware threat level achieving a predefined threshold such that the network adopts an "under attack" pre-defined configuration. The initiation of such "under attack" responses or configuration may be based on the detection of malware and/or policy counters exceeding a predefined threshold number or instances of attack.

[0080] The various embodiments and logical components may be implemented on any of a variety of commercially available server devices, such as the server 700 illustrated in FIG. 7. Such a server 700 typically includes a processor 701 coupled to volatile memory 702 and a large capacity nonvolatile memory, such as a disk drive 703. The server 700 may also include a floppy disc drive, compact disc (CD) or DVD disc drive 706 coupled to the processor 701. The server 700 may also include network access ports 704 coupled to the processor 701 for establishing data connections with a network 705, such as a local area network coupled to other broadcast system computers and servers.

[0081] The processor 701 may be any programmable microprocessor, microcomputer or multiple processor chip or chips that can be configured by software instructions (applications) to perform a variety of functions, including the functions of the various embodiments described below. Multiple processors 701 may be provided,

EX1002
CISCO SYSTEMS, INC. / Page 358 of 1453

such as one processor dedicated to wireless communication functions and one processor dedicated to running other applications. Typically, software applications may be stored in the internal memory 702, 703 before they are accessed and loaded into the processor 701. The processor 701 may include internal memory sufficient to store the application software instructions.

[0082] The foregoing method descriptions and the process flow diagrams are provided merely as illustrative examples and are not intended to require or imply that the steps of the various embodiments must be performed in the order presented. As will be appreciated by one of skill in the art the order of steps in the foregoing embodiments may be performed in any order. Words such as "thereafter," "then," "next," etc. are not intended to limit the order of the steps; these words are simply used to guide the reader through the description of the methods. Further, any reference to claim elements in the singular, for example, using the articles "a," "an" or "the" is not to be construed as limiting the element to the singular.

[0083] The various illustrative logical blocks, modules, circuits, and algorithm steps described in connection with the embodiments disclosed herein may be implemented as electronic hardware, computer software, or combinations of both. To clearly illustrate this interchangeability of hardware and software, various illustrative components, blocks, modules, circuits, and steps have been described above generally in terms of their functionality. Whether such functionality is implemented as hardware or software depends upon the particular application and design constraints imposed on the overall system. Skilled artisans may implement the described functionality in varying ways for each particular application, but such implementation decisions should not be interpreted as causing a departure from the scope of the present invention.

[0084] The hardware used to implement the various illustrative logics, logical blocks, modules, and circuits described in connection with the aspects disclosed herein may be implemented or performed with a general purpose processor, a digital signal processor (DPC), an application specific integrated circuit (ASIC), a field programmable gate array (FPGA) or other programmable logic device, discrete gate or transistor logic, discrete hardware components, or any combination thereof designed to perform the functions described herein. A general-purpose processor may be a microprocessor, but, in the alternative, the processor may be any conventional processor, controller, microcontroller, or state machine. A processor may also be implemented as a combination of computing devices, e.g., a combination of a DPC and a microprocessor, a plurality of microprocessors, one or more microprocessors in conjunction with a DPC core, or any other such configuration. Alternatively, some steps or methods may be performed by circuitry that is specific to a given function.

[0085] In one or more exemplary aspects, the functions described may be implemented in hardware, software, firmware, or any combination thereof. If implemented in software, the functions may be stored on or transmitted over as one or more instructions or code on a non-transitory computer-readable medium. The steps of a method or algorithm disclosed herein may be embodied in a processor-executable software module which may reside on a non-transitory computer-readable storage medium. Non-transitory computer-readable storage media may be any available media that may be accessed by a computer (e.g., a server) or processor of a computer or server. By way of example, and not limitation, non-transitory computer-readable media may include RAM, ROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other storage medium that may be used to store desired program code in the form of processor-executable instructions or data structures and that may be accessed by a computer. Disk and disc, as used herein, includes compact disc (CD), laser disc, optical disc, digital versatile disc (DVD), floppy disk, and blu-ray disc where disks usually reproduce data magnetically, while discs reproduce data optically with lasers. Combinations of the above should also be included within the scope of non-transitory computer-readable media. Additionally, the operations of a method or algorithm may reside as one or any combination or set of codes and/or instructions on a non-transitory machine readable medium and/or computer-readable medium, which may be incorporated into a computer program product.

[0086] The preceding description of the disclosed embodiments is provided to enable any person skilled in the art to make or use the present invention. Various modifications to these embodiments will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other embodiments without departing from the scope of the invention. Thus, the present invention is not intended to be limited to the embodiments shown herein but is to be accorded the widest scope consistent with the following claims and the principles and novel features disclosed herein.

Claims

1. A communication method, comprising:

   receiving in a server from one or more communication system control network components data flow parameters identifying characteristics of a data flow;

   performing in the server a detection method to determine if the data flow carries malicious content;

   generating restrictive policy rules in response to determining the data flow carries malicious content;

   generating non-restrictive policy rules in response to determining the data flow does not

EX1002
CISCO SYSTEMS, INC. / Page 359 of 1453

carry malicious content; and
pushing the generated policy rules to a communication system gateway configured to control a flow of packet-based data between a wireless device and an external network.

2. The method of claim 1, wherein generating restrictive policy rules in response to determining the data flow carries malicious content comprises generating restrictive policy rules based on a subscriber's usage history and a subscription level.

3. The method of claim 1, wherein generating restrictive policy rules in response to determining the data flow carries malicious content comprises generating constraints that are proportional to a threat-level associated with the malicious content and generating restrictive policy rules that impose the generated constraints on the communication system gateway.

4. The method of claim 1, further comprising transmitting malware detection feedback to a network component in a second external network.

5. The method of claim 1, further comprising interacting with a wireless device user to determine user preferences in real-time via alert messages sent through a notification server to receive user preference parameters.

6. The method of claim 1, wherein the data flow originates from the wireless device, and generating restrictive policy rules in response to determining the data flow carries malicious content comprises generating restrictive policy rules that instruct the communication system gateway to block future data flows originating from the wireless device.

7. The method of claim 1, wherein performing a detection method to determine if the data flow carries content that is a security risk comprises performing a pattern matching detection method.

8. The method of claim 7, wherein:

receiving in a server from one or more communication system control network components data flow parameters identifying characteristics of a data flow comprises receiving parameters identifying binary-file characteristic information; and
performing a pattern matching detection method comprises comparing the identified binary-file characteristic information with a binary-file characteristic of a known malware type to determine if the data flow carries content having binary-file characteristics of known malware.

9. The method of claim 7, wherein:

receiving in a server from one or more communication system control network components data flow parameters identifying characteristics of a data flow comprises receiving parameters identifying source and destination information; and
performing in the server a pattern matching detection method comprises comparing the identified source and destination information against a list of known offender sources and destinations to determine if the data flow originates from a wireless device known to engage in malicious activity and if the data flow is destined for a website/server known to engage in malicious activities.

10. The method of claim 7, wherein:

receiving in a server from one or more communication system control network components data flow parameters identifying characteristics of a data flow comprises receiving parameters identifying destination information; and
performing in the server a pattern matching detection method comprises comparing the identified destination information against a list of destinations known to be under attack to determine if a destination of the data flow is a network server under attack.

11. The method of claim 7, wherein:

receiving in a server from one or more communication system control network components data flow parameters identifying characteristics of a data flow comprises receiving parameters identifying messaging information; and
performing in the server a pattern matching detection method comprises comparing the identified messaging information with spam heuristics.

12. The method of claim 1, wherein performing in the server a detection method to determine if the data flow carries content that is a security risk comprises performing a behavior oriented detection method.

13. The method of claim 12, wherein performing a behavior oriented detection method comprises accessing information stored in one of a user repository of a control network and a charging system of a control network.

14. The method of claim 12, wherein performing a behavior oriented detection method comprises updating a counter value to monitor a number of data flows

EX1002
CISCO SYSTEMS, INC. / Page 360 of 1453

matching a specific behavior.

15. The method of claim 12, wherein performing a behavior oriented detection method comprises performing monitoring operations in order to detect an unexpected rise in a number of requests matching a defined behavior from a specific wireless device.

16. A server, comprising:

a memory; and
a processor coupled to the memory, wherein the processor is configured with processor-executable instructions to perform operations comprising:

receiving data flow parameters identifying characteristics of a data flow;
performing a detection method to determine if the data flow carries malicious content;
generating restrictive policy rules in response to determining the data flow carries malicious content;
generating non-restrictive policy rules in response to determining the data flow does not carry malicious content; and
pushing the generated policy rules to a communication system gateway configured to control a flow of packet-based data between a wireless device and an external network.

17. A non-transitory computer readable medium having stored thereon processor-executable software instructions configured to cause a processor to perform operations comprising:

receiving from one or more communication system control network components data flow parameters identifying characteristics of a data flow;
performing a detection method to determine if the data flow carries malicious content;
generating restrictive policy rules in response to determining the data flow carries malicious content;
generating non-restrictive policy rules in response to determining the data flow does not carry malicious content; and
pushing the generated policy rules to a communication system gateway configured to control a flow of packet-based data between a wireless device and an external network.

EX1002
CISCO SYSTEMS, INC. / Page 361 of 1453

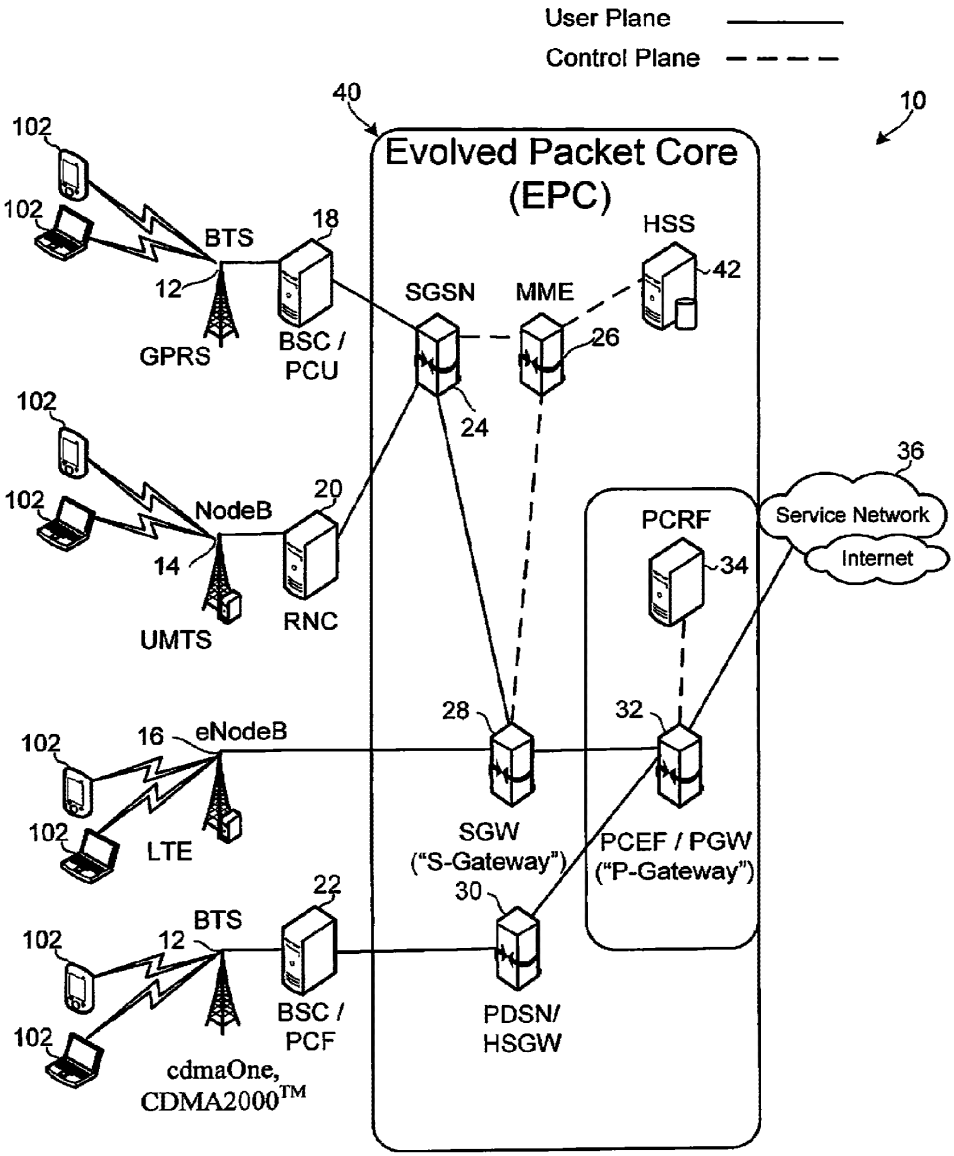

User Plane
Control Plane
40
10
Evolved Packet Core
(EPC)
102
102
BTS
18
12
GPRS
BSC /
PCU
SGSN
MME
HSS
42
26
24
102
102
NodeB
20
14
UMTS
RNC
36
Service Network
Internet
PCRF
34
28
32
102
102
16
eNodeB
LTE
SGW
("S-Gateway")
PCEF / PGW
("P-Gateway")
30
22
102
102
BTS
12
BSC /
PCF
PDSN/
HSGW
cdmaOne,
CDMA2000™

FIG. 1

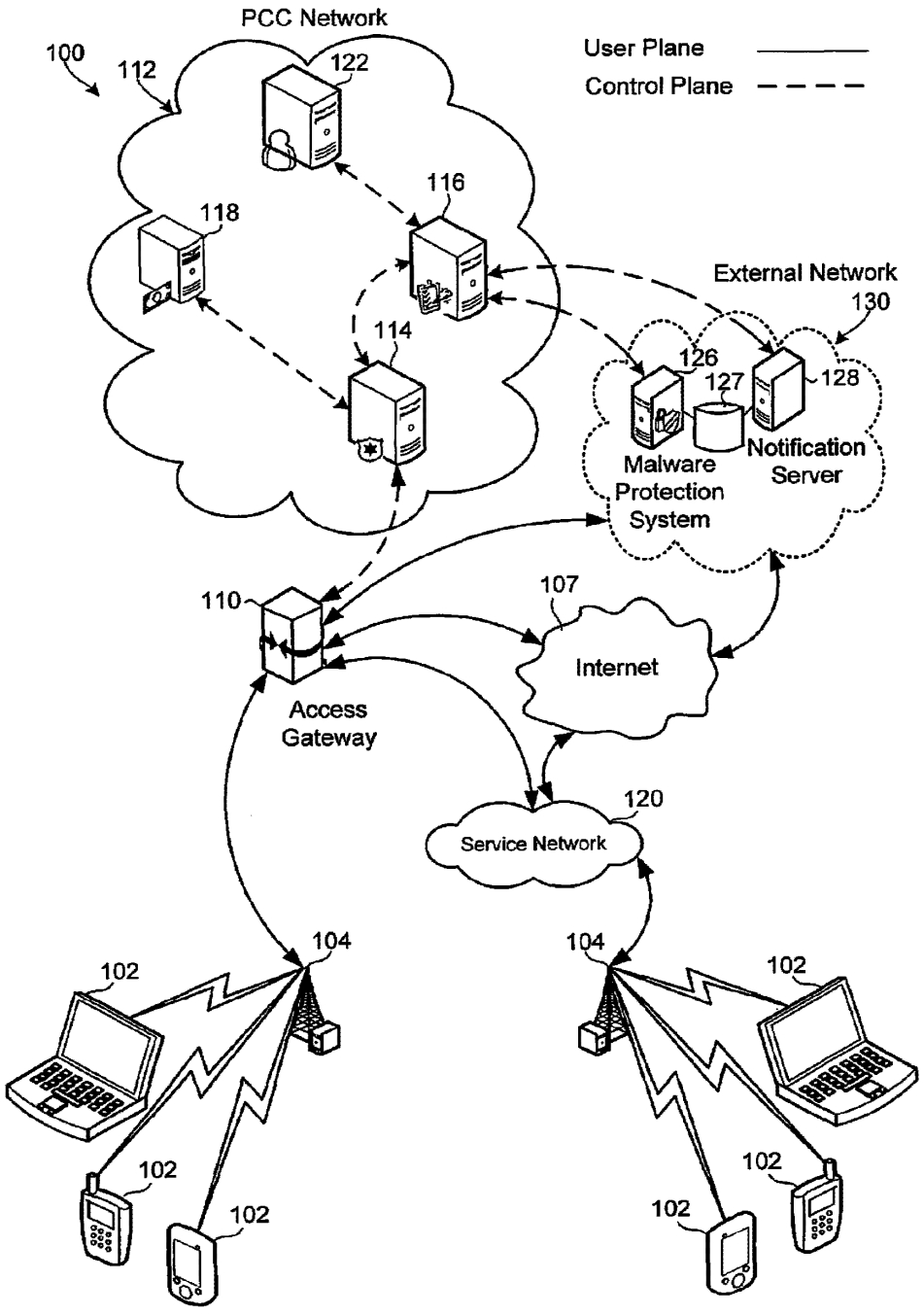

PCC Network
100
112
122
User Plane
Control Plane
116
118
114
External Network
130
126
127
128
Malware Protection System
Notification Server
110
107
Internet
Access Gateway
120
Service Network
104
104
102
102
102
102
102
102

FIG. 2

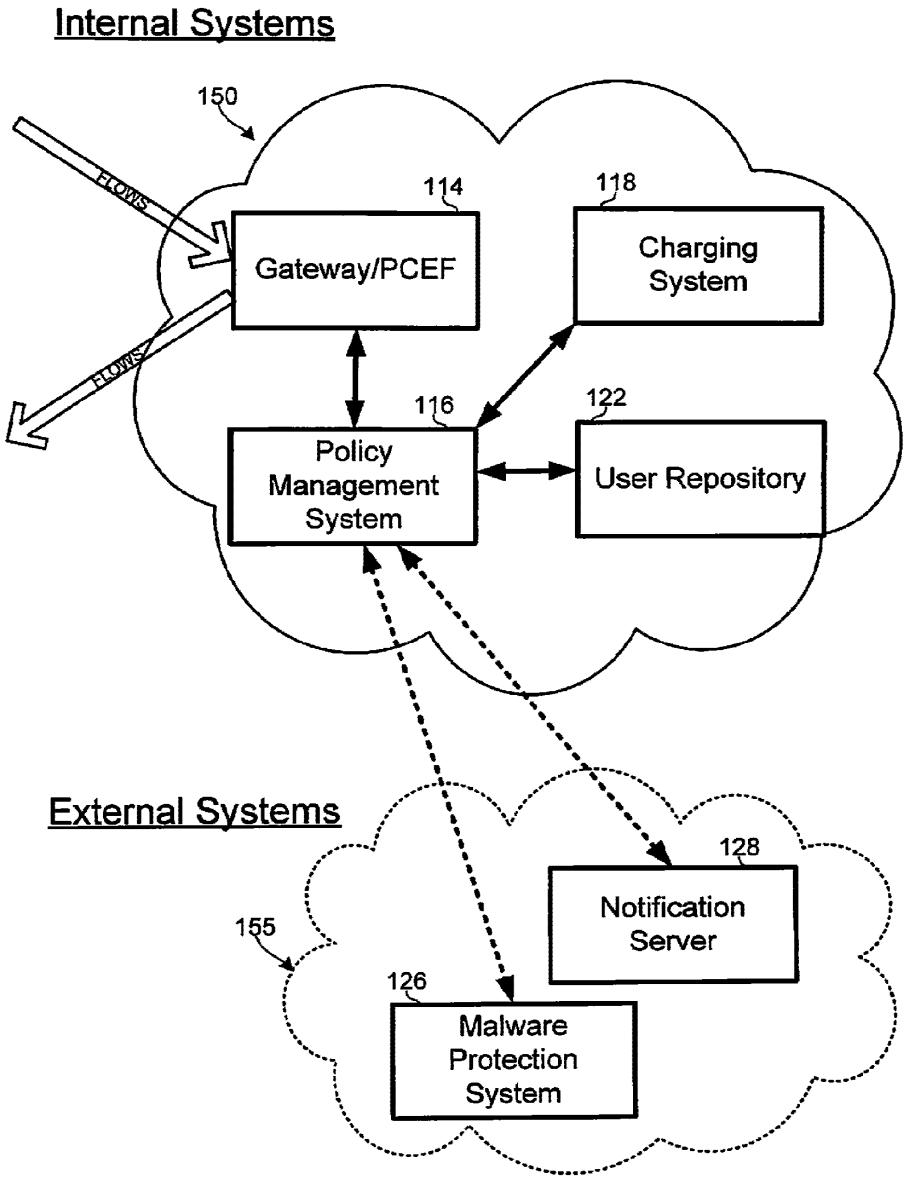

Internal Systems
150
FLOWS
FLOWS
114
Gateway/PCEF
118
Charging System
116
Policy Management System
122
User Repository
External Systems
155
128
Notification Server
126
Malware Protection System

FIG. 3A

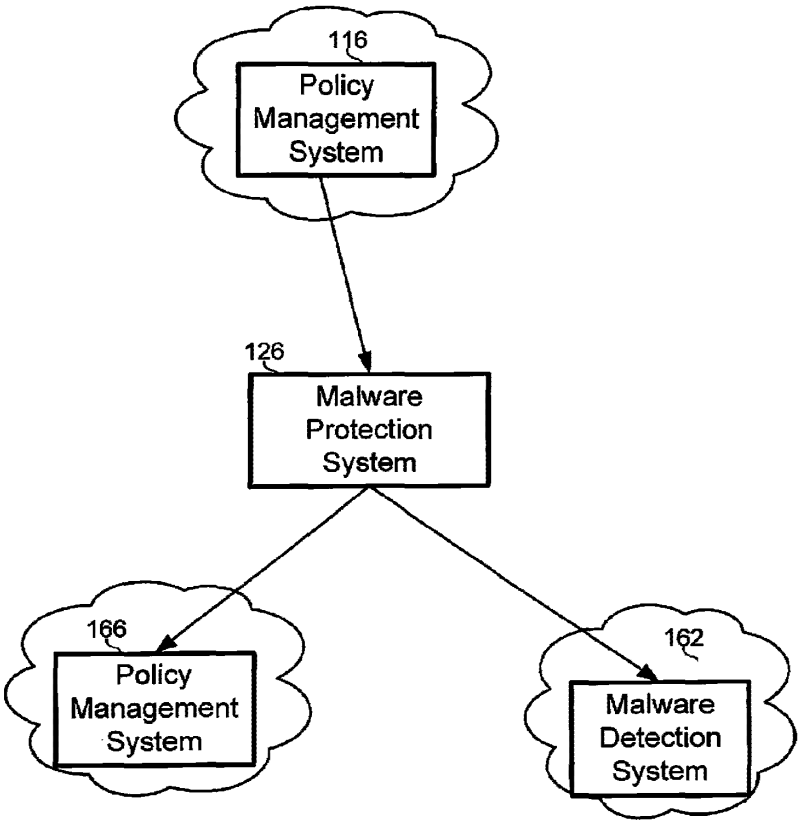


FIG. 3B

EX1002
CISCO SYSTEMS, INC. / Page 365 of 1453

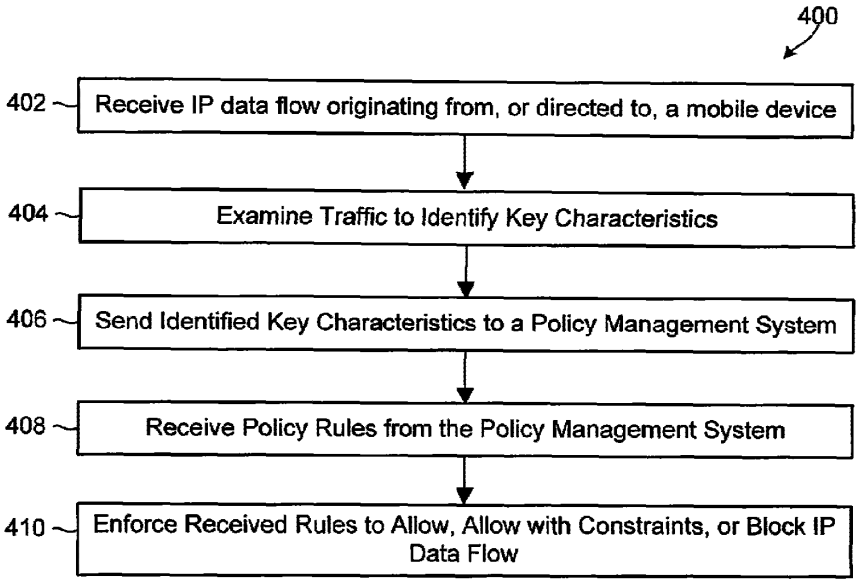


FIG. 4A

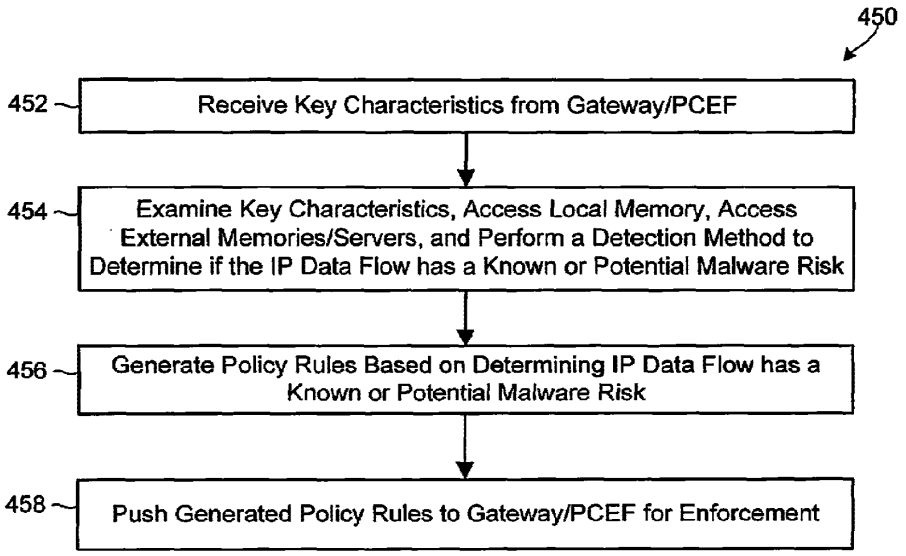


FIG. 4B

EX1002
CISCO SYSTEMS, INC. / Page 366 of 1453

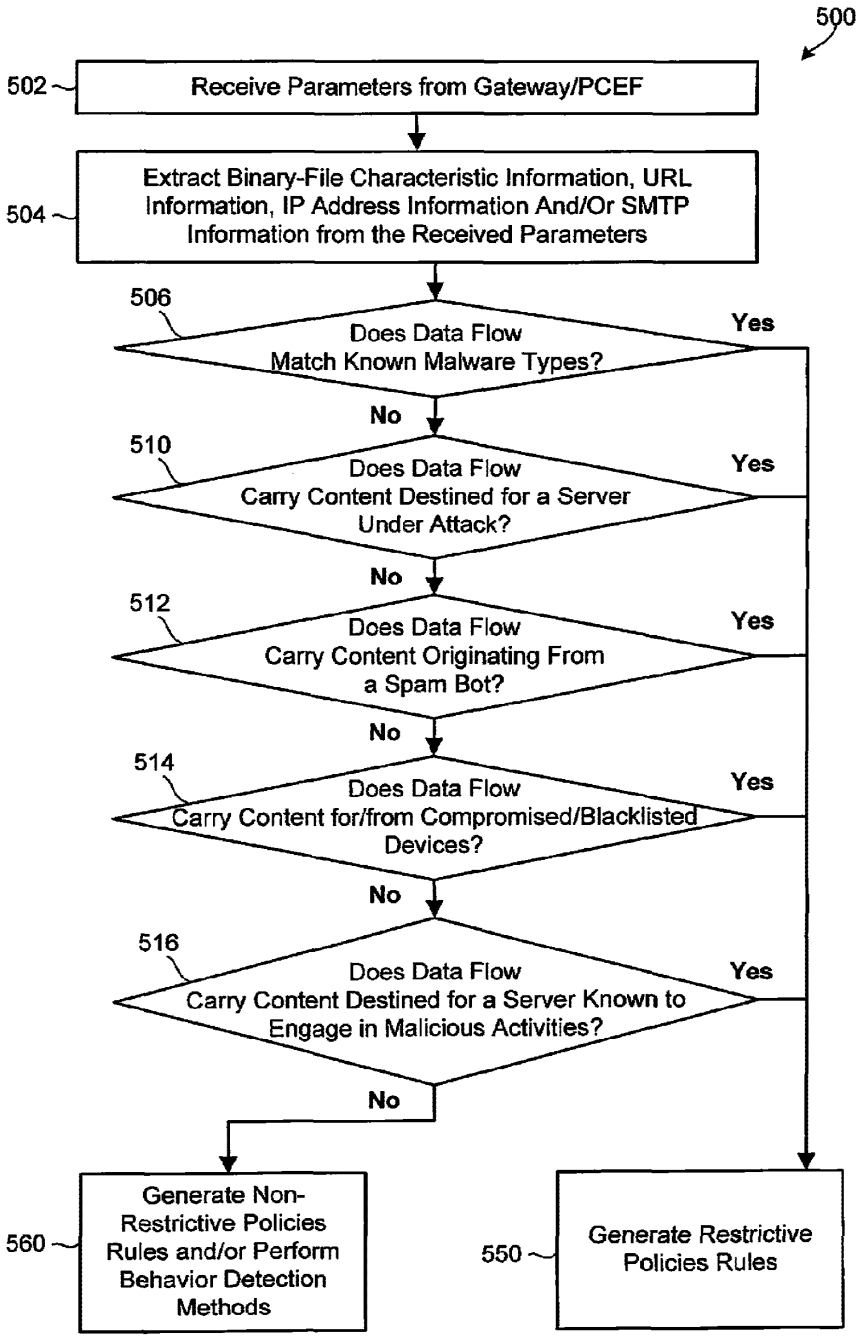

500
502
Receive Parameters from Gateway/PCEF
504
Extract Binary-File Characteristic Information, URL Information, IP Address Information And/Or SMTP Information from the Received Parameters
506
Does Data Flow Match Known Malware Types?
Yes
No
510
Does Data Flow Carry Content Destined for a Server Under Attack?
Yes
No
512
Does Data Flow Carry Content Originating From a Spam Bot?
Yes
No
514
Does Data Flow Carry Content for/from Compromised/Blacklisted Devices?
Yes
No
516
Does Data Flow Carry Content Destined for a Server Known to Engage in Malicious Activities?
Yes
No
560
Generate Non-Restrictive Policies Rules and/or Perform Behavior Detection Methods
550
Generate Restrictive Policies Rules

FIG. 5

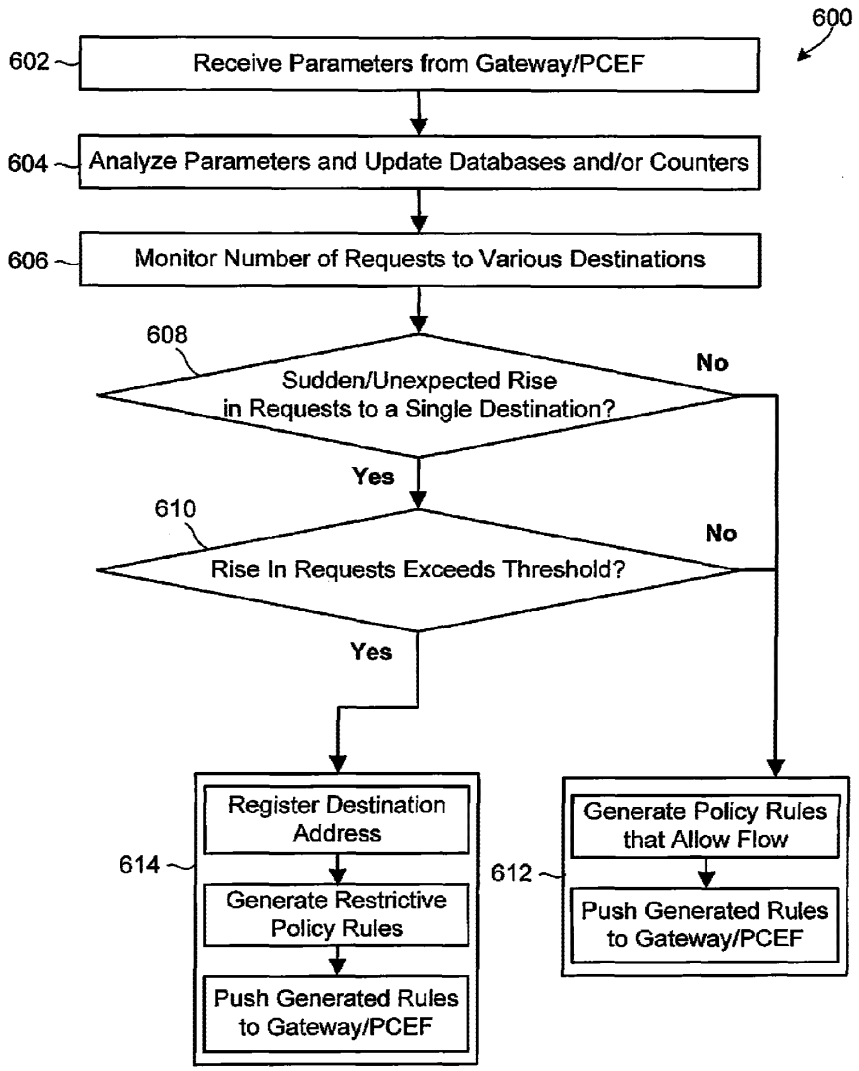


FIG. 6A

EX1002
CISCO SYSTEMS, INC. / Page 368 of 1453

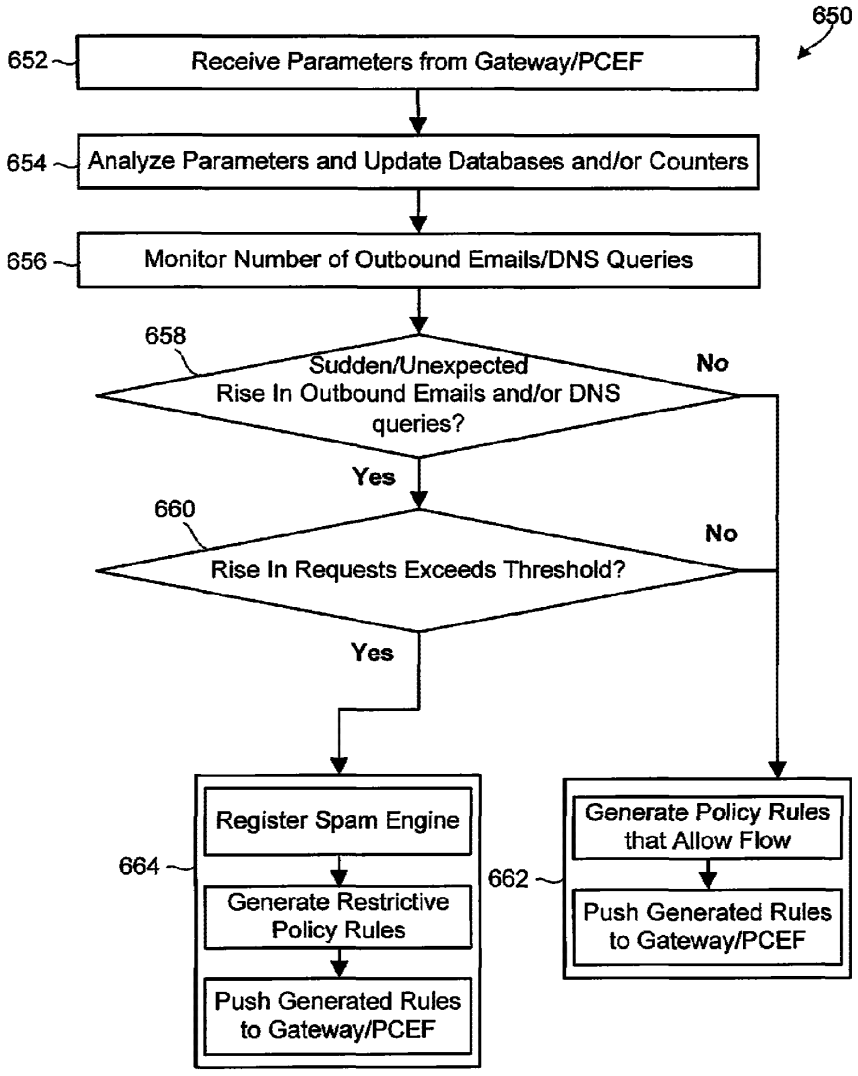


FIG. 6B

EX1002
CISCO SYSTEMS, INC. / Page 369 of 1453

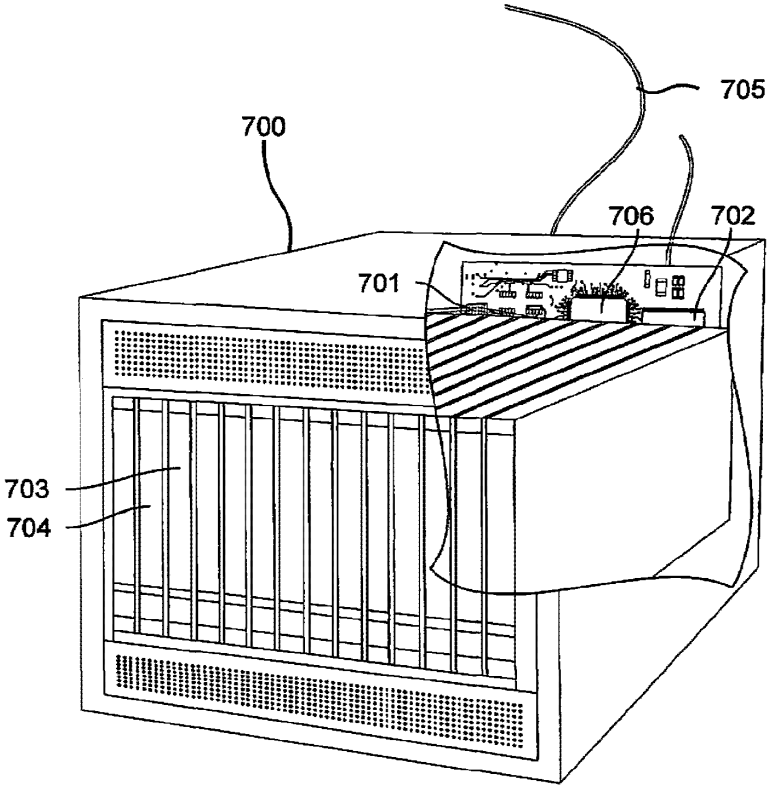


FIG. 7

EX1002
CISCO SYSTEMS, INC. / Page 370 of 1453

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 12 15 8921

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	WO 2009/132700 A1 (ERICSSON TELEFON AB L M [SE]; STENFELT JOHN [SE]) 5 November 2009 (2009-11-05) * page 6, lines 4-10 * * page 8, lines 6-10 * * page 15, line 25 - page 17, line 16 * * page 17, lines 29-31 * * claim 12; figures 1,4 *	1-17	INV. H04L12/24 H04L29/06 H04W12/08 H04W12/12 ADD. H04W24/00 H04W88/16
X	US 2004/193912 A1 (LI HONG C [US] ET AL) 30 September 2004 (2004-09-30) * paragraphs [0024], [0039] - [0041] * * figure 3 *	1-17	
A	US 2007/006309 A1 (HERBERT HOWARD C [US] ET AL SMITH NED M [US] ET AL) 4 January 2007 (2007-01-04) * paragraph [0026]; figure 2 *	1-17	

TECHNICAL FIELDS SEARCHED (IPC)
H04L
H04W

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	20 June 2012	Pajatakis, Emmanouil

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

EX1002
CISCO SYSTEMS, INC. / Page 371 of 1453

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 12 15 8921

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

20-06-2012

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2009132700 A1	05-11-2009	EP 2304915 A1	06-04-2011
		US 2011041182 A1	17-02-2011
		WO 2009132700 A1	05-11-2009
US 2004193912 A1	30-09-2004	CN 1768518 A	03-05-2006
		DE 112004000428 B4	26-11-2009
		DE 112004000428 T5	09-02-2006
		GB 2412540 A	28-09-2005
		JP 2006521598 A	21-09-2006
		JP 2009187587 A	20-08-2009
		KR 20050118223 A	15-12-2005
		TW I253571 B	21-04-2006
		US 2004193912 A1	30-09-2004
		WO 2004095801 A1	04-11-2004
US 2007006309 A1	04-01-2007	TW I323102 B	01-04-2010
		US 2007006309 A1	04-01-2007
		WO 2007002875 A1	04-01-2007

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

EX1002
CISCO SYSTEMS, INC. / Page 372 of 1453

Espacenet

Bibliographic data: KR20010079361 (A) — 2001-08-22

FIRE WALL SYSTEM BASED ON NETWORK STATUS AND METHOD THEREOF

Inventor(s): JANG HUI JIN [KR]; KIM SANG WOOK [KR]; PARK BO SEOK [KR]; PARK IN SEONG [KR]; SONG BYEONG UK [KR] ± (JANG, HUI JIN, ; KIM, SANG WOOK, ; PARK, BO SEOK, ; PARK, IN SEONG, ; SONG, BYEONG UK)

Applicant(s): KIM SANG WOOK [KR] ± (KIM, SANG WOOK)

Classification: **- international:** ***H04L12/22; H04L12/26; H04L12/70;*** (IPC1-7): H04L12/56

- cooperative:

Application number: KR20010040894 20010709

Priority number(s): KR20010040894 20010709

Abstract of KR20010079361 (A)

PURPOSE: A fire wall system based on network status and a method thereof are provided to interrupt all illegal packet or traffic flowing into an internal network through an external information communication networks by analyzing the status of network traffic from various angles and differentially reflecting a traffic control policy together with recognition for status through a status graph. CONSTITUTION: A fire wall system based on network status consists of a network traffic collection unit(100), a static status information collection unit(200), a dynamic status information analysis unit(300), a traffic monitor unit(400), a rule generation unit(500), and a traffic control unit(600). The network traffic collection unit(100) classifies the network packets collected from an external information communication network by hosts, protocols and connections. The static status information collection unit(200), comprised of a statistics analyzer(230), a status unit table(220) and a packet manager(210), analyzes the information of the network packets transmitted from the network traffic collection unit(100), updates the information of the status unit table(220), and processes traffic information. The dynamic status information analysis unit(300), containing a traffic log table(310) and a traffic history analyzer(320), analyzes and records the long-term inclination and pattern of the network traffic of the traffic information processed at the static status information collection unit(200). The traffic monitor unit(400) monitors the trend of network traffic using each information provided from the static status information collection unit(200) and the dynamic status information analysis unit(300), recognizes an abnormal situation and outputs a state transition signal. The rule generation unit(500), composed of a policy manager(510), a status graph table(520) and an action manager(530), receives the state transition signal from the traffic monitor unit(400), creates a status graph, generates a packet filtering rule using the graph, and transfers the rule to the

traffic control unit(600) so that the traffic control unit(600) can cope with the abnormal situation.

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 특2001-0079361
(43) 공개일자 2001년08월22일

(51) 국제분류코드
H04L 12/56 (2006.01)

(21) 출원번호 10-2001-0040894

(22) 출원일자 2001년07월09일

(71) 출원인
김상욱
대구광역시 수성구 수성1가 신세계타운 10동 501호, 대한민국

(72) 발명자
김상욱
대구광역시 수성구 수성1가 신세계타운 10동 501호, 대한민국
송병욱
대구광역시북구산격3동1313-37, 대한민국
박인성
경상북도경주시석장동858번지, 대한민국
장희진
대구광역시수성구지산동서한청산맨션102동1105호, 대한민국
박보석
대구광역시동구신암1동652-11, 대한민국

(74) 대리인
이영필
이해영

(77) 심사관
있음

전체 청구항 수 : 총 9 항

(54) 네트워크 상태 기반의 방화벽 장치 및 그 방법

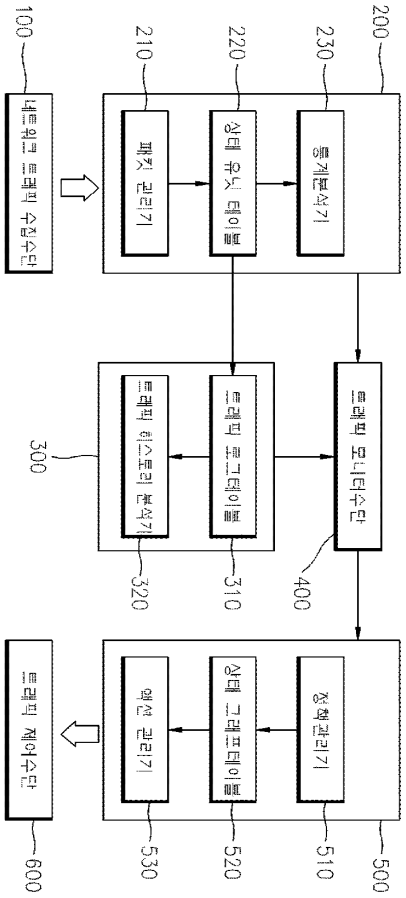
(57)요 약

본 발명은 외부 정보 통신망으로부터 유입되는 모든 패킷의 정보를 분석하여 유효성과 불법성을 분석하고, 내부 네트워크의 비정상적인 상황을 유도하는 트래픽 패턴을 인식하며, 비정상적 상황을 파악하고 네트워크 관리 정책에 따라 대응하기 위한 네트워크 상태 기반의 방화벽 장치 및 그 방법에 관한 것으로,

본 발명의 장치는, 외부 정보 통신망으로부터 수집한 네트워크 패킷을 호스트, 프로토콜, 커넥션별로 구분하여 출력하는 네트워크트래픽수집수단; 상기 네트워크트래픽수집수단에서 전송되는 상기 네트워크 패킷의 정보를 분석하고, 상태 유닛 테이블 정보를 갱신하여 트래픽 정보를 가공하는 정적상태정보수집수단; 상기 정적상태정보수집수단에서 가공된 상기 트래픽 정보의 네트워크 트래픽의 장기적인 성향과 패턴을 분석하고 기록하는 동적상태정보분석수단; 상기 정적상태정보수집수단과 상기 동적상태정보분석수단에서 각각 제공하는 정보를 이용하여 상기 네트워크트래픽의 동향을 감시하고 비정상적인 상황을 인식하여 상태 전이 신호를 출력하는 트래픽모니터수단; 및 상기 트래픽모니터수단에서 출력되는 상태 전이 신호를 받아서 생성된 상태 그래프 테이블을 이용하여 비정상적인 네트워크 상황을 정상적으로 유도하기 위한 패킷 필터링 룰을 생성하는 룰생성수단를 포함하는데 특징이 있다. 또한, 본 발명의 방법은, 게이트웨이를 통과하는 네트워크 패킷을 수집하여 상태 유닛별로 분류하는 제 1 과정; 상기 제 1 과정에서 수집된 상기 네트워크 패킷을 통계 및 패턴 분석 처리하여 현재의 트래픽 상황에 대한 정보를 생성하는 제 2 과정; 상기 제 2 과정에서 생성된 트래픽 상황에 대한 정보를 분석하고 감시하여 네트워크의 비정상적인 상황의 발생을 인지하여 상태 전이 신호를 생성하는 제 3 과정; 상기 제 3 과정에서 생성된 상태 전이 신호에 따라 상태 전이를 발생시켜, 그에 따른 정책을 재택하고 새로운 패킷 필터링 룰을 생성하는 제 4 과정; 및 상기 제 4 과정이 완료되면 현재 적용되고 있는 정책과 필터링 룰을 기록하고 상태 정보와 로그를 저장하는 제 5 과정을 포함하는데 특징이 있다.

키워드 : 트래픽, 상태 유닛, 통계 분석, 히스토리, 로그, 정책, 상태 그래프, 액션

대 표 도 - 도 2



This Facsimile Page has been artificially created from KIPO data.

청구의 범위

청구항 1

외부 정보 통신망으로부터 수집한 네트워크 패킷을 호스트, 프로토콜, 커넥션별로 구분하여 출력하는 네트워크트래픽수집수단;

상기 네트워크트래픽수집수단에서 전송되는 상기 네트워크 패킷의 정보를 분석하고, 상태 유닛 테이블 정보를 갱신하여 트래픽 정보를 가공하는 정적상태정보수집수단;

상기 정적상태정보수집수단에서 가공된 상기 트래픽 정보의 네트워크 트래픽의 장기적인 성향과 패턴을 분석하고 기록하는 동적상태정보분석수단;

상기 정적상태정보수집수단과 상기 동적상태정보분석수단에서 각각 제공하는 정보를 이용하여 상기 네트워크 트래픽의 동향을 감시하고 비정상적인 상황을 인식하여 상태 전이 신호를 출력하는 트래픽모니터수단; 및

상기 트래픽모니터수단에서 출력되는 상태 전이 신호를 받아서 생성된 상태 그래프 테이블을 이용하여 비정상적인 네트워크 상황을 정상적으로 유도하기 위한 패킷 필터링 룰을 생성하는 룰생성수단를 포함하는 것을 특징으로 하는 네트워크 상태 기반의 방화벽 장치.

청구항 2

제 1 항에 있어서, 상기 정적상태정보수집수단은

상기 네트워크 패킷의 정보를 분석하는 패킷관리기; 및

상기 패킷관리기에서 분석된 상기 네트워크 패킷의 정보에 따라 상태 유닛 테이블의 정보를 갱신하는 통계분석기를 포함함을 특징으로 하는 네트워크 상태 기반의 방화벽 장치.

청구항 3

제 1 항에 있어서, 상기 동적상태정보분석수단은

발생하는 모든 이벤트에 대한 로그를 기록하여 관리자에게 네트워크와 방화벽의 관리에 대한 참고 자료를 제공하는 트래픽로그테이블; 및

상기 트래픽로그테이블에서 제공되는 참고 자료를 받아서 상기 네트워크 트래픽의 패턴과 그에 따른 대응 방식을 기록, 분석하는 트래픽히스토리분석기를 포함함을 특징으로 하는 네트워크 상태 기반의 방화벽 장치.

청구항 4

제 1 항에 있어서, 상기 룰생성수단은

상기 트래픽모니터수단에 의하여 생성된 상태 전이 신호를 받아 상태 그래프 테이블을 생성하는 정책관리기; 및

상기 정책관리기에서 생성된 상태 그래프 테이블에서 일어난 상태 전이에 따라 현재의 상황 지시자가 새로운 상태 노드로 이동하면 채택되는 새로운 네트워크 트래픽 관리 정책에 따라 현재 적용되고 있는 패킷 데이터 룰을 제거하거나 새로운 룰을 추가하는 액션관리기를 포함함을 특징으로 하는 네트워크 상태 기반의 방화벽 장치.

청구항 5

제 1 항에 있어서,

비정상적인 네트워크 상황을 정상적으로 유도하기 위한 패킷 필터링 룰을 전달받아 네트워크의 비정상적 상황에 대응하는 트래픽제어수단을 더 포함함을 특징으로 하는 네트워크 상태 기반의 방화벽 장치.

청구항 6

게이트웨이를 통과하는 네트워크 패킷을 수집하여 상태 유닛별로 분류하는 제 1 과정;

상기 제 1 과정에서 수집된 상기 네트워크 패킷을 통계 및 패턴 분석 처리하여 현재의 트래픽 상황에 대한 정보를 생성하는 제 2 과정;

상기 제 2 과정에서 생성된 트래픽 상황에 대한 정보를 분석하고 감시하여
네트워크의 비정상적인 상황의 발생을 인지하여 상태 전이 신호를 생성하는 제 3 과정;

상기 제 3 과정에서 생성된 상태 전이 신호에 따라 상태 전이를 발생시켜, 그에 따른 정책을 채택하고 새로운 패킷 필터링 룰을 생성하는 제 4 과정; 및

상기 제 4 과정이 완료되면 현재 적용되고 있는 정책과 필터링 룰을 기록하고 상태 정보와 로그를 저장하는 제 5 과정을 포함하는 것을 특징으로 하는 네트워크 상태 기반의 방화 방법.

청구항 7

제 6 항에 있어서, 상기 제 2 과정은

수집되는 상기 네트워크 패킷을 서브 네트워크에 포함되어 있는 호스트, 프로토콜, TCP 및 UDP 커넥션별로 분류하고, 각각의 특성에 따른 정보를 차별하여 분석하는 제 1 단계;

수집되는 상기 네트워크 패킷이 이미 생성되어 있는 상태 유닛에 포함된다면 상기 네트워크 패킷의 정보를 추출하여 상태 유닛의 정보를 갱신하고, 상태 유닛 테이블에 존재하지 않는 것이라면 상기 네트워크 패킷의 정보에 따라 상태 유닛을 생성하는 제 2 단계;

상기 네트워크 패킷의 시간적, 논리적 상관 관계를 트래픽 히스토리 정보 테이블을 이용하여 유효성을 검사하고 논리적 오류가 발견되면 상기 네트워크 패킷을 패기하는 제 3 단계;

트래픽의 전체적인 형태를 파악하기 위하여 유효성이 검사된 상기 네트워크

패킷의 정보를 대상으로 통계 정보를 생성하는 제 4 단계;

트래픽의 전체적 형태와 장기간적 동향을 파악하기 위하여 트래픽 패턴의 기록 및 그에 따른 대응 형태 등을 트래픽 히스토리 테이블에 기록하는 제 5 단계;

네트워크와 방화벽의 관리에 참조하기 위하여 상기 네트워크 패킷의 유효성 검사와 통계 정보 생성, 상태 유닛 테이블의 관리에 수반되는 로그를 로그 테이블에 기록하는 제 6 단계; 및

네트워크 상태의 비정상적 상황을 인식하기 위한 트래픽모니터수단에 트래픽 상태 정보를 제공하는 제 7 단계를 포함하는 것을 특징으로 하는 네트워크 상태 기반의 방화 방법.

청구항 8

제 6 항에 있어서, 상기 제 3 과정은

정적상태정보수집수단으로부터 제공되는 트래픽 상태 정보에서 정적으로 설정되어 있는 트래픽 정상 조건의 보정을 위한 평균 트래픽 정보를 추출하는 제 1 단계;

상기 제 1 단계에서 추출된 평균 트랙픽 정보를 이용하여 트래픽 정상 조건을 보정하는 제 2 단계;

트래픽 정상 조건과 트래픽 상태 정보를 비교하여 현재 네트워크의 상황의 비정상 여부를 판단하는 제 3 단계;

네트워크의 상태가 비정상적 상황임이 판명될 경우 새로운 트래픽 제어 정책의 채택을 위한 상태 전이 신호를 생성하는 제 4 단계; 및

상기 제 4 단계에서 생성된 상태 전이 신호를 룰생성수단의 상태 그래프에 전달하는 제 5 단계를 포함함을 특징으로 하는 네트워크 상태 기반의 방화 방법.

청구항 9

제 6 항에 있어서, 상기 제 4 과정은 트래픽모니터수단에서 전달된 상태 전이 신호에서 현재 네트워크 상태에 대한 정보를 추출하고, 비정상적인 요인을 추출하여 상태 그래프 테이블에 적용하는 제 1 단계;

상태 그래프 테이블에서 현재 상태 노드에서 전이 가능한 노드를 선별하여, 그 중에 상태 전이 신호의 정보를 수용할 수 있는 노드를 추출한 후 상태 전이를 수행하는 제 2 단계;

상태 그래프 테이블을 참조하여 새로운 상태 노드의 트래픽 제어 정책을 채택하고, 그에 따른 패킷 필터링 룰을 생성하는 제 3 단계; 및

상기 제 3 단계에서 새롭게 생성된 패킷 필터링 룰을 트래픽제어수단에 전달하여 네트워크의 비정상적 상황에 대응하는 제 4 단계를 포함함을 특징으로 하는 네트워크 상태 기반의 방화 방법.

명세서

발명의 명칭

네트워크 상태 기반의 방화벽 장치 및 그 방법{Apparatus for firewall of network status based Method thereof}

도면의 간단한 설명

[0001] 도 1은 일반적인 홈 네트워크 구조에서의 방화벽 배치도,

[0002] 도 2는 본 발명에 따른 네트워크 상태 기반의 방화벽 장치의 구성도,

[0003] 도 3은 본 발명에 따른 네트워크 상태 기반의 방화벽 장치를 구현하는 방법의 전체 흐름도,

[0004] 도 4는 도 3에 도시된 네트워크 상태 기반의 방화벽 장치를 구현하는 방법의 상태 정보 수집을 위한 흐름도,

[0005] 도 5는 도 3에 도시된 네트워크 상태 기반의 방화벽 장치를 구현하는 방법의 상태 전이 신호 생성을 위한 흐름도,

[0006] 도 6은 도 3에 도시된 네트워크 상태 기반의 방화벽 장치를 구현하는 방법의 패킷 필터링 룰 생성을 위한 흐름도.

[0007] <도면의 주요 부분에 대한 부호의 설명>

[0008] 100 : 네트워크트래픽수집수단 200 : 정적상태정보수집수단

[0009] 300 : 동적상태정보분석수단 400 : 트래픽모니터수단

[0010] 500 : 룰생성수단 600 : 트래픽제어수단

발명의 상세한 설명

[0011] 본 발명은 네트워크 상태 기반의 방화벽 장치 및 그 방법에 관한 것으로, 보다 상세하게는 외부 정보 통신망으로부터 유입되는 모든 패킷의 정보를 분석하여 유효성과 불법성을 분석하고, 내부 네트워크의 비정상적인 상황을 유도하는 트래픽 패턴을 인식하며, 비정상적 상황을 파악하고 네트워크 관리 정책에 따라 대응하기 위한 네트워크 상태 기반의 방화벽 장치 및 그 방법에 관한 것이다.

[0012] 최근에는 네트워크가 가정으로까지 확산되어 블루투스, 하비, 지니와 같은 홈네트워킹에 필요한 제반 기술 및 응용 분야가 개발되고 있다. 이와 같은 홈네트워크가 네트워크 분야에서 한 주류를 형성하면서 이질적인 기기들의 집합체인 홈네트워크를 제어, 관리하기 위한 에이전트가 필요한데 반하여, 에이전트로의 불법적 접근은 가정의 안전을 해칠 수도 있다. 이러한 기업, 가정 및 그 밖의 네트워크에서 외부로부터의 안전을 지키기 위해서는 네트워크의 특성에 따라 침입탐지, 침입차단, 역추적, 바이러스 방지 등의 많은 기술을 요구한다. 그 중 가장 기본적이고 모든 네트워크에 적용할 수 있는 것이 침입 차단 기술을 이용한 방화벽 시스템인 바, 방화벽은 외부로부터 내부 네트워크 자원을 보호하기 위해 필수적인 요소이며, 네트워크 내부의 구조와는 관계없이 외부와 내부의 접점에서 내부로의 패킷 흐름을 통제하고, 내부 사용자의 통신에 투명성을 제공하여야 한다. 도 1은 일반적인 홈 네트워크 구조에서의 방화벽 배치도

로서, 홈 네트워크 구조는 액세스 네트워크(10), 홈 게이트웨이 및 방화벽(11), 홈서버(12), PLC(13), DTV(14),
IEEE1394카메라(15), DVCR(16), 디지털오디오(17), 게임기(18), 수도(19), 보안기(20), 불루투스카메라(21), 팬(Fan)(22), 전등(23), 세탁기(24), 냉장고(25), 윈도우/커튼(26), 웹패드(27), PDA(28), 휴대폰(29), 화상전화기(30), 프린터(31), 스캐너(32), 팩스(33), PC(34), 콘센트(35) 등으로 구성되는데, 방화벽(11)은 그 발전 과정에 따라 세대별로 구분할 수 있는데, 제 1 세대 방화벽인 패킷 필터링은 각 패킷의 헤더 정보들에 기반하여 네트워크 사이의 전달을 허가하거나 거부하는 프로세스이다. 이와 같은 패킷 필터링은 한 서비스가 외부 네트워크에 항상 열려 있기 때문에 정적 상태를 갖으며, 장점으로는 오버헤드가 적고, 높은 성능을 보이며 구현하는데 비용이 적거나 들지 않고 트래픽 관리가 쉬운데 반하여, 단점으로는 서비스를 위해 열려있는 포트가 외부 클라이언트로부터 직접적인 연결을 허가하며, 서비스를 제공하는 포트가 외부 클라이언트에게 항상 열려있고, 복잡한 환경에서 신속한 관리가 어려우며, 특정 IP를 막더라도 IP 눈속임으로 공격당하기 쉽고, 사용자 인증과 투명성을 제공하지 않는다. 또한, 제 1 세대 방화벽과 비교되는 제 2 세대 방화벽의 가장 큰 차이점은 제 1 세대 방화벽에서는 방화벽(11)쪽의 서버 프로그램이 클라이언트쪽의 클라이언트 소프트웨어와 통신하면서 클라이언트의 존재를 감지해야만 하는 바, 서버(12)와 클라이언트들 각각에 대해 소프트웨어를 설치해야하는 번거러움이 있으며, 방화벽은 인지된 클라이언트들에 대해서만 방화벽 기능을 제공하는데 반하여, 제 2 세대 방화벽은 이러한 단점을 해결하여 클라이언트에 존재를 감지할 필요 없이 내부 호스트들에 대한 방화벽 기능을 수행하는 투명성을 제공하며, 또 하나의 제 1 세대 방화벽의 단점인 지속적 포트 개방
으로 인한 공격자의 공격 기회를 줄이기 위해 동적으로 제어하도록 설계되는데, 이와 같은 제 2 세대 방화벽 역시 제 1 세대 방화벽과 마찬가지로 사용자의 인증을 제공할 수 없고 IP 눈속임 공격에 대응하지 못하는 문제점이 있다.

[0013] 따라서, 본 발명은 이와 같은 문제점을 해결하기 위한 것으로서, 본 발명의 목적은 네트워크 트래픽의 상태를 다양한 관점에서 분석하고 상태 그래프를 통하여 상황에 대한 인식과 함께 트래픽 제어 정책을 차별적으로 반영함으로써, 외부 정보 통신망을 통하여 내부 네트워크로 유입되는 모든 불법적인 패킷 또는 패킷의 연속으로 이루어지는 트래픽을 차단하고, 내부 네트워크의 비정상적인 상황을 초래하는 패킷 흐름을 제어하여 원활하고 안전한 네트워크 상태를 유지할 수 있는 네트워크 상태 기반의 방화벽 장치 및 그 방법을 제공하는데 있다.

[0014] 본 발명의 다른 목적은 네트워크의 전반적인 상황을 파악할 수 있는 다양한 정보 및 로그를 제공하는 네트워크 상태 기반의 방화벽 장치 및 그 방법을 제공하는데 있다.

[0015] 이와 같은 목적을 달성하기 위한 본 발명의 특징은, 외부 정보 통신망으로부터 수집한 네트워크 패킷을 호스트, 프로토콜, 커넥션별로 구분하여 출력하는 네트워크트래픽수집수단; 상기 네트워크트래픽수집수단에서 전송되는 상기 네트워크 패킷의 정보를 분석하고, 상태 유닛 테이블 정보를 갱신하여 트래픽 정보를 가공하는 정적상태정보수집수단; 상기 정적상태정보수집수단에서 가공된 상기 트래픽 정보의
네트워크 트래픽의 장기적인 성향과 패턴을 분석하고 기록하는 동적상태정보분석수단; 상기 정적상태정보수집수단과 상기 동적상태정보분석수단에서 각각 제공하는 정보를 이용하여 상기 네트워크 트래픽의 동향을 감시하고 비정상적인 상황을 인식하여 상태 전이 신호를 출력하는 트래픽모니터수단; 및 상기 트래픽모니터수단에서 출력되는 상태 전이 신호를 받아서 생성된 상태 그래프 테이블을 이용하여 비정상적인 네트워크 상황을 정상적으로 유도하기 위한 패킷 필터링 룰을 생성하는 룰생성수단를 포함하는데 있다.

[0016] 바람직하게, 상기 정적상태정보수집수단은 상기 네트워크 패킷의 정보를 분석하는 패킷관리기; 및 상기 패킷관리기에서 분석된 상기 네트워크 패킷의 정보에 따라 상태 유닛 테이블의 정보를 갱신하는 통계분석기를 포함함을 특징으로 한다.

[0017] 바람직하게, 상기 동적상태정보분석수단은 발생하는 모든 이벤트에 대한 로그를 기록하여 관리자에게 네트워크와 방화벽의 관리에 대한 참고 자료를 제공하는 트래픽로그테이블; 및 상기 트래픽로그테이블에서 제공되는 참고 자료를 받아서 상기 네트워크 트래픽의 패턴과 그에 따른 대응 방식을 기록, 분석하는 트래픽히스토리분석기를 포함함을 특징으로 한다.

[0018] 바람직하게, 상기 룰생성수단은 상기 트래픽모니터수단에 의하여 생성된 상태 전이 신호를 받아 상태 그래프 테이블을 생성하는 정책관리기; 및 상기 정책관리기에서 생성된 상태 그래프 테이블에서 일어난 상태 전이에 따라 현재의 상황 지시자가 새로운 상태 노드로 이동하면 책택되는 새로운 네트워크 트래픽 관리 정책에 따라 현재 적용되고 있는 패킷 데이터 룰을 제거하거나 새로운 룰을 추가하는
액션관리기를 포함함을 특징으로 한다.

[0019] 바람직하게, 비정상적인 네트워크 상황을 정상적으로 유도하기 위한 패킷 필터링 룰을 전달받아 네트워크의 비정상적 상황에 대응하는 트래픽제어수단을 더 포함함을 특징으로 한다.

[0020] 본 발명의 다른 특징은, 게이트웨이를 통과하는 네트워크 패킷을 수집하여 상태 유닛별로 분류하는 제 1 과정; 상기 제 1 과정에서 수집된 상기 네트워크 패킷을 통계 및 패턴 분석 처리하여 현재의 트래픽 상황에 대한 정보를 생성하는 제 2 과정; 상기 제 2 과정에서 생성된 트래픽 상황에 대한 정보를 분석하고 감시하여 네트워크의 비정상적인 상황의 발생을 인지하여 상태 전이 신호를 생성하는 제 3 과정; 상기 제 3 과정에서 생성된 상태 전이 신호에 따라 상태 전이를 발생시켜, 그에 따른 정책을 채택하고 새로운 패킷 필터링 룰을 생성하는 제 4 과정; 및 상기 제 4 과정이 완료되면 현재 적용되고 있는 정책과 필터링 룰을 기록하고 상태 정보와 로그를 저장하는 제 5 과정을 포함하는데 있다.

[0021] 바람직하게, 상기 제 2 과정은 수집되는 상기 네트워크 패킷을 서브 네트워크에 포함되어 있는 호스트, 프로토콜, TCP 및 UDP 커넥션별로 분류하고, 각각의 특성에 따른 정보를 차별하여 분석하는 제 1 단계; 수집되는 상기 네트워크 패킷이 이미 생성되어 있는 상태 유닛에 포함된다면 상기 네트워크 패킷의 정보를 추출하여 상태 유닛의 정보를 갱신하고, 상태 유닛 테이블에 존재하지 않는 것이라면 상기 네트워크 패킷의 정보에 따라 상태 유닛을 생성하는 제 2 단계; 상기 네트워크 패킷의 시간적, 논리적 상관관계를 트래픽 히스토리 정보 테이블을 이용하여 유효성을 검사하고 논리적 오류가 발견되면 상기 네트워크 패킷을 폐기하는 제 3 단계; 트래픽의 전체적인 형태를 파악하기 위하여 유효성이 검사된 상기 네트워크 패킷의 정보를 대상으로 통계 정보를 생성하는 제 4 단계; 트래픽의 형태 및 그에 따른 대응 형태 등을 트래픽 히스토리 테이블에 기록하는 제 5 단계; 네트워크와 방화벽의 관리에 참조하기 위하여 상기 네트워크 패킷의 유효성 검사와 통계 정보 생성, 상태 유닛 테이블의 관리에 수반되는 로그를 로그 테이블에 기록하는 제 6 단계; 및 네트워크 상태의 비정상적 상황을 인식하기 위한 트래픽모니터수단에 트래픽 상태 정보를 제공하는 제 7 단계를 포함하는데 있다.

[0022] 바람직하게, 상기 제 3 과정은 정적상태정보수집수단으로부터 제공되는 트래픽 상태 정보에서 정적으로 설정되어 있는 트래픽 정상 조건의 보정을 위한 평균 트래픽 정보를 추출하는 제 1 단계; 상기 제 1 단계에서 추출된 평균 트랙픽 정보를 이용하여 트래픽 정상 조건을 보정하는 제 2 단계; 트래픽 정상 조건과 트래픽 상태 정보를 비교하여 현재 네트워크의 상황의 비정상 여부를 판단하는 제 3 단계; 네트워크의 상태가 비정상적 상황임이 판명될 경우 새로운 트래픽에 정책을 적용하는 제 4 단계; 및 상기 제 4 단계에서 생성된 상태 전이 신호를 룰생성수단의 상태 그래프에 전달하는 제 5 단계를 포함함을 특징으로 한다.

[0023] 바람직하게, 상기 제 4 과정은 트래픽모니터수단에서 전달된 상태 전이 신호에서 현재 네트워크 상태에 대한 정보를 추출하고, 비정상적인 요인을 추출하여 상

태 그래프 테이블에 적용하는 제 1 단계; 상태 그래프 테이블에서 현재 상태 노드에서 전이 가능한 노드를 선별하여, 그 중에 상태 전이 신호의 정보를 수용할 수 있는 노드를 추출한 후 상태 전이를 수행하는 제 2 단계; 상태 그래프 테이블을 참조하여 새로운 상태 노드의 트래픽 제어 정책을 채택하고, 그에 따른 패킷 필터링 룰을 생성하는 제 3 단계; 및 상기 제 3 단계에서 새롭게 생성된 패킷 필터링 룰을 트래픽제어수단에 전달하여 네트워크의 비정상적 상황에 대응하는 제 4 단계를 포함함을 특징으로 한다.

[0024] 이하, 본 발명의 바람직한 실시예에 대하여 첨부 도면을 참조하여 상세히 설명한다.

[0025] 도 2는 본 발명에 따른 네트워크 상태 기반의 방화벽 장치의 구성도이다.

[0026] 도 2에 있어서, 본 발명은 네트워크트래픽수집수단(100), 정적상태정보수집수단(200), 동적상태정보분석수단(300), 트래픽모니터수단(400), 룰생성수단(500), 트래픽제어수단(600)으로 구성된다.

[0027] 네트워크트래픽수집수단(100)은 도 1의 액세스네트워크(10)인 외부 정보 통신망으로부터 수집한 네트워크 패킷을 호스트, 프로토콜, 커넥션별로 구분하여 출력하며, 정작상태정보수집수단(200)은 네트워크 패킷의 정보를 분석하는 패킷관리기(210) 및 패킷관리기(210)에서 분석된 네트워크 패킷의 정보에 따라 상태 유닛 테이블(220)의 정보를 갱신하는 통계분석기(230)를 포함하여, 네트워크트래픽수집수단(100)에서 전송되는 네트워크 패킷의 정보를 분석하고, 상태 유닛 테이블 정보를 갱신하여 트래픽 정보를 가공한다.

[0028] 동적상태정보분석수단(300)은 발생하는 모든 이벤트에 대한 로그를 기록하여 관리자에게 네트워크와 방화벽의 관리에 대한 참고 자료를 제공하는 트래픽로그테이블(310) 및 트래픽로그테이블(310)에서 제공되는 참고 자료를 받아서 네트워크 트래픽의 패턴과 그에 따른 대응 방식을 기록, 분석하는 트래픽히스토리분석기(320)를 포함하여, 정적상태정보수집수단(200)에서 가공된 트래픽 정보의 네트워크 트래픽의 장기적인 성향과 패턴을 분석하고 기록하며, 트래픽모니터수단(400)은 정적상태정보수집수단(200)과 동적상태정보분석수단(300)에서 각각 제공하는 정보를 이용하여 네트워크 트래픽의 동향을 감시하고 비정상적인 상황을 인식하여 상태 전이 신호를 출력한다.

[0029] 한편, 룰생성수단(500)은 트래픽모니터수단(400)에 의하여 생성된 상태 전이 신호를 받아 상태 그래프를 생성하는 정책관리기(510) 및 정책관리기(510)에서 생성된 상태 그래프 테이블(520)에서 일어난 상태 전이에 따라 현재의 상황 지시자가 새로운 상태 노드로 이동하면 채택되는 새로운 네트워크 트래픽 관리 정책에 따라 현재 적용되고 있는 패킷 데이터 룰을 제거하거나 새로운 룰을 추가하는 액션관리기(530)를 포함하여, 트래픽모니터수단(400)에서 출력되는 상태 전이 신호를 받아서 생성된 상태 그래프를 이용하여 비정상적인 네트워크 상황을 정상적으로 유도하기 위한 패킷 필터링 룰을 생성하여 트래픽제어수단(600)에 전달하여, 트래픽제어수단(600)으로 하여금 네트워크의 비정상적 상황에 대응하도록 한다.

[0030] 도 3은 본 발명에 따른 네트워크 상태 기반의 방화벽 장치를 구현하는 방법의 전체 흐름도이다.

[0031] 도 3에 있어서, 도 1에 도시된 게이트웨이(11)를 통과하는 네트워크 패킷을 수집하여 상태 유닛별로 분류하여(단계 S100), S100 단계에서 수집된 네트워크 패킷의 상태 정보를 수집하여, 통계 및 패턴 분석 처리하고 현재의 트래픽 상황에 대한 정보를 생성한다(단계 200). S200 단계에서 생성된 트래픽 상황에 대한 정보를 분석하고 감시하여 네트워크의 비정상적인 상황의 발생을 인지하여 상태 전이 신호를 생성하며(단계 S300), S300 단계에서 생성된 상태 전이 신호에 따라 상태 전이를 발생시켜, 그에 따른 정책을 채택하고 새로운 패킷 필터링 룰을 생

성한다(단계 S400). S400 단계에서 새로운 패킷 필터링 룰이 생성되면 현재 적용되고 있는 정책과 필터링 룰을 기록하고 상태 정보와 로그를 저장한다(단계 S500).

[0032] 도 4는 도 3에 도시된 네트워크 상태 기반의 방화벽 장치를 구현하는 방법의 상태 정보 수집을 위한 흐름도이다.

[0033] 도 4에 있어서, 수집되는 네트워크 패킷을 서브 네트워크에 포함되어 있는 호스트, 프로토콜, TCP 및 UDP 커넥션별로 분류하고, 각각의 특성에 따른 정보를 차별하여 분석한다(단계 S201). S201 단계에서 네트워크 정보를 분석한 후에, 수집되는 네트워크 패킷이 이미 생성되어 있는 상태 유닛에 포함된다면 네트워크 패킷의 정보를 추출하여 상태 유닛의 정보를 갱신하고, 상태 유닛 테이블(220)에 존재하지 않는 것이라면 네트워크 패킷의 정보에 따라 상태 유닛을 생성한다(단계 S202).

[0034] S202 단계에서 상태 유닛이 생성되면 네트워크 패킷의 시간적, 논리적 상관 관계를 트래픽 히스토리분석기(320)에 내장된 트래픽 히스토리 정보 테이블을 이용
하여 유효성을 검사하고(단계 S203), S203 단계에서 논리적 오류가 발견되는가에 따라 유효한가 판단한다(단계 S204). S204 단계에서 유효하지 않으면 네트워크 패킷을 패기하고(단계 S205), S204 단계에서 유효하면 트래픽의 전체적인 형태를 파악하기 위하여 유효성이 검사된 상기 네트워크 패킷의 정보를 대상으로 통계 정보를 생성한다(단계 206).

[0035] S206 단계에서 통계 정보를 처리하면 트래픽의 전체적 형태와 장기간적 동향을 파악하기 위하여 트래픽 패턴의 기록 및 그에 따른 대응 형태 등을 트래픽히스토리분석기(320)에 내장된 트래픽 히스토리 테이블에 기록하고(단계 S207), 네트워크와 방화벽의 관리에 참조하기 위하여 네트워크 패킷의 유효성 검사와 통계 정보 생성, 상태 유닛 테이블의 관리에 수반되는 로그를 트래픽 로그 테이블(310)에 기록한다(단계 S208). S208 단계에서 상태 정보 생성 로그 처리가 되면 네트워크 상태의 비정상적 상황을 인식하기 위한 트래픽모니터수단(400)에 트래픽 상태 정보를 제공한다(단계 S209).

[0036] 도 5는 도 3에 도시된 네트워크 상태 기반의 방화벽 장치를 구현하는 방법의 상태 전이 신호 생성을 위한 흐름도이다.

[0037] 도 5에 있어서, 정적상태정보수집수단(200)으로부터 제공되는 트래픽 상태 정보에서 정적으로 설정되어 있는 트래픽 정상 조건의 보정을 위한 평균 트래픽 정보를 추출하여(단계 S301), S301 단계에서 수집, 추출된 평균 트랙픽 정보를 이용하여 트래픽 정상 조건을 보정한다(단계 S302).

[0038] S302 단계에서 트래픽 정상 조건이 보정되면 트래픽 비정상 검사를 수행함으
로써(단계 S303), 트래픽 정상 조건과 트래픽 상태 정보를 비교하여 현재 네트워크의 상황의 비정상 여부를 판단한다(단계 S304). S304 단계에서 네트워크의 상태가 비정상적 상황이 아니면 S301 단계로 복귀하고, S304 단계에서 네트워크의 상태가 비정상적 상황임이 판명될 경우 새로운 트래픽 제어 정책의 채택을 위한 상태 전이 신호를 생성하여 룰생성수단(500)의 상태 그래프(520)에 전달한다(단계 S305).

[0039] 도 6은 도 3에 도시된 네트워크 상태 기반의 방화벽 장치를 구현하는 방법의 패킷 필터링 룰 생성을 위한 흐름도이다.

[0040] 도 6에 있어서, 트래픽모니터수단(400)에서 룰생성수단(500)에 전달된 상태 전이 신호를 분석하고(단계 S401), S401 단계에서 상태 전이 신호가 분석되면 현재 네트워크 상태에 대한 정보를 추출하여(단계 S402), 비정상적인 요인을 추출하여 상태 그래프 테이블에 적용한다. S402 단계에서 트래픽 상황 정보가 추출되면 상태 그래프 테이블(520)에서 현재 상태 노

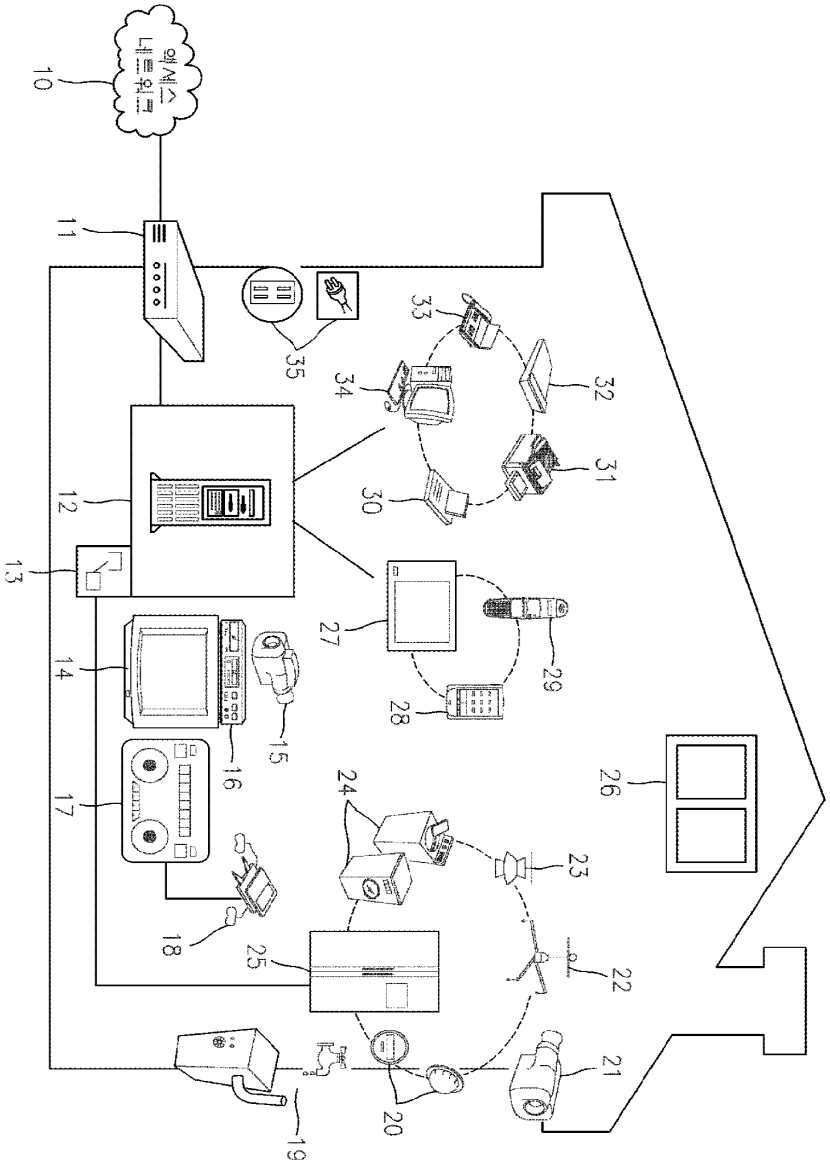
드에서 전이 가능한 노드를 선별하여(단계 S403), 그 중에 상태 전이 신호의 정보를 수용할 수 있는 노드를 추출한 후 상태 전이가 가능한가 판단한다(단계 S404).

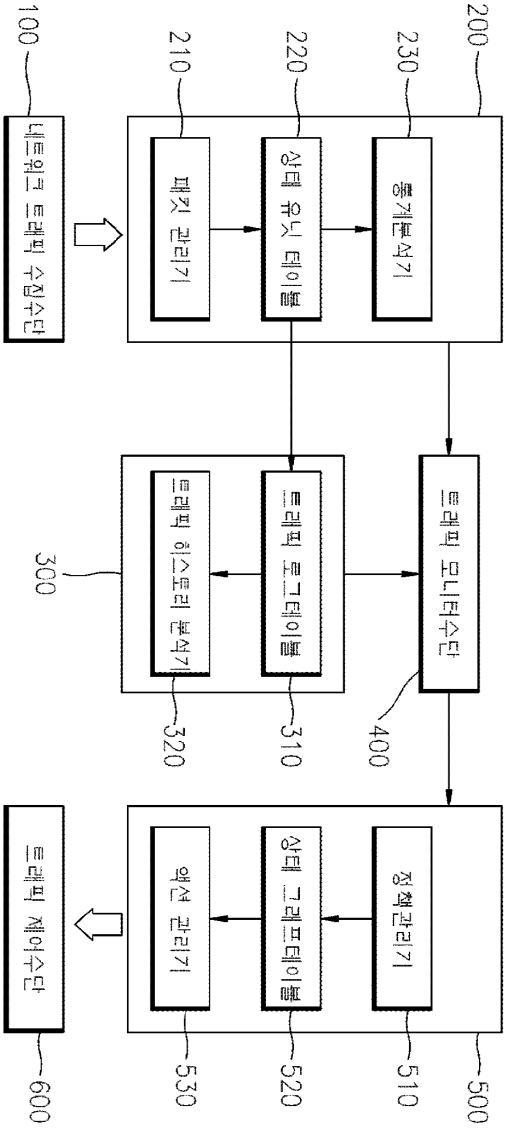
[0041] S404 단계에서 상태 전이가 가능하면 상태 전이를 수행하여(단계 S405), 상태 그래프 테이블(520)을 참조하여 새로운 상태 노드의 트래픽 제어 정책을 채택하고, 그에 따른 패킷 필터링 룰을 생성한다(단계 S406). S406 단계에서 새롭게 생성된 패킷 필터링 룰을 트래픽제어수단(600)에 전달하여 네트워크의 비정상적 상황에 대응하기 위하여 트래픽 제어를 수행한다(단계 S407).

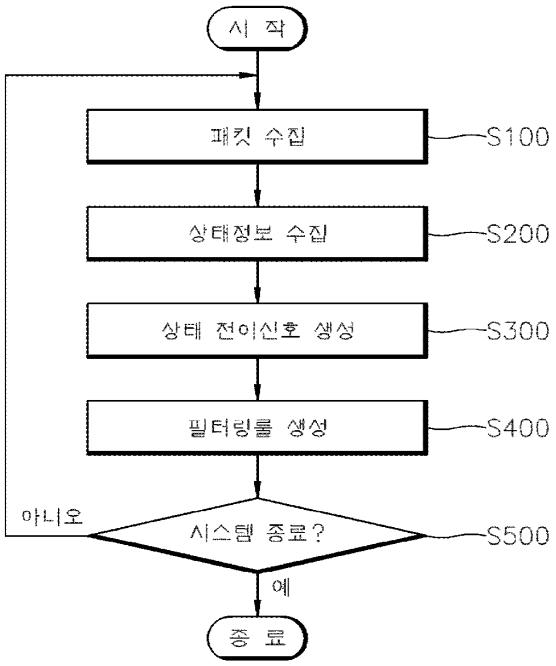
[0042] 이와 같이, 본 발명의 상세한 설명에서는 구체적인 실시예에 관해 설명하였으나, 본 발명의 범주에서 벗어나지 않는 한도 내에서 여러가지 변형이 가능함은 물론이다. 그러므로, 본 발명의 범위는 설명된 실시예에 국한되어 정해져서는 안되며 후술하는 특허청구범위 뿐만 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

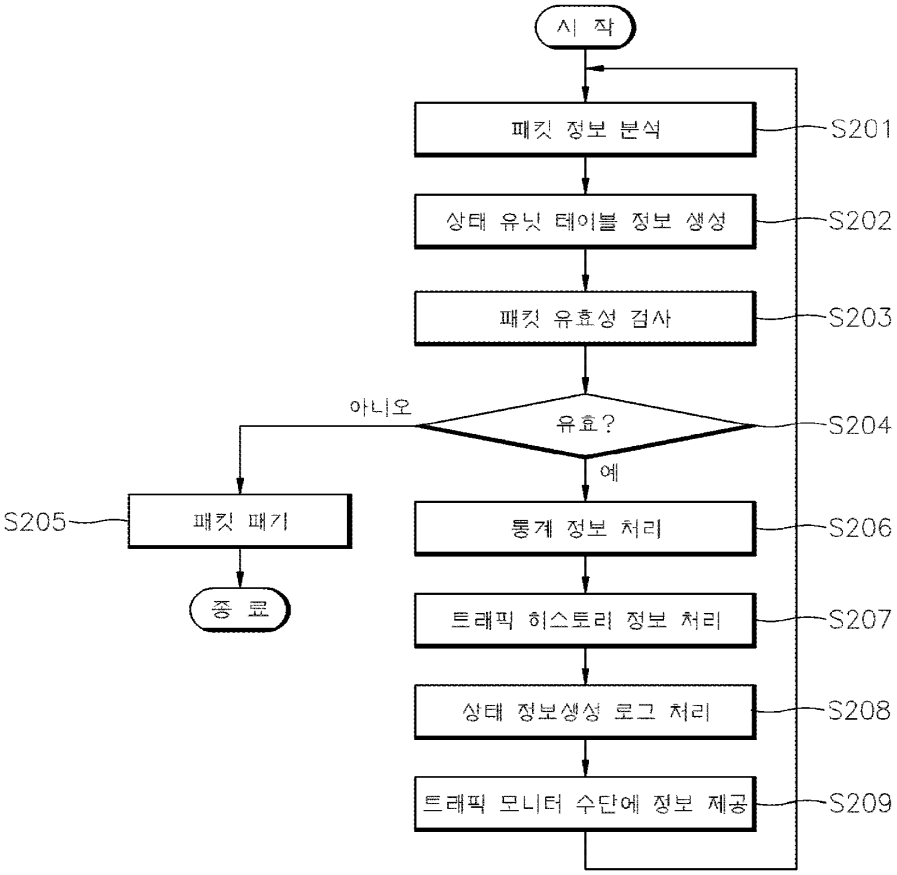
[0043] 결국, 본 발명에 의한 네트워크 상태 기반의 방화벽 장치 및 그 방법에 따르면 다음과 같은 이점이 발생한다.

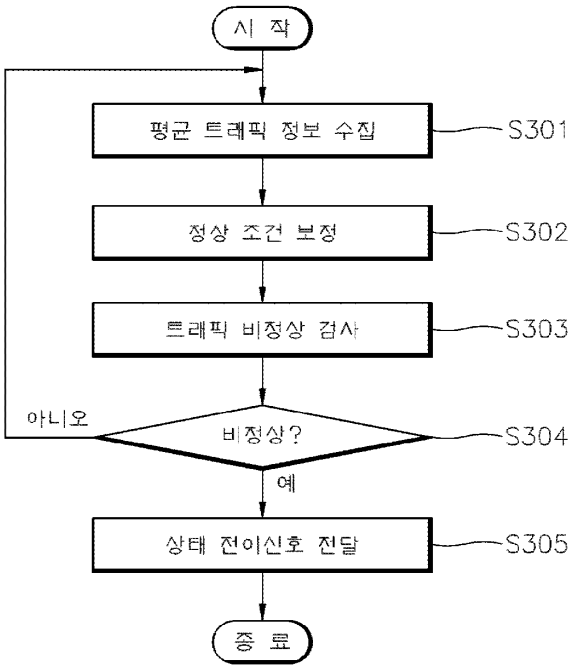
[0044] 즉, 불법적인 패킷 조작을 통한 해킹 및 침입 시도를 차단하고 비정상적 패킷 흐름을 이용하여 내부 네트워크의 혼란을 일으키는 서비스 거부 공격과 같은 공격에 신속하고 효과적으로 대응함으로써 내부 호스트와 네트워크의 안전 및 신뢰성을 보장할 수 있다.

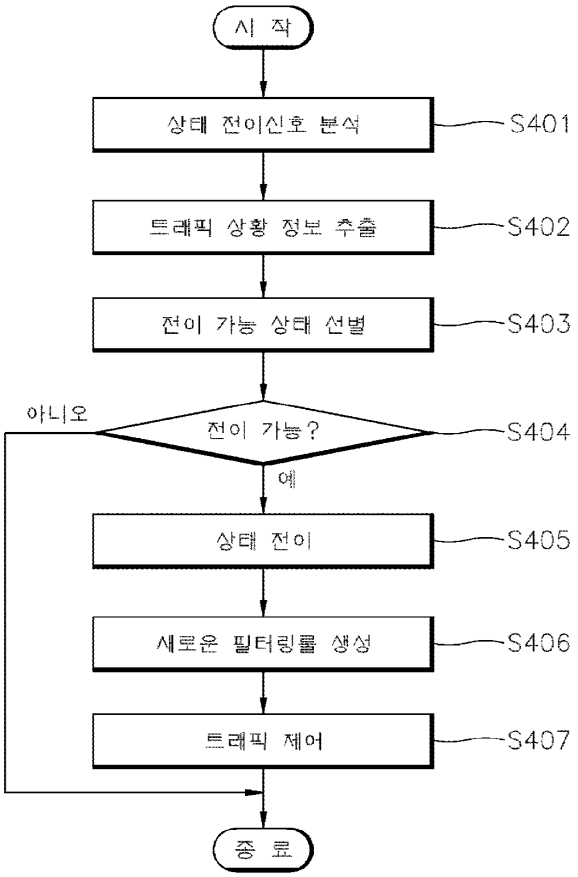

액세스 네트워크
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35


100
네트워크 트래픽 수집수단
200
210
패킷 관리기
220
상태 유닛 테이블
230
통계분석기
300
트래픽 히스토리 분석기
320
트래픽 로그테이블
310
트래픽 모니터수단
400
500
정책관리기
510
상태 그래프테이블
520
액션 관리기
530
트래픽 제어수단
600


시 작
패킷 수집
S100
상태정보 수집
S200
상태 전이신호 생성
S300
필터링룰 생성
S400
시스템 종료?
S500
아니오
예
종 료


시 작
패킷 정보 분석
S201
상태 유닛 테이블 정보 생성
S202
패킷 유효성 검사
S203
유효?
S204
아니오
예
S205
패킷 폐기
종 료
통계 정보 처리
S206
트래픽 히스토리 정보 처리
S207
상태 정보생성 로그 처리
S208
트래픽 모니터 수단에 정보 제공
S209


시 작
평균 트래픽 정보 수집
S301
정상 조건 보정
S302
트래픽 비정상 검사
S303
아니오
비정상?
S304
예
상태 전이신호 전달
S305
종 료


시 작
상태 전이신호 분석
S401
트래픽 상황 정보 추출
S402
전이 가능 상태 선별
S403
아니오
전이 가능?
S404
예
상태 전이
S405
새로운 필터링룰 생성
S406
트래픽 제어
S407
종 료

Espacenet

Bibliographic data: EP1006701 (A2) — 2000-06-07

Adaptive re-ordering of data packet filter rules

Inventor(s): KRISHNAN P [US]; RAZ DANNY [US]; SUGLA BINAY [US] ± (KRISHNAN, P, ; RAZ, DANNY, ; SUGLA, BINAY)

Applicant(s): LUCENT TECHNOLOGIES INC [US] ± (LUCENT TECHNOLOGIES INC)

Classification: - international: ***G06F13/00; G06F17/30; H04L29/06;*** (IPC1-7): H04L29/06
- cooperative: **H04L63/0227**; **H04L63/0263**

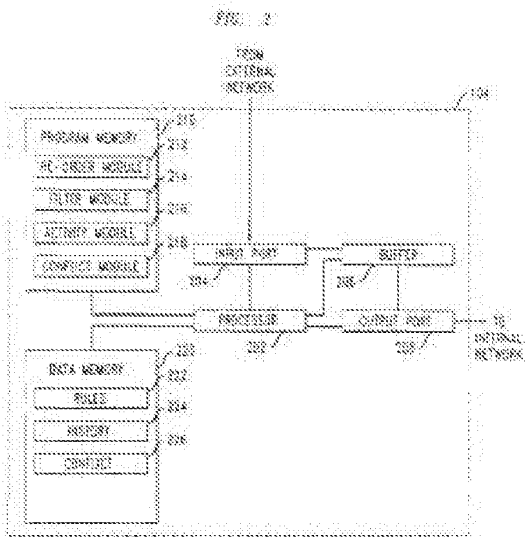
Application number: EP19990309593 19991130

Priority number (s): US19980204464 19981203

Also published as: EP1006701 (A3) EP1006701 (B1) CA2287689 (A1) CA2287689 (C) US2003051165 (A1) more

Abstract of EP1006701 (A2)

A packet data filter which stores ordered rules and sequentially applies the rules to received data packets to determine the disposition of the data packet. The packet filter maintains a match count in memory which indicates the number of times each rule matched an incoming data packet. Periodically, at the initiation of a user, or based on operating parameters of the filter, the rules are automatically re-ordered based on the match count. As a result of the re-ordering, rules with higher match counts are moved earlier in the sequential evaluation order and rules with lower match counts are moved later in the sequential evaluation order. As such, rules which are more likely to match incoming data packets are evaluated earlier, thus avoiding the evaluation of later rules.; In order to prevent a re-ordering which would change the overall security policy of the packet filter, pairs of rules are compared to determine if they conflict (i.e., the swapping of the two rules would result in a change in the overall security policy). During re-ordering, the swapping of conflicting rules is prevented.



(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 006 701 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
07.06.2000 Bulletin 2000/23

(51) Int Cl.[7]: **H04L 29/06**

(21) Application number: **99309593.4**

(22) Date of filing: **30.11.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **03.12.1998 US 204464**

(71) Applicant: **LUCENT TECHNOLOGIES INC.**
Murray Hill, New Jersey 07974-0636 (US)

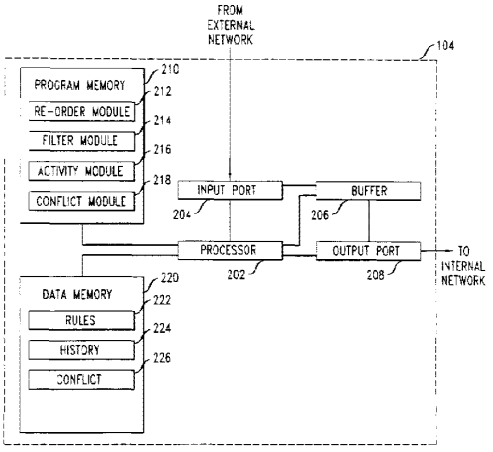
(72) Inventors:
- **Krishnan, P.**
  Matawan, New Jersey 07747 (US)
- **Raz, Danny**
  Aberdeen, New Jersey 07747 (US)
- **Sugla, Binay**
  Aberdeen, New Jersey 07747 (US)

(74) Representative:
Buckley, Christopher Simon Thirsk et al
Lucent Technologies (UK) Ltd,
5 Mornington Road
Woodford Green, Essex IG8 0TU (GB)

(54) Adaptive re-ordering of data packet filter rules

(57) A packet data filter which stores ordered rules and sequentially applies the rules to received data packets to determine the disposition of the data packet. The packet filter maintains a match count in memory which indicates the number of times each rule matched an incoming data packet. Periodically, at the initiation of a user, or based on operating parameters of the filter, the rules are automatically re-ordered based on the match count. As a result of the re-ordering, rules with higher match counts are moved earlier in the sequential evaluation order and rules with lower match counts are moved later in the sequential evaluation order. As such, rules which are more likely to match incoming data packets are evaluated earlier, thus avoiding the evaluation of later rules. In order to prevent a re-ordering which would change the overall security policy of the packet filter, pairs of rules are compared to determine if they conflict (i.e., the swapping of the two rules would result in a change in the overall security policy). During re-ordering, the swapping of conflicting rules is prevented.

FIG. 2



EP 1 006 701 A2

Printed by Jouve, 75001 PARIS (FR)

Description

Field of the Invention

[0001] The present invention relates to data packet filters. More particularly, the present invention relates to adaptive re-ordering of data packet filter rules to improve the performance of the filter while maintaining a security policy.

Background of the Invention

[0002] Data networks are becoming increasingly prevalent. For example, many companies have internal data networks to allow for intra-company communication. Such communication includes email, documents, voice, video, and multimedia. Further, these internal data networks are generally connected to an external data network (e.g. Internet), to allow for the exchange of information between the internal and external networks. However, as a result of the interconnection of data networks, security has become a major concern. The unauthorized access to a company's data network can result in the loss of valuable proprietary information. Further, unauthorized access can also result in attacks on the company's data network and computing system, resulting in loss of data and computer system crashes.

[0003] A computer programmed to implement a security policy for a data network is called a firewall. Typically, firewalls are located at strategic points in the network such that all incoming and outgoing data traffic must pass through a firewall. At these points, all network traffic is trapped and examined by the firewall to determine if the traffic should be allowed to pass through the firewall. There are various techniques for implementing a firewall. One such implementation is a computer programmed to implement a data packet filter. A data packet filter examines all received data packets, and either denies or allows passage of the data packet based on the contents of the data packet. In one implementation, this decision is based on rules stored in the data packet filter which define which data packets are allowed to pass and which data packets will be blocked. Each stored rule defines certain parameters of data packets (e.g. source and destination) and also includes the disposition of data packets which match these parameters. For example, a rule may indicate that any data packet from source X will be blocked, while another rule may indicate that any data packet from source Y to destination Z will be allowed to pass. The rules are stored in sequential order in the data packet filter and every data packet received by the firewall is tested against the rules in sequential order. The first rule whose parameters match the received packet is applied to the packet and the packet is treated as indicated by the rule.

[0004] In such a rules based data packet filter, a system administrator must first define a security policy to be implemented by the firewall, and then must program the data packet filter with rules which will implement that security policy. One major problem with these types of firewalls is that sophisticated security policies require a large number of rules in order to implement the policy. Since every data packet which passes through the firewall must be checked against these rules, the performance of the firewall degrades as the number of rules increases.

[0005] One known solution to the performance problem in a data packet filter firewall is to use a memory cache. In such a system, when a data packet arrives, the relevant parameters (e.g. source and destination) of the data packet are stored in a cache. In addition, after the packet filter rules have been applied to the received data packet, the disposition (e.g. allow or deny) is also stored in the cache associated with the relevant parameters of the received data packet. Thereafter, if a data packet is received with parameters which are the same as parameters previously stored in the cache, the firewall can apply the associated disposition without applying all the rules to the data packet. This enhances performance in view of the fact that for certain applications, ongoing communications will occur between two computers, and there is no need to check every data packet exchanged between the computers during the communication session (i.e., connection). Thus, while this technique improves performance for data packets exchanged during connections, the technique does not improve performance for new connections.

[0006] Packet filters may also be implemented on a client computer, for example a personal computer running World Wide Web (WWW) browsing software (e.g., Microsoft Explorer or Netscape Navigator). Many WWW sites contain material which parents may deem unsuitable for children. As such, several companies offer filtering software which implements packet filters for blocking unsuitable material. These packet filters implement a security policy through the use of rules as described above. As the number of rules increases, these client based packet filters suffer from the same performance problems as described above.

[0007] What is needed is a technique for improving the performance of a data packet filter as the number of rules required to implement a security policy increases.

Summary of the Invention

[0008] As described above, a data packet filter stores a plurality of ordered rules which are sequentially applied to received data packets to implement a security policy. In accordance with the invention, the rules are automatically re-

EX1002
CISCO SYSTEMS, INC. / Page 395 of 1453

ordered to improve the performance of the packet filter. Rules which match incoming data packets more frequently are moved earlier in the ordering, and rules which match incoming data packets less frequently are moved later in the ordering. Since the first rule that matches a received data packet controls the disposition of the packet, once a rule matches a packet, the remaining rules need not be evaluated. By re-ordering the rules, data packets are matched against rules more quickly, and the performance of the data packet filter is improved.

[0009] In one embodiment of the invention, the packet filter dynamically maintains, during operation of the packet filter, a count of the number of times each rule matches a received data packet. The packets are then re-ordered based on these counts with the rules having higher match counts being moved earlier in the rules order. Such re-ordering is made on the premise that past history of the packet filter provides a reliable indication of future operation. Thus, by dynamically maintaining match counts during operation, the packet filter can adaptively re-order its rules based on past operating parameters. Such adaptive re-ordering is beneficial to protect against so-called denial of service attacks, as described in further detail below.

[0010] In one embodiment of the invention, rules are re-ordered by swapping pairs of rules in the rules order. However, the sequence of the rules plays a part in defining the security policy of the packet filter. As such, the indiscriminate swapping of rules may result in changing the security policy of the packet filter. Such a result is undesirable and must be prevented. As such, rules are evaluated to determine re-orderings which are not allowed because they result in a change in the security policy. In one embodiment, such an evaluation is made by comparing pairs of rules to determine which pairs of rules conflict with each other. Two rules are said to conflict with each other if swapping the rules would result in changing the security policy of the packet filter. The result of this conflict evaluation is stored in the memory of the packet filter and subsequent re-ordering refers to this information in order to prevent the swapping of conflicting rules.

[0011] The re-ordering in accordance with the invention may be performed periodically, at the initiation of a user, or based on the some operating parameters of the packet filter (e.g. when the performance of the packet filter drops below a threshold).

[0012] The principles of the present invention may be applied to various types of computing devices. For example, and without limitation, the invention may be implemented in a dedicated network firewall which filters data packets for many computers and networks, or in a stand-alone personal computer such that the packet filter only filters data packets for the personal computer.

[0013] These and other advantages of the invention will be apparent to those of ordinary skill in the art by reference to the following detailed description and the accompanying drawings.

Brief Description of the Drawings

[0014]

Fig. 1 shows a network of the type in which the present invention may be implemented;
Fig. 2 shows a computer configured to implemented a firewall in accordance with the present invention;
Fig. 3 shows the format of an exemplary data packet;
Fig. 4 shows an example of a rule set;
Fig. 5 shows a conflict table; and
Fig. 6 shows a personal computer in which the principles of the present invention may be implemented.

Detailed Description

[0015] A network of the type in which the present invention may be implemented is shown in Fig. 1. An internal data network, such as a corporate intranet, is shown as network 102. An external data network, such as the Internet, is shown as network 106. Firewall 104 is shown positioned such that all data traffic exchanged between internal network 102 and external network 106 must pass through the firewall 104. These data networks communicate with each other using the well known Internet Protocol (IP) for data packet communication. Assume that firewall 104 is administered by the same entity which administers internal network 102. The purpose of firewall 104 is to implement the security policy of the internal network 102.

[0016] The firewall 104 may be implemented by a properly configured computer, further details of which are shown in Fig. 2. Fig. 2 shows firewall 104 comprising a processor 202 which controls the overall operation of the firewall 104. Processor 202 is connected to input port 204, buffer 206, output port 208, program memory 210, and data memory 220. Program memory 210 and data memory 220 may be any type of well known computer storage device. In operation, processor 202 controls the operation of the firewall 104 by executing computer program instructions stored in program memory 210. Program memory 210 includes the following program modules: re-order module 212, filter module 214, activity module 216, and conflict module 218. These modules contain computer program code which, when executed

EX1002
CISCO SYSTEMS, INC. / Page 396 of 1453

by processor 202, implements a packet filter in accordance with the present invention. It is to be understood that the program modules shown in program memory 210 are high level representations of functional computer program modules. In various implementations, these modules could include program source code, object code, or a combination of source and object code. These modules will be discussed in further detail below. Of course, a computer implementing a firewall would have other well known components as well. Such other components are not shown in Fig. 2 for clarity.

[0017] The operation of firewall 104 is as follows. When a data packet is received at firewall 104 from external network 106, the data packet is received at input port 204. The format of an exemplary data packet 302 is shown in Fig. 3. Data packet 302 contains a header portion 304 and data portion 306. The header portion 304 contains the following fields: protocol 308, source address 310, destination address 312, source port 314, and destination port 316. The protocol field 308 indicates the protocol with which the current packet is being transmitted. For example, the protocol field 308 may indicate that the data packet 302 is being transmitted using the well known TCP/IP protocol. The source address 310 indicates the IP address of the source of the data packet 302. IP addressing is well known in data networking. IP addresses are 32 bits, and are most commonly represented in a dotted notation as 4 integers, each between 0 and 255, and each separated by a dot (e.g. 125.180.104.4). The destination address 312 indicates the IP address of the destination of the data packet 302. The source port 314 indicates the port number of the source computer. A port number is an integer between 0 and 65,535, and generally is associated with an application that runs on a particular machine. For example, web servers are typically associated with port number 80. The destination port 316 indicates the port number of the destination computer. The data portion 306 of the packet 302 contains the payload of the packet which will be used by an application executing on the destination computer.

[0018] Upon receipt of the data packet at input port 204, the data packet 302 is stored in buffer 206 while the processor 202 executes the filter module 214 in order to apply the filter rules 222 stored in data memory 220 against the received data packet. The filter module 214 applies the rules to the received data packet in sequential order. The first rule that matches the data packet is the rule which will decide whether the data packet is allowed or denied. Once a rule matches the data packet, there is no need to apply the remaining rules.

[0019] An example of a rule set which would be stored as rules 222 is shown in Fig. 4. As shown in Fig. 4, each rule has a sequence number, which indicates the order in which the rules will be applied against an incoming data packet. Each rule also has fields indicating protocol, source address, destination address, source port, destination port, and an action. Each rule indicates the action to be taken when a data packet is received which matches the information in the rule's fields. A packet is said to match the rule if the header information in the packet falls within the defined ranges of values in the above described fields. For example, rule number 1 indicates that any packet received using the TCP protocol with a source address of 125.30.20.200 is to be denied (i.e. blocked), regardless of the contents of the other fields of the packet. The "*" in a rule field indicates a wildcard which will match any value. Rule number 2 indicates that any packet received using the TCP protocol with a source address in the range 135.180.104.4 to 135.180.104.225, a destination address in the range 135.180.204.4 to 135.180.204.255, a source port in the range 1024-65535, and a destination port of 80 is to be allowed (i.e. passed to its destination). Rule number 3 indicates that any packet received using the TCP protocol from a source address in the range 125.180.100.0 - 125.180.100.255 is to be allowed, regardless of the values in the other fields. Finally, rule number 4 indicates that all data packets are to be denied. Since rules are applied in sequential order, rule number 4 will only be applied if none of the rules 1-3 match the incoming data packet. The inclusion of a rule such as rule number 4 is common practice in firewalls and implements a security policy that all packets are denied unless specifically allowed. As would readily be recognized by one skilled in the art, a wide variety of security policies may be implemented by storing different rule sets as rules 222 in data memory 220. It is also noted that the action indicated in a rule may be something other than allow or deny. For example, it is possible that an action indicates that packets matching the rule be forwarded to some other location for further processing.

[0020] Thus, while the received data packet is stored in buffer 206, processor 202 sequentially applies rules 222 to the data packet until a rule matches the data packet. If the matched rule indicates that the data packet is to be allowed, then the packet is transferred to output port 208 and is allowed to pass to the internal network 102. If the matched rule indicates that the data packet is to be denied, then the packet is deleted from the buffer 206 and is thus not allowed to pass to the internal network 102. It is noted that although the rules are applied in sequential order, they will not necessarily be stored internally in data memory 220 in that sequential order. For various reasons, the internal representation of the rules may be different from the logical representation shown in fig. 4. However, regardless of the internal representation, each rule will be associated with a sequence number or other indication of order of evaluation (e.g. priority), such that the filter module 214 will apply the rules to a received data packet in a given sequence.

[0021] As the number of stored rules 222 increases, the performance of the firewall 104 generally degrades because it takes longer to apply the rules to each incoming data packet. The present invention solves this performance problem by re-ordering the stored rules 222 such that rules which are more likely to match incoming data packets are placed earlier in the sequential order (i.e. assigned a lower sequence number). This improves the performance of the firewall because once a rule is matched, the remaining rules are not applied, thus avoiding the processing time required to apply those remaining rules. If rules which are more likely to match data packets can be moved earlier in the rules

EX1002
CISCO SYSTEMS, INC. / Page 397 of 1453

sequence, performance of the firewall will improve.

[0022] However, prior to re-ordering the rules, it must be determined which rules may be re-ordered without having an affect on the overall security policy of the firewall 104. Due to the nature of the rules and the sequential application of the rules to received data packets, certain re-orderings may result in a change in the overall security policy. Such re-orderings must be prevented. For example, referring to the example rule set of fig. 4, rule number 4 could not be swapped with rule 1, because such a swap will result in rule number 4 being applied first. Since rule number 4 indicates that all data packets are to be denied, placing it first in the rules sequence would result in all data packets being denied. None of the other rules would be reached to allow the data packets to pass. Therefore, it is necessary to determine which rules may be re-ordered while still maintaining the security policy of the firewall.

[0023] In order to determine which rules may be re-ordered, conflict module 218 is executed by processor 202. The conflict module analyzes the rule set 222 to determine whether pairs of rules are in conflict such that the swapping of the pair would result in a change in the security policy. Generally, two rules are said to conflict with each other if at least one data packet could match either one of the rules and the actions of the rules are not the same. In the embodiment described herein, the conflict algorithm to determine whether a Rule-A conflicts with a Rule-B is as follows:

```
If ACTION of Rule-A is not the same as ACTION of Rule-B then

    if the PROTOCOL of Rule-A does not intersect with the
    PROTOCOL OF Rule-B then
```

```
                    if the SOURCE ADDRESS of Rule-A does not intersect
                    with the SOURCE ADDRESS of Rule-B then

                          if the DESTINATION ADDRESS of Rule-A does not
                          intersect with the DESTINATION ADDRESS of Rule-
                          B then

                                if the SOURCE PORT of Rule-A does not
                                intersect with the SOURCE PORT of Rule-B
                                then

                                      if the DESTINATION PORT of Rule-A
                                      does not intersect with the
                                      DESTINATION PORT of Rule-B then

                                            no conflict between Rule-A
                                            and Rule-B
                                      else
                                otherwise
                          else
                    else
              else
                    conflict between Rule-A and Rule-B.
        else

              no conflict.
```

[0024] In accordance with the algorithm, a particular of a rule is said to *intersect* with a particular field of another rule if there is any intersection in the range of values of the two fields. For example, with respect to fields which contains IP addresses, the fields will intersect if there is any overlap between the addresses. For example, an IP address field containing the address range 123.30.20.100 intersects with an IP address field containing the address range 123.30.20.70 - 123.30.20.150 in the address range 123.30.20.70 - 123.30.20.100. For example, the IP address 123.30.20.85 would fall within both ranges. Thus, in accordance with the algorithm, if the actions of two rules are different, and if the there is an intersection in any of the fields of the two rules, then the rules conflict. Otherwise, the rules do not conflict. Of course, one skilled in the art could modify the above algorithm in order to detect the conflict between rules with a different set of fields. Such an algorithm would analyze each field of each rule to determine if there were an intersection. If there is any intersection, and if the action of the two rules is different, then the rules conflict.

[0025] It is noted that the conflict module 218 is executed once when the rule set 222 changes (i.e. a rule is added or deleted). The results of the execution of the conflict module 218 are stored in data memory 220 as conflict data 226 which indicates, for every possible pair of rules, whether that pair conflicts. In one embodiment, a two-dimensional conflict table such as conflict table 500 shown in Fig. 5 could be stored as conflict data 226 as a result of the execution of conflict module 218. For each pair of rules, the intersection point in the conflict table 500 indicates whether the rules are in conflict (C) or not in conflict (NC). For example, the intersection of row 3 and column 2 in conflict table 500

EX1002
CISCO SYSTEMS, INC. / Page 399 of 1453

contains NC indicating that rule 3 and rule 2 do not conflict. If a rule is added, only the interaction of the new rule with the other rules needs to be checked with the conflict module 218. The interaction of the other rules will not change. It is noted that the conflict table 500 is symmetrical in that the intersection of column x and row y will contain the same value as the intersection of column y and row x. As such, only half of the table needs to be stored in conflict data 226 in data memory 220. However, the entire table is shown in Fig. 5 for purposes of this description.

[0026] Returning now to the re-ordering of rules, as was stated above, in accordance with the invention, the performance of a packet data filter is improved by re-ordering the stored rules 222 such that rules which are more likely to match incoming data packets are placed earlier in the sequential order. In accordance with one aspect of the invention, the decision as to which rules are more likely to match incoming data packets is made with reference to past history of the firewall 104. In one embodiment, this past history is a record of the number of times each rule has matched an incoming data packet. In accordance with this embodiment, during operation of the firewall 104, an activity module 216 dynamically maintains a running count of the number of times each rule matched an incoming packet. This count is stored as a table in the history section 224 of data memory 220. The table associates a count with each rule. Thus, rules associated with higher counts matched incoming packets more often than rules associated with lower counts. It is noted that the counts can periodically be reinitialized to zero.

[0027] The re-ordering of the rule set 222 may be performed periodically (e.g. every 30 minutes), may be initiated by a system administrator, or may be initiated by the firewall 104 based on certain operating parameters of the firewall 104. For example, the firewall 104 may initiate a re-ordering when the performance of the firewall 104 drops below a certain predetermined threshold. The re-ordering is performed by the re-order module 212 by swapping rules having a lower count in history section 224 with rules having a higher count in history section 224. This results in rules which matched data packets more often being placed earlier in the sequential ordering.

[0028] One algorithm for swapping rules is as follows.

```
For i = 1 to N

    J = N

    While J > 0

        If match count for Rule J > match count for Rule J-1
        then

            if Rule J does not conflict with Rule J-1 then

                Swap Rule J with Rule J-1.

        J = J - 1.
```

This algorithm attempts to move the rules with a higher match count earlier in the sequence of rules. One constraint of the re-ordering of rules is that rules are only swapped if doing so will not change the overall security policy of the rule set (i.e. the rules do not conflict). While this algorithm uses a well known bubble sort type of algorithm, one skilled in the art could readily implement various types of re-ordering algorithms.

[0029] One benefit of the present invention is that the filter rules are re-ordered based on the activity of the firewall. As such, the firewall is dynamically adaptable to changing operating conditions. As an example, one type of attack on a computer system is known as a denial of service attack, which is aimed at reducing the availability of network elements. One technique for mounting such an attack is to continuously transmit packets to a network, which packets are known to be blocked by the network's firewall. If the rule which rejects such packets is late in the sequential ordering of rules, then every time such a packet is received by the firewall, the firewall must apply many rules before rejecting the packet. For example, if the rule which will eventually reject the data packet is rule number 100, then each time

EX1002
CISCO SYSTEMS, INC. / Page 400 of 1453

such a packet is received, the firewall must apply 100 rules prior to rejecting the packet. By sending many such packets, an attacker may seriously impair the performance of the firewall.

[0030] The present invention can improve the performance during a denial of service attack as follows. If an attacker is continuously sending packets which are rejected by rule number 100, then the match count for rule number 100 will increase quickly. Further, since one of the parameters for initiating a re-ordering of rules is the performance of the firewall, then a denial of service attack will substantially degrade the performance such that a re-ordering will be initiated. At such time, since the match count of rule 100 will be high, the re-ordering module will attempt to move rule 100 earlier in the sequential ordering. For example, if the rule were moved to rule 5, then further receipt of the attacking packets will result in the packets being blocked after only 5 rules, rather than 100, an improvement of 95%.

[0031] It is to be understood that although the invention has been described in the context of a firewall implemented in a network as shown in Fig. 1, the principles of the present invention may also be implemented in a personal computer configured to filter data packets received from a data network. In one well known configuration, a personal computer is connected to the Internet using a modem and a dial-up connection to the Internet via the telephone network. Since it is often desirable to limit the Internet sites which a user of a personal computer may access, there are various filter programs available which filter incoming data packets based on filtering rules. The principles of the present invention may be implemented in such a personal computer. Such an embodiment of the invention is shown in Fig. 6 as personal computer 600. Personal computer 600 includes a processor 610 connected to a modem 612 which is used to establish a connection to a data network, such as the Internet. In one embodiment, the computer 600 executes a browser program 604 which allows the computer 600 to communicate with World Wide Web (WWW) sites and to receive information from such sites. In accordance with the invention, the computer 600 also includes a packet filter program module 606, which contains a re-order module, filter module, activity module, and intersection module, which operate to implement a packet filter as described above. Also, the computer 600 contains data memory 608 including rules, history, and conflict data, also as described above. A user of the computer 600 interacts with the computer 600 via keyboard 614, graphical input device 618 (e.g. mouse), and display 616 in a conventional manner. In operation, a user of computer 600 may request information from the Internet, and the packet filter module 606 will operate as described above in order to filter data packets in accordance with stored filter rules. The filter rules may be re-ordered to improve the performance of the packet filter, as long as such re-ordering does not change the overall security policy of computer 600.

[0032] It is noted that network routers may optionally be configured to filter data packets in a manner similar to that described above in connection with firewalls. Thus, the principles of the present invention may be implemented in a network router which is configured for data packet filtering.

[0033] The foregoing Detailed Description is to be understood as being in every respect illustrative and exemplary, but not restrictive, and the scope of the invention disclosed herein is not to be determined from the Detailed Description, but rather from the claims as interpreted according to the full breadth permitted by the patent laws. It is to be understood that the embodiments shown and described herein are only illustrative of the principles of the present invention and that various modifications may be implemented by those skilled in the art without departing from the scope and spirit of the invention.

Claims

1. A method for operation of a data packet filter which implements a security policy by filtering data packets by sequentially evaluating a plurality of ordered rules, said method comprising the step of:
   automatically re-ordering said ordered rules.

2. The method of claim 1 wherein said step of re-ordering is based on prior activity of said data packet filter.

3. The method of claim 2 further comprising the step of:

   dynamically maintaining, during operation of said data packet filter, match data indicating the number of times each of said rules is matched by a data packet; and
   wherein said step of re-ordering is based on said match data.

4. The method of claim 3 wherein said rules are re-ordered such that rules which are matched more often are evaluated earlier.

5. The method of claim 1 wherein said step of automatically re-ordering is performed periodically.

6. The method of claim 1 wherein said step of automatically re-ordering is performed when the performance of said

EX1002
CISCO SYSTEMS, INC. / Page 401 of 1453

data packet filter falls below a threshold.

7. The method of claim 1 wherein said step of re-ordering is performed by swapping pairs of rules, said method further comprising the step of:
determining pairs of rules which can be swapped without changing said security policy.

8. The method of claim 7 wherein said step of re-ordering is performed such that said security policy is not changed.

9. The method of claim 7 wherein said step of determining further comprises the step of determining the intersection of fields of pairs of said rules.

10. A data packet filter for implementing a security policy comprising:

a memory for storing a plurality of ordered rules;
a filter module for sequentially applying said rules to received data packets; and
a re-ordering module for re-ordering said ordered rules.

11. The data packet filter of claim 10 wherein said memory further stores information representing past activity of said data packet filter and wherein said re-ordering is based on said past activity.

12. The data packet filter of claim 11 wherein said information representing past activity comprises match data indicating the number of times each of said rules is matched by a data packet.

13. The data packet filter of claim 12 further comprising:
an activity module for dynamically maintaining said match data.

14. The data packet filter of claim 10 further comprising:
a conflict module for determining pairs of said rules which can be swapped without altering said security policy.

15. The data packet filter of claim 14 wherein said re-ordering module only swaps pairs of rules which can be swapped without altering said security

16. The data packet filter of claim 14 wherein said conflict module determines pairs of said rules which can be swapped without altering said security policy by determining the intersection of fields of pairs of rules.

17. A computer readable medium storing computer program instructions which are executable on a computer system implementing a data packet filter, said computer program instructions comprising instructions defining the steps of:

filtering received data packets by sequentially applying a plurality of ordered rules, said rules defining a security policy; and
automatically re-ordering said ordered rules.

18. The computer readable medium of claim 17 wherein said computer program instructions further comprise instructions defining the steps of:
re-ordering said rules based on prior activity of said computer system.

19. The computer readable medium of claim 18 wherein said computer program instructions further comprise instructions defining the steps of:

dynamically maintaining, during operation of said computer system, match data indicating the number of times each of said rules is matched by a data packet; and
re-ordering said rules based on said match data.

20. The computer readable medium of claim 19 wherein said computer program instructions further comprise instructions defining the steps of:
re-ordering said rules such that rules which are matched more often are applied earlier.

21. The computer readable medium of claim 17 wherein said computer program instructions further comprise instruc-

EX1002
CISCO SYSTEMS, INC. / Page 402 of 1453

tions defining the step of:
periodically automatically re-ordering said rules.

22. The computer readable medium of claim 17 wherein said computer program instructions further comprise instructions defining the step of:
automatically re-ordering said rules when the performance of said computer system falls below a threshold.

23. The computer readable medium of claim 17 wherein said computer program instructions further comprise instructions defining the step of:
determining pairs of rules which can be swapped without changing said security policy.

24. The computer readable medium of claim 23 wherein said computer program instructions further comprise instructions defining the step of:
re-ordering said rules by swapping only those rules which may be swapped without changing said security policy.

25. The computer readable medium of claim 23 wherein said computer program instructions further comprise instructions defining the step of:
determining pairs of said rules which can be swapped without changing said security policy by determining the intersection of fields of pairs of rules.

26. A firewall for filtering data traffic between a first network and a second network comprising:

an input port for receiving data packets;
a memory storing a plurality of ordered rules defining a security policy of said firewall;
a filter module for sequentially applying said ordered rules to received data packets; and
a re-order module for automatically re-ordering said plurality of rules.

27. The firewall of claim 26 further comprising:
a conflict module for determining whether pairs of rules can be swapped without altering said security policy.

28. The firewall of claim 27 wherein said conflict module determines whether pairs of rules can be swapped without altering said security policy by determining the intersection of fields of pairs of rules.

29. The firewall of claim 27 wherein said re-order module only swaps pairs of rules which can be swapped without altering said security policy.

30. The firewall of claim 26 further comprising an activity module for dynamically maintaining activity information about the operation of said firewall.

31. The firewall of claim 30 wherein said activity information comprises match data indicating the number of times each of said rules is matched by a data packet.

32. The firewall of claim 30 wherein said re-order module re-orders said plurality of rules based on said activity information.

EX1002
CISCO SYSTEMS, INC. / Page 403 of 1453

FIG. 1

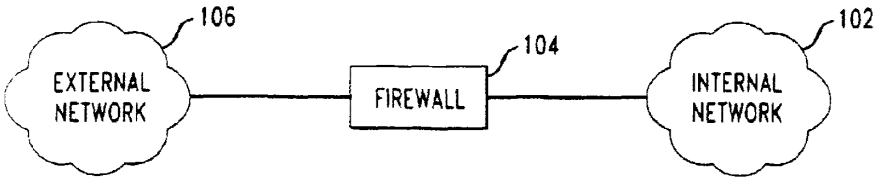
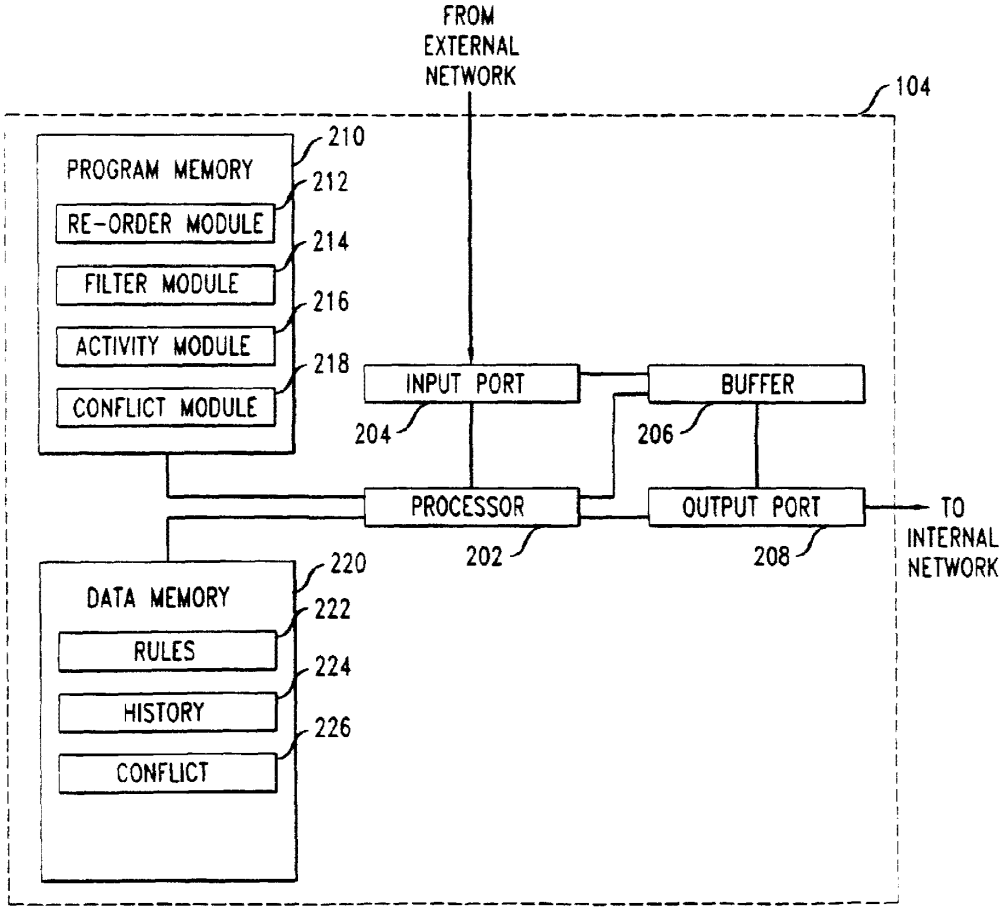


FIG. 2



EX1002
CISCO SYSTEMS, INC. / Page 404 of 1453

FIG. 3

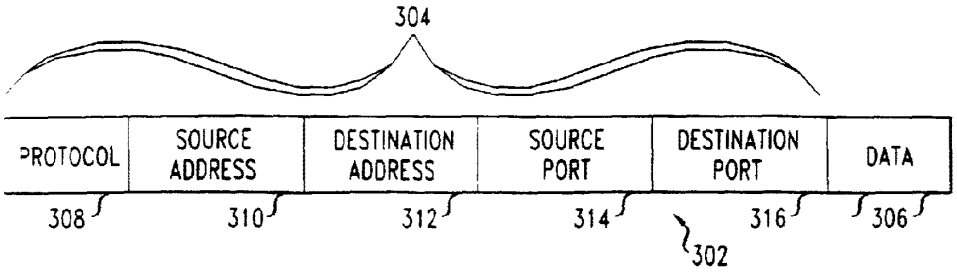


FIG. 4

SEQ. NO.	PROTOCOL	SOURCE ADDRESS	DESTINATION ADDRESS	SOURCE PORT	DESTINATION PORT	ACTION
1	TCP	125.30.20.200	*	*	*	DENY
2	TCP	135.180.104.4-135.180.104.255	135.180.204.4-135.180.204.255	1024-65535	80	ALLOW
3	TCP	125.180.100.*	*	*	*	ALLOW
4	*	*	*	*	*	DENY

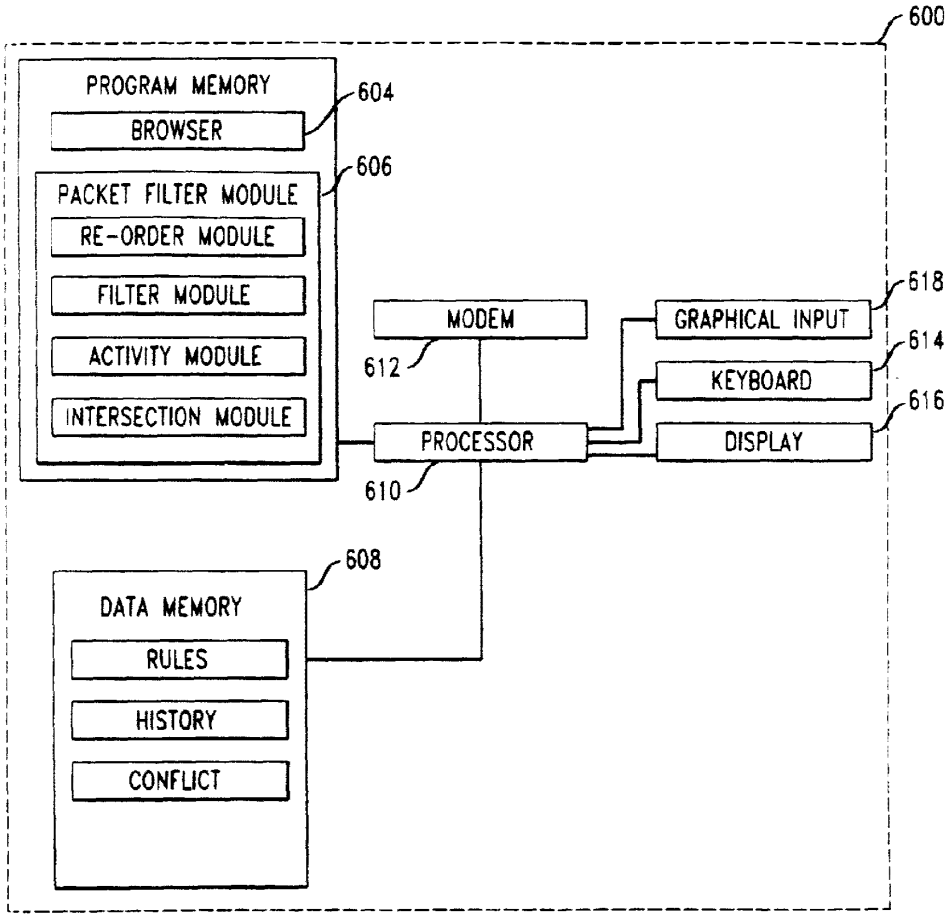
FIG. 5

	1	2	3	4	5	
1	NC	C	C	NC	C	
2	C	NC	NC	C	NC	
3	C	NC	NC	NC	C	
4	NC	C	NC	NC	C	
5	C	NC	C	C	NC	

500

EX1002
CISCO SYSTEMS, INC. / Page 405 of 1453

FIG. 6



EX1002
CISCO SYSTEMS, INC. / Page 406 of 1453

Espacenet

Bibliographic data: WO2006105093 (A2) — 2006-10-05

METHODS, SYSTEMS, AND COMPUTER PROGRAM PRODUCTS FOR NETWORK FIREWALL POLICY OPTIMIZATION

Inventor(s): FULP ERRIN W [US]; TARSA STEPHEN J [US] ± (FULP, ERRIN, W, ; TARSA, STEPHEN, J)

Applicant(s): UNIV WAKE FOREST [US]; FULP ERRIN W [US]; TARSA STEPHEN J [US] ± (WAKE FOREST UNIVERSITY, ; FULP, ERRIN, W, ; TARSA, STEPHEN, J)

Classification: **- international:** ***G06F15/16***
- cooperative: **H04L63/0263**; **H04L63/20**

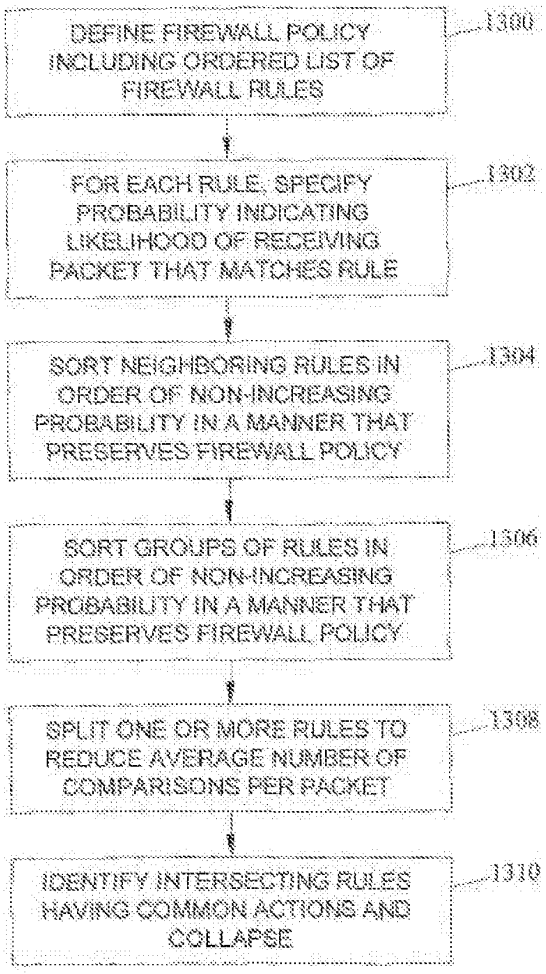
Application number: WO2006US11291 20060328

Priority number (s): US20050665664P 20050328

Also published as: WO2006105093 (A3) US2006248580 (A1) US8042167 (B2) EP1864226 (A2) EP1864226 (A4) more

Abstract of WO2006105093 (A2)

Methods, systems, and computer program products for firewall policy optimization are disclosed. According to one method, a firewall policy including an ordered list of firewall rules is defined. For each rule, a probability indicating a likelihood of receiving a packet matching the rule is determined. The rules are sorted in order of non-increasing probability in a manner that preserves the firewall policy.


DEFINE FIREWALL POLICY INCLUDING ORDERED LIST OF FIREWALL RULES
1300
FOR EACH RULE, SPECIFY PROBABILITY INDICATING LIKELIHOOD OF RECEIVING PACKET THAT MATCHES RULE
1302
SORT NEIGHBORING RULES IN ORDER OF NON-INCREASING PROBABILITY IN A MANNER THAT PRESERVES FIREWALL POLICY
1304
SORT GROUPS OF RULES IN ORDER OF NON-INCREASING PROBABILITY IN A MANNER THAT PRESERVES FIREWALL POLICY
1306
SPLIT ONE OR MORE RULES TO REDUCE AVERAGE NUMBER OF COMPARISONS PER PACKET
1308
IDENTIFY INTERSECTING RULES HAVING COMMON ACTIONS AND COLLAPSE
1310

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 October 2006 (05.10.2006)

PCT

(10) International Publication Number
WO 2006/105093 A2

(51) International Patent Classification:
G06F 15/16 (2006.01)

(21) International Application Number:
PCT/US2006/011291

(22) International Filing Date: 28 March 2006 (28.03.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/665,664 28 March 2005 (28.03.2005) US

(71) Applicant *(for all designated States except US)*: **WAKE FOREST UNIVERSITY** [US/US]; OFFICE OF TECHNOLOGY ASSET MANAGEMENT, WAKE FOREST UNIVERSITY HEALTH SCIECNES, 200 East First Street, Suite 101, Winston Salem, North Carolina 27101 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **FULP, Errin, W.** [US/US]; 308 N. Hawthorne Road, Winston-Salem, North Carolina 27104 (US). **TARSA, Stephen, J.** [US/US]; 135 King Phillips Path, Duxbury, Massachusetts 02332-3503 (US).

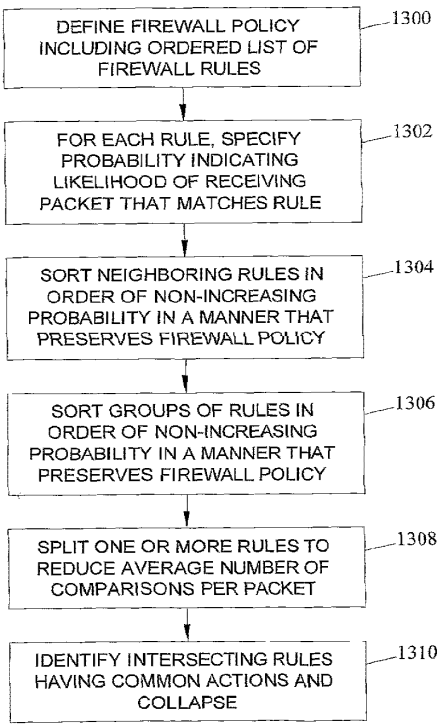
(74) Agent: **HUNT, Gregory, A.**; JENKINS, WILSON, TAYLOR & HUNT, P.A., Suite 1200 University Tower, 3100 Tower Boulevard, Durham, North Carolina 27707 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),

[Continued on next page]

(54) Title: METHODS, SYSTEMS, AND COMPUTER PROGRAM PRODUCTS FOR NETWORK FIREWALL POLICY OPTIMIZATION



(57) Abstract: Methods, systems, and computer program products for firewall policy optimization are disclosed. According to one method, a firewall policy including an ordered list of firewall rules is defined. For each rule, a probability indicating a likelihood of receiving a packet matching the rule is determined. The rules are sorted in order of non-increasing probability in a manner that preserves the firewall policy.

WO 2006/105093 A2

European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

DESCRIPTION

METHODS, SYSTEMS, AND COMPUTER PROGRAM PRODUCTS FOR NETWORK FIREWALL POLICY OPTIMIZATION

RELATED APPLICATIONS

This application claims the benefit of U.S. Provisional Patent Application Serial No. 60/665,664, filed March 28, 2005; the disclosure of which is incorporated herein by reference in its entirety.

GOVERNMENT INTEREST

This invention was made with Government support under Grant No. DE-FG02-03ER25581 awarded by U.S. Department of Energy, Mathematical and Computational Information Sciences Division. The Government has certain rights in the invention.

TECHNICAL FIELD

The subject matter described herein relates to optimizing polices for network firewalls. More particularly, the subject matter described herein relates to methods, systems, and computer program products for optimizing performance of network firewalls.

BACKGROUND ART

Network firewalls remain the forefront defense for most computer systems. Guided by a security policy, these devices provide access control, auditing, and traffic control [3, 30, 31]. A security policy is a list of ordered rules, as seen in Table 1, that defines the action to perform on matching packets. For example, an accept action passes the packet into or from the secure network, while deny causes the packet to be discarded. In many implementations, the rule set is stored internally as a linked list. A packet is sequentially compared to the rules, starting with the first, until a match is found; otherwise, a default action is performed [30, 31]. This is referred to as a first-match policy and is used in many firewall systems including the Linux firewall implementation iptables [25].

No.	Proto.	Source IP	Source Port	Destination IP	Destination Port	Action	Prob.
1	UDP	1.1.*	*	*	80	deny	0.01
2	TCP	2.*	*	1.*	90	accept	0.02
3	UDP	*	*	1.*	*	accept	0.10
4	TCP	2.*	*	1.*	20	accept	0.17
5	UDP	1.*	*	*	*	accept	0.20
6	*	*	*	*	*	deny	0.50

Table 1: Example Security Policy Consisting of Multiple Ordered Rules

Traditional firewall implementations consist of a single, dedicated machine, similar to a router, that sequentially applies rules to each arriving packet. However, packet filtering represents a significantly higher processing load than routing decisions [24, 29, 31]. For example, a firewall that interconnects two 100 Mbps networks would have to process over 300,000 packets per second [30]. Successfully handling these traffic loads becomes more difficult as rule sets become more complex [4, 22, 31]. Furthermore, firewalls must be capable of processing even more packets as interface speeds increase. In a high-speed environment (e.g. Gigabit Ethernet), a single firewall can easily become a bottleneck and is susceptible to DoS attacks [4, 9, 13, 14]. An attacker could simply inundate the firewall with traffic, delaying or preventing legitimate packets from being processed.

One approach to increase firewall performance focuses on improving hardware design. Current research is investigating different distributed firewall designs to reduce processing delay [4, 9, 22], and possibly provide service differentiation [11]. Another approach focuses on improving performance via better firewall software [6, 7, 12, 16, 17, 24]. Similar to approaches that address the longest matching prefix problem for packet classification [8, 10, 25, 28], solutions typically represent the firewall rule set in different fashions (e.g. tree structures) to improve performance. While both approaches, together or separate, show great promise, each requires radical changes to the firewall system, and therefore are not amenable to current or legacy systems.

Accordingly, there exists a need for improved methods, systems, and computer program products for network firewall policy optimization.

SUMMARY

The subject matter described herein includes methods, systems, and computer program products for network firewall policy optimization. According to one method, a firewall policy including an ordered list of firewall rules is defined. For each rule, a probability indicating a likelihood of receiving a packet matching the rule is defined. Neighboring rules are sorted in order of non-increasing probability in a manner that preserves the firewall policy.

As used herein, the term "firewall" refers to a logical entity that is adapted to filter packets at the ingress and/or egress portions of a network based on a policy. The term "firewall" is intended to include systems that block packets from entering or leaving a network and systems that perform intrusion detection and intrusion protection functions for packets entering or leaving a network. Thus, the methods and systems described herein for firewall policy optimization can be used to optimize policies for intrusion detection and intrusion protection firewalls.

The subject matter described herein includes a method to improve firewall performance and lower packet delay that can be applied to both legacy and current systems. In one implementation, a firewall rule set may be re-ordered to minimize the average number of rule comparisons to determine the action, while maintaining the integrity of the original policy. Integrity is preserved if the reordered and original rules always arrive at the same result. To maintain integrity, a firewall rule set may be modeled as a Directed Acyclical Graph (DAG), where vertices are firewall rules and edges indicate precedence relationships. Given this representation, any linear arrangement of the DAG is proven to maintain the original policy integrity. Unfortunately, determining the optimal rule order from all the possible linear arrangements is proven to be *NP*-complete, since it is equivalent to sequencing jobs with precedence constraints for a single machine [15]. Although determining the optimal order is *NP*-complete, a heuristic will be described below to order firewall rules that reduces the average number of comparisons while maintaining integrity. Simulation

results show the proposed reordering method yields rule orders that are comparable to optimal; thus, provides a simple means to significantly improve firewall performance and lower packet delay.

The subject matter described herein for network firewall policy optimization may be implemented using any combination of hardware, software, or firmware. For example, the subject matter described herein may be implemented using a computer program product comprising computer executable instructions embodied in a computer readable medium. Exemplary computer readable media suitable for implementing the subject matter described herein include disk memory devices, chip memory devices, programmable logic devices, application specific integrated circuits, and downloadable electrical signals. In addition, a computer program product that implements the subject matter described herein may be implemented using a single device or computing platform or may be distributed across multiple devices or computing platforms.

BRIEF DESCRIPTION OF THE DRAWINGS

Preferred embodiments of the subject matter described herein will now be explained with reference to the accompanying drawings of which:

Figure 1A is a block diagram of a rule list Directed Acyclical Graph (DAG) for the firewall rules in Table 1;

Figure 1B is a linear arrangement of firewall rules corresponding to the original rule order;

Figure 2A is a policy DAG representing a reordered version of the firewall rule set in Figure 1 after sorting;

Figure 2B is a policy DAG for the rule set illustrated in Table 1 illustrating an optimal rule order;

Figure 3A is a graph illustrating average numbers of packet comparisons versus intersection percentage for different orderings of a firewall policy;

Figure 3B is a graph illustrating the percent difference in average numbers of packet comparisons between sorted and optimal sortings of a firewall policy;

Figure 4A is a graph of percent difference comparisons between original and sorted versions of a firewall policy;

Figure 4B is a graph illustrating the performance impact of considering rule intersection and actions in performing firewall rule sorting;

Figure 5A is a table illustrating a firewall policy before sorting;

Figure 5B is a table illustrating a sorted version of the firewall policy of Figure 5A;

Figure 6A is a policy trie representation of the firewall policy of Figure 5B;

Figure 6B is a table representing the firewall policy of Figure 5A after TCP and UDP sub-trie rotation;

Figure 7A is a policy trie illustrating the splitting of rule r_5 into rules r_{5a} and r_{5b};

Figure 7B is a table illustrating the firewall policy of Figure 5A after splitting rule r_5 into rules r_{5a} and r_{5b};

Figure 8A is a graph illustrating firewall performance with and without rule splitting;

Figure 8B is a graph illustrating locations and probabilities where splitting is better;

Figure 9A is a policy DAG of a firewall rule set;

Figure 9B is a policy DAG illustrating compression of rules r_1 and r_5;

Figure 10A is a policy DAG of a firewall rule list;

Figure 10B is an original policy trie before sorting;

Figure 10C is a policy trie illustrating the firewall rules after rotating sub-tries T_1 and T_2;

Figure 11A is a policy DAG illustrating a firewall policy;

Figure 11B is a policy trie illustrating firewall rules of the policy before sorting;

Figure 11C is a policy trie illustrating the firewall policy after exchanging nodes r_1 and r_2 and nodes r_7 and r_8;

Figure 11D is a policy trie illustrating the firewall policy after exchanging sub-tries T_3 and T_4;

Figure 11E is a policy trie illustrating the firewall policy after exchanging sub-tries T_1 and T_2;

Figure 12A is a policy DAG illustrating an original order for a firewall policy;

Figure 12B is a policy DAG illustrating a sorted version of the firewall policy of Figure 12A after exchanging neighbors;

Figure 12C is a policy DAG illustrating a sorted version of the firewall policy after exchanging lists L_1 including rules r_1 and r_3 and lists L_2 including rules r_2 and r_4;

Figure 13 is a flow chart illustrating exemplary steps for network firewall policy optimization according to an embodiment of the subject matter described herein;

Figure 14 is a block diagram illustrating exemplary components of a system for firewall policy optimization according to an embodiment of the subject matter described herein; and

Figure 15 is a block diagram illustrating a plurality of firewall nodes for implementing a firewall policy according to an embodiment of the subject matter described herein.

DETAILED DESCRIPTION OF THE INVENTION

Modeling Firewall Security Policies

As described above, a firewall rule set, also known as a firewall policy, is traditionally an ordered list of firewall rules. Firewall policy models have been the subject of recent research [1, 2, 16]; however, the primary purpose is anomaly detection and policy verification. In contrast, the policy model described in this herein is designed for firewall performance optimization and integrity. Firewall performance refers to reducing the average number of comparisons required to determine an action, while integrity refers to maintaining the original policy intent. Although improving the worst-case performance is important, it is not possible without changing the list-based representation [16, 24].

Firewall Rule and Policy Models

In the examples described herein, a rule r is modeled as an ordered tuple of sets, $r = (r[1], r[2], ..., r[k])$. Order is necessary among the tuples since

comparing rules and packets requires the comparison of corresponding tuples. Each tuple $r[l]$ is a set that can be fully specified, specify a range, or contain wildcards '*' in standard prefix format. For the Internet, security rules are commonly represented as a 5-tuple consisting of: protocol type, IP source address, source port number, IP destination address, and destination port number [30, 31]. Given this model, the ordered tuples can be supersets and subsets of each other, which forms the basis of precedence relationships. In addition to the prefixes, each filter rule has an action, which is to accept or deny. However, the action will not be considered when comparing packets and rules. Similar to a rule, a packet (IP datagram) d can be viewed as an ordered k-tuple $d = (d[1], d[2], ..., d[k])$; however, ranges and wildcards are not possible for any packet tuple.

Using the previous rule definition, a standard security policy can be modeled as an ordered set (list) of n rules, denoted as $R = \{r_1, r_2, ..., r_n\}$. A packet d is sequentially compared against each rule r_i starting with the first, until a match is found ($d \Rightarrow r_i$) then the associated action is performed. A match is found between a packet and rule when every tuple of the packet is a subset of the corresponding tuple in the rule.

Definition Packet d matches r_i if

$$d \Rightarrow r_i \quad \text{iff} \quad d[l] \subseteq r_i[l], \quad l = 1, ..., k$$

The rule list R is comprehensive if for every possible legal packet d a match is found using R. Furthermore, two rule lists R and R' are equivalent if for every possible legal packet d the same action is performed by the two rule lists. If R and R' are different (e.g. a reorder) and the lists are equivalent, then the policy integrity is maintained.

As previously mentioned, a rule list has an implied precedence relationship where certain rules must appear before others if the integrity of the policy is to be maintained. For example consider the rule list in Table 1. Rule r_1 must appear before rules r_3 and r_5, likewise rule r_6 must be the last rule in the policy. If for example, rule r_3 was moved to the beginning of the policy, then it will shadow [2] the original rule r_1. However, there is no precedence relationship between rules r_2 and r_4 given in Table 1. Therefore, the relative ordering of these two rules will not impact the policy integrity and can be

changed to improve performance. The present example assumes that the original policy is free from any anomalies. Likewise, when a policy is reordered to improve performance it should not introduce any anomalies, which will occur if precedence relationships are not maintained. As a result, a model is needed to effectively represent precedence relationships.

Modeling Rule List Precedence Relationships

The precedence relationship between rules in a policy will be modeled as a Directed Acyclical Graph (DAG) [23, 18]. Such graphs have been successfully used to represent the relative order of individual tasks that must take place to complete a job (referred to as a task graph model). Since certain rules must appear before others to maintain policy integrity, this structure is well suited for modeling the precedence of firewall rules. Let $G = (R, E)$ be a rule list DAG for a rule list R, where vertices are rules and edges E are the precedence relationships (constraint). A precedence relationship, or edge, exists between rules r_i and r_j, if $i < j$, the actions for each rule are different, and the rules intersect.

Definition The intersection of rule r_i and r_j, denoted as $r_i \cap r_j$ is

$$r_i \cap r_j = (r_i[l] \cap r_j[l]), \qquad l = 1, \ldots, k$$

Therefore, the intersection of two rules results in an ordered set of tuples that collectively describes the packets that match both rules. The rules r_i and r_j intersect if every tuple of the resulting operation is non-empty. In contrast, the rules r_i and r_j do not intersect, denoted as $r_i \not\cap r_j$, if at least one tuple is the empty set. Note the intersection operation is symmetric; therefore, if r_i intersects r_j, then r_j will intersect r_i. The same is true for rules that do not intersect.

For example consider the rules given in Table 1, the intersection of r_1 and r_3 yields (UDP, 1.1.*, *, 1.*, 80). Again, the rule actions are not considered in the intersection or match operation. Since these two rules intersect, a packet can match both rules for example d = (UDP, 1.1.1.1, 80, 1.1.1.1, 80). Furthermore, the actions of the two rules are different. Therefore, the relative order must be maintained between these two rules and an edge drawn from r_1 to r_3 must be present in the rule list DAG, as seen in Figures 1A and 1B. More

particularly, Figure 1A illustrates a rule list DAG for the rules in Table 1. Figure 1B illustrates a linear arrangement of the rules in Figure 1A. In Figures 1A and 1B, the vertices represent rules, the circles represents an accept rules, and the squares represents deny rules. Edges that connect the vertices represent precedence requirements. As can be seen from Figure 1B, because of the edge between rules r_1 and r_3, precedence between rules r_1 and r_3 must be maintained. In contrast consider the intersection of rules r_3 and r_5. These two rules intersect, indicating packets belonging to the set (UDP, 1.*, *, 1.*, *) would match both rules. However, it does not matter which of the two rules a packet matches first, since the action is the same for both rules. Therefore, an edge does not exist between rules r_3 and r_5 in the diagram. Similarly, rules r_2 and r_4 do not intersect due to the fifth tuple (destination port). A packet cannot match both rules indicating the relative order can change; therefore, an edge will not exist between them.

The match operation can be used to identify precedence relationships, but it cannot do so in every case. Consider a partial-match example [1], where r_a = (UDP, *, 80, 10.*, 90, accept) and r_b = (UDP, 10.*, 80, *, 90, deny). The intersection of r_a and r_b is (UDP, 10.*, 80, 10.*, 90); therefore a packet, such as d = (UDP, 10.10.10.10, 80, 10.10.10.10, 90), can match both rules. If r_a appears before r_b then the packet d is accepted, but if r_b occurs before r_a then d is rejected. As a result, the order of r_a and r_b in the original policy must be maintained. However, the match operation is unable to identify the precedence in this example. A partial match exists in between rules r_3 and r_5 in Table 1, but as previously discussed an edge does not exist between the rules since the actions are the same.

Using the rule list DAG representation a linear arrangement is sought that improves the firewall performance. As depicted in Figure 1B, a linear arrangement (permutation or topological sort) is a list of DAG vertices where all the successors of a vertex appear in sequence after that vertex [23]. Therefore it follows that a linear arrangement of a rule list DAG represents a rule order, if the vertices are read from left to right. Furthermore, it is proven in the following theorem that any linear arrangement of a rule list DAG maintains integrity.

Theorem Any linear arrangement of a rule list DAG maintains integrity.

Proof Assume a rule list DAG *G* is constructed from the security policy *R* that is free of anomalies. Consider any two rules r_i and r_j in the policy, where $i < j$. If an edge between r_i and r_j in *G* does not exist, then a linear arrangement of *G* can interchange the order of the two rules. An edge will not exist if the rules do not intersect; however, a reorder will not affect integrity since a packet cannot match both rules. Shadowing is not introduced due to the reorder since the intersection operation is symmetric. An edge will not exist if the two rules intersect but have the same action; however, a reorder will not affect integrity since the same action will occur regardless of which rule is matched first. If an edge does exist between the rules, then their relative order will be maintained in every linear arrangement of *G*; thus maintaining precedence and integrity.

Rule List Optimization

As described above, it is important to inspect packets as quickly as possible given increasing network speeds and QoS requirements. Using the rule list DAG to maintain policy integrity, a linear arrangement is sought that minimizes the average number of comparisons required. However, this will require information not present in the firewall rule list. Certain firewall rules have a higher probability of matching a packet than others. As a result, it is possible to develop a policy profile over time that indicates frequency of rule matches (similar to cache hit ratio). Let $P = \{p_1, p_2, ..., p_n\}$ be the policy profile, where p_i is the probability that a packet will match rule *i* (first match in the policy). Furthermore, assume a packet will always find a match, $\sum_{i=1}^{n} p_i = 1$; therefore *R* is comprehensive. Using this information, the average number of rule comparisons required is

$$E[n] = \sum_{i=1}^{n} i \cdot p_i \qquad (1)$$

For example, the average number of comparisons required for the rule set in Table 1 is 5.03.

EX1002
CISCO SYSTEMS, INC. / Page 420 of 1453

Given a rule list DAG $G = (R, E)$ and policy profile $P = \{p_1, p_2, ..., p_n\}$ a linear arrangement π of G is sought that minimizes Equation 1. In the absence of precedence relationships, the average number of comparisons is minimized if the rules are sorted in non-increasing order according to the probabilities [26], which is also referred to as Smith's algorithm [27]. Precedence constraints cause the problem to be more realistic; however, such constraints also make determining the optimal permutation more problematic.

Determining the optimal rule list permutation can be viewed as job scheduling for a single machine with precedence constraints [15, 21]. The notation for such scheduling problems is $\alpha|\beta|\gamma|\delta$, where α is the number of machines, β is the precedence (or absence of) which can be represented as a DAG, γ is a restriction on processing time, and δ is the optimality criterion [15]. Determining the optimal rule order is similar to the $1|\beta|1|\sum \omega C_i$ scheduling problem, or optimality criterion, where ω is a weight associated with a job (for example, importance) and C_i is the completion time. As previously noted, the $1|||\sum \omega C_i$ problem can be solved in linear time the using Smith's algorithm [27], which orders jobs according to non-decreasing $\frac{t_i}{\omega}$ ratio, where t_i is the processing time of job i. In this case set $t_i = 1$ and $\omega = p_i \ \forall i$. However, Lawler [19] and Lenstra et al. [21] proved $1|\beta|1|\sum \omega C_i$ to be *NP*-complete via the linear arrangement problem, which implies determining the optimal firewall rule order is also *NP*-complete. Note, determining the number of possible permutations has been proven to be *NP*-hard [5].

Theorem $1|\beta|1|\sum \omega C_i \ \alpha$ *Determining the optimal order of a firewall rule list*

Proof Consider the $1|\beta|1|\sum \omega C_i$ problem. Each of n jobs J_i, $i \in I$, has to be processed without preemption on a single machine that can handle at most one job at a time. For each $i \in I$, let ω be the associated weight. Furthermore, let $G = (V, E)$ be a DAG that represents the precedence order of the jobs J_i. Assume the processing time of each job equals 1 time unit, the weights to be $0 \leq \omega \leq 1$ such that $\sum \omega = 1$, and β, which is G, to be a rule list DAG. In this case, the

optimization criterion $\sum \omega \cdot C_i$ is the same as $\sum p_i \cdot i$, which is given in equation 1. Clearly, the optimal firewall rule ordering problem has a solution if and only if $1|\beta|1|\sum \omega C_i$ has a solution. Therefore, determining the optimal permutation of firewall rules is *NP*-complete.

Exemplary Rule Sorting Algorithm

Although determining the optimal rule permutation was proven to be *NP*-complete, reducing the average number of comparisons required to process a packet remains an important objective. As previously discussed, a sorting algorithm must maintain the precedence relationships among rules. Of course an exhaustive search is possible if the number of rules is small (generate and test all possible topological orders); however as proven in the previous section, this is not feasible with a realistic rule list.

One exemplary algorithm starts with the original the rule set, then sorts neighboring rules based on nonincreasing probabilities. However, an exchange of neighbors should never occur if the rules intersect and have different actions. This test preserves any precedence relationships in the policy. For example, the following sorting algorithm uses such a comparison to determine if neighboring rules should be exchanged. Note a_i denotes the action associated with the ith rule.

```
done = false
while(!done)
    done = true
    for(i = 1; i <n; i++)
        if(p_i < p_i+1 AND (r_i ∩ r_i+1 OR a_i == a_i+1))then
            exchange rules, actions, and probabilities
            done = false
        endif
    endfor
endwhile
```

Other sorting algorithms are possible if the completion time of the sort is an issue; however, the method presented is easy to implement and only requires a simple neighbor comparison. Assume the match probabilities for the rule list given in Table 1. Applying the sorting algorithm to this rule list results in the ordering depicted in Figure 2A, which has 10% fewer comparisons on

average. However when using the algorithm, it is possible that one rule can prevent another rule from being reordered. For example, rule r_1 prevents rule r_5 from being placed closer to the beginning of the rule set. However, if both rules r_1 and r_5 are placed closer to the beginning of the policy while maintaining their relative order, the average number of comparison will be further reduced, 15% fewer. This is the optimal order for the 6 rule set, which is depicted in Figure 2B. Although this simple sorting algorithm is unable to move groups of rules, it can still improve the performance of the firewall system. Its effectiveness is measured experimentally in the next section.

Experimental Results

In this section, the average number of rule comparisons required after sorting the rules is compared with average number of comparisons required using the original order and the optimal order. Note the optimal rule ordering was determined via an exhaustive search. As a result, it was not feasible to determine the optimal ordering once the number of rules equaled 15 given the number of permutations to consider. Two different variations of the rule sorting method described in the preceding section were implemented. The difference between the methods was the comparison used to determine if neighboring rules should be exchanged. The first sorting algorithm exchanged neighboring rules if they were out of order and did not intersect. The if-condition was as follows.

if ($p_i < p_{i+1}$ **AND** $r_i \not\cap r_{i+1}$) **then**

Therefore, rule actions were not considered and the method will be referred to as *non-action sort*. The second sorting method did consider the rule action (as described in the preceding section) and will be referred to as *action sort*. The comparison between the two sorting algorithms will indicate the importance of considering rule actions when ordering rules.

In the first experiment, lists of 10 firewall rules were generated with random precedence relationships. The match probability of each rule was given by a Zipf distribution [20], which assigns probabilities according to the rank of an item. For this simulation, the last rule had the highest probability

which is consistent with most policies (last rules are more general). As a result, the original order yields the worst average number of comparisons. The intersection percentage measured the percentage of rules that intersect in the policy. This metric gives a value for the dependency level in the policy; however note, rule action is not considered when calculating this metric. Rules were equally likely to have an accept or deny action and the results (average number of rule comparisons) for a particular intersection percentage were averaged over 1000 simulations.

Results of the first experiment are given in Figures 3A and 3B. More particularly, Figure 3A is a graph illustrating the average number of packet comparisons versus intersection percentage for the original rule sorting, the non-action sort, the action sort, and the optimal sort. Figure 3B is a graph illustrating the percent difference in the average number of comparisons required between the sorted and optimal firewall policy configurations. The average number of comparisons required was lower for the sorted and the optimal lists when the intersection percentage was low, as seen in Figure 3A. This was expected since there is a large number of possible rule permutations (few edges in the DAG). When the intersection percentage approached 100%, the values converged to the number required for the original list. This is due to the limited number of possible rule orders, only one order in the extreme case. The percent difference between the sorted and optimal order is shown in Figure 3B. At zero intersection percentage the sorted and optimal orders are equal, since any ordering is possible. Similarly at an intersection percentage of 100, the sorted and optimal orders are equal since only one order is possible. Between these two extremes, the action sorting algorithm remains close to the optimal value. In contrast, the non-action sort had a maximum difference of 33%.

The benefit of rule sorting on larger policies is also of interest; however as previously described, it was not possible to determine the optimal ordering once the number of rules approaches 15. Therefore, the second experiment used larger rule sets, but only compared the original order and the sorted orders. The number of rules ranged from 10 to 1000, while the matching probabilities and intersection percentages were the same as the previous

experiment. The results of this experiment are depicted in Figure 4A. The sorted rule sets always performed equal to or better than the original order, while the action sort consistently performed better than the non-action sort. As noted in the previous experiment, the percent difference is very large given few intersections (e.g. 80% decrease for 1000 rules with 0% dependency), but approaches zero as all the rules intersect. As the number of rules increases, sorting is increasingly beneficial, although only at low intersection percentages. The benefit of sorting drops more significantly as the intersection percentage increases with larger rule sets. This is primarily due to the low matching probabilities of each rule, which requires a complete reordering to have a significant impact on the average number of comparisons. As a result, large rule sets can benefit from sorting if the intersection percentage is low.

The impact of considering rule actions when sorting is illustrated in Figure 4B. In this experiment lists of 1000 rules were generated, where the intersection percentages ranged from 0% to 100% and the percentage of rules with the same action varied from 50% to 100%. The performance of the action sort to the original list was then compared. As the percentage of rules with the same action increased, the percent difference (reduction) in the average number of comparisons also increased. This is due to the increased number of permutations possible when the rule actions are increasingly the same (fewer edges in the rule list DAG to consider). This is depicted in Figure 4B where a policy with a 100% intersection percentage can significantly reduce the number of comparisons (80% reduction) if all the rules have the same action. This performance increase is not possible with the non-action sort. Therefore, considering the rule action increases the number of possible rule orders, thereby providing more possibilities to improve firewall performance.

Conclusions

Network firewalls enforce a security policy by comparing arriving packets to a list of rules. An action, such as accept or deny, is then performed on the packet based on the matching rule. Unfortunately packet filtering can impose significant delays on traffic due to the complexity and size of rule sets.

Therefore, improving firewall performance is important, given network Quality of Service (QoS) requirements and increasing network traffic loads.

The sections above describe rule ordering methods to improve the performance of network firewalls. Assuming each rule has a probability of a packet matching, firewall rules should be sorted such that the matching probabilities are non-increasing. This reduces the average number of comparisons and the delay across the firewall. However, a simple sort is not possible given precedence relations across rules. It is common in a security policy that two rules may match the same packet yet have different actions. It is this precedence relationship between rules that must be maintained to preserve integrity. The method described above uses Directed Acyclical Graphs (DAG) to represent the precedence order rules must maintain. Given this representation, a topological sort can be used to determine the optimal order (minimum average number of comparisons); however, the examples above prove this problem to be *NP*-complete (similar to job scheduling for a single nonpreemptive machine with precedence constraints). As an alternative, a simple sorting method was introduced that maintained the precedence order of the rules. Simulation results indicate this method can significantly reduce the average number of comparisons required and is comparable to optimal ordering.

Several areas exist for future research in optimizing firewall rule lists. The sorting method proposed above is based on a simple algorithm. Although it can offer an improvement over the original rule order, algorithms that can move groups of rules could provide a larger reduction in the average number of comparisons. The effect of stateful firewalls should also be addressed in future research. Security can be enhanced with connection state and packet audit information. For example, a table can be used to record the state of each connection, which is useful for preventing certain types of attacks (e.g., TCP SYN flood) [30, 31]. The impact of such rules on the firewall needs to be investigated and whether sorting can be done on-line to reflect temporal changes. In addition, more research is needed to determine more accurate probability distributions for packet matching and dependency percentages.

EX1002
CISCO SYSTEMS, INC. / Page 426 of 1453

Given this information, better algorithms can be designed and more realistic simulations can be performed.

Trie-Based Network Firewall Optimization Methods and Rule Splitting Overview

As described above, while assuring firewall policy integrity is critical, performance is equally important given increasing network speeds and traffic volumes. Firewall processing delay can be reduced via hardware as well as policy optimization, where rules are manipulated to reduce the number of comparisons. For a given firewall installation, it can be determined that certain security rules have a higher probability of matching a packet than others. As a result, it is possible to develop a *policy profile* over time that indicates frequency of rule matches (similar to cache hit ratio). Given this information, trie-based methods are described herein to minimize the average number of comparisons required per packet. Although most firewall systems still utilize an ordered list representation, the proposed enhancements still are applicable to current firewall systems since a policy trie can be converted into an ordered list using an inorder traversal.

Rule Sorting

As described above, rule sorting of neighboring rules based on ascending probabilities in a manner that considers rules intersection and rule actions can be used to improve firewall performance by reducing the number of packet comparisons. The methods described above use Directed Acyclic Goal Graphs (DAGs) to represent firewalls. The methods described in this section will use the rule sorting algorithms in combination with policy trie representations to perform sorting of groups of rules in a manner that improves firewall performance.

In this example, it is assumed that a security policy contains a list of n ordered rules, $\{r_1, r_2, ..., r_n\}$. In addition, let p_i represent the probability that a packet will match rule i (first match in the policy). Therefore, the policy is comprehensive, which means every packet will have a match, if $\sum_{i=1}^{n} p_i = 1$.

Using this information, the average number of rule comparisons required can be calculated as

$$E[n] = \sum_{i=1}^{n} i \cdot p_i$$

The average number of comparisons is minimized if the rules are sorted in non-ascending order according to the probabilities. However, this can only be achieved if the sorting algorithm considers the probabilities and whether one rule is a superset of another. For example, sorting algorithms must use the following comparison to determine if neighboring rules should be interchanged Note, a_i denotes the action associated with the ith rule.

if ($p_i < p_{i+1}$ **AND** $r_i \not\subset r_{i+1}$ **OR** $a_i == a_{i+1}$)) **then**

Sorting rules in this fashion can have positive impact on the average number of comparisons required. Figure 5A is a table illustrating a firewall policy prior to rule sorting. The expected number of comparisons for the policy of Figure 5A is 4.26 comparisons per packet. Figure 5B is a table illustrating the firewall policy of Figure 5A after sorting using the above-described algorithm. In Figure 5B, the expected number of comparisons per packet has been reduced to 3.94. Thus, using the method described above, the number of comparisons per packet can be reduced by 8%.

However, it can be seen from Figures 5A and 5B that one rule can prevent another rule from being reordered. For example in Figure 5B, rule r_1 prevents rule r_4 from being placed closer to the beginning of the rule set. However, if both rules r_1 and r_4 are placed closer to the beginning of the policy while maintaining their relative order, the average number of comparison will be reduced.

To solve this problem, rule sets can be sorted a using policy tries. First, the rule list is converted into an equivalent policy trie. Each sub-trie will have an associated probability $\overline{p}$ that is average probability (hit-ratio) of the rules comprising the sub-trie. Sub-tries can be rotated around their parent node to increase performance, using the method described earlier. Since the policy trie (or equivalent rule set) is tested from left to right, rotation should occur if the

probability of the right sub-trie is greater than the left sub-trie. As a result, the average number of comparisons required will be reduced and the policy integrity is maintained. Figure 6A is a trie representation of the rules in Figure 5B. Figure 6B is a table representing resulting rule set after rotating the TCP and UDP sub-tries. The TCP sub-trie in Figure 6A has an expected packet matching probability of 0.095 while the UDP sub-trie has an expected packet matching probability of 0.155. Thus, the UDP sub-trie and the TCP sub-trie should be rotated so that the UDP sub-trie becomes the left sub-trie and the TCP sub-trie becomes the right sub-trie. In the table illustrated in Figure 6B, which lists the ordering of the rules after rotating the sub-tries, the average number of comparisons per packets has been reduced to 3.70.

Rule Splitting

Rule splitting takes a general rule and creates more specific rules that collectively perform the same action over the same set of packets. Here, rule splitting is used to reduce the average number of comparisons. For example in Figure 7A, rule r_5 is split into two separate rules, r_{5a} for UDP and r_{5b} for TCP. Figure 7B is a table corresponding to the policy trie of Figure 7A. Once the rules are positioned based on their probabilities and their relation to other rules, the average number of rule comparisons is reduced to 2.98 (after sort, trie rotation, and splitting) which is a 30% less.

It many not be advantageous to split a general rule since it adds another rule to the policy. For example, assume a policy contains 20 rules where the first 19 rules have the same probability. Assume the last rule can be split and the new specific rule has a probability that is $\frac{3}{4}$ of the last rule. The impact of the probability of the last rule and the location of the new split rule, *m*, is depicted in Figures 8A and 8B. More particularly, Figure 8A is a graph illustrating the average number of comparisons for firewalls with and without rule splitting. Figure 8B is a graph illustrating average number of comparisons versus different locations of the new rule and probabilities. The average number of comparisons is reduced as the split rule is located closer to the first rule (surface decreases as *m* approaches one). Furthermore, splitting yields

EX1002
CISCO SYSTEMS, INC. / Page 429 of 1453

better results when the general rule has a high probability. However as illustrated in Figure 8B, the closer the specific rule is to the location of the original rule the average number of comparisons increases, which is the penalty of adding one more rule to the policy.

The effect of splitting a single rule can be described mathematically as follows. Consider n rules where rule r_n can be split into rules $r_{n,1}$ and $r_{n,r}$ (whose union is the original rule). In addition, assume the split rule $r_{n,1}$ will be located at the mth position ($1 \leq m < n$), while rule $r_{n,r}$ will remain at the nth location. The goal is to determine the best location m, which yields a lower average number of comparisons as compared to the original rule set. This can be defined mathematically in the following formula.

$$\sum_{i=1}^{n} i \cdot p_i > \sum_{i=1}^{m-1} i \cdot p_i + m \cdot p_{n,l} + \sum_{i=m}^{n-1} (i+1) \cdot p_i + (n+1) \cdot p_{n,r}$$

The left side of the inequality is the average number of comparisons for the original rule set. The right hand side of the inequality is the average number of comparisons with the specific rule at location m. If it is assumed that the rules located between m and n have an equal probability (denoted as p) the previous equation can be solved for m.

$$m < \frac{n \cdot p - n \cdot p_n + (n+1) \cdot p_{n,r}}{p - p_{n,l}}$$

The new rule must be located between the first and m^{th}; however, its final location will depend on the relationship with the other rules (cannot be placed before any rule for which it is a superset). This result can be applied iteratively to multiple rules and repeatedly to the same rule.

Rule Optimization for QoS

In the preceding sections, optimizing the entire security policy has been discussed. However, it may be desirable to optimize the rules for a certain type of traffic, in order to reduce the average number of comparisons this traffic encounters. This can be done by organizing the policy trie via traffic

classification, then optimizing the sub-tries. The result is an ordering where the rules for the most important traffic are tested first.

Network Firewall Optimization Using Rule Compression

Another method for network firewall optimization is referred to as rule compression. Given a security policy R, one objective in optimizing firewall performance is to reduce number of rules in the policy while maintaining the original integrity. A method for reducing the number of rules called *rule compression*, which combines and replaces two rules in the policy will now be described. Although compression does reduce the number of rules, it can only be done if the integrity of the original policy is maintained.

Consider two rules r_i and r_j in policy R, where r_i appears before r_j. The two rules can be compressed if and only if the following conditions are true

1. The two rules intersect, $r_i \cap r_j \neq \emptyset$ (an edge between r_i and r_j exists in the policy DAG) (Tuples that are proper subsets and supersets are considered. Compression may still occur if the rules do not intersect or are adjacent in the set space, the resulting rule may contain ranges.)
2. The action of r_i and r_j is the same.
3. Rule r_i is not dependent on any rule r_k that is directly or indirectly dependent on r_j (only one path from r_i to r_j exists in the policy DAG).

The result of compression is a new rule, $r_{i,j}$ whose tuples are the union of the corresponding tuples of rules r_i and r_j. The new rule $r_{i,j}$ replaces both r_i and r_j in R; however, the location of $r_{i,j}$ in R may require the relocation of other rules. Let D_j be the ordered set of rules that appear after r_i that directly or indirectly depend upon r_j. The new rule is placed at the original location of r_i in R and the rules D_j are placed before $r_{i,j}$.

For example, consider the policy given in Table 2. It is possible to compress rules r_1 and r_5, creating the new rule $r_{1,5}$ =[TCP, *, *, 2.*, *, accept]. The ordered set D_j in this example consists of the rules r_3 and r_4. As a result, the new rule $r_{1,5}$ is placed at the original location of r_1 while the rules in D_j are placed before the new rule. Figures 9A and 9B respectively illustrate the

original policy DAG for Table 2 and the policy DAG after rules r_1 and r_5 are compressed.

No.	Proto.	Source IP	Source Port	Destination IP	Destination Port	Action
1	TCP	1.1.*	*	2.2.*	*	accept
2	TCP	1.*	*	*	80	deny
3	TCP	3.3.*	*	*	80	accept
4	TCP	3.*	*	*	*	deny
5	TCP	*	*	2.*	90	accept

Table 2: Example Policy Consisting of Multiple Ordered Rules

Theorem *Compressing rules r_i and r_j of policy R will maintain integrity if the three conditions are met and method described is used.*

Proof Before r_i and r_j are compressed, relocate the rules D_j immediately before r_i and D_i. This relocation will maintain integrity due to the third requirement for compression (no rule in D_i can be dependent on any rule in D_j). Now place r_j directly after r_i. This relocation will not affect integrity since no rule in D_i can have an edge to r_j (again, due to the third condition). Compressing the neighboring rules r_i and r_j creates $r_{i,j}$. This does not affect integrity since the resulting rule only matches the packets that match r_i or r_j in the original policy. Therefore, the result is the compression of rule r_i and r_j , and the integrity of the policy is maintained.

Determining if Compression Should Occur

Although compression may be possible, it may not improve the performance of the policy due to the relocation of rules. Compression should only occur if the average number of comparisons required for the new policy R_c is less than the original policy R; therefore, $E[R_c] < E[R]$.

Firewall Rule Sub-Trie and Sub-List Ordering

Policy Sub-Trie Ordering

Additional methods for firewall optimization are referred to as firewall sub-trie and sub-list ordering. Given a policy trie T, it may be desirable to order all sub-tries such that the average number of tuple comparisons is reduced and policy integrity is maintained. Consider a policy trie T that contains sub-tries T_i and T_j having the same parent node, as seen in Figures 10A-10C. Let P_i denote the sum of the probabilities of the rules contained in sub-trie i, while C_i denotes the number of comparisons required to completely traverse sub-trie i (which is equal to the number of branches). In order to reduce the average number of tuple comparisons, sub-tries that share the same parent node should be ordered such that the following two conditions are observed.

1. Sub-tries that share a parent node are ordered such that the P_i values are non-ascending (higher match probabilities occur first, from left to right).
2. If sub-tries that share a parent node have the same probability (P_i equals P_j), then order the sub-tries such that the C_i values are non-descending (sub-tries consisting of fewer comparisons occur first, from left to right).

These conditions are recursively applied throughout the policy trie as seen in Figures 11A-11D. However, these conditions do not necessarily maintain policy integrity.

Consider a group of n sub-tries that share the same parent node that are numbered sequentially from left to right. Consider any two non-intersecting sub-tries T_i and T_{i+k} in this group that are out of order. If two sub-tries do not intersect, denoted as $T_i \pitchfork T_j$, then no rule in one sub-trie will intersect with any rule in the other sub-trie, $r_k \pitchfork r_l$, $\forall r_k \in T_i$, $\forall r_l \in T_j$. The following *integrity condition* must be observed when reordering the sub-tries. The two sub-tries can be exchanged (rotated about the parent) if and only the sub-tries T_i through T_{i+k-1} do not intersect with T_{i+k} and the sub-tries T_{i+1} through T_{i+k} do not intersect with T_i. Similar to finding the linear sequence of a policy DAGs, these conditions maintain the policy trie integrity. This is observed in Figure 10A,

where no edge exists between any rule in T_1 and T_2. More particularly, Figure 10A is a policy DAG of a six-rule firewall list. Figure 10B is a policy trie representation of the firewall rule list represented by Figure 10A. In Figure 10B, the average number of tuple compares required per packet is 5.5. Figure 10C illustrates the policy trie after rotating sub-tries T_1 and T_2. In Figure 10C, the average number of tuple compares required is 4.5. In Figures 10A-10C, the following probabilities are assumed:

$P_1 = 0.5$

$C_1 = 4$

$P_2 = 0.5$; and

$C_2 = 2$.

The average number of tuple comparisons is an estimate based on the longest trie path.

Using the conditions for comparing and ordering, the following sorting algorithm sorts neighboring sub-tries that share the same parent node.

```
m = a parent node in T
done = false
while(!done)
    done = true
    for each sub-trie Ti having parent m AND a right neighboring sub-trie
        if((Pi < Pi+1 AND (Pi == Pi+1 AND Ci > Ci+1)) AND Ti ⋔ Ti+1) then
        interchange Ti and Ti+1
        done = false
        endif
    endfor
endwhile
```

Figures 11A-11D illustrate policy trie rotation for an eight-rule firewall policy. More particularly, Figure 11A illustrates the policy DAG representation of an eight-rule firewall policy. Figure 11B is a policy trie representation of the original firewall policy. In this example, ordering occurs in three stages, starting at the bottom level and moving towards the top level of the trie. In Figure 11C, the leaves are ordered at the lowest level. More particularly, nodes r_1 and r_2 are exchanged with nodes r_7 and r_8. The average number of tuple compares for the ordering represented by Figure 11C is 10.45. In Figure 11D, the sub-

tries on the second lowest level (T_3, T_4, T_5, and T_6) are ordered. More particularly, Figure 11D illustrates the policy trie after exchanging sub-tries T_3 and T_4. The average number of tuple compares for the representation in Figure 11D is 10.275. In Figure 11E, the sub-tries on the second highest level, (T_1 and T_2) are ordered. Figure 11E illustrates the final ordering after exchanging T_1 and T_2. In the policy trie of Figure 11E, the average number of tuple compares required is 6.775. The average number of tuple comparisons is an estimate based on the longest trie path.

Policy Sub-List Ordering

The preceding section describes conditions for sorting policy sub-tries, which allow the exchange of groups of rules (sub-tries). The same conditions can be applied to list based policies, where sub-lists are ordered to improve the average number of rule comparisons.

In the sections above relating to rule sorting, a method is described to exchange neighboring rules in a list-based security policy, as seen in Figure 12B. However, it was observed that when ordering rules in this fashion it is possible that one rule can block the exchange of another. If groups of rules were allowed to be exchanged the average number of rule comparisons could be further reduced.

Given a policy list L, it may be desirable to order all sub-lists such that the average number of rule comparisons is reduced and policy integrity is maintained. Consider a policy list L that contains sub-tries L_i and L_j. Let P_i denote the sum of the probabilities of the rules contained in sub-list i, while C_i denotes the number of rules in sub-list i. In order to reduce the average number of rule comparisons, sub-lists should be ordered such that the following two conditions are observed.

1. Sub-lists are ordered such that the P_i values are non-ascending (higher match probabilities occur first, from left to right).
2. If sub-lists have the same probability (P_i equals P_j), then order the sub-lists such that the C_i values are non-descending (sub-lists consisting of fewer comparisons occur first, from left to right).

These conditions are applied throughout the policy list; however as with policy tries, these conditions do not necessarily maintain policy integrity.

Consider a group of n sub-lists that are numbered sequentially from left to right. Consider any two non-intersecting sub-lists L_i and L_{i+k} in this group that are out of order. If two sub-lists do not intersect, denoted as $L_i \pitchfork L_j$, then no rule in one sub-list will intersect with any rule in the other sub-list, $r_k \pitchfork r_l$, $\forall r_k \in L_i$, $\forall r_l \in L_j$. The following *integrity condition* must be observed when reordering the sub-lists. The two sub-lists can be exchanged if and only if the sub-lists L_i through L_{i+k-1} do not intersect with any rule in L_{i+k} and sub-lists L_{i+1} through L_{i+k} do not intersect with L_i. Similar to finding the linear sequence of a policy DAGs, these conditions maintain the policy trie integrity. For example, consider the sub-lists $L_1 = \{r_1, r_3\}$ and $L_2 = \{r_2, r_4\}$ given in Figure 12B. No edge exists between any rule in L_1 and L_2. The two sub-lists are out of order with respect to P and should be exchanged. The resulting list is given in Figure 12C. Figure 12A illustrates the original policy order and results in an average number of rule comparisons of 3.4. In the sorted version in Figure 12B, the average number of rule comparisons is 3.3. In Figure 12C, the average number of rule comparisons has been reduced to 2.7. Using the conditions for comparing and ordering, the following sorting algorithm sorts neighboring sub-lists.

```
done = false
while(!done)
    done = true
    for each sub-list Li having a right neighboring sub-list
        if ((Pi < Pi+1 OR (Pi == Pi+1 AND Ci > Ci+1)) AND Li ⋔ Li+1)then
            interchange rules and probabilities
            done = false
        endif
    endfor
endwhile
```

Summary of Firewall Policy Optimization Techniques and Methods

As stated above, the methods and systems described herein for a network firewall policy optimization can be implemented using any combination of hardware, software, and/or firmware. Alternatively, the steps for firewall policy optimization can be performed manually with the number of rules being optimized is small enough. Figure 13 is a flow chart illustrating an exemplary process for firewall policy optimization according to an embodiment of the subject matter described herein. Referring to Figure 13, in block **1300**, a firewall policy including an ordered list of firewall rules is defined. In block **1302**, for each rule, a probability indicating a likelihood of receiving a packet that matches each rule is specified. In block **1304**, neighboring rules are sorted in order of non-increasing probability in a manner that preserves firewall policy. In block **1306**, groups of rules are sorted in order of non-increasing probability in a manner that preserves firewall policy. For example, any of the policy-trie-based methods described above may be used. In block **1308**, one or more rules are split to reduce the number of average packet comparisons. In block **1310**, intersecting rules having common actions are identified and collapsed into single rules.

As described above, the subject matter described herein may be implemented in hardware, software, and/or firmware. In one implementation, the subject matter described herein for firewall policy optimization may be implemented on a general purpose computing platform. Figure 14 is a block diagram of a general purpose computing platform including software for firewall policy optimization according to an embodiment of the subject matter described herein. Referring to Figure 14, computing platform **1400** may be a general purpose computer, such as a personal computer, that includes a microprocessor **1402**, memory **1404**, and I/O interfaces **1406**. Microprocessor **1400** may be any suitable microprocessor, such as any of the Intel or AMD families of microprocessors. Memory **1404** may include volatile memory for running programs and persistent memory, such as one or more disk storage devices. I/O interface **1406** may include interfaces with I/O devices, such as user input devices and output devices.

In the illustrated example, software that may be resident in memory **1404** includes a firewall policy editor **1408** and a firewall policy optimizer **1410**. Firewall policy editor **1408** may allow a user to define a firewall policy. For example, firewall policy editor **1408** may allow a user to define a firewall policy by specifying different rules. The rules may be specified in a graphical manner, for example using policy DAGs as described above. Alternatively, firewall policy editor **1408** may allow a user to input rules in a tabular manner, as illustrated in any of the tables described herein. Firewall policy optimizer **1410** may implement any or all of the firewall policy optimization techniques to order rules entered via firewall policy editor **1408** in a manner that preserves policy integrity and that enhances firewall performance.

A firewall rule set that is optimized using the subject matter described herein may be implemented on any firewall system that includes one or more firewalls. For example, an optimized firewall rule set according to embodiments of the subject matter described herein may be implemented using any of the hierarchical, multi-node firewall systems described in commonly assigned, co-pending U.S. patent application no. 11/316,331, filed December 22, 2005, the disclosure of which is incorporated herein by reference in its entirety. Figure 15 illustrates an example of a multi-node firewall system suitable for implementing the firewall rules according to an embodiment of the subject matter described herein. Referring to Figure 15, a plurality of firewall nodes **1500**, **1502**, **1504**,and **1506** may collectively implement any of the optimized firewall policies described herein. For example, the firewall nodes may collectively implement different portions of a firewall policy data structure including an ordered list of firewall rules. A firewall policy engine **1508** resident on each firewall node may filter packets using its local portion **1510** of the firewall policy data structure. A control node **1512** may include a firewall policy optimizer **1514** that measures the average number of comparisons per packets for the current rule configuration and may dynamically reorder the rules to reduce the average number of comparisons per packet. For example, firewall policy optimizer **1514** may utilize any of the methods described herein to rearrange rules and improve firewall performance. Rules may be tested for rearrangement at user-specified

intervals or when average number of packet comparisons increases by a user-specified amount.

References

The disclosure of each of the following references is hereby incorporated herein by reference in its entirety.

[1] E. Al-Shaer and H. Hamed. Firewall Policy Management Advisor for Anomaly Detection and Rule Editing. In *Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management*, 2003.

[2] E. Al-Shaer and H. Hamed. Modeling and Management of Firewall Policies. *IEEE Transactions on Network and Service Management*, 1(1), 2004.

[3] S. M. Bellovin and W. Cheswick. Network Firewalls. *IEEE Communications Magazine*, pages 50–57, Sept. 1994.

[4] C. Benecke. A Parallel Packet Screen for High Speed Networks. In *Proceedings of the 15th Annual Computer Security Applications Conference*, 1999.

[5] G. Brightwell and P. Winkler. Counting Linear Extensions is #P-Complete. In *Proceedings of the Twenty-Third Annual ACM Symposium on Theory of Computing*, 1991.

[6] M. Christiansen and E. Fleury. Using Interval Decision Diagrams for Packet Filtering. Technical report, BRICS, 2002.

[7] D. Decasper, Z. Dittia, G. Parulkar, and B. Plattner. Router Plugins: A Software Architecture for Next-Generation Routers. *IEEE/ACM Transactions on Networking*, 8(1), February 2000.

[8] M. Degermark, A. Brodnik, S. Carlsson, and S. Pink. Small Forwarding Tables for Fast Routing Lookups. In *Proceedings of ACM SIGCOMM*, pages 4 – 13, 1997.

[9] U. Ellermann and C. Benecke. Firewalls for ATM Networks. In Proceedings of *INFOSEC'COM*, 1998.

[10] A. Feldmann and S. Muthukrishnan. Tradeoffs for Packet Classification. In Proceedings of the *IEEE INFOCOM*, pages 397 – 413, 2000.

EX1002
CISCO SYSTEMS, INC. / Page 439 of 1453

[11] E. W. Fulp. Firewall Architectures for High Speed Networks. Technical Report 20026, Wake Forest University Computer Science Department, 2002.

[12] E. W. Fulp. Firewall Policy Models Using Ordered-Sets. Technical report, Wake Forest University Computer Science Department, 2004.

[13] R. Funke, A. Grote, and H.-U. Heiss. Performance Evaluation of Firewalls in Gigabit-Networks. In *Proceedings of the Symposium on Performance Evaluation of Computer and Telecommunication Systems*, 1999.

[14] S. Goddard, R. Kieckhafer, and Y. Zhang. An Unavailability Analysis of Firewall Sandwich Configurations. In *Proceedings of the 6th IEEE Symposium on High Assurance Systems Engineering*, 2001.

[15] R. L. Graham, E. L. Lawler, J. K. Lenstra, and A. H. G. R. Kan. Optimizing and Approximation in Determinstic Sequencing and Scheduling: A Survey. *Annals of Discrete Mathematics*, 5:287 – 326, 1979.

[16] A. Hari, S. Suri, and G. Parulkar. Detecting and Resolving Packet Filter Conflicts. In *Proceedings of IEEE INFOCOM*, pages 1203–1212, 2000.

[17] HiPAC. High Performance Packet Classification. http://www.hipac.org.

[18] E. Horowitz, S. Sahni, and D. Mehta. *Fundamentals of Data Structures in C++*. Compuer Science Press, 1995.

[19] E. L. Lawler. Sequencing Jobs to Minimize Total Weighted Completion Time Subject to Precedence Constraints. *Annals of Discrete Mathematics*, 2:75 – 90, 1978.

[20] W. E. Leland, M. S. Taqqu, W. Willinger, and D. V. Wilson. On the Self-Similar Nature of Ethernet Traffic. *IEEE Transactions on Networking*, 2:1 – 15, 1994.

[21] J. K. Lenstra and A. H. G. R. Kan. Complexity of Scheduling under Precedence Constraints. *Operations Research*, 26(1):22 – 35, 1978.

[22] O. Paul and M. Laurent. A Full Bandwidth ATM Firewall. In Proceedings of the 6th European Symposium on *Research in Computer Security ESORICS'2000*, 2000.

[23] B. R. Preiss. *Data Structures and Algorithms with Object-Oriented Design Patterns in C++*. John Wiley & Sons, 1999.

[24] L. Qui, G. Varghese, and S. Suri. Fast Firewall Implementations for Software and Hardware-Based Routers. In *Proceedings of ACM SIGMETRICS*, June 2001.

[25] V. P. Ranganath and D. Andresen. A Set-Based Approach to Packet Classification. In *Proceedings of the IASTED International Conference on Parallel and Distributed Computing and Systems*, pages 889–894, 2003.

[26] R. Rivest. On Self-Organizing Sequential Search Heuristics. *Communications of the ACM*, 19(2), 1976.

[27] W. E. Smith. Various Optimizers for Single-Stage Production. *Naval Research Logistics Quarterly*, 3:59 – 66, 1956.

[28] V. Srinivasan, G. Varghese, S. Suri, and M. Waldvogel. Fast and Scalable Layer Four Switching. In *Proceedings of ACM SIGCOMM*, pages 191–202, 1998.

[29] S. Suri and G. Varghese. Packet Filtering in High Speed Networks. In *Proceedings of the Symposium on Discrete Algorithms*, pages 969 – 970, 1999.

[30] R. L. Ziegler. *Linux Firewalls*. New Riders, second edition, 2002.

[31] E. D. Zwicky, S. Cooper, and D. B. Chapman. *Building Internet Firewalls*. O'Reilly, 2000.

It will be understood that various details of the invention may be changed without departing from the scope of the invention. Furthermore, the foregoing description is for the purpose of illustration only, and not for the purpose of limitation.

CLAIMS

What is claimed is:

1. A method for producing a performance optimized firewall policy, the method comprising:
   (a) defining a firewall policy including an ordered list of firewall rules;
   (b) for each rule, defining a probability indicating the likelihood of receiving a packet matching each rule; and
   (c) sorting neighboring rules in order of non-increasing probability in a manner that preserves the firewall policy.
2. The method of claim 1 wherein sorting neighboring rules in order of non-increasing probability in a manner that preserves the firewall policy includes, for each pair of neighboring rules, rearranging the rules if a first rule of the pair has a lower probability than a second rule of the pair and the first rule of the pair is not a subset of the second rule of the pair with a different action.
3. The method of claim 1 comprising sorting groups of two or more rules in order of non-increasing probability in a manner that preserves the firewall policy.
4. The method of claim 3 wherein sorting groups of two or more rules in a manner that preserves firewall policy includes assigning each group of rules to a sub-trie in a policy trie, computing a sum of packet matching probabilities for rules in each sub-trie, and, in response to determining that a first sub-trie has a lower sum than a second sub-trie, rotating the first and second sub-tries about a common parent so that rules in the second sub-trie will be applied before the rules in the first sub-trie in the firewall policy .
5. The method of claim 4 comprising, in response to determining that the first and second sub-tries have equal sums, determining whether the second sub-trie has an lower number of branches than the first sub-trie, and, in response to determining that the second sub-trie has a lower number of branches than the first sub-trie, rotating the first and second sub-tries about a common parent so that the rules in the second sub-trie will be applied before the rules in the first sub-trie in the firewall policy.

6. The method of claim 3 wherein sorting groups of two or more rules in a manner that preserves the firewall policy includes:

(a) identifying first and second sub-lists of rules in the ordered list of firewall rules, the first sub-list preceding the second sub-list in the ordered list of firewall rules;

(b) determining a sum of packet matching probabilities for each of the first and second sub-lists;

(c) determining whether the first and second sub-lists intersect; and

(d) in response to determining that the sum of the packet matching probabilities for the second sub-list is greater than the sum of the packet matching probabilities for the first sub-list and that the first and second sub-lists do not intersect, switching the order of the first and second sub-lists in the ordered list of firewall rules.

7. The method of claim 6 comprising, in response to determining that the sums of the packet matching probabilities for the first and sub-lists are equal, determining whether the second sub-list has a lower number of rules than the first sub-list, and, in response to determining that the second sub-list has a lower number of rules than the first sub-list, switching the order of the first and second sub-lists in the ordered list of firewall rules.

8. The method of claim 1 comprising splitting at least one of the firewall rules to reduce an average number of comparisons required per received packet.

9. The method of claim 1 comprising identifying intersecting rules having a common action and collapsing the rules into a single rule representing a union of the intersecting rules.

10. The method of claim 1 wherein sorting neighboring rules includes sorting rules such that comparisons for a particular class of packets are reduced.

11. The method of claim 1 comprising assigning the rules to vertices in a directed acyclical graph (DAG), determining precedence relationships between the rules, assigning the precedence relationships to edges that connect the vertices in the DAG, and wherein sorting the neighboring

rules in order of non-increasing probability in a manner that preserves the firewall policy includes sorting the neighboring rules in a manner that preserves the precedence relationships represented by the DAG.

12. The method of claim 1 wherein the rules comprise intrusion detection rules.

13. The method of claim 1 wherein the rules comprise intrusion protection rules.

14. A system for firewall policy optimization, the system comprising:

(a) a firewall policy editor for allowing a user to define a firewall policy including an ordered list of firewall rules and for receiving input regarding probabilities indicating the likelihood of receiving a packet matching each rule; and

(b) a firewall policy optimizer for sorting neighboring rules in order of non-increasing probability in a manner that preserves the firewall policy.

15. The system of claim 14 wherein the firewall policy optimizer is adapted to, for each pair of neighboring rules, rearrange the rules if a first rule of the pair has a lower probability than a second rule of the pair and the first rule of the pair is not a subset of the second rule of the pair with a different action.

16. The system of claim 14 wherein the firewall policy optimizer is adapted to sort groups of two or more rules in order of non-increasing probability in a manner that preserves the firewall policy.

17. The system of claim 16 wherein the firewall policy optimizer is adapted to assign each group of rules to a sub-trie in a policy trie, to compute a sum of packet matching probabilities for rules in each sub-trie, and, in response to determining that a first sub-trie has a lower sum than a second sub-trie, to rotate the first and second sub-tries about a common parent so that rules in the second sub-trie will be applied before the rules in the first sub-trie in the firewall policy.

18. The system of claim 17 wherein the firewall policy optimizer is adapted to, in response to determining that the first and second sub-tries have equal sums, determine whether the second sub-trie has an lower

number of branches than the first sub-trie, and, in response to determining that the second sub-trie has a lower number of branches than the first sub-trie, rotate the first and second sub-tries about a common parent so that the rules in the second sub-trie will be applied before the rules in the first sub-trie in the firewall policy.

19. The system of claim 16 wherein the firewall policy optimizer is adapted to:

(a) identify first and second sub-lists of rules in the ordered list of firewall rules, the first sub-list preceding the second sub-list in the ordered list of firewall rules;

(b) determine a sum of packet matching probabilities for each of the first and second sub-lists;

(c) determine whether the first and second sub-lists intersect; and

(d) in response to determining that the sum of the packet matching probabilities for the second sub-list is greater than the sum of the packet matching probabilities for the first sub-list and that the first and second sub-lists do not intersect, switch the order of the first and second sub-lists in the ordered list of firewall rules.

20. The system of claim 19 wherein the firewall policy optimizer is adapted to, in response to determining that the sums of the packet matching probabilities for the first and sub-lists are equal, determine whether the second sub-list has a lower number of rules than the first sub-list, and, in response to determining that the second sub-list has a lower number of rules than the first sub-list, switch the order of the first and second sub-lists in the ordered list of firewall rules.

21. The system of claim 14 wherein the firewall policy optimizer is adapted to split at least one of the firewall rules to reduce an average number of comparisons required per received packet.

22. The system of claim 14 wherein the firewall policy optimizer is adapted to identify intersecting rules having a common action and collapse the rules into a single rule representing a union of the intersecting rules.

23. The system of claim 14 wherein the firewall policy optimizer is adapted to sort neighboring rules such that comparisons for a particular class of packets are reduced.

24. The system of claim 14 wherein the firewall policy optimizer is adapted to assign the rules to vertices in a directed acyclical graph (DAG), determine precedence relationships between the rules, assign the precedence relationships to edges that connect the vertices in the DAG, and to sort the neighboring rules in a manner that preserves the precedence relationships represented by the DAG.

25. The system of claim 14 wherein the rules comprise intrusion detection rules.

26. The system of claim 14 wherein the rules comprise intrusion protection rules.

27. A network firewall comprising:

(a) a firewall policy data structure for storing an ordered list of firewall rules;

(b) a firewall policy engine for implementing a firewall policy by comparing packets to the rules in the order specified by the firewall policy data structure; and

(c) a firewall policy optimizer for optimizing performance of the network firewall by reordering the rules in a manner that reduces an average number of rule comparisons per packet and hat preserves the firewall policy.

28. The network firewall of claim 27 wherein the firewall policy optimizer is adapted to measure average number of comparisons per packet for a rule ordering specified by the firewall policy data structure and to dynamically re-order to rules to reduce the average number of comparisons per packet.

29. A computer program product comprising computer executable instructions embodied in a computer readable medium for performing steps comprising:

(a) defining a firewall policy including an ordered list of firewall rules;

(b) for each rule, defining a probability indicating the likelihood of receiving a packet matching each rule; and

(c) sorting neighboring rules in order of non-increasing probability in a manner that preserves the firewall policy.

30. The computer program product of claim 29 wherein sorting neighboring rules in order of non-increasing probability in a manner that preserves the firewall policy includes, for each pair of neighboring rules, rearranging the rules if a first rule of the pair has a lower probability than a second rule of the pair and the first rule of the pair is not a subset of the second rule of the pair with a different action.

31. The computer program product of claim 29 comprising sorting groups of two or more rules in order of non-increasing probability in a manner that preserves the firewall policy.

32. The computer program product of claim 31 wherein sorting groups of two or more rules in a manner that preserves firewall policy includes assigning each group of rules to a sub-trie in a policy trie, computing a sum of packet matching probabilities for rules in each sub-trie, and, in response to determining that a first sub-trie has a lower sum than a second sub-trie, rotating the first and second sub-tries about a common parent so that rules in the second sub-trie will be applied before the rules in the first sub-trie in the firewall policy .

33. The computer program product of claim 32 comprising, in response to determining that the first and second sub-tries have equal sums, determining whether the second sub-trie has an lower number of branches than the first sub-trie, and, in response to determining that the second sub-trie has a lower number of branches than the first sub-trie, rotating the first and second sub-tries about a common parent so that the rules in the second sub-trie will be applied before the rules in the first sub-trie in the firewall policy.

34. The computer program product of claim 31 wherein sorting groups of two or more rules in a manner that preserves the firewall policy includes:

EX1002
CISCO SYSTEMS, INC. / Page 447 of 1453

(a) identifying first and second sub-lists of rules in the ordered list of firewall rules, the first sub-list preceding the second sub-list in the ordered list of firewall rules;

(b) determining a sum of packet matching probabilities for each of the first and second sub-lists;

(c) determining whether the first and second sub-lists intersect; and

(d) in response to determining that the sum of the packet matching probabilities for the second sub-list is greater than the sum of the packet matching probabilities for the first sub-list and that the first and second sub-lists do not intersect, switching the order of the first and second sub-lists in the ordered list of firewall rules.

35. The computer program product of claim 34 comprising, in response to determining that the sums of the packet matching probabilities for the first and sub-lists are equal, determining whether the second sub-list has a lower number of rules than the first sub-list, and, in response to determining that the second sub-list has a lower number of rules than the first sub-list, switching the order of the first and second sub-lists in the ordered list of firewall rules.

36. The computer program product of claim 29 comprising splitting at least one of the firewall rules to reduce an average number of comparisons required per received packet.

37. The computer program product of claim 29 comprising identifying intersecting rules having a common action and collapsing the rules into a single rule representing a union of the intersecting rules.

38. The computer program product of claim 29 wherein sorting neighboring rules includes sorting rules such that comparisons for a particular class of packets are reduced.

39. The computer program product of claim 29 comprising assigning the rules to vertices in a directed acyclical graph (DAG), determining precedence relationships between the rules, assigning the precedence relationships to edges that connect the vertices in the DAG, and wherein sorting the neighboring rules in order of non-increasing probability in a manner that preserves the firewall policy includes sorting the

neighboring rules in a manner that preserves the precedence relationships represented by the DAG.

40. The computer program product of claim 29 wherein the rules comprise intrusion detection rules.

41. The computer program product of claim 29 wherein the rules comprise intrusion protection rules.

EX1002
CISCO SYSTEMS, INC. / Page 449 of 1453

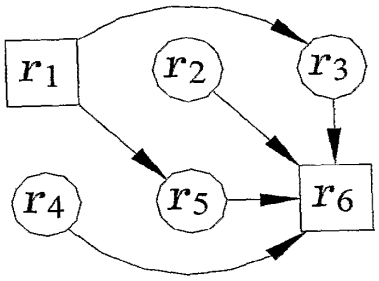


FIG. 1A

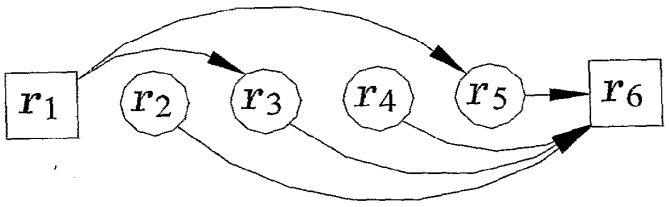


FIG. 1B

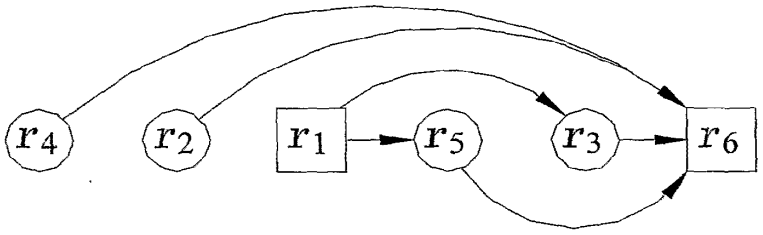


FIG. 2A

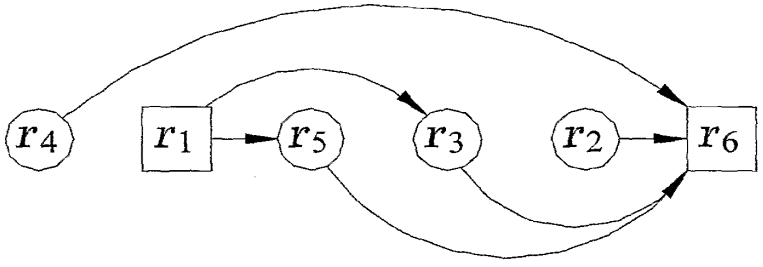


FIG. 2B

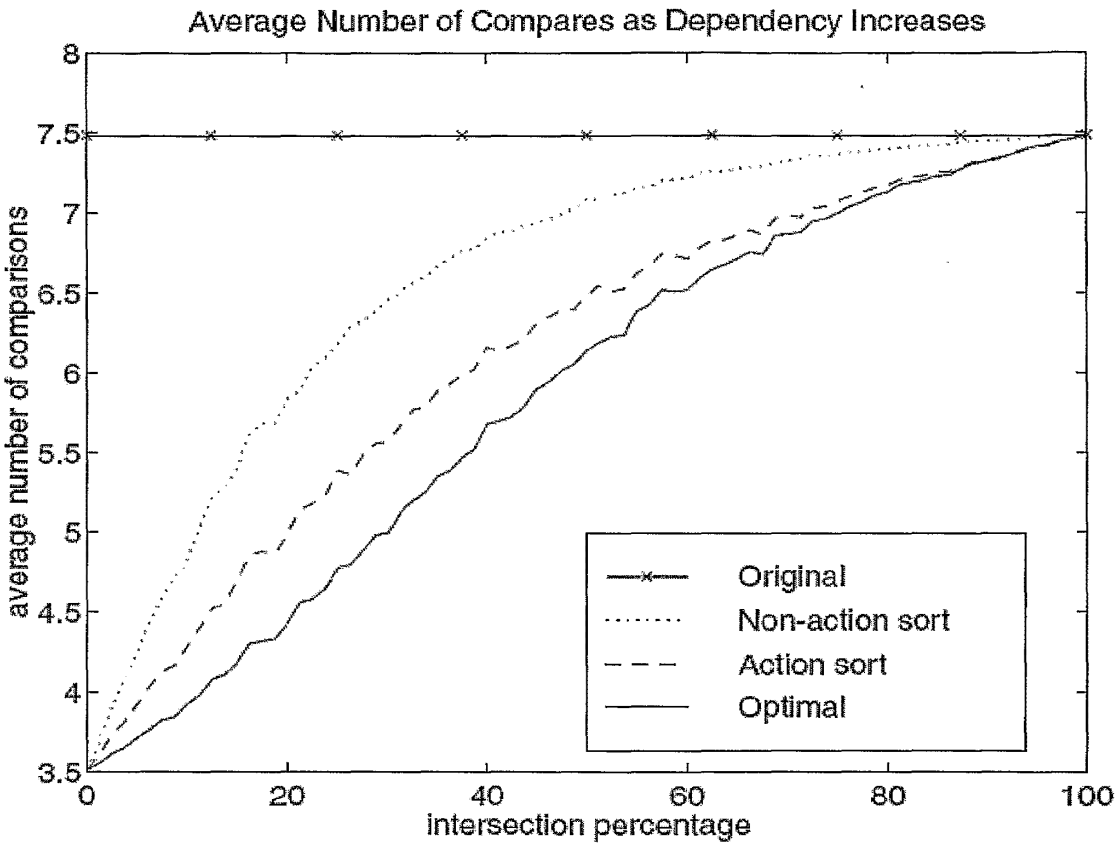

Average Number of Compares as Dependency Increases
average number of comparisons
intersection percentage
8
7.5
7
6.5
6
5.5
5
4.5
4
3.5
0
20
40
60
80
100
Original
Non-action sort
Action sort
Optimal

FIG. 3A

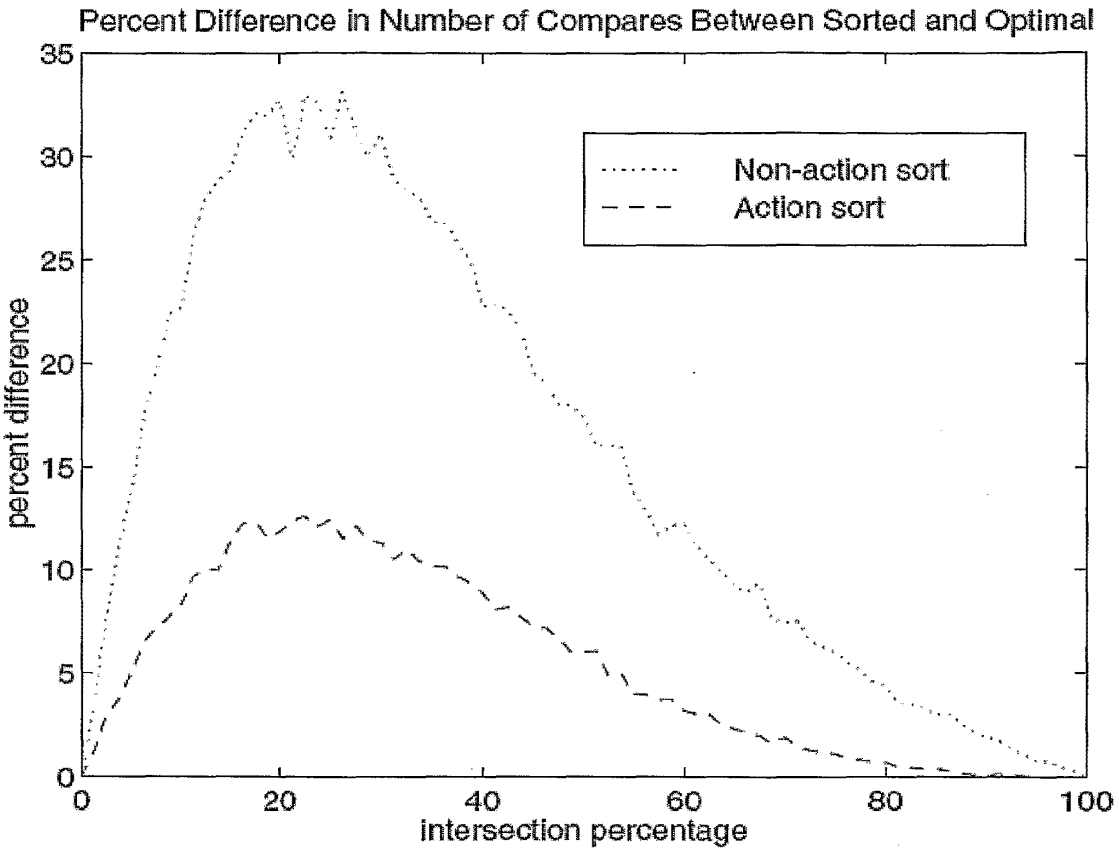

Percent Difference in Number of Compares Between Sorted and Optimal
percent difference
intersection percentage
Non-action sort
Action sort
0
5
10
15
20
25
30
35
0
20
40
60
80
100

FIG. 3B

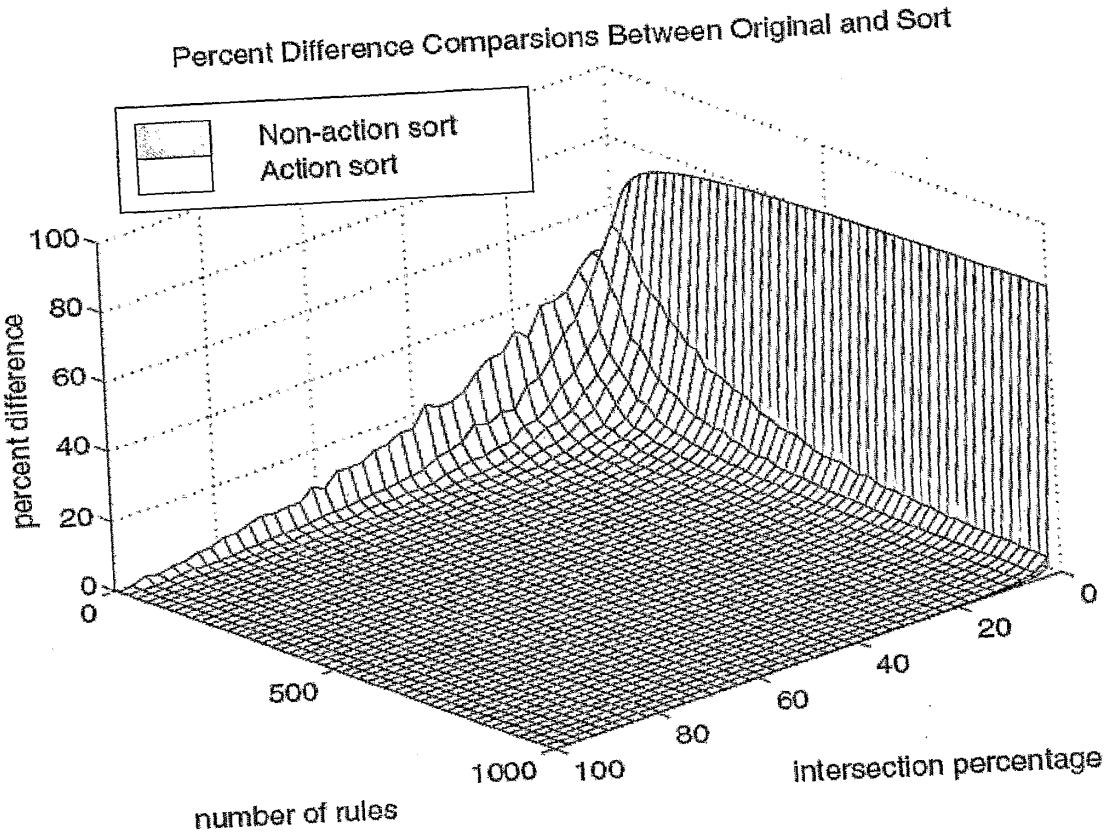

Percent Difference Comparsions Between Original and Sort
Non-action sort
Action sort
percent difference
100
80
60
40
20
0
0
500
1000
number of rules
0
20
40
60
80
100
intersection percentage

FIG. 4A

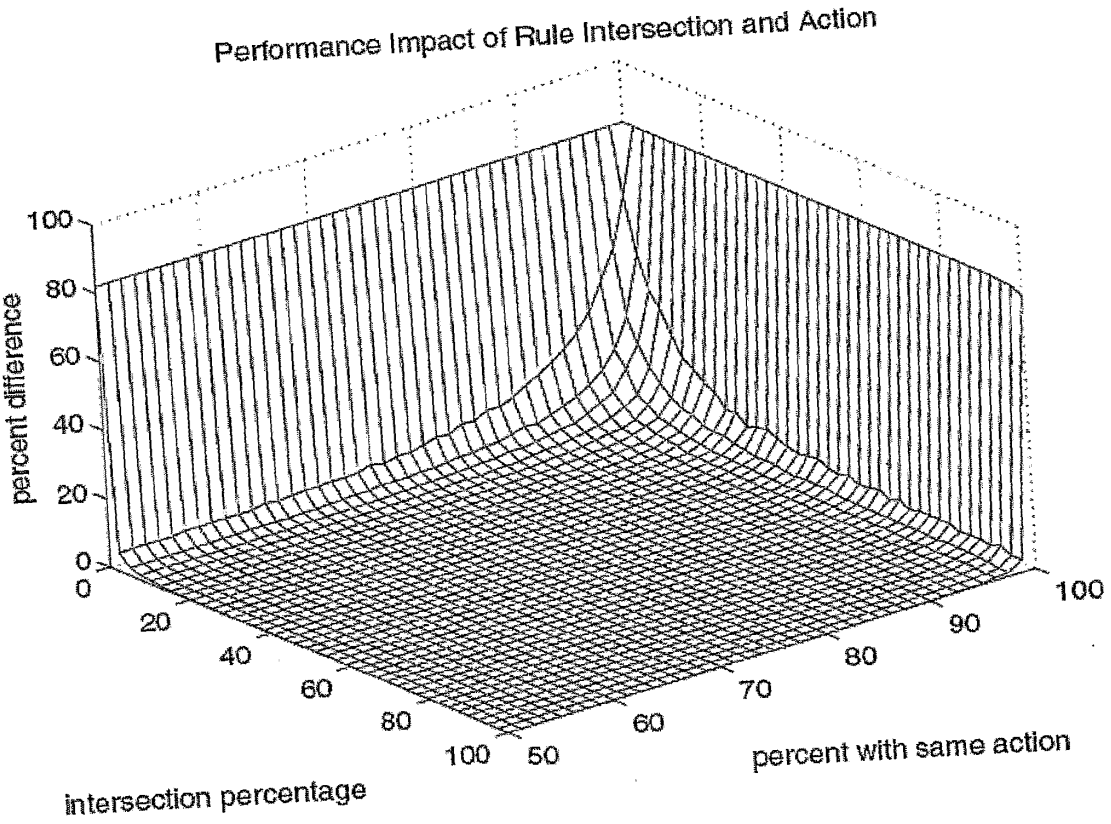

Performance Impact of Rule Intersection and Action
percent difference
100
80
60
40
20
0
0
20
40
60
80
100
intersection percentage
50
60
70
80
90
100
percent with same action

FIG. 4B

r_1	(UDP,	1.1.*,	ACCEPT)	$p_1 = 0.01$
r_2	(TCP,	1.*,	ACCEPT)	$p_2 = 0.02$
r_3	(TCP,	2.*,	ACCEPT)	$p_3 = 0.17$
r_4	(UDP,	1.*,	DENY)	$p_4 = 0.30$
r_5	(*,	*,	DENY)	$p_5 = 0.50$

FIG. 5A

r_3	(TCP,	2.*,	ACCEPT)	$p_3 = 0.17$
r_2	(TCP,	1.*,	ACCEPT)	$p_2 = 0.02$
r_1	(UDP,	1.1.*,	ACCEPT)	$p_1 = 0.01$
r_4	(UDP,	1.*,	DENY)	$p_4 = 0.30$
r_5	(*,	*,	DENY)	$p_5 = 0.50$

FIG. 5B

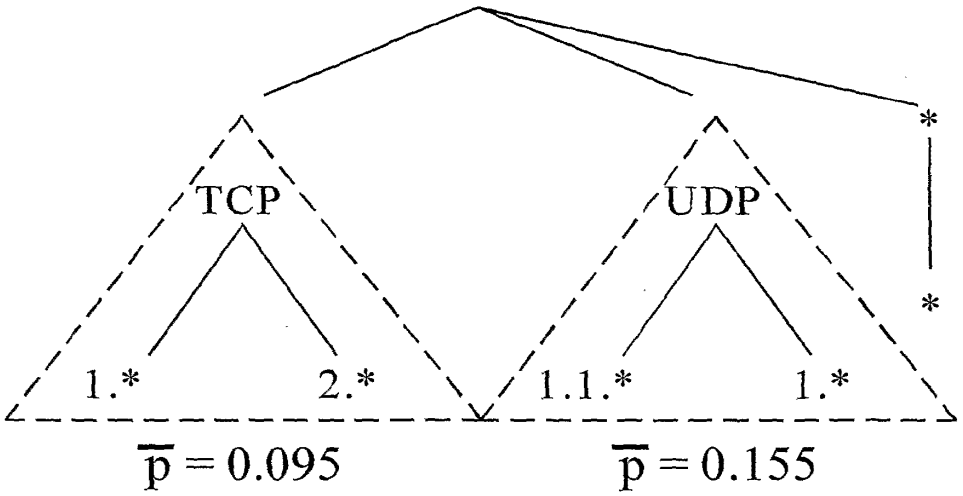


FIG. 6A

r_1	(UDP,	1.1.*,	ACCEPT)	$p_1 = 0.01$
r_4	(UDP,	1.*,	DENY)	$p_4 = 0.30$
r_3	(TCP,	2.*,	ACCEPT)	$p_3 = 0.17$
r_2	(TCP,	1.*,	ACCEPT)	$p_2 = 0.02$
r_5	(*,	*,	DENY)	$p_5 = 0.50$

FIG. 6B

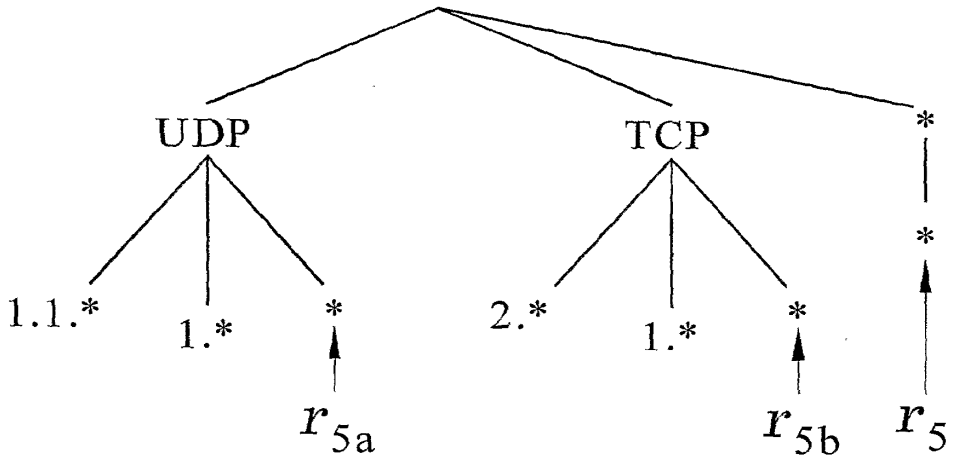


FIG. 7A

r_1	(UDP,	1.1.*,	ACCEPT)	$p_1 = 0.01$
r_4	(UDP,	1.*,	ACCEPT)	$p_4 = 0.30$
r_{5a}	(UDP,	*,	DENY)	$p_{5a} = 0.47$
r_3	(TCP,	2.*,	ACCEPT)	$p_3 = 0.17$
r_2	(TCP,	1.*,	ACCEPT)	$p_2 = 0.02$
r_{5b}	(TCP,	*,	DENY)	$p_{5b} = 0.03$

FIG. 7B

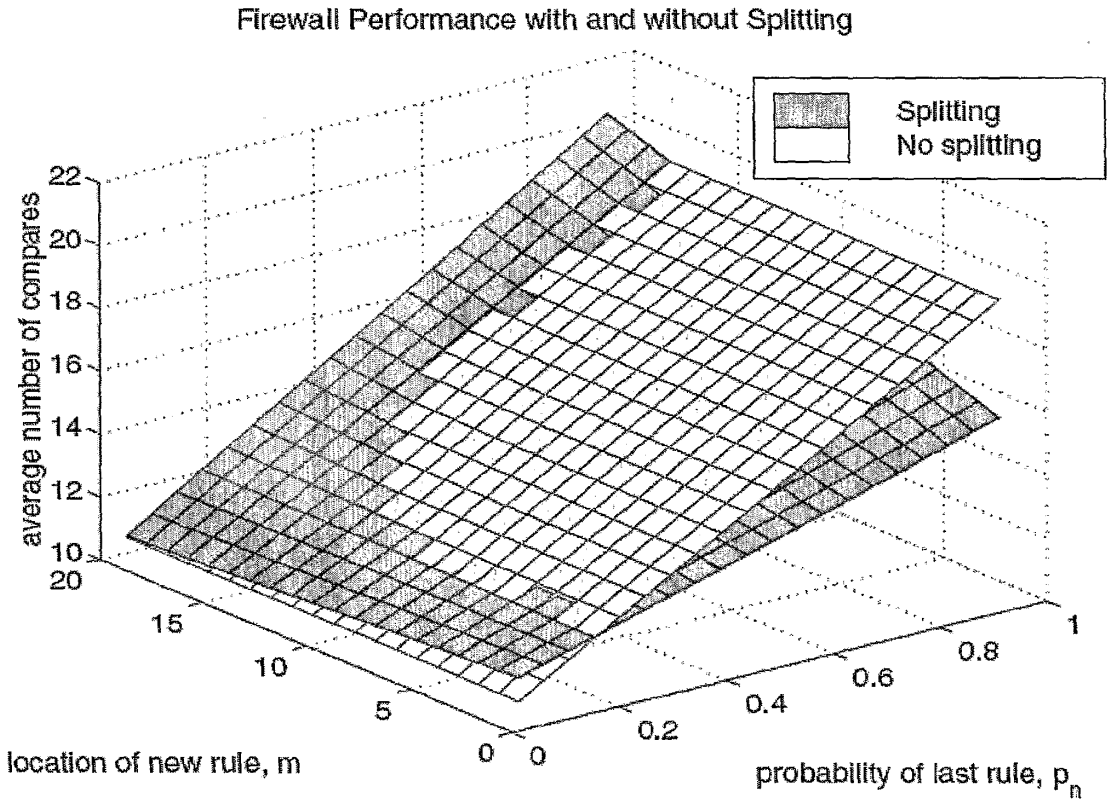

Firewall Performance with and without Splitting
Splitting
No splitting
average number of compares
22
20
18
16
14
12
10
20
15
10
5
0
location of new rule, m
0
0.2
0.4
0.6
0.8
1
probability of last rule, p_n

FIG. 8A

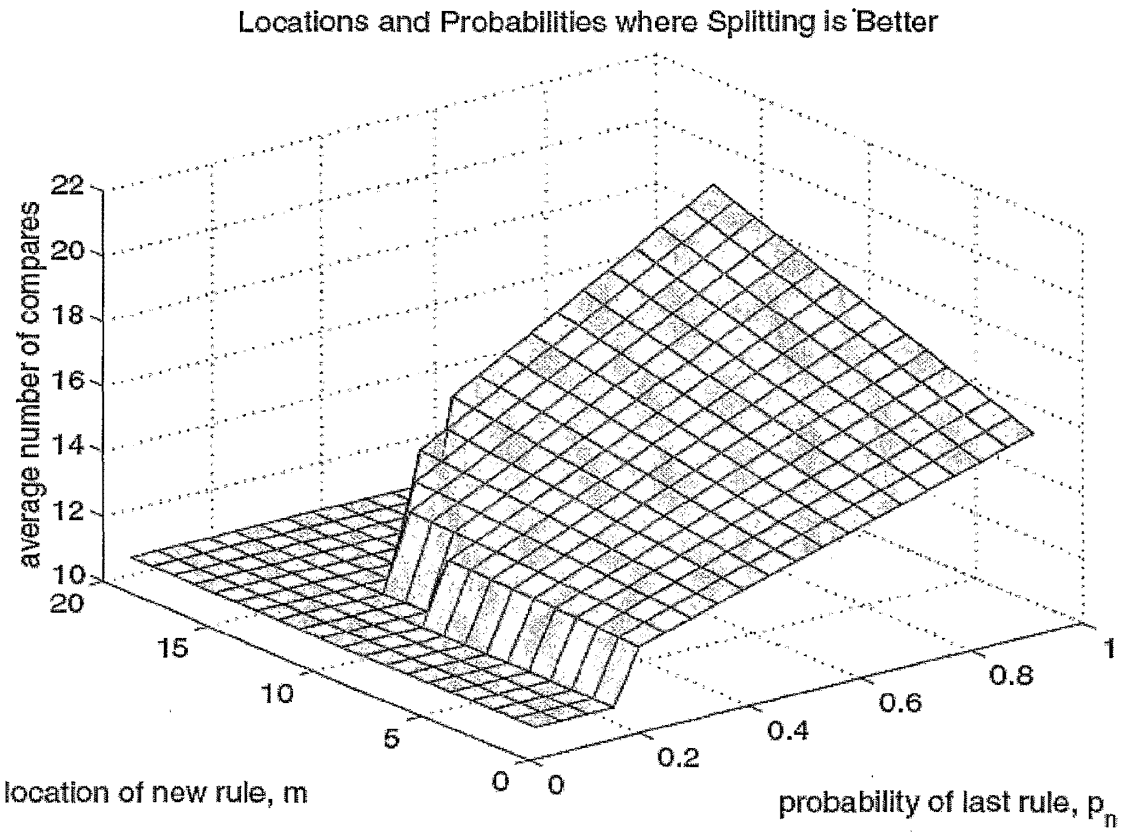

Locations and Probabilities where Splitting is Better
average number of compares
22
20
18
16
14
12
10
20
15
10
5
0
location of new rule, m
0
0.2
0.4
0.6
0.8
1
probability of last rule, p_n

FIG. 8B

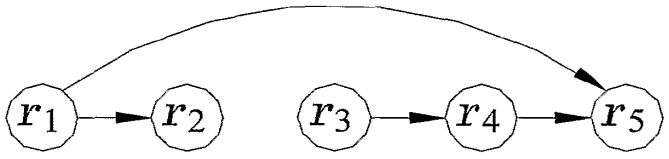


FIG. 9A

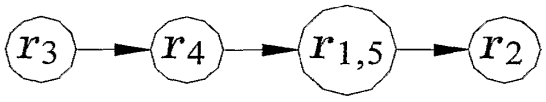


FIG. 9B

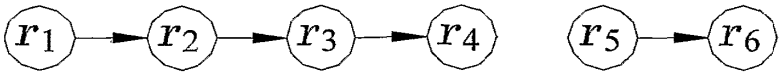


FIG. 10A

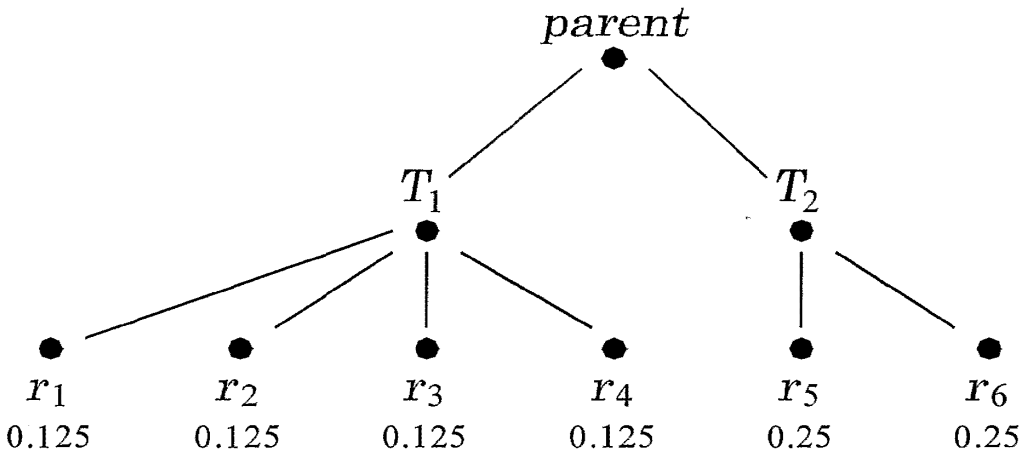


FIG. 10B

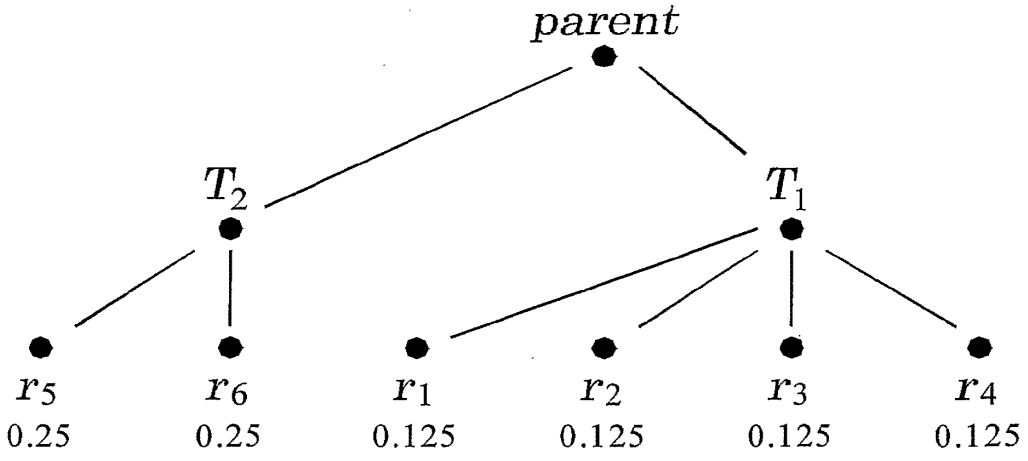


FIG. 10C

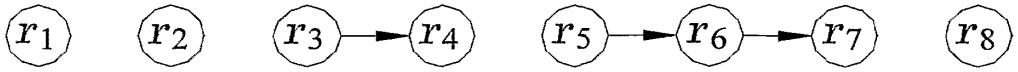


FIG. 11A

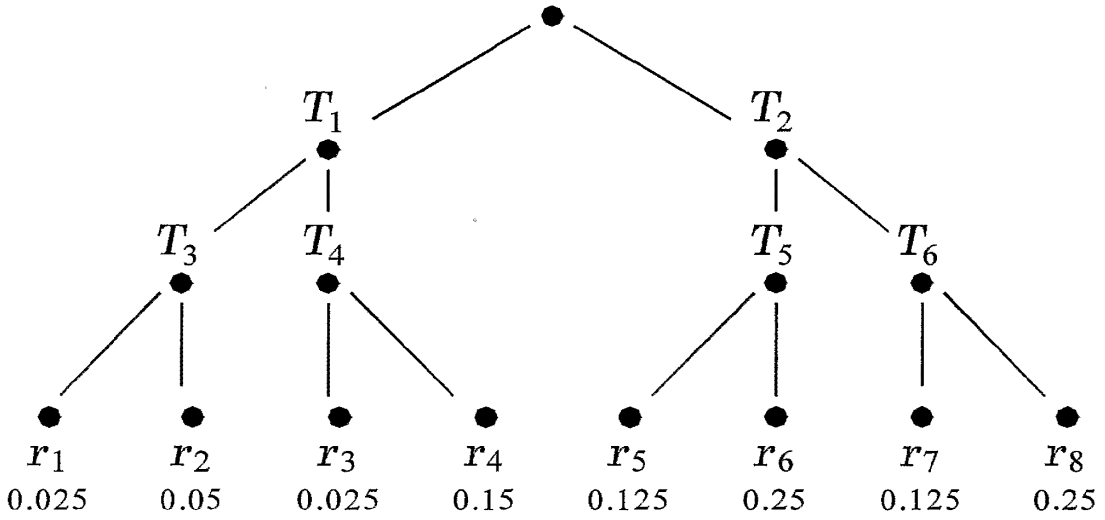


FIG. 11B

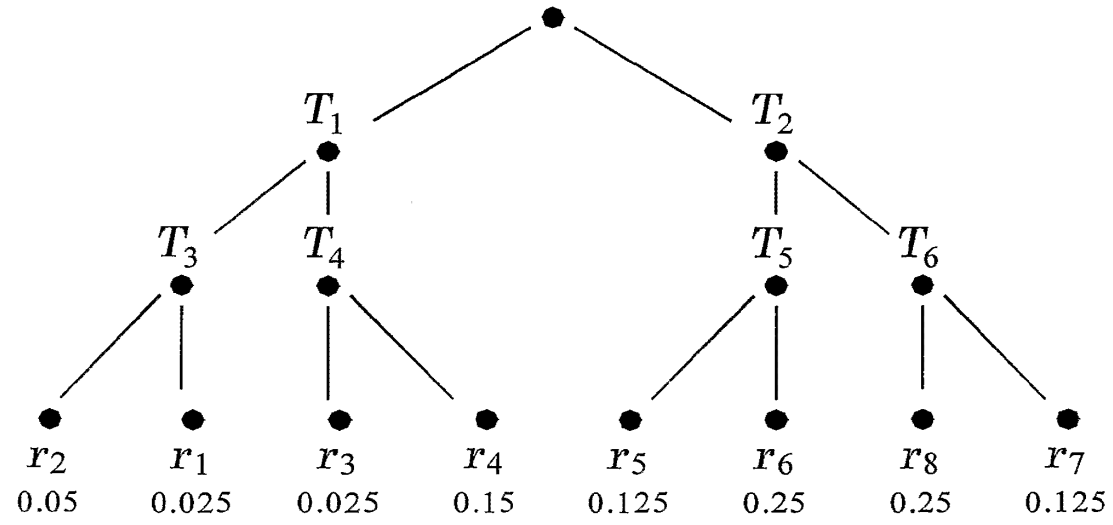


FIG. 11C

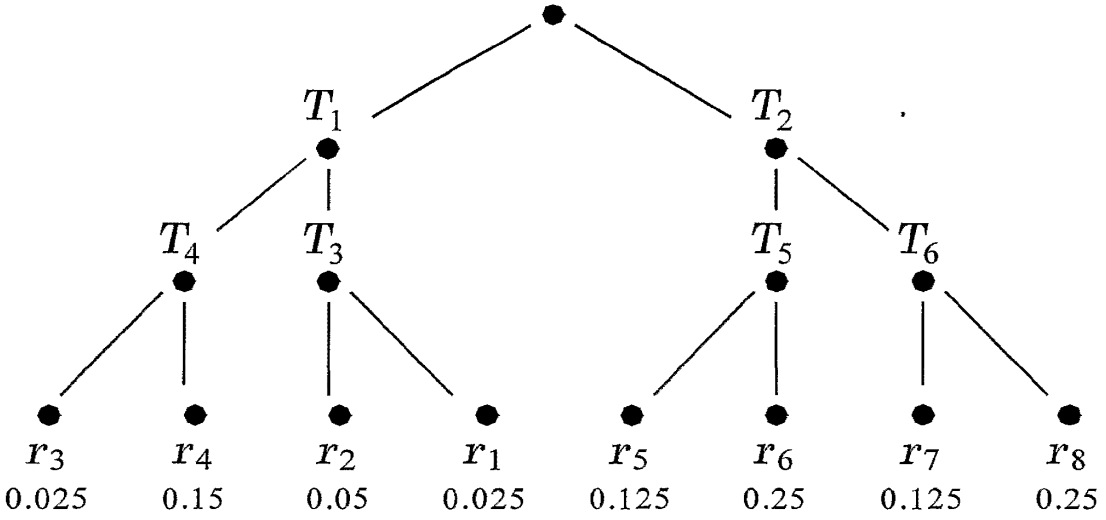


FIG. 11D

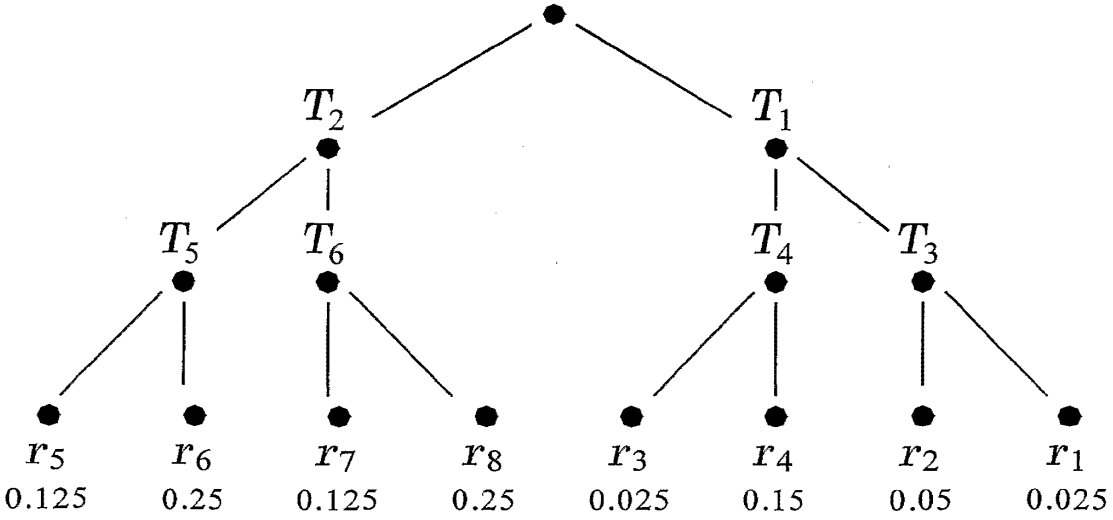


FIG. 11E

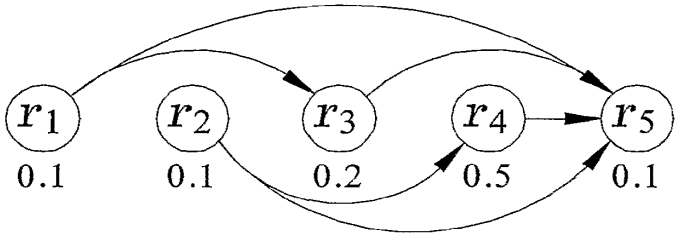


FIG. 12A

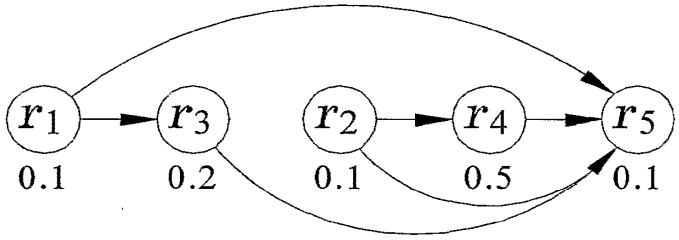


FIG. 12B

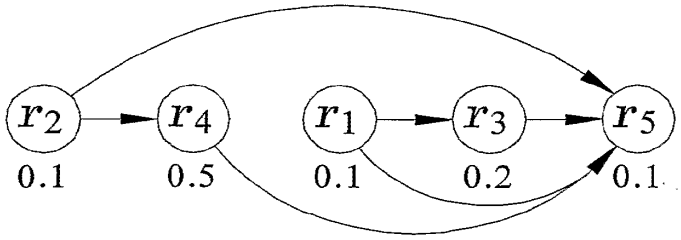


FIG. 12C

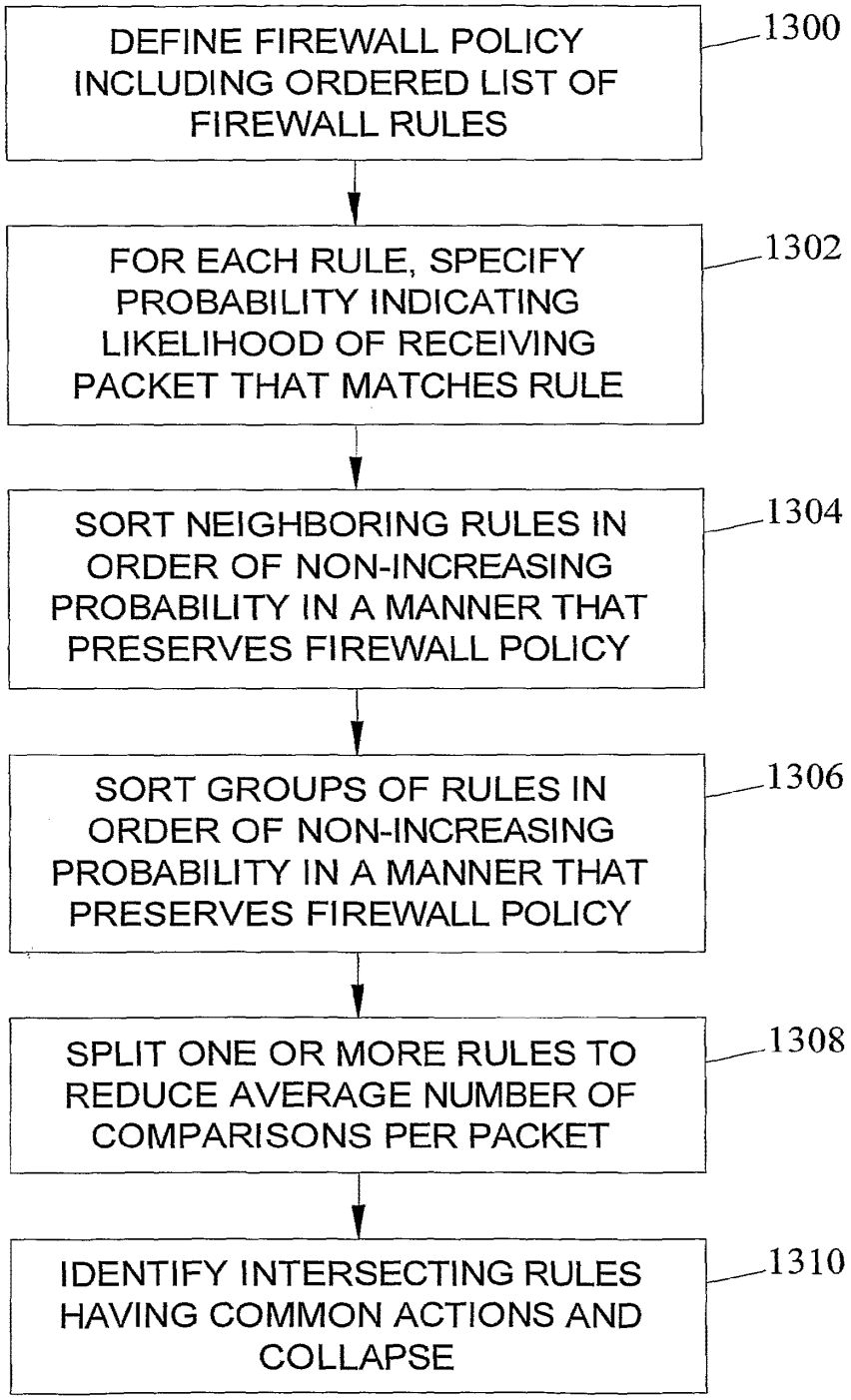

DEFINE FIREWALL POLICY INCLUDING ORDERED LIST OF FIREWALL RULES
1300
FOR EACH RULE, SPECIFY PROBABILITY INDICATING LIKELIHOOD OF RECEIVING PACKET THAT MATCHES RULE
1302
SORT NEIGHBORING RULES IN ORDER OF NON-INCREASING PROBABILITY IN A MANNER THAT PRESERVES FIREWALL POLICY
1304
SORT GROUPS OF RULES IN ORDER OF NON-INCREASING PROBABILITY IN A MANNER THAT PRESERVES FIREWALL POLICY
1306
SPLIT ONE OR MORE RULES TO REDUCE AVERAGE NUMBER OF COMPARISONS PER PACKET
1308
IDENTIFY INTERSECTING RULES HAVING COMMON ACTIONS AND COLLAPSE
1310

FIG. 13

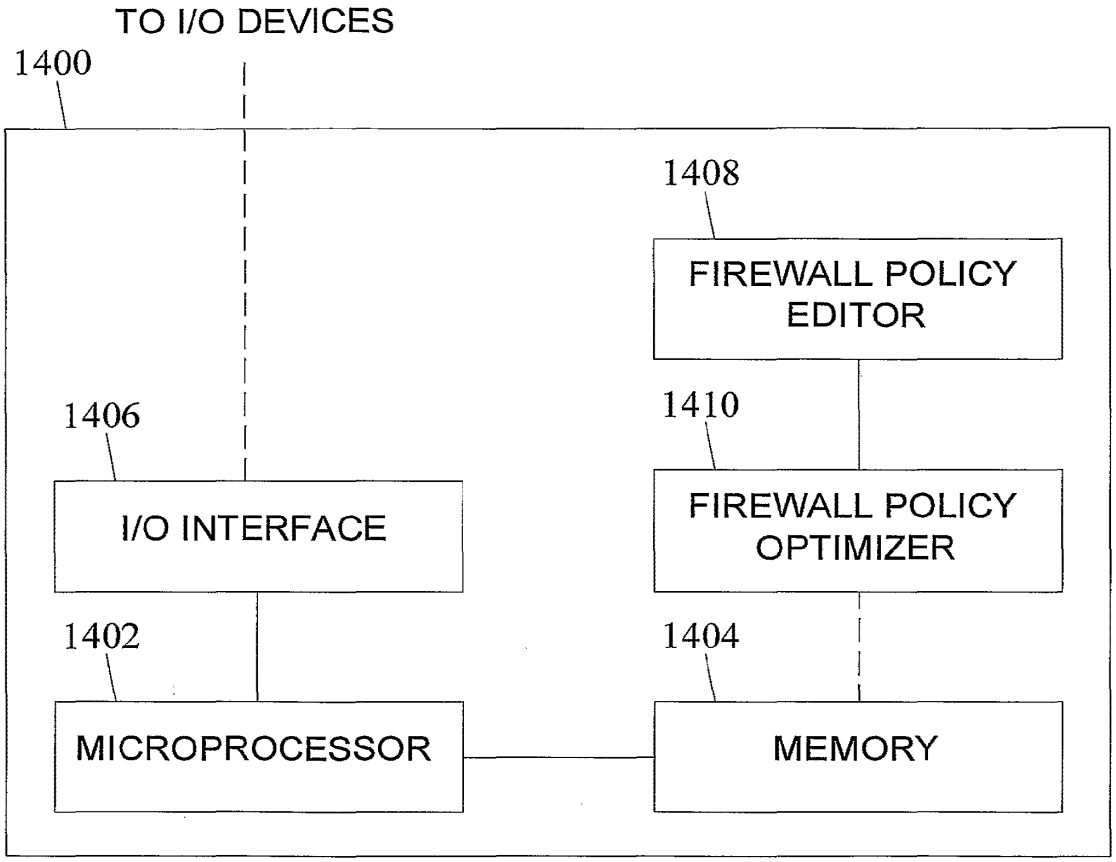

TO I/O DEVICES
1400
1408
FIREWALL POLICY EDITOR
1406
1410
I/O INTERFACE
FIREWALL POLICY OPTIMIZER
1402
1404
MICROPROCESSOR
MEMORY

FIG. 14

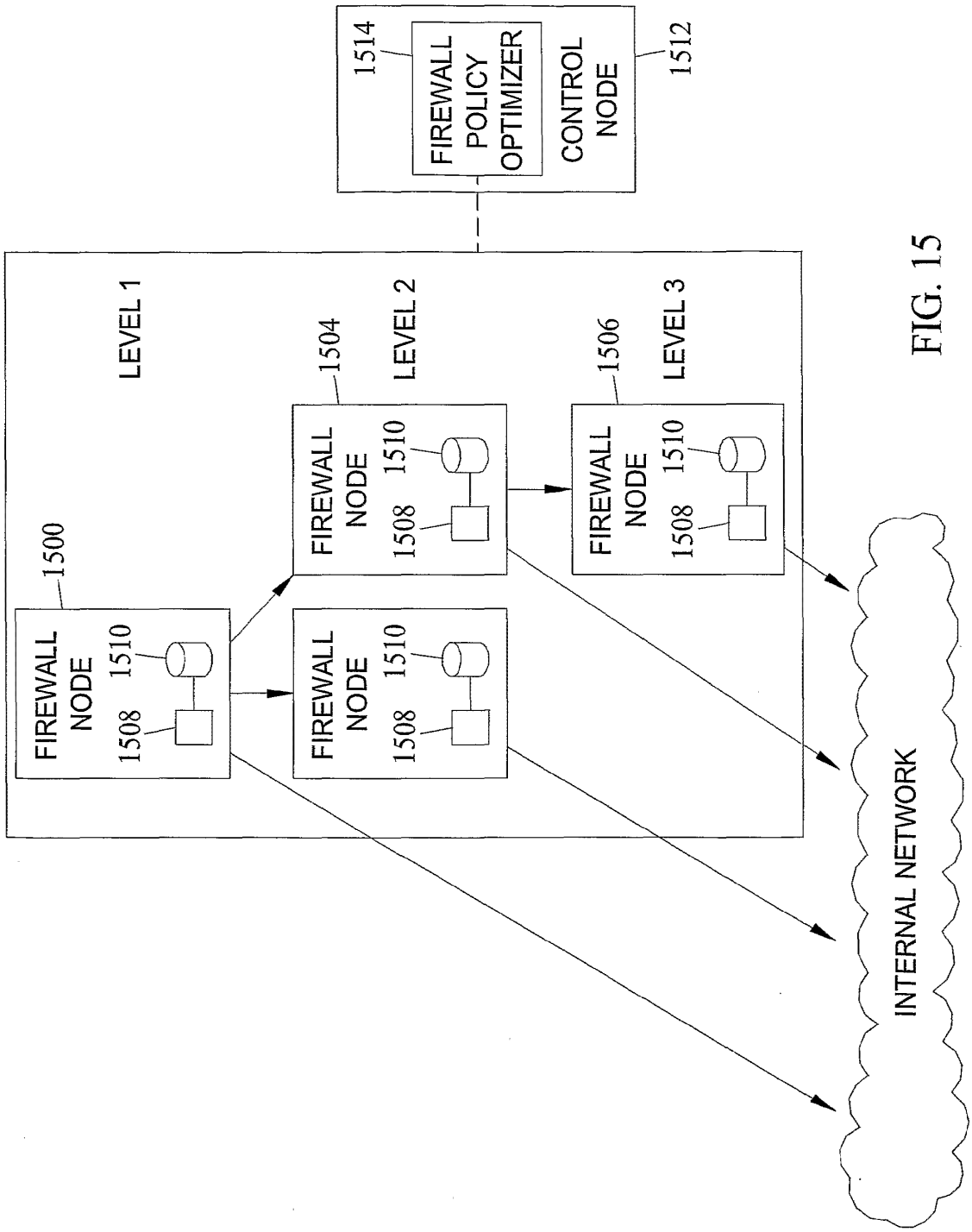

1514
FIREWALL POLICY OPTIMIZER
CONTROL NODE
1512
LEVEL 1
LEVEL 2
LEVEL 3
1500
1504
1506
FIREWALL NODE
1508
1510
INTERNAL NETWORK

FIG. 15

Espacenet

Bibliographic data: WO2006093557 (A2) — 2006-09-08

METHOD, SYSTEMS, AND COMPUTER PROGRAM PRODUCTS FOR IMPLEMENTING FUNCTION-PARALLEL NETWORK FIREWALL

Inventor(s): FULP ERRIN W [US]; FARLEY RYAN J [US] ± (FULP, ERRIN, W, ; FARLEY, RYAN, J)

Applicant(s): UNIV WAKE FOREST [US]; FULP ERRIN W [US]; FARLEY RYAN J [US] ± (WAKE FOREST UNIVERSITY, ; FULP, ERRIN, W, ; FARLEY, RYAN, J)

Classification: **- international:**
- cooperative: H04L63/0218; H04L63/0263

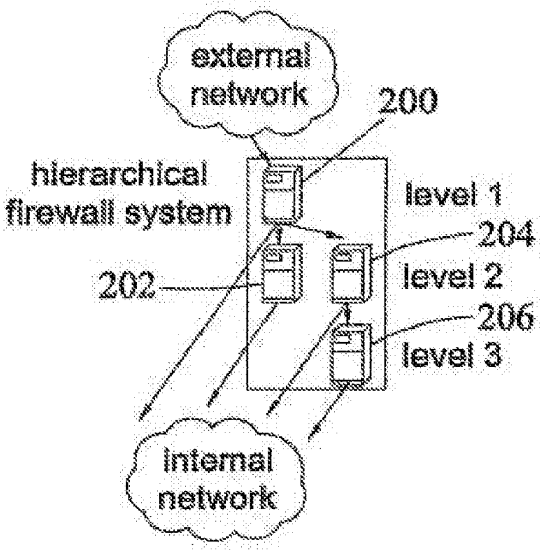
Application number: WO2005US47008 20051222

Priority number (s): US20040638436P 20041222

Also published as: WO2006093557 (A3) US2006195896 (A1) US8037517 (B2) EP1839188 (A2) EP1839188 (A4) more

Abstract of WO2006093557 (A2)

Methods, systems, and computer program products for providing function-paralell firewalls are disclosed. According to one aspect, a function-parallel firewall includes a first firewall node for filtering received packets using a first portion of a rule set including a plurality of rules. The first portion includes less than all of the rules in the rule set. At least one second firewall node filters packets using a second portion of the rule set. The second portion includes at least one rule in the rule set that is not present in the first portion. The first and second portions together include all of the rules in the rule set.



(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 September 2006 (08.09.2006)

PCT

(10) International Publication Number
WO 2006/093557 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/US2005/047008

(22) International Filing Date:
22 December 2005 (22.12.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/638,436 22 December 2004 (22.12.2004) US

(71) Applicant *(for all designated States except US)*: **WAKE FOREST UNIVERSITY** [US/US]; OFFICE OF TECHNOLOGY ASSET MANAGEMENT, WAKE FOREST UNIVERSITY HEALTH SCIENCES, 200 East First Street, Suite 101, Winston Salem, North Carolina 27101 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **FULP, Errin, W.** [US/US]; 308 N. Hawthorne Road, Winston-salem, North Carolina 27104 (US). **FARLEY, Ryan, J.** [US/US]; 212 Radford Street, Winston-salem, North Carolina 27106 (US).

(74) Agent: **HUNT, Gregory, A.**; JENKINS, WILSON & TAYLOR, P.A., SUITE 1400 UNIVERSITY TOWER, 3100 Tower Boulevard, Durham, North Carolina 27707 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

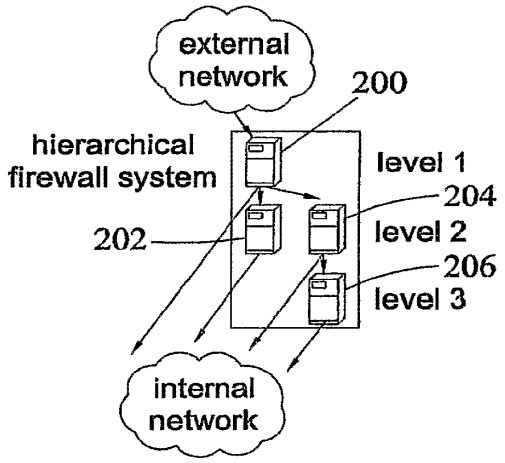
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD, SYSTEMS, AND COMPUTER PROGRAM PRODUCTS FOR IMPLEMENTING FUNCTION-PARALLEL NETWORK FIREWALL



(57) Abstract: Methods, systems, and computer program products for providing function-paralell firewalls are disclosed. According to one aspect, a function-parallel firewall includes a first firewall node for filtering received packets using a first portion of a rule set including a plurality of rules. The first portion includes less than all of the rules in the rule set. At least one second firewall node filters packets using a second portion of the rule set. The second portion includes at least one rule in the rule set that is not present in the first portion. The first and second portions together include all of the rules in the rule set.

WO 2006/093557 A2

DESCRIPTION

METHOD, SYSTEMS, AND COMPUTER PROGRAM PRODUCTS FOR IMPLEMENTING FUNCTION-PARALLEL NETWORK FIREWALL

RELATED APPLICATIONS

This application claims the benefit of U.S. Provisional Patent Application Serial No. 60/638,436, filed December 22, 2004; the disclosure of which is incorporated herein by reference in its entirety.

GOVERNMENT INTEREST

This invention was made with Government support under Grant No. DE-FG02-03ER25581 awarded by U.S. Department of Energy, Mathematical and Computational Information Sciences Division. The U.S. Government has certain rights in the invention.

TECHNICAL FIELD

The subject matter described herein relates to implementing network firewalls. More particularly, the subject matter described herein relates to methods, systems, and computer program products for implementing a function-parallel network firewall.

BACKGROUND ART

Firewalls remain the frontier defense for securing networks that are vital to private industry, government agencies, and the military. They enforce a security policy by inspecting and filtering traffic arriving at or departing from a secure network [3, 21, 22]. Meaningful inspections often involve a complex process, and if firewalls are to remain effective, they must adapt to constantly changing network demands, technology, and security threats.

As firewall technology evolves to meet new demands and threats, it must continue to act transparently to legitimate users, with little or no effect on the perceived network performance. The networks between two communicating machines should be invisible, especially if traffic requires specific network Quality of Service (QoS), such as bounds on the packet delay, jitter, and throughput. The firewall should process the legitimate traffic quickly, efficiently,

and never violate the desired QoS. Unfortunately, the firewall can easily become a bottleneck, given increasing traffic loads and network speeds [12, 14, 18, 20, 21]. Packets must be inspected and compared against complex rule sets and tables, which is a time-consuming process. In addition, audit files must be updated with current connection information. As a result, current firewalls have difficulty maintaining QoS guarantees. Since a firewall can be overwhelmed with traffic, it is also susceptible to Denial of Service (DoS) attacks [21]. Such attacks merely overload/saturate the firewall with illegitimate traffic. Audit files and state tables quickly fill available storage space and legitimate traffic queued behind suspicious traffic encounters long delays. Legitimate users notice poor network performance, and, in the worst case, the secure network is disconnected from the outside world.

Inspecting traffic sent between networks, a firewall provides access control, auditing, and traffic control based on a security policy [3, 21, 22]. The security policy is a list of ordered rules, as seen in Table 1, that defines the action to perform on matching packets. A rule r can be viewed as a k-tuple ($r[1]$, $r[2]$, $r[3]$, ..., $r[k]$), where $r[i]$ is specified as a variable length prefix.

No.	Proto.	Source		Destination		Action
		IP	Port	IP	Port	
1	TCP	140.*	*	*	80	accept
2	TCP	150.*	*	120	80	accept
3	TCP	140.*	*	130	20	accept
4	UDP	150.*	*	*	3030	accept
5	*	*	*	*	*	deny

Table 1: Example Security Policy Consisting of Multiple Ordered Rules

In the examples described herein, rules will initially be represented as the 5-tuple (protocol, IP source address, source port number, IP destination address, destination port number). Fields can be fully specified or contain wildcards '*' in standard prefix format. For example the prefix 192.* would represent any IP address that has 192 as the first dotted-decimal number. In addition to the prefixes, each filter rule has an action, which is to accept or deny. An accept action passes the packet into or from the secure network,

while deny causes the packet to be discarded. Rules are applied in order to every arriving packet until a match is found; otherwise, a default action is performed [21, 22].

Unfortunately, security policies may contain anomalies, such as a packet that matches multiple rules, where the matching rules specify conflicting actions. Security policy anomaly detection and correction is the subject of continued research [13, 21] and is not the focus of the present subject matter. Given the type of security policy required, rule sets can become quite large and complex. Security can be further enhanced with connection state and packet audit information. For example, a table can be used to record the state of each connection, which is useful for preventing certain types of attacks (e.g., TCP SYN flood) [21, 22].

Traditional firewall implementations consist of a single dedicated machine, similar to a router, that sequentially applies the rule set to each arriving packet. However, packet filtering represents a significantly higher processing load than routing decisions [15, 18, 22]. For example, a firewall that interconnects two 100 Mbps networks would have to process over 300,000 packets per second [21]. Successfully handling this high traffic becomes more difficult as rule sets become more complex [4, 14, 22]. Furthermore, firewalls must be capable of processing even more packets as interface speeds increase. In a high-speed environment (e.g. Gigabit Ethernet), a single firewall can easily become a bottleneck and is susceptible to DoS attacks [4, 7, 10, 12]. An attacker could simply inundate the firewall with traffic, delaying or preventing legitimate packets from being processed. Building a faster single firewall is possible [8, 15, 18, 19, 20]; however, the benefits are temporary (traffic loads and interface speeds are increasing); it is not scalable; it is a single point of failure; and it is generally not cost-effective for all installations.

A data-parallel firewall (or firewall sandwich) where each firewall node implements an entire firewall rule set is another approach to increase the speed of processing traffic [4, 12, 14, 22]. As shown in Figure 1, the system consists of multiple identical firewalls **100** connected in parallel. Each machine implements the complete security policy and arriving packets are distributed across the machines for processing in parallel [4]. A packet distributor **102**

implements a load balancing algorithm to distribute different packets to different firewall nodes. How the load-balancing algorithm distributes packets is vital to the system and is typically implemented as a high-speed switch in commercial products [11, 12]. Although data-parallel firewalls achieve higher throughput than traditional firewalls [4] and have a redundant design, they have difficulty maintaining QoS across networks. For example, legitimate traffic can encounter delays if it is queued behind traffic that requires more processing. Under these circumstances, users notice poor network performance, which is growing concern as more network applications require QoS assurances. Furthermore, stateful inspection requires all traffic from a certain connection or exchange to traverse the same parallel machine, which is difficult to perform at high speeds [14]. Therefore, new firewall architectures are needed to meet the demands of future networks and the challenges of increasing security threats.

SUMMARY

According to one aspect, the subject matter described herein includes a function-parallel firewall. The function-parallel firewall includes a first firewall node for filtering received packets using a portion of a rule set. The portion of the rule set may be less than all of the rules in the rule set. At least one second firewall node filters packets using at least one rule in the rule set that is not present in the portion implemented by the first firewall node. The first and second potions together include all of the rules in the rule set.

The term "firewall node," as used herein refers to a physical entity that implements one or more packet filtering rules. For example, a firewall node may be a single-processor computing device that implements the packet filtering rules. Alternatively, a firewall node may be a processor within a multi-processor computing device that implements one or more packet filtering rules. Thus, a multi-processor device may include multiple firewall nodes.

According to another aspect, the subject matter described herein includes a stateful function-parallel firewall system. The system includes a first function-parallel firewall subsystem including a plurality of firewall nodes implementing a first rule set for filtering packets arriving at a network. The first function-parallel firewall subsystem includes at least first and second firewall nodes respectively implementing first and second portions of the first rule set.

The first portion includes at least one rule that is not present in the second portion. A second function-parallel firewall subsystem includes a second set of firewall nodes. The second set of firewall nodes implements a firewall rule set for filtering packets departing from the network. The second function-parallel firewall subsystem includes at least third and fourth firewall nodes. The third and fourth firewall nodes implement at least one rule that is not present in the second portion of the second rule set. The function-parallel firewall subsystems share state information regarding connections established through the first and second sets of firewall nodes.

According to another aspect, the subject matter described herein includes a firewall grid. The firewall grid includes a plurality of firewall nodes that are physically connected to each other via a network for filtering packets. A controller controls logical connections between the firewall nodes. The controller is adapted to configure the firewall nodes in a logical firewall hierarchy without changing physical connections between the firewall nodes.

According to yet another aspect, the subject matter described herein includes a method for distributing rules in a function-parallel firewall. The method includes defining a rule set for a function-parallel firewall. The method further includes assigning rules in the rule set to nodes and branches in a trie data structure. Each node in the trie data structure corresponds to a data field and each branch represents a value for each data field to be compared to be values in corresponding fields of received packets. The trie data structure is pruned in a manner that preserves ordering of the rules in the rule set.

According to yet another aspect, the subject matter described herein includes a method for assigning rules to a plurality of firewall nodes. The method includes assigning rules to nodes in a directed acyclical graph (DAG). Relationships between rules are represented by edges in the DAG. Rules are distributed among a plurality of firewall nodes using the DAG in a function-parallel manner and such that relationships between the rules specified in the DAG are preserved.

As used herein, the term "firewall" refers to a logical entity that is adapted to filter packets at the ingress and/or egress portions of a network based on a policy. The term "firewall" is intended to include systems that block packets from entering or leaving a network and systems that perform intrusion

detection and intrusion protection functions for packets entering or leaving a network. Thus, the term "function-parallel firewall" is also intended to include an intrusion detection system or an intrusion protection system that operates in a function-parallel manner as described herein.

The subject matter described herein can be implemented using any combination of hardware, software, or firmware. In one exemplary implementation, the subject matter described herein may be implemented using a computer program product comprising computer executable instructions embodied in a computer readable medium. Exemplary computer readable media suitable for implementing the subject matter described herein include disk memory devices, chip memory devices, programmable logic devices, application specific integrated circuits, and downloadable electrical signals. In addition, a computer program product that implements the subject matter described herein may be located on a single device or computing platform or may be distributed across multiple devices or computing platforms.

One objective of the subject matter described herein is to provide a new security architecture, referred to herein as a hierarchical firewall, that provides the functionality of a traditional firewall (enforcing a security policy) and includes the following improvements:

1. **Suitable for high speed networks and scalable for large traffic loads**. Firewalls must continue to perform security tasks quickly and efficiently, appearing transparent to legitimate users under varying traffic loads.

2. **Maintains QoS requirements and traffic differentiation**. A growing number of network applications require QoS for their operation. Firewalls must not violate these guarantees while performing their security tasks.

3. **Greatly lessens the impact of DoS attacks**. Firewalls are candidates for DoS attacks, since they serve as the point of entry between two networks. New architectures must be capable of handling these new threats.

4. **Highly available**. Firewalls introduce a single point of failure between two networks. New firewall architectures must provide redundancy that prevents segmenting the secure network from the external network.

According to one aspect, the subject matter described herein includes a set of hierarchically configured computers that collectively enforce a desired security policy. Given this distributed configuration, traffic is quickly divided among the machines based on perceived threat. In one exemplary implementation, traffic that is considered safe may be promptly forwarded into the secure network, while the remaining traffic may be forwarded to different machines in the hierarchy for further scrutiny. Hence, traffic is segregated and queued based on security threat, yielding minimal delays for legitimate traffic. The system is also robust and highly available, since multiple machines are employed for the architecture and low cost, since Linux-installed PCs and open source software can be used for its implementation [21]. The proposed architecture is believed to be applicable to a wide variety of agencies in the public and private sectors.

The firewall architecture described herein will provide a scalable solution to varying traffic loads and QoS requirements, which are increasingly important as computing becomes more ubiquitous and applications become more diverse. The architecture is of interest to the networking community, since the architecture will result in new security policy models and optimization methods. The architecture is also relevant to the military and business community, since it provides a new, robust and cost-effective solution to security threats.

Some of the objects of the subject matter described herein having been stated hereinabove, and which are addressed in whole or in part by the subject matter described herein, other objects will become evident as the description proceeds when taken in connection with the accompanying drawings as best described hereinbelow.

BRIEF DESCRIPTION OF THE DRAWINGS

Preferred embodiments of the subject matter described herein will now be explained with reference to the accompanying drawings of which: