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 NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/728,766	12/27/2019	Steven Rogers	007742.00151\US	8018

22907 7590 11/30/2022

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

EXAMINER	
CHANG, KENNETH W	

ART UNIT	PAPER NUMBER
2438	

NOTIFICATION DATE	DELIVERY MODE
11/30/2022	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

GPD@bannerwitcoff.com
eofficeaction@bannerwitcoff.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

In re Patent No. 10,785,266	:	
Issue Date: September 22, 2020	:	
Application No. 16/728,766	:	
Filing or 371(c) Date: December 27, 2019	:	DECISION ON PETITION
Attorney Docket No. 007742.0011\US	:	
For: METHODS AND SYSTENS FOR PROTECTING A SECURED NETWORK	:	

This is a Notice regarding the request for acceptance of a fee deficiency submission under 37 CFR 1.28(c) filed July 11, 2022.

The Office no longer investigates or rejects original or reissue applications under 37 CFR 1.56. 1098 Off. Gaz. Pat. Office 502 (January 3, 1989). Therefore, nothing in this Notice is intended to imply that an investigation was done.

The fee deficiency submission under 37 CFR 1.28(c) is **ACCEPTED**. Accordingly, status as a small entity has been removed and any future fee(s) submitted must be paid at the undiscounted rate.

Telephone inquiries related to this communication should be directed to undersigned at (571) 272-1642.

/APRIL M WISE/
Paralegal Specialist, Office of Petitions

Document Code:WFEE

User :Gloria Arias

Sale Accounting Date:11/23/2022

Sale Item Reference Number	Effective Date
16728766	07/11/2022

Document Number	Fee Code	Fee Code Description	Amount Paid	Payment Method
I2022AM050203511	1461	1.28(C) SUBMISSIONS - APPLIC FILE FEE	$4,745.00	Deposit Account

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Steven Rogers et al.

Application No.: 16/728,766 Confirmation No.: 8018

Filed: December 27, 2019 Art Unit: 2438

For: METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK Examiner: K. W. Chang

NOTICE OF TEMPORARY LOSS OF ENTITLEMENT TO SMALL ENTITY STATUS AND PAYMENT OF DEFICIENCY OF FEES OWED

U.S. Patent and Trademark Office
Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Dear Sir:

In accordance with 37 C.F.R. § 1.28(c), Applicant recently realized that it was not entitled to small entity status at the time it made certain payments to the Office as noted in the table below, and Applicant submits this payment of deficiency of fees owed. The loss of entitlement to small entity status occurred prior to the earliest of the below-noted payments. Applicant's failure to previously notify the Office of the loss of entitlement to small entity status as required by 37 C.F.R. § 1.27(g)(2) occurred in good faith and without any deceptive intent.

Applicant regained entitlement to small entity status as of January 1, 2022, and Applicant claims small entity status as of that date and continuing through the present date.

As required by 37 C.F.R. § 1.28(c)(1) and (2), Applicant itemizes the deficiency of fees owed for the above-identified application as follows:

Type of Fee	Date Paid	Fee Paid	Current Fee	Deficiency Owed
Processing fee, except in provisional applications (Fee Code 2830)	12/27/2019	70.00	140.00	70.00
Each independent claim in excess of three (Fee Code 2201)	12/27/2019	230.00	480.00	250.00
Basic filing fee-Utility (Fee Code 4011)	12/27/2019	75.00	320.00	245.00
Utility Search Fee (Fee Code 2111)	12/27/2019	330.00	700.00	370.00
Utility Examination Fee (Fee Code 2311)	12/27/2019	380.00	800.00	420.00
Request for Prioritized Examination (Fee Code 2817)	12/27/2019	2000.00	4,200.00	2,200.00
Each claim in excess of 20 (Fee Code 2202)	12/27/2019	350.00 (7 extra claims at $50)	700.00 (7 extra claims at $100)	350.00
Submission of an Information Disclosure Statement (Fee Code 2806)	7/10/2020	120.00	260.00	140.00
Utility Issue Fee (Fee Code 2501)	8/20/2020	500.00	1,200.00	700.00
TOTAL		**4,055.00**	**8,800.00**	**4,745.00**

Total deficiency owed is $8,800.00 - $4,055.00 = $4,745.00

The Commissioner is authorized to charge the requisite fees owed to Deposit Account No. 19-0733.

If any other fees are required or if an overpayment is made, the Commissioner is authorized to debit or credit our Deposit Account No. 19-0733, accordingly.

Dated: July 11, 2022

Respectfully submitted,

By: /Scott M Kelly/
Scott M. Kelly
Registration No.: 65,121

BANNER & WITCOFF, LTD.
1100 13th St. NW
STE 1200
Washington, DC 20005
(202) 824-3000

Electronic Acknowledgement Receipt

EFS ID:	46155214
Application Number:	16728766
International Application Number:	
Confirmation Number:	8018
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	Scott M Kelly/Holly Parker
Filer Authorized By:	Scott M Kelly
Attorney Docket Number:	007742.00151\US
Receipt Date:	11-JUL-2022
Filing Date:	27-DEC-2019
Time Stamp:	12:05:36
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	Assertion of entitlement to small entity status	Notice_Of_Temporary_Loss_Of_Entitlement_To_Small_Entity_Status_And_Payment_Of_Defi_22003905.pdf	25672 a3d5fa07fb38b3e773ef289306122b34cab851ad	no	3

Warnings:

Information:	
Total Files Size (in bytes):	25672

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.

Trials@uspto.gov
571–272–7822

Paper 11
Entered: January 24, 2022

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PALO ALTO NETWORKS, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, INC.,
Patent Owner.

Case IPR2021-01154
Patent 10,785,266 B2

Before KEVIN F. TURNER, BRYAN F. MOORE, and LYNNE E. PETTIGREW, *Administrative Patent Judges*.

MOORE, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
37 C.F.R. § 42.108

I. INTRODUCTION

Palo Alto Networks, Inc. ("Petitioner") filed a Petition (Paper 2, "Pet.") requesting an *inter partes* review of claims 1–27 of U.S. Patent No. 10,785,266 B2 (Ex. 1001, "the '266 patent"). Centripetal Networks, Inc. ("Patent Owner") filed a Preliminary Response to the Petition. Paper 7 ("Prelim. Resp."). We have jurisdiction under 35 U.S.C. § 314, which provides that an *inter partes* review may not be instituted "unless . . . there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." 35 U.S.C. § 314(a). With our authorization, Petitioner filed a Preliminary Reply (Paper 8, "*Fintiv* Reply") and Patent Owner filed a Preliminary Sur-reply (Paper 9, "*Fintiv* Sur-Reply") to address Board discretion under 35 U.S.C. § 314(a).

For the reasons explained below, we do not institute an *inter partes* review in this proceeding.

A. *Real Parties in Interest*

Petitioner identifies itself as the sole real party-in-interest. Pet. 3. Patent Owner identifies itself as the sole real party-in-interest. Paper 4, 1 (Patent Owner's Mandatory Notices).

B. *Related Proceedings*

The parties indicate that the '266 patent is the subject of the following co-pending district court case: *Centripetal Networks, Inc. v. Palo Alto Networks, Inc.*, Case No. 2:21-cv-00137-RCY-RJK (E.D. Virginia). Pet. 3; Paper 4, 1. The Petition is related to the co-pending petition for *inter partes* review in IPR2021-01153, challenging U.S. Patent No. 10,567,437 B2.

C. *The '266 Patent*

The '266 patent discloses methods and systems for protecting a

secured network. Ex. 1001, code (57). Figure 1 illustrates a network environment that includes packet security gateways (PSGs) situated between networks and a security policy management server (SPMS) that communicates dynamic security policies to the PSGs. *Id.* at 4:59–5:10, 5:14–18, Fig. 1. "At each of the packet security gateways, a dynamic security policy may be received from the security policy management server, packets associated with a network protected by the packet security gateway may be received, and at least one of multiple packet transformation functions specified by the dynamic security policy may be performed on the packets." *Id.* at 3:60–4:1. "Performing the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets may include performing at least one packet transformation function other than forwarding or dropping the packets." *Id.* at 2:1–6.

The PSGs perform packet transformation functions on received packets according to rules in a dynamic security policy that specifies one or more packet transformation functions that should be performed on packets associated with specific criteria. *Id.* at 4:59–5:11, 6:24–28, 7:23–26.

> The specified criteria may take the form of a five-tuple of values selected from packet header information, specifying a protocol type of the data section of the IP packet (e.g., TCP, UDP, ICMP, or any other protocol), one or more source IP addresses, one or more source port values, one or more destination IP addresses, and one or more destination ports.

Ex. 1001, 7:26–32, Fig. 3.

Various combinations of rules may implement services, such as a blocklist service within a network environment that may include one or more rules specifying criteria for which associated packets should be blocked or

denied, and at least one rule specifying that all packets outside the blocked sets should be forwarded, accepted, or allowed. *Id.* at 8:23–44.

D. *Illustrative Claim*

Of the challenged claims 1, 8, 15, and 21 are independent. Claim 1 is illustrative and is reproduced below.

> 1. A method of filtering packets at a packet security gateway, of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway and one or more networks other than the network protected by the packet security gateway, the method comprising:
>
> receiving, by the packet security gateway and from a security policy management server external from the network protected by the packet security gateway, a dynamic security policy comprising a first set of packet filtering rules to be applied to all network traffic traversing the boundary, wherein
>
> each packet filtering rule of the first set of packet filtering rules comprises at least one packet matching criterion and a corresponding packet transformation function, and
>
> one or more first packet filtering rules of the first set of packet filtering rules comprise packet matching criteria corresponding to one or more network addresses and were automatically created or altered by the security policy management server based on aggregated malicious traffic information received from at least one third party malicious host tracker service located in the one or more networks other than the network protected by the packet security gateway, that comprises network addresses that have been determined, by the at least one third party malicious host tracker service, to be associated with malicious network traffic;
>
> performing, on a packet by packet basis, packet filtering on a first portion of packets corresponding to network traffic traversing the boundary via the packet security gateway based on the first set of packet filtering rules by performing at least one packet transformation function specified by at least one packet

filtering rule of the first set of packet filtering rules on the first portion of packets;

receiving, by the packet security gateway and after performing packet filtering on the first portion of the packets, an updated second set of packet filtering rules for the dynamic security policy from the security policy management server, wherein the updated second set of packet filtering rules comprises an update to the one or more first packet filtering rules created or altered by the security policy management server based on updated malicious traffic information received from the at least one third party malicious host tracker service; and

performing, on a packet by packet basis, packet filtering on a second portion of the packets corresponding to network traffic traversing the boundary via the packet security gateway based on the updated second set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the second set of packet filtering rules on the second portion of packets.

Ex. 1001, 20:64–21:52.

E. *Evidence of Record*

Petitioner cites the following references in its challenges to patentability:

Reference	Designation	Exhibit No.
U.S. Patent Appl. Publ. No. 2007/0262741 A1	Jungck	Ex. 1051
U.S. Patent Appl. Publ. No. 2007/0097976 A1	Wood	Ex. 1052
U.S. Patent Appl. Publ. No. 2009/0249482 A1	Sarathy	Ex. 1063

Pet. 5–6.

Petitioner also relies on the Declaration of Dr. Vijay Madisetti (Ex. 1004, the "Declaration").

F. *Asserted Grounds of Unpatentability*

Petitioner asserts the following grounds of unpatentability (Pet. 6):

Challenged Claims	Basis	References
1–27	§ 103[1]	Jungck, Wood
1–27	§ 103	Jungck, Sarathy, Wood

II. ANALYSIS

A. Level of Ordinary Skill in the Art

Noting that relevant experience and education can substitute for each other, Petitioner states that a person of ordinary skill in the relevant art on October 22, 2012 (the filing date of the application that matured in the '266 patent), would have had a bachelor's degree in computer science, computer engineering, or an equivalent, four years of professional experience, and a working knowledge of packet-switched networking, firewalls, security policies, communication protocols and layers, and the use of customized rules to address cyber-attack. Pet. 18 (citing Ex. 1004 [Declaration of Dr. Vijay Madisetti] ¶¶ 34–36). Petitioner's definition of a person of ordinary skill, which Patent Owner does not dispute at this stage, appears appropriate for the technology addressed by this proceeding.

[1] The Leahy-Smith America Invents Act ("AIA"), Pub. L. No. 112-29, 125 Stat. 284, 285–88 (2011), revised 35 U.S.C. § 103 effective March 16, 2013. Because the '266 patent has an effective filing date prior to the effective date of the applicable AIA amendment, we refer to the pre-AIA version of § 103.

B. Claim Construction

We construe the challenged claims by applying "the standard used in federal courts, in other words, the claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. [§] 282(b), which is articulated in *Phillips* [*v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc)]." 37 C.F.R. § 42.100(b) (2020). Under *Phillips*, the words of a claim are generally given their "ordinary and customary meaning," which is the meaning they would have to a person of ordinary skill in the art at the time of the invention, in light of the specification and prosecution history. *See Phillips*, 415 F.3d at 1312–13.

Petitioner asks the Board to adopt constructions from prior IPRs challenging related patents. Pet. 19–20. Petitioner does not explain the necessity of these constructions, nor does Patent Owner dispute them. *Id.*; *see generally* Prelim. Resp. Because we decline to institute on the basis of other claim limitations, we do not adopt Petitioner's proposed constructions.

Patent Owner requests that the preamble of independent claims 1, 8, and 15 be treated as limiting. Prelim. Resp. 16–17. These preambles provide antecedent basis for "packet security gateway," "boundary," "network," and "one or more other networks." *Id.* at 16 (citing Ex. 1001, 20:64–21:2, 22:13–18, 23:35–42). The preambles also recite the "plurality of packet security gateways that collectively provide an entire interface across a boundary of a [protected] network," which is "essential to understand" the "all traffic" limitation in the body of these claims and thus "'give life, meaning, and vitality'" to the claims. *Id.* (citing *Catalina Mktg. Int'l, Inc. v. Coolsavings.com, Inc.*, 289 F.3d 801, 808 (Fed. Cir. 2002) (citation omitted)).

The preambles provide the context for the body of the independent claims by defining the arrangement of the "plurality of packet security gateways" relative to the "boundary" of the protected network and thus the basis for applying "packet filtering rules . . . to all network traffic traversing the boundary." *Id.* (citing Ex. 1001, 20:64–21:8). The "entire interface" limitation also was relied on during prosecution of the parent '437 Patent's claims to distinguish them from the prior art. *Id.* at 16–17 (citing Ex. 2008, 254–61; *Catalina*, 289 F.3d at 808–09). Petitioner does not dispute the preambles are limiting. Pet. 18–21, 37. For, the reasons above, we construe the preambles of independent claims 1, 8, and 15 as limiting.

After review of the current record, we conclude that, other than determining the preambles are limiting, no express claim construction is necessary to determine whether to institute review of the challenged claims. *See, e.g.*, *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)) ("[W]e need only construe terms 'that are in controversy, and only to the extent necessary to resolve the controversy.'").

C. Principles of Law

A patent claim is unpatentable under 35 U.S.C. § 103 if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. *KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations including: (1) the scope and content of the prior art;

(2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) objective evidence of nonobviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

In that regard, an obviousness analysis "need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ." *KSR*, 550 U.S. at 418; *see also In re Translogic Tech., Inc.*, 504 F.3d 1249, 1259, 1262 (Fed. Cir. 2007) (quoting *KSR*, 550 U.S. at 418).

The level of ordinary skill in the art may be reflected by the prior art of record. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001); *In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995); *In re Oelrich*, 579 F.2d 86, 91 (CCPA 1978).

D. Obviousness of Claims over Jungck and Wood

Petitioner asserts that claims 1–27 are unpatentable under 35 U.S.C. § 103(a) as obvious over Jungck and Wood. Pet. 6. To support its contentions, Petitioner provides explanations as to how the prior art allegedly teaches each claim limitation. *Id.* at 21–65. For convenience, all references cited in the grounds of the Petition are summarized below.

1. Jungck (Ex. 1051)

Jungck discloses a packet interceptor apparatus that applies to intercepted packets one or more rules that execute one or more functions on a dynamically specified portion of the packet, and takes one or more actions with the packets. Ex. 1051, code (57). Jungck states that "[t]he apparatus is capable of analyzing any portion of the packet including the header and the

payload," and that the actions "include releasing the packet, logging/storing information about the packet or forwarding the packet to an external device for subsequent processing." *Id.* Jungck's rules may be "dynamically modified" by the external devices. *Id.*

2. Wood (Ex. 1052)

Wood is directed to improved network security by "provid[ing] real-time detection and diagnostic information" on suspect or malicious traffic associated with possible network threats. Ex. 1052 ¶ 6, code (57). Wood teaches a router and an interrogation module that detects and redirects traffic associated with one or more suspect network addresses. *Id.* ¶ 7.

Wood discloses an adaptive interrogation module 204 that is located within a protected subnetwork 202, or remotely connected; and a router 212 that is configured to redirect suspect traffic to the adaptive interrogation module for analysis. *Id.* ¶¶ 32, 40. The adaptive interrogation module 204 receives suspect addresses 206 (e.g., a suspect address list that includes "IP addresses of known threats") from one or more suspect address sources 210 that are external to the protected network. *Id.* ¶¶ 29, 32–33. Using the suspect addresses 206, the adaptive interrogation module 204 configures or reconfigures a router 212 to redirect potentially malicious traffic associated with the suspect addresses, for example, to a null address to effectively block the traffic. *Id.* ¶¶ 21, 32, 34.

Wood discloses updating the suspect addresses 206 "as any one of the suspect address sources 210 receives a change to its suspect address data (e.g., a new IP address block is legitimately allocated . . . or a new hacker site is identified)." *Id.* ¶¶ 34–36.

3. Sarathy (Ex. 1063)

Sarathy (Ex. 1063) teaches a threat management facility (purple) having "policy management facility 112 . . . to update the policies of all corporate computing assets," including access permissions, of an enterprise network 102. Ex. 1063 ¶¶ 34, 37–38, 45. Access permissions are stored as block lists, black lists, allowed lists, or white lists. *Id.* ¶ 45, Fig 1. Threat management facility, including policy management facility, is "integrated into a third-party product," where the enterprise "subscribe[s] to services through the third-party product, and threat protection to the enterprise may be provided by the threat management facility 100 through the third-party product." *Id.* ¶ 38.

4. Claim 1

> *"A method of filtering packets at a packet security gateway, of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway . . . comprising: a first set of packet filtering rules to be applied to all network traffic traversing the boundary. . ."*

a. Petitioner's Contentions

Petitioner relies only on Jungck for this limitation. Pet. 37–46. Petitioner relies on Jungck's disclosure of ingress filtering at plurality of edge servers 602A, 602B (packet security gateways) to provide the claimed "an entire interface across a boundary of a network protected by the packet security gateway" (hereinafter, the "entire boundary" limitation). *Id.* at 37–38. For example, Petitioner contends Jungck discloses "intercept[ing] all network traffic flowing between the POP's 114, 116 and the network 100" and "isolating the core infrastructure and servers of the network/internet

from the edge where the clients are located" across a boundary (e.g., POPs 114, 116) of a network protected by the packet security gateway (e.g., "network 100," which is a "private network") and one or more networks other than the network protected by the packet security gateway (e.g., "client 102," which is a "private network . . . coupled with the network 100"). *Id.* (citing Ex. 1051 ¶¶ 31, 38, 39, 41, 107, 113, 116, Figs 1, 6).

Petitioner also relies on Jungck's rule set 726 to show a first set of packet filtering rules. *Id.* at 41–42. Petitioner contends edge server 602 is provided with "one or more rules 732 which are applied" to "all network traffic," thus meeting the limitation of "all network traffic traversing the boundary" (hereinafter the "all traffic" limitation). *Id.* at 41–42 (citing Ex. 1051 ¶¶ 107, 111). As such, Petitioner contends Jungck discloses edge servers that "intercept all network traffic" and monitor it for "malicious program code" using rules. *Id.* at 42 (citing Ex. 1051 ¶¶ 107, 111). Petitioner also contends device 900 performs "ingress and egress filtering" on packets entering (*i.e.*, ingress) and leaving (*i.e.*, egress) the protected network. *Id.* at 43–44 (citing Ex. 1051 ¶ 269). Petitioner also contends collateral estoppel applies based on determinations made in IPR2018-01443, 1444, 1513 (the "'1443 IPR," "'1444 IPR," and '1513 IPR," respectively). *Id.* at 39, 42.

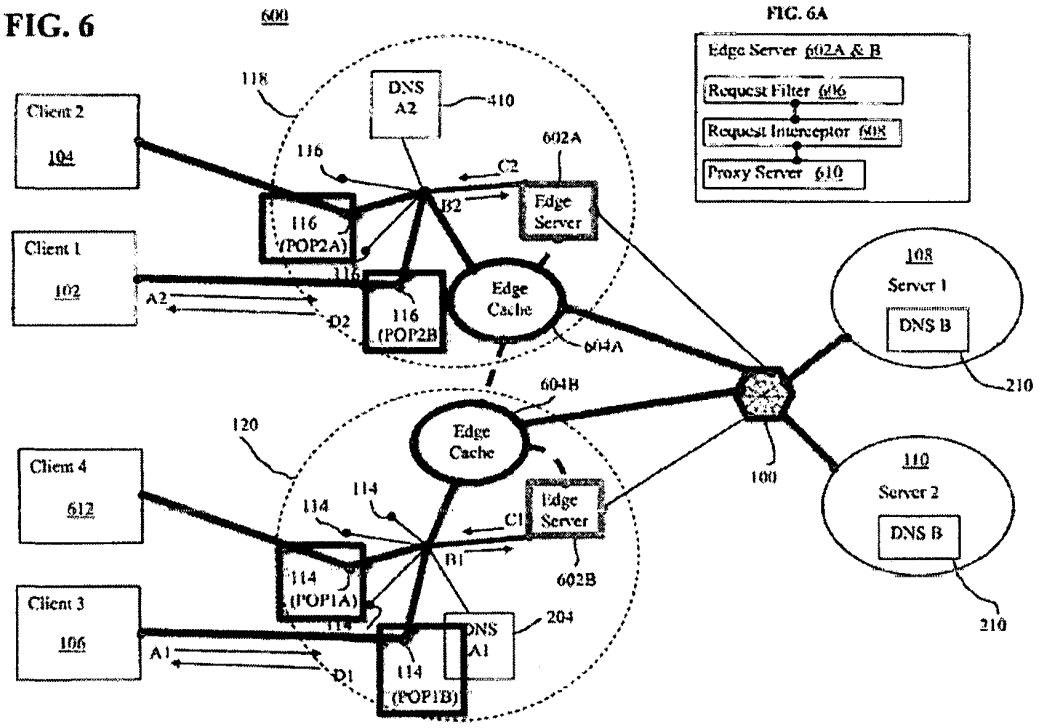
b. Patent Owner's Arguments

i. Petitioner Disregards "Edge Caches"

Patent Owner argues that "Petitioner's obviousness grounds disregard the role of *Jungck's* edge caches, which are located in network paths that

bypass the edge servers entirely." Prelim. Resp. 33.[2] We agree. In fact, Petitioner avoids reciting the words "edge cache" anywhere in the Petition. *See generally* Pet. Additionally, although Petitioner's declarant uses quotes from Jungck that recite the "edge cache," the Petition removes those references. *Compare* Ex. 1004 ¶ 221 *with* Pet. 41; *see also* Prelim. Resp. 33–34 (listing citations in the Petition that omit the term edge cache).

Patent Owner argues Jungck teaches network paths that bypass its edge servers when carrying network traffic through the POPs as shown in the annotated version of Figure 6 of Jungck. Ex. 1051, Fig. 6.



[2] We do not address Patent Owner's argument that "*Jungck* fails to disclose 'packet filtering rules to be applied to all network traffic traversing the boundary' because the client requests disclosed in *Jungck* never traverse the boundary at all." Prelim Resp. 39–40.

Patent Owner's annotated Figure 6 above, shows network paths (**red**) exist between Jungck's clients 102–106 and 612, POPs 114 and 116 (**purple**), routing equipment (206 in Figure. 5), edge caches 604A–B, network 100, and servers 108, 110—all of which Patent Owner argues bypass Jungck's edge servers (**green**). Prelim. Resp. 35 (citing Ex. 1051 ¶ 107 ("edge cache 604A, 604B coupled with the routing equipment 206"), Fig. 6). Thus, according to Patent Owner, Petitioner fails to show "an entire interface across a boundary of a network," because "*Jungck* describes network paths across the alleged 'boundary' that bypass *Jungck's* edge servers, demonstrating that the edge servers do not form the 'entire interface' across the alleged boundary." Prelim. Resp. 34. We find that Petitioner does not adequately explain the working of that boundary because it chooses not to explain or discount the contribution of the edge caches. Additionally, to the extent that this is explained in any related IPRs, Petitioner does not cite to any such explanation.

As to whether Petitioner has shown that Jungck teaches the limitation of "all network traffic traversing the boundary," Patent Owner asserts that there are pathways for content that do not include the edge server. Prelim. Resp. 34, 41. For example, Patent Owner asserts Jungck's edge servers redirect clients to request content from the edge caches or send content request packets to the edge caches for handling. *Id.* at 34, 41 (citing Ex. 1051 ¶¶ 69, 74, 95 ("[T]his effectively redirects the client 102, 104 to make all of its content requests from the edge cache" . . . "edge cache . . . attempt[s] to satisfy content requests from its cache storage"), 109 ("requests will be redirected and served from the edge cache 604"), 113).

Patent Owner also argues that "after a client request[s] content from server 108, the edge server translates server 108's domain name into the IP address of the edge cache so that the client communicates directly with the edge cache instead of either the edge server or server 108." *Id.* at 36 (citing Ex. 1051 ¶¶ 95, 111); *see Fintiv* Sur-Reply 9.[3] In sum, Patent Owner asserts "[t]here are many circumstances in which traffic bypasses the edge servers via the edge caches." Prelim. Resp. 35–36.

We agree with Patent Owner that the Petition's avoidance of the operation of edge caches when edge caches are important in the processing of traffic flowing across the boundary undermines this ground of the Petition. If Petitioner wished to rely on an embodiment or configuration in which the edge caches were irrelevant, the edge caches were redundant to the edge server, or the edge caches were unnecessary, it was incumbent upon Petitioner to explain sufficiently how and why that was the case. Petitioner was aware of the edge caches because it appears to have omitted all references to them in the Petition yet did not explain why this was done.

Additionally, although Petitioner's declarant does include references to edge caches, its declarant also does not explain sufficiently the relevance of those edge caches. Ex. 1004 ¶¶ 148, 212, 214, 215, 227, 323. Additionally, Petitioner's references to collateral estoppel do not relieve Petitioner from the burden to describe its contentions regarding obviousness in the Petition.

[3] Patent Owner also relies on Jungck's treatment of a cache miss. Because Patent Owner's other evidence is sufficient we do not rely on Patent Owner's arguments regarding a cache miss. *See* Prelim. Resp. 42.

ii. Petitioner's Reliance on Device 900 is Insufficient

Patent Owner also argues Petitioner's apparent alternative reliance on the fifth embodiment of Jungck is insufficient to cure the deficiencies of its other contentions as to the "all traffic" limitation. Prelim. Resp. 43. For example, as explained above, Petitioner's analysis of the "all traffic" limitation also mentions "ingress and egress filtering" and the use of "blocklists" by Jungck's fifth embodiment.[4] Pet. at 43–44 (citing Ex. 1051 ¶ 269). Specifically, Petitioner's complete contention is that:

> **Jungck** discloses device 900, coupled to network 100 (*e.g.*, upstream network 100A and downstream network 100B), which includes primary processing elements 904A and 904B that "may be consolidated into a single processing element." Jungck, [0266], [0268]. Elements 904A/904B perform "ingress and egress filtering" on packets entering (*i.e.*, ingress) and leaving (*i.e.*, egress) the protected network. Jungck, [0269]. Device 900 maintains "block lists" that include a range of network addresses of upstream and downstream network devices. Jungck, [0269]. The network addresses of incoming packets are compared to the "block lists" and filtered out of the packet stream if they are "out of range." Jungck, [0269]. A POSITA would have understood that all packets entering or leaving the protected network would be compared against the blocklists (or another rule) to "ensur[e] that packets arriving from a particular portion of the network actually came from that portion of the network," or at minimum would have found that to have been obvious, because applying filtering rules to all packets entering and leaving a network was well-known, and a POSITA would have been motivated to apply filtering rules to all such packets to prevent malicious intrusions into the network, and to block devices inside the network from accessing known malicious sites or devices outside of the network. Jungck, [0269]; Madisetti, ¶¶238-241.

[4] We note that Petitioner does not cite to the fifth embodiment to meet the "entire boundary" limitation. *See* Pet. 37–41.

Id.

Patent Owner argues the discussion quoted above regarding device 900 is untethered to the claim language and only describes filtering packets within network 100, and not traversing any network boundary. Prelim. Resp. 43 (citing Ex. 1051 ¶¶ 108, 112, 269, Fig. 9). Patent Owner also argues that paragraph 269 from Jungck, cited by Petitioner, merely discusses filtering packets by a single device ("device 900") that "intercept[s] and process[es]" all packets that the device happens to receive, not "all packets entering and leaving" Jungck's network as a whole. *Id.* at 43 (citing Ex. 1051 ¶¶ 266, 268). We agree with both arguments.[5] The discussion of device 900 above is not tied to the rules and filtering done by the edge servers on which Petitioner relies.

iii. Petitioner's Reliance on "All Traffic" Being "Well Known" is Insufficient

We find Petitioner's discussion of device 900 quoted above appears to be presented as support for the proposition that "applying filtering rules to all packets entering and leaving a network" was "well-known." Pet. 44 (citing Ex. 1051 ¶ 269). In further support of that proposition, Petitioner states also that "POSITA would have been motivated to apply filtering rules to all such packets to prevent malicious intrusions into the network, and to block devices inside the network from accessing known malicious sites or devices outside of the network." *Id.* We are not persuaded by this contention.

[5] We find not that Petitioner fails to provide a rationale to combine or motivation to combine, but rather that Petitioner fails to explain sufficiently how device 900 relates to the specific limitations of the claims.

Whether or not this was known as a general proposition does not address reasons why Jungck's traffic appears to bypass the edge servers upon which Petitioner relies and why a person of ordinary skill would have modified Jungck's operation to apply its rules to all traffic or why a person of ordinary skill would have modified Jungck's operation to use device 900 instead of the edge servers and what effect that would have on the rest of the operation of Jungck. Also, Petitioner does not rely on device 900 to meet the "entire boundary" limitation. *See* Pet. 37–41.

Petitioner also appears to rely on its declarant who testifies it was well-known to block all incoming traffic. *Fintiv* Reply (citing Ex. 1004 [Declaration of Dr. Vijay Madisetti] ¶¶ 72–73). Nevertheless, this section of the Declaration was not cited in the Petition but rather is referred to indirectly in a portion of the Declaration which *is* cited in the Petition. Pet. 44 (citing Ex. 1004 ¶ 241). Paragraph 241 of the Declaration states "*as discussed in Section IV*, applying filtering rules to all packets entering and leaving a network was well-known," but does not refer to paragraphs 72 and 73. As the Court of Appeals for the Seventh Circuit has explained, "[a] brief must make all arguments accessible to the judges, rather than ask them to play archaeologist with the record." *DeSilva v. DiLeonardi*, 181 F.3d 865, 867 (7th Cir. 1999); *see also United States v. Dunkel*, 927 F.2d 955, 956 (7th Cir. 1991) ("Judges are not like pigs, hunting for truffles buried in briefs.").

Additionally, paragraph 72 of the Declaration contains new argument regarding "firewall" and "standard networking practice" based on references (Bharali and Wood) not cited for that proposition in the Petition. Ex. 1004 ¶ 72. We find the Petition improperly incorporates this section of the Declaration by reference because the basis of the "firewall" argument is not

explained sufficiently in the Petition. *Cisco Systems, Inc., v. C-Cation Technologies, LLC*, IPR2014-00454, Paper 12 at 8 (PTAB Aug. 29, 2014) (informative opinion) (describing the proper course of action as "to not consider arguments that are not made in the Petition, but are instead incorporated by reference").

iv. Collateral Estoppel Does Not Apply

1. Collateral Estoppel in the Petition

Petitioner also suggests in conclusory fashion that collateral estoppel may apply to its contentions as to the "entire boundary" limitation (Pet. 38 ("***Collateral estoppel applies.*** 1513 FWD, *19-33, *43, *45-47; 1443 FWD, *49-50, *52-54.")) and the "all traffic" limitation" (Pet. 41 ("***Collateral estoppel applies.*** 1443 FWD, *13-18, *42, *49-50, *52-54; 1444 FWD, *13-19, *42.")).

Our reviewing court has held that "[c]ollateral estoppel protects a party from having to litigate issues that have been fully and fairly tried in a previous action and adversely resolved against a party-opponent." *Nestle USA, Inc. v. Steuben Foods, Inc.*, 884 F.3d 1350, 1351–1352 (Fed. Cir. 2018) (quoting *Ohio Willow Wood Co. v. Alps S., LLC*, 735 F.3d 1333, 1342 (Fed. Cir. 2013)). "It is well established that collateral estoppel, also known as issue preclusion, applies in the administrative context." *MaxLinear, Inc. v. CF CRESPE LLC*, 880 F.3d 1373, 1376 (Fed. Cir. 2018) (citations omitted); *Webpower, Inc. v. WAG ACQUISITION, LLC*, Case IPR2016-01239, Paper 21 at 26–28 (PTAB Dec. 26, 2017).

"Issue preclusion [i.e., collateral estoppel] is appropriate only if: (1) the issue is identical to one decided in the first action; (2) the issue was actually litigated in the first action; (3) resolution of the issue was essential

to a final judgment in the first action; and (4) plaintiff had a full and fair opportunity to litigate the issue in the first action." *In re Freeman*, 30 F.3d 1459, 1465 (Fed. Cir. 1994); *see also MaxLinear, Inc.*, 880 F.3d at 1377 (citing *Blonder-Tongue Labs., Inc. v. Univ. of Illinois Found.*, 402 U.S. 313, 91 S. Ct. 1501, 28 L.Ed. 2d 788 (1971) (finding collateral estoppel applies to a patentee who had a full and fair opportunity to litigate the validity of a patent in a prior federal case.)).

Patent Owner points out that the claims at issue in IPR2018-01443, 1444, 1513 ("prior IPRs") did not include the "entire boundary" or "all traffic" limitations. Prelim. Resp. 26–27, 32, 44. We agree. Collateral estoppel does not apply because there are differences between the claim limitation at issue here and the adjudicated claim limitations at issue in the prior IPRs. *See In re Freeman*, 30 F.3d at 1465; *accord MaxLinear, Inc.*, 880 F.3d at 1377–1378; *cf. In re Arunachalam*, 709 F. App'x 699, 702 (Fed. Cir. 2017) (unpublished) (finding collateral estoppel applies to an adjudicated claim that is not "materially different" than the adjudicated claims).

To the extent that Petitioner has some theory why a prior proceeding regarding a different patent with different claim limitations would be considered a proper basis for collateral estoppel, Petitioner should have explained that theory in its Petition – a mere string citation is insufficient. *See, e.g., Trading Techs. Int'l, Inc. v. IBG LLC*, 921 F.3d 1378, 1385 (Fed. Cir. 2019) (holding that a conclusory assertion with no analysis was not adequately developed); *Novartis AG v. Torrent Pharms.*, 853 F.3d 1316, 1326 n.2 (Fed. Cir. 2017) (finding that an argument presented in one conclusory sentence and a string cite was "far from sufficient to raise a

meaningful challenge" and "amount[ed] to little more than a request that the Board peruse the cited evidence and piece together a coherent argument on Novartis' behalf").

2. *Collateral Estoppel in the Fintiv Reply*

In its Reply to Patent Owner's arguments regarding discretionary denial under § 314(a), Petitioner responds to Patent Owner's argument that the Petition fails to show that Jungck meets the "entire boundary" and "all traffic" limitations. *Fintiv* Reply 8–9.[6] As an initial matter, we note that our authorization of a responsive brief regarding *Fintiv* is not an invitation to respond to all issues on the merits raised in a Patent Owner preliminary response. Also, Petitioner's *Fintiv* Reply does not relieve it of the burden of explaining sufficiently its contentions, including contentions based on collateral estoppel, in its Petition. "In an IPR, the petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable." *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016).

Nevertheless, we address Petitioner's *Fintiv* Reply arguments here. Petitioner asserts "as the Board previously found, Jungck 'broadly teach[es] *protecting entire networks*' such that the 'edge servers located at the POPs

[6] Petitioner argues that Patent Owner "incorrectly suggest[s] that an edge cache necessarily bypasses the edge server 'in the event that there is a cache miss." *Fintiv* Reply. 8–9 (citing Prelim. Resp. 34 (citing Ex. 1051, 96, 112)). Patent Owner does not rely solely on the cache miss but, as explained above, relies on Figure 6 and other disclosures including Ex. 1051 ¶ 95 to show that the edge caches bypass the edge servers. We do not rely on Patent Owner's cache miss argument, but rather we rely on the other arguments cited above. Petitioner does not address Figure 6, Ex. 1051 ¶ 95, or the other arguments Patent Owner makes.

are . . . capable of 'intercept[ing] *all network traffic*,'" citing the Final Written Decision in the '1513 IPR ("'1513 FWD"). *Fintiv* Reply 8 (citing Ex. 1012, 24, 29). Thus, according to Petitioner, "Jungck teaches providing 'an entire interface' that protects entire networks by filtering 'all network traffic.'" *Id.* We examine the '1513 FWD's discussion of the "entire network" and "all traffic" limitations, respectively, below.

We begin with the limitation of "an entire interface across a boundary of a network protected by the packet security gateway." In the '1513 IPR, Patent Owner argued "Jungck only protects 'subscribing servers,' i.e., servers that pay a fee for protection, and not other, non-subscribing servers on the network." Ex. 1012 ['1513 FWD], 23. The Board found, however, "Patent Owner does not sufficiently explain how the claim language and intrinsic record support its view that protecting only subscribing servers in a network is excluded from the scope of claim 1 . . . Petitioner need only show that Jungck *teaches or suggests* a network protected by a plurality of devices." *Id.* at 23–24. Only after making this determination does the Board suggest that "omitting restrictions based on subscriptions is simpler and advantageously protects the entire network." *Id.* at 24.

Thus, although the Board referenced the term "entire network," it was not necessary for the ultimate finding of non-obviousness because the Board had already declined to adopt Patent Owner's claim construction. *In re Freeman*, 30 F.3d at 1465 (collateral estoppel applies to issues the "resolution of [which] was essential to a final judgment in the first action"). For that reason, collateral estoppel does not apply and the statement relied on by the Petition was arguably dicta. Additionally, the pages cited by

Petitioner do not address the relationship between edge servers and edge cache which is at issue in this IPR.

In the '1513 FWD, the Board also stated the edge servers located at the POPs are described as capable of "intercept[ing] all network traffic flowing between the POPs 114, 116 and the network 100." Ex. 1012 ['1513 FWD], 29 (citing IPR2018-01513, Ex. 1008 ¶ 107 [Jungck]). As an initial matter, the text portion of Jungck cited and relied on in the '1513 FWD actually states "service providers 118, 120 each include an edge server 602A, 602B ***and an edge cache 604A, 604B*** coupled with the routing equipment 206 of the service providers 118, 120 so as to be able to intercept all network traffic" and, thus, the '1513 IPR does not address the issue in this case regarding the distinction between the operation of the edge server and edge cache. Ex. 1051 ¶ 107 (emphasis added).

Additionally, because the issue in the '1513 FWD was simply whether the claimed boundary existed in Jungck between the protected network and one or more other networks, so the Board did not need to determine whether all traffic goes through the edge servers to reach a decision on obviousness. Ex. 1012 ['1513 FWD], 29; *In re Freeman*, 30 F.3d at 1465 (collateral estoppel applies to issues the "resolution of [which] was essential to a final judgment in the first action"). For that reason, collateral estoppel does not apply and the reference to "all network traffic" was arguably dicta.

In its *Fintiv* Reply, Petitioner also asserts "PO does not even address the evidence that it was well-known to filter both inbound and outbound traffic." *Fintiv* Reply 9 (citing Pet. 43–44; Ex. 1004 ¶¶ 72–73, 238–241). As noted above, Patent Owner does respond to the "well-known" argument and we are persuaded by Patent Owner's response. Petitioner also cites to

portions of the Declaration (Ex. 1004 ¶¶ 72–73) to support the "well-known" argument. *Id.* However, as explained above, those paragraphs of the Declaration are not cited or explained in the Petition. *Id.*

c. Summary of Claim 1

In sum, Petitioner does not explain how the edge cache devices contribute or detract from Jungck's ability to teach or suggest the "entire boundary" and "all traffic" limitations of the challenged claims. The evidence of device 900 and claims of collateral estoppel do not remedy this deficiency. In the absence of such evidence, Petitioner has failed to "identif[y], in writing and with particularity, . . . the evidence that supports the grounds for the challenge." *See Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1369 ("It is of the utmost importance that petitioners in the IPR proceedings adhere to the requirement that the initial petition identify 'with particularity' the 'evidence that supports the grounds for the challenge to each claim.'") (quoting 35 U.S.C. § 312(a)(3)); 37 C.F.R. § 42.104(b). For the reasons above, Petitioner has not shown sufficiently that the combination of Jungck and Wood meets the limitation of "[a] method of filtering packets at a packet security gateway, of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway . . . comprising: a first set of packet filtering rules to be applied to all network traffic traversing the boundary."

d. Independent Claims 8, 15, and 21 and Dependent Claims 2–7, 9–14, 16–20, 22–27

Petitioner asserts that Jungck and Wood teach the limitations of independent claims 8, 15, and 21 and dependent claims 2–7, 9–14, 16–20, 22–27. These claims also recite the "entire boundary" and "all traffic"

limitations and thus, for the same reasons as above, Petitioner has not demonstrated a reasonable likelihood of success in establishing the unpatentability of any of independent claims 1, 8, 15, and 21, and claims 2–7, 16–20, and 22–27 which depend therefrom, as having been obvious over Jungck and Wood.

E. Obviousness of Claims over Jungck, Sarathy, and Wood

Petitioner asserts that claims 1–27 are unpatentable under 35 U.S.C. § 103(a) as obvious over Jungck, Sarathy, and Wood. Pet. 6. To support its contentions, Petitioner provides explanations as to how the prior art allegedly teaches each claim limitation. *Id.* at 65 68.

Petitioner's contentions that Jungck, Sarathy, and Wood teach the limitations of independent claims 8, 15, and 21 and dependent claims 2–7, 9–14, 16–20, 22–27 do not cure the deficiencies discussed above as to the "entire boundary" and "all traffic" limitations. Thus, for the same reasons as above, Petitioner has not demonstrated a reasonable likelihood of success in establishing the unpatentability of any of independent claims 1, 8, 15, and 21, and claims 2–7, 16–20, and 22–27 which depend therefrom, as having been obvious over Jungck, Sarathy, and Wood.

F. Summary

For the foregoing reasons, we determine that Petitioner has not demonstrated a reasonable likelihood of success in establishing the unpatentability of any of independent claims 1, 8, 15, and 21, and claims 2–7, 16–20, and 22–27 which depend therefrom, on the obviousness grounds asserted in the Petition.

G. *Discretionary Denial Under 35 U.S.C. § 314(a) and/or 325(d)*

Because we deny institution upon consideration of the merits of Petitioner's challenges, we need not address Patent Owner's arguments that we should exercise our discretion under 35 U.S.C. § 314(a) and/or § 325(d) to deny institution.

II. CONCLUSION

Petitioner has not demonstrated a reasonable likelihood of prevailing with respect to any of claims 1–27 of the '266 patent under any of the proffered grounds.

III. ORDER

For the reasons given, it is:

ORDERED that, pursuant to 35 U.S.C. § 314(a), an *inter partes* review is not instituted for claims 1–27 of U.S. Patent No. 10,785,266 B2.

PETITIONER:

Scott A. McKeown
Mark D. Rowland
James R. Batchelder
Andrew Radsch
ROPES & GRAY LLP
scott.mckeown@ropesgray.com
mark.rowland@ropesgray.com
james.batchelder@ropesgray.com
andrew.radsch@ropesgray.com

PATENT OWNER:

James Hannah
Jeffrey H. Price
KRAMER LEVIN NAFTALIS & FRANKEL, LLP
jhannah@kramerlevin.com
Jprice@kramerlevin.com

Bradley C. Wright
Scott M. Kelly
Blair A. Silver
BANNER & WITCOFF, LTD.
bwright@bannerwitcoff.com
skelly@bannerwitcoff.com
bsilver@bannerwitcoff.com

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 10,785,266 B2
APPLICATION NO. : 16/728766
DATED : September 22, 2020
INVENTOR(S) : Steven Rogers et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

On the Title Page

Page 4, Column 1, item (56) under Other Publications, Line 13:
Please delete "Mar. 21, 2020" and insert --Mar. 31, 2020--

In the Claims

Column 21, Claim 1, Line 19:
After "information" insert --,--

Column 23, Claim 15, Line 57:
After "information" insert --,--

Column 24, Claim 21, Line 66-67:
After "information" insert --,--

Signed and Sealed this
Fifth Day of January, 2021

Andrei Iancu
Director of the United States Patent and Trademark Office

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re U.S. Patent No. 10,785,266	)	Serial No. 16/728,766
	)	
Inventor(s): Steven Rogers, et al.	)	Filed: December 27, 2019
	)	
Issue Date: September 22, 2020	)	Attorney Docket No. 007742.00151

For: METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK

REQUEST FOR CERTIFICATE OF CORRECTION

U.S. Patent and Trademark Office
Customer Service Window
Randolph Building, Mail Stop: Certificate of Correction Branch
401 Dulany Street
Alexandria, VA 22314

Sir:

Pursuant to 35 U.S.C. § 254 and 37 C.F.R. § 1.322, Applicant requests the issuance of a Certificate of Correction in the above-identified patent. A copy of PTO Form 1050 is appended. The complete Certificate of Correction involves one page.

The mistake identified in the appended Form occurred through no fault of the Applicant, as clearly disclosed by the records of the application, which matured into this patent. Enclosed for your convenience are copies of the List of References cited by applicant and considered by Examiner dated April 16, 2020 and the Claims as filed July 16, 2020.

Issuance of the Certificate of Correction containing the corrections is respectfully requested. Since these changes are necessitated through no fault of the Applicant, no fee is believed to be associated with this request. Nonetheless, should the Patent and Trademark Office determine that a fee is required, please charge our Deposit Account No. 19-0733.

Respectfully submitted,
BANNER & WITCOFF, LTD.
By: */Kirk A. Sigmon/*
Kirk A. Sigmon
Registration No. 76,326

Dated: Dec. 7, 2020
Banner & Witcoff, Ltd
1100 13th Street, N.W., Suite 1200
Washington, D.C. 20005-4051
(202) 824-3000

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO.: 10,785,266

DATED: September 22, 2020

INVENTOR(S): Steven Rogers, et al.

It is certified that errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Page 4, Column 1, under Other Publications, Line 13:
Please delete "Mar. 21, 2020" and insert --Mar. 31, 2020—

Column 21, Claim 1, Line 19:
After "information" insert --,--

Column 23, Claim 15, Line 57:
After "information" insert --,--

Column 24, Claim 21, Line 66-67:
After "information" insert --,--

Mailing Address of Sender:

Banner & Witcoff, Ltd.
1100 13th Street, N.W., Suite 1200
Washington, DC 20005-4051

U.S. PAT. NO
10.785,266
No. of add'l copies
@ $0.50 per page

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

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. 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	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\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]

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\US

/KC/	1	2020 Feb 11 (US) Final Written Decision Determining All Challenged Claims Unpatentable of U.S. Patent 9,137,205 B2 - IPR 2018-01444
	2	2020 Feb 11 (US) Final Written Decision Determining All Challenged Claims Unpatentable of U.S. Patent 9,137,205 B2 - IPR 2018-01443
	3	2020 Mar 19 (US) Final Written Decision Determining All Challenged Claims Unpatentable of U.S. Patent 9,565,213 B2 - IPR 2018-01512
	4	2020 Jan 23 (US) Final Written Decision Determining All Challenged Claims Unpatentable of U.S. Patent 9,565,213 B2 - IPR 2018-01386
	5	2020 Mar 31 (US) Final Written Decision Determining All Challenged Claims Unpatentable of U.S. Patent 9,560,077 B2 - IPR 2018-01513

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

EXAMINER SIGNATURE

Examiner Signature	/KENNETH W CHANG/	Date Considered	04/12/2020

*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.

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A method of filtering packets at a packet security gateway, of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway and one or more networks other than the network protected by the packet security gateway, the method comprising:

receiving, by the packet security gateway and from a security policy management server external from the network protected by the packet security gateway, a dynamic security policy comprising a first set of packet filtering rules to be applied to all network traffic traversing the boundary, wherein:

each packet filtering rule of the first set of packet filtering rules comprises at least one packet matching criterion and a corresponding packet transformation function, and

one or more first packet filtering rules of the first set of packet filtering rules comprise packet matching criteria corresponding to one or more network addresses and were automatically created or altered by the security policy management server based on aggregated malicious traffic information, received from at least one third party malicious host tracker service located in the one or more networks other than the network protected by the packet security gateway, that comprises network addresses that have been determined, by the at least one third party malicious host tracker service, to be associated with malicious network traffic;

performing, on a packet by packet basis, packet filtering on a first portion of packets corresponding to network traffic traversing the boundary via the packet security gateway based on the first set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets;

receiving, by the packet security gateway and after performing packet filtering on the first portion of the packets, an updated second set of packet filtering rules for the

dynamic security policy from the security policy management server, wherein the updated second set of packet filtering rules comprises an update to the one or more first packet filtering rules created or altered by the security policy management server based on updated malicious traffic information received from the at least one third party malicious host tracker service; and

performing, on a packet by packet basis, packet filtering on a second portion of the packets corresponding to network traffic traversing the boundary via the packet security gateway based on the updated second set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the second set of packet filtering rules on the second portion of packets.

2. (Currently Amended) The method of claim 1, wherein the at least one packet matching criterion corresponding to the one or more first packet filtering rules automatically created or altered by the security policy management server comprises at least one of the one or more network addresses ~~indicated by the malicious traffic information~~.

3. (Currently Amended) The method of claim 1, wherein the at least one third party malicious host tracker service comprises a subscription service that aggregates information associated with malicious network traffic.

4. (Currently Amended) The method of claim 1, wherein the ~~malicious traffic information comprises a list of~~one or more network addresses were associated, by a subscription service, with malicious network traffic~~known to be associated with malicious network traffic~~.

5. (Original) The method of claim 1, wherein at least one packet transformation function comprises a network protective action.

6. (Original) The method of claim 1, further comprising:

receiving, by the packet security gateway, packets in a network layer transparent manner using an interface that is not addressed at the network layer; and

performing the at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets at the network layer.

7. (Original) The method of claim 1, wherein one or more packet filtering rules of the first set of packet filtering rules specify a packet transformation function other than forwarding or dropping the corresponding packets.

8. (Currently Amended) A packet security gateway, of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway and one or more networks other than the network protected by the packet security gateway, comprising:

one or more processors; and

memory storing instructions that, when executed by the one or more processors, cause the packet security gateway to:

receive, from a security policy management server external from the network protected by the packet security gateway, a dynamic security policy comprising a first set of packet filtering rules to be applied to all network traffic traversing the boundary, wherein:

each packet filtering rule of the first set of packet filtering rules comprises at least one packet matching criterion and a corresponding packet transformation function, and

one or more first packet filtering rules of the first set of packet filtering rules comprise packet matching criteria corresponding to one or more network addresses and were automatically created or altered by the security policy management server based on aggregated malicious traffic information, received from at least one third party malicious host tracker service located in the one or more networks other than the network protected by the packet security gateway, that comprises network addresses that have been determined, by the at least one

third party malicious host tracker service, to be associated with malicious network traffic;

perform, on a packet by packet basis, packet filtering on a first portion of packets corresponding to network traffic traversing the boundary via the packet security gateway based on the first set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets;

receive, after performing packet filtering on the first portion of the packets, an updated second set of packet filtering rules for the dynamic security policy from the security policy management server, wherein the updated second set of packet filtering rules comprises an update to the one or more first packet filtering rules created or altered by the security policy management server based on updated malicious traffic information received from the at least one third party malicious host tracker service; and

perform, on a packet by packet basis, packet filtering on a second portion of the packets corresponding to network traffic traversing the boundary via the packet security gateway based on the updated second set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the second set of packet filtering rules on the second portion of packets.

9. (Currently Amended) The packet security gateway of claim 8, wherein the at least one packet matching criterion corresponding to the one or more first packet filtering rules automatically created or altered by the security policy management server comprises at least one of the one or more network addresses ~~indicated by the malicious traffic information~~.

10. (Currently Amended) The packet security gateway of claim 8, wherein the at least one third party malicious host tracker service comprises a subscription service that aggregates information associated with malicious network traffic.

11. (Currently Amended) The packet security gateway of claim 8, wherein the ~~malicious traffic information comprises a list of~~one or more network addresses were associated, by a

subscription service, with malicious network traffic~~known to be associated with malicious network traffic~~.

12. (Original) The packet security gateway of claim 8, wherein at least one packet transformation function comprises a network protective action.

13. (Original) The packet security gateway of claim 8, wherein the instructions further cause the packet security gateway to:

receive packets in a network layer transparent manner using an interface that is not addressed at the network layer; and

perform the at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets at the network layer.

14. (Original) The packet security gateway of claim 8, wherein one or more packet filtering rules of the first set of packet filtering rules specify a packet transformation function other than forwarding or dropping the corresponding packets.

15. (Currently Amended) One or more non-transitory computer readable media storing instructions that, when executed by at least one processor, cause a packet security gateway, of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway and one or more networks other than the network protected by the packet security gateway, to perform steps comprising:

receiving, from a security policy management server external from the network protected by the packet security gateway, a dynamic security policy comprising a first set of packet filtering rules to be applied to all network traffic traversing the boundary, wherein:

each packet filtering rule of the first set of packet filtering rules comprises at least one packet matching criterion and a corresponding packet transformation function, and

one or more first packet filtering rules of the first set of packet filtering rules comprise packet matching criteria corresponding to one or more network addresses and were automatically created or altered by the security policy management server based on aggregated malicious traffic information, received from at least one third party malicious host tracker service located in the one or more networks other than the network protected by the packet security gateway, that comprises network addresses that have been determined, by the at least one third party malicious host tracker service, to be associated with malicious network traffic;

performing, on a packet by packet basis, packet filtering on a first portion of packets corresponding to network traffic traversing the boundary via the packet security gateway based on the first set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets;

receiving, after performing packet filtering on the first portion of the packets, an updated second set of packet filtering rules for the dynamic security policy from the security policy management server, wherein the updated second set of packet filtering rules comprises an update to the one or more first packet filtering rules created or altered by the security policy management server based on updated malicious traffic information received from the at least one third party malicious host tracker service; and

performing, on a packet by packet basis, packet filtering on a second portion of the packets corresponding to network traffic traversing the boundary via the packet security gateway based on the updated second set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the second set of packet filtering rules on the second portion of packets.

16. (Currently Amended) The computer readable media of claim 15, wherein the at least one packet matching criterion corresponding to the one or more first packet filtering rules automatically created or altered by the security policy management server comprises at least one of the one or more network addresses ~~indicated by the malicious traffic information~~.

17. (Currently Amended) The computer readable media of claim 15, wherein the at least one third party malicious host tracker service comprises a subscription service that aggregates information associated with malicious network traffic, and wherein the ~~malicious traffic information comprises a list of~~one or more network addresses were associated, by a subscription service, with malicious network traffic~~known to be associated with malicious network traffic~~.

18. (Original) The computer readable media of claim 15, wherein at least one packet transformation function comprises a network protective action.

19. (Original) The computer readable media of claim 15, further comprising:

receiving, by the packet security gateway, packets in a network layer transparent manner using an interface that is not addressed at the network layer; and

performing the at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets at the network layer.

20. (Original) The computer readable media of claim 15, wherein one or more packet filtering rules of the first set of packet filtering rules specify a packet transformation function other than forwarding or dropping the corresponding packets.

21. (Currently Amended) A method of filtering packets at a packet security gateway configured for protection of a network and associated with a security policy management server external from the network, the method comprising:

receiving, by the packet security gateway, a dynamic security policy comprising a first set of packet filtering rules from the security policy management server, wherein each packet filtering rule of the first set of packet filtering rules comprises at least one packet matching criterion and a corresponding packet transformation function, and wherein one or more first packet filtering rules of the first set of packet filtering rules comprise packet matching criteria corresponding to one or more network addresses and

were automatically created or altered by the security policy management server based on aggregated malicious traffic information, received from at least one third party malicious host tracker service located in the one or more networks other than the network protected by the packet security gateway, that comprises network addresses that have been determined, by the at least one third party malicious host tracker service, to be associated with malicious network traffic;

performing, on a packet by packet basis, packet filtering on a first portion of packets associated with the network protected by the packet security gateway based on the first set of packet filtering rules by performing at least one of multiple packet transformation functions specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets;

receiving, by the packet security gateway and after performing packet filtering on the first portion of the packets, an updated second set of packet filtering rules for the dynamic security policy from the security policy management server, wherein the updated second set of packet filtering rules comprises an update to the one or more first packet filtering rules created or altered by the security policy management server based on updated malicious traffic information received from the at least one third party malicious host tracker service; and

performing, on a packet by packet basis, packet filtering on a second portion of the packets associated with the network protected by the packet security gateway based on the updated second set of packet filtering rules.

22. (Currently Amended) The method of claim 21, wherein the at least one packet matching criterion corresponding to the one or more first packet filtering rules automatically created or altered by the security policy management server comprises at least one of the one or more network addresses ~~indicated by the malicious traffic information~~.

23. (Currently Amended) The method of claim 21, wherein the at least one third party malicious host tracker service comprises a subscription service that aggregates information associated with malicious network traffic.

24. (Currently Amended) The method of claim 21, wherein the ~~malicious traffic information comprises a list of~~one or more network addresses were associated, by a subscription service, with malicious network traffic~~known to be associated with malicious network traffic~~.

25. (Original) The method of claim 21, wherein at least one packet transformation function comprises a network protective action.

26. (Original) The method of claim 21, further comprising:

receiving, by the packet security gateway, packets in a network layer transparent manner using an interface that is not addressed at the network layer; and

performing the at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets at the network layer.

27. (Original) The method of claim 21, wherein one or more packet filtering rules of the first set of packet filtering rules specify a packet transformation function other than forwarding or dropping the corresponding packets.

Electronic Acknowledgement Receipt

EFS ID:	41312409
Application Number:	16728766
International Application Number:	
Confirmation Number:	8018
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	Kirk Allen Sigmon/Kelly Pilkerton
Filer Authorized By:	Kirk Allen Sigmon
Attorney Docket Number:	007742.00151\US
Receipt Date:	07-DEC-2020
Filing Date:	27-DEC-2019
Time Stamp:	15:29:43
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	Request for Certificate of Correction	Request_for_CoC_as_filed_20893644.PDF	593270 f8ec1f5ca07e63457bb497874deaa9db17356141	no	13

Warnings:

Information:	
Total Files Size (in bytes):	593270

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 NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/728,766	09/22/2020	10785266	007742.00151\US	8018

22907 7590 09/02/2020

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

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Steven Rogers, Leesburg, VA;
Centripetal Networks, Inc., Portsmouth, NH;
Sean Moore, Hollis, NH;

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 USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

Docket No.: 007742.00151\US
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Steven Rogers et al.

Application No.: 16/728,766 Confirmation No.: 8018

Filed: December 27, 2019 Art Unit: 2438

For: METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK Examiner: K. W. Chang

COMMENTS ON STATEMENT OF REASONS FOR ALLOWANCE

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

Applicant thanks Examiner Chang for the allowance of this application. In brief response to the Statement of Reasons for Allowance, Applicant submits that the claimed features are defined only by the language recited in the claims as allowed. There are many features in the independent and dependent claims, and the features quoted in the excerpts are not necessarily the only reasons for distinguishing the claims from the various references. Also, to the extent there is any deviation between the quoted excerpts and the language of the claims, the language of the claims will control.

Dated: Aug. 20, 2020

Respectfully submitted,

By: */Kirk A. Sigmon/*
Kirk A. Sigmon
Registration No.: 76,326

BANNER & WITCOFF, LTD.
1100 13th St. NW
STE 1200
Washington, DC 20005
(202) 824-3000

Electronic Patent Application Fee Transmittal

Application Number:	16728766
Filing Date:	27-Dec-2019
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Filer:	Kirk Allen Sigmon/MARIAMA SEASAY
Attorney Docket Number:	007742.00151\US

Filed as Small 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:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
UTILITY APPL ISSUE FEE	2501	1	500	500

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**500**

Electronic Acknowledgement Receipt

EFS ID:	40339565
Application Number:	16728766
International Application Number:	
Confirmation Number:	8018
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	Kirk Allen Sigmon/MARIAMA SEASAY
Filer Authorized By:	Kirk Allen Sigmon
Attorney Docket Number:	007742.00151\US
Receipt Date:	20-AUG-2020
Filing Date:	27-DEC-2019
Time Stamp:	14:35:04
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$500
RAM confirmation Number	E20208JE40135131
Deposit Account	190733
Authorized User	MARIAMA SEASAY

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

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	Issue Fee Payment (PTO-85B)	Issue_Fee_Transmittal_20705205.pdf	37556 4a647fec5bad2f806fd8ad8ae25be5a9eb5ace98	no	1
Warnings:					
Information:					
2	Miscellaneous Incoming Letter	USAN_16_728766_Comments_on_Statement_of_Reasons_for_Allowance_20705179.pdf	17844 548d434ba9c64b52c618dd37b4e0f90810ad2765	no	1
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30353 326e7b90c456d2ab209b053f9c37cb4667f0dc82	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	85753		

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.

PART B–FEE(S) TRANSMITTAL

Complete and send this form, together with the applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

By fax, send to: (571) 273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

BANNER & WITCOFF, LTD.
1100 13th St. NW
STE 1200
Washington, DC 20005

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)

(Signature)

(Date)

APPLICATION NO	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO	CONFIRMATION NO
16/728,766	12/27/2019	Steven Rogers	007742.00151\US	8018

TITLE OF INVENTION: METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK

APPLN: TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$500.00			$500.00	11/04/2020

EXAMINER	ART UNIT	CLASS-SUBCLASS
K. W. Chang	2438	726-010

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363)

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1. **Banner & Witcoff, Ltd.**
2.
3.

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: **Centripetal Networks, Inc.**

(B) RESIDENCE: (CITY and STATE or COUNTRY): **Portsmouth, New Hampshire**

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. Fees Submitted: ☒ Issue Fee ☐ Publication Fee (if required) ☐ Advance Order - # of Copies _____

4b. Method of Payment (*Please first reapply any previously paid fee shown above*):

☒ Electronic Payment via EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. 19-0733

5. Change of Entity Status (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29. NOTE: Absent a valid Certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

☐ Applicant asserting small entity status. See 37 CFR 1.27. NOTE: If the application was previously under micro entity status, checking this box will be taken as a notification of loss of entitlement to micro entity status.

☐ Applicant changing to regular undiscounted fee status. NOTE: Checking this box will be taken as a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Kirk A. Sigmon/ Date August 20, 2020

Typed or printed name Kirk A. Sigmon Registration No. 76,326

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

22907 7590 08/04/2020
BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

EXAMINER
CHANG, KENNETH W

ART UNIT	PAPER NUMBER
2438	

DATE MAILED: 08/04/2020

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/728,766	12/27/2019	Steven Rogers	007742.00151\US	8018

TITLE OF INVENTION: METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$500	$0.00	$0.00	$500	11/04/2020

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

22907 7590 08/04/2020

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

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/728,766	12/27/2019	Steven Rogers	007742.00151\US	8018

TITLE OF INVENTION: METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$500	$0.00	$0.00	$500	11/04/2020

EXAMINER	ART UNIT	CLASS-SUBCLASS
CHANG, KENNETH W	2438	726-010000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. Fees submitted: ❑ Issue Fee ❑ Publication Fee (if required) ❑ Advance Order - # of Copies _____

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

❑ Electronic Payment via EFS-Web ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

❑ Applicant asserting small entity status. See 37 CFR 1.27

❑ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

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 NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/728,766	12/27/2019	Steven Rogers	007742.00151\US	8018

22907 7590 08/04/2020

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

EXAMINER	
CHANG, KENNETH W	
ART UNIT	**PAPER NUMBER**
2438	

DATE MAILED: 08/04/2020

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. 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, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. 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.

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 disclosure of these records is required by the Freedom of Information Act.
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 inspection 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.

Keysight Technologies Ex. 1002

Notice of Allowability	Application No. 16/728,766	Applicant(s) Rogers et al.	
	Examiner Kenneth W Chang	Art Unit 2438	AIA (FITF) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☑ This communication is responsive to the filing on 07/16/2020.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☑ The allowed claim(s) is/are 1-27 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☑ Notice of References Cited (PTO-892)
2. ☑ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date. _____.
5. ☐ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/KENNETH W CHANG/
Primary Examiner, Art Unit 2438

DETAILED ACTION

1. This Notice and Reasons for Allowance is in response to applicants' amendment and remarks filed on 07/16/2020. Claims 1-4, 8-11, 15-17, and 21-24 have been amended. **Claims 1-27** are currently pending and have been considered as follows.

2. The text of those sections of Title 35 U.S. Code not included in this section can be found in the prior office action.

3. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.

4. The present application is being examined under the pre-AIA first to invent provisions.

Information Disclosure Statement

5. The information disclosure statement (IDS) submitted on 07/10/2020 has been placed in the application file, and the information referred therein has been considered as to the merits.

Allowable Subject Matter

6. **Claims 1-27** are allowed.

Examiner's Statement for Reasons of Allowance

7. The following is an examiner's statement of reasons for allowance:

In interpreting the currently amended claims in light of the specification, the Examiner finds the claimed invention to be patentably distinct from the prior art of record.

Independent **Claims 1, 8, 15, and 21** are allowed in view of applicants' amendment and remarks filed on 07/16/2020 which are persuasive and the telephone interview conducted on 07/14/2020. Claims **2-7, 9-14, 16-20, and 22-27** depend upon respective independent claims above and are allowed by virtue of their dependencies.

Although, the closest prior art found **Jalava et al. (US 20030118038 A1)** discloses **"A personalized firewall or other network gateway is provided by a method of matching a data packet to a rule in a network gateway having a rule base. One or more identification values are determined (302) on the basis of the data packet and property value(s) associated with said one or more identification values are queried (304) and received from a property server. The property value(s) describe for example allowed connections and services for an entity associated with the identification value(s). The property value(s) are compared (306) to at least one rule in the rule base, said at least one rule comprising property value(s) and an action, and the action defined in said at least one rule is taken (310), if said property value(s) of the rule match corresponding property value(s) associated with said one or more identification values" [Abstract])**,

None of the prior art of record teaches individually or in combination the particular limitations listed below [emphasis added] as recited in applicants' amended independent claims:

- [Claim 1] "one or more first packet filtering rules of the first set of packet filtering rules comprise packet matching criteria corresponding to one or more network addresses and were ***automatically created or altered by the security policy management server based on aggregated malicious traffic information,***

received from at least one third party malicious host tracker service located in the one or more networks other than the network protected by the packet security gateway, that comprises network addresses that have been determined, by the at least one third party malicious host tracker service, to be associated with malicious network traffic";

- [Claim 1] "***wherein the updated second set of packet filtering rules comprises an update to the one or more first packet filtering rules created or altered by the security policy management server based on updated malicious traffic information received from the at least one third party malicious host tracker service***";
- [Claim 8] "one or more first packet filtering rules of the first set of packet filtering rules comprise packet matching criteria corresponding to one or more network addresses and were ***automatically created or altered by the security policy management server based on aggregated malicious traffic information, received from at least one third party malicious host tracker service located in the one or more networks other than the network protected by the packet security gateway, that comprises network addresses that have been determined, by the at least one third party malicious host tracker service, to be associated with malicious network traffic***";
- [Claim 8] "***wherein the updated second set of packet filtering rules comprises an update to the one or more first packet filtering rules created or altered by the security policy management server based on updated***

malicious traffic information received from the at least one third party malicious host tracker service";

- [Claim 15] "one or more first packet filtering rules of the first set of packet filtering rules comprise packet matching criteria corresponding to one or more network addresses and were ***automatically created or altered by the security policy management server based on aggregated malicious traffic informations received from at least one third party malicious host tracker service located in the one or more networks other than the network protected by the packet security gateway, that comprises network addresses that have been determined, by the at least one third party malicious host tracker service, to be associated with malicious network traffic***";
- [Claim 15] "***wherein the updated second set of packet filtering rules comprises an update to the one or more first packet filtering rules created or altered by the security policy management server based on updated malicious traffic information received from the at least one third party malicious host tracker service***";
- [Claim 21] "one or more first packet filtering rules of the first set of packet filtering rules comprise packet matching criteria corresponding to one or more network addresses and were ***automatically created or altered by the security policy management server based on aggregated malicious traffic information, received from at least one third party malicious host tracker service located in the one or more networks other than the network protected by the packet security gateway, that comprises network addresses that have been***

determined, by the at least one third party malicious host tracker service, to be associated with malicious network traffic";

- [Claim 21] "***wherein the updated second set of packet filtering rules comprises <u>an updated second set of packet filtering rules comprises an update to the one or more first packet filtering rules created or altered by the security policy management server based on updated malicious traffic information received from the at least one third party malicious host tracker service</u>***".

The **closest** prior art made of record and cited consisted of the following references.

<u>Baum et al.</u> (US 6400707 B1) disclosed a system and method for conducting a voice communication through a hybrid network which includes a packet internetwork, such as the Internet, connected to a circuit switched telephone network. The packet internetwork is connected to the switched telephone network through a static filter device, a packet switch, and a telephone network controlled gateway. A control processor is connected to the packet switch and to the filter device. The filter device generates a real time copy of call set up signaling dialog between the party requesting connection and the gateway which passes through or to the filter device. This duplicate of set up signaling is delivered from the filter device through the packet switch to the control processor. The control processor generates therefrom a filter device control signal which specifies the filter parameters derived from the set-up signaling dialog. This filter device control signal is delivered to the filter device and reconfigures the filter device to set filter parameters which are customized to the specific communication. The filter device thereupon filters the conversation stream of packetized voice.

Vaidya (US 6279113 B1) disclosed a signature based dynamic network intrusion detection system (IDS) includes attack signature profiles which are descriptive of characteristics of known network security violations. The attack signature profiles are organized into sets of attack signature profiles according to security requirements of network objects on a network. Each network object is assigned a set of attack signature profiles which is stored in a signature profile memory together with association data indicative of which sets of attack signature profiles correspond to which network objects. A monitoring device monitors network traffic for data addressed to the network objects. Upon detecting a data packet addressed to one of the network objects, packet information is extracted from the data packet. The extracted information is utilized to obtain a set of attack signature profiles corresponding to the network object based on the association data. A virtual processor executes instructions associated with attack signature profiles to determine if the packet is associated with a known network security violation. An attack signature profile generator is utilized to generate additional attack signature profiles configured for processing by the virtual processor in the absence of any corresponding modification of the virtual processor.

Sawada et al. (US 20020016858 A1) disclosed a packet communications apparatus comprising a plurality of network interfaces (NIFs), a learned address table, a packet forwarding unit (PFU) and a processor for directive packets to change state (PDPCS). The learned address table contains information for identifying a NIF through which to send a packet. The PFU selects a port through which to forward a packet by referring to the learned address table, according to the state of the NIFs, and forwards or discards a packet received from a user terminal. The PDPCS receives a packet

including a directive to change the state of a specific NIF to one of the connected state, disconnected state and stateless. The PDPCS changes the state of the specific NIF to one of the connected state, disconnected state and stateless, according to the directive in the packet.

Jalava et al. (US 20030118038 A1) disclosed a method of matching a data packet to a rule in a network gateway having a rule base. One or more identification values are determined (302) on the basis of the data packet and property value(s) associated with said one or more identification values are queried (304) and received from a property server. The property value(s) describe for example allowed connections and services for an entity associated with the identification value(s). The property value(s) are compared (306) to at least one rule in the rule base, said at least one rule comprising property value(s) and an action, and the action defined in said at least one rule is taken (310), if said property value(s) of the rule match corresponding property value(s) associated with said one or more identification values.

Talpade et al. (US 20040148520 A1) disclosed a sensor that examines the traffic entering the customer network for attack traffic. When an attack is detected, the sensor notifies an analysis engine within the ISP network to mitigate the attack. The analysis engine configures a filter router to advertise new routing information to the border and edge routers of the ISP network. The new routing information instructs the border and edge routers to reroute attack traffic and non-attack traffic destined for the customer network to the filter router. At the filter router, the attack traffic and non-attack traffic are automatically filtered to remove the attack traffic. The non-attack traffic is passed back onto the ISP network for routing towards the customer network.

Kang et al. (US 20050076227 A1) disclosed an in-line mode network intrusion detecting and preventing system coupled between a protection network and an external network, for detecting intrusion states between the networks and preventing the intrusion. The system comprises a first network processor unit for monitoring the packets communicated between the networks to collect various statistical data, and performing a packet filtering process according to a packet preventing rule and a packet sensing process according to a sensing rule; and a second network processor unit for checking payloads of the packets with reference to attack signatures to detect the attack states to one of the networks.

Bhatnagar et al. (US 20060123481 A1) disclosed deep packet inspection that may be dynamically updated with patterns associated with malicious code, so that malicious code may be detected and blocked at the network level. As new threats are identified by a security service, new patterns may be created for those threats, and the new patterns may then be passed out onto the network in real time. The real time availability of patterns enables filter rules derived from the patterns to be applied by the network elements so that malicious code may be filtered on the network before it reaches the end users. The filter rules may be derived by security software resident in the network elements or may be generated by a filter generation service configured to generate network element specific filter rules for those network elements that are to be implemented as detection points on the network.

Joshi et al. (US 20060262798 A1) disclosed an apparatus and method to isolate ports on layer 2 switches on the same VLAN to restrict traffic flow. The apparatus comprises a switch having said plurality of ports, each port configured as a protected

port or a non-protected port. An address table memory stores an address table having a destination address and port number pair. A forwarding map generator generates a forwarding map which is responsive to a destination address of a data packet. The method for isolating ports on a layer 2 switch comprises configuring each of the ports on the layer 2 switch as a protected port or a non-protected port. A destination address on an data packet is matched with a physical address on said layer 2 switch and a forwarding map is generated for the data packet based upon the destination address on the data packet. The data packet is then sent to the plurality of ports pursuant to the forwarding map generated based upon whether the ingress port was configured as a protected or nonprotected port.

Lok (US 20070056038 A1) disclosed an intrusion protection system that fuses a network instrumentation classification with a packet payload signature matching system. Each of these kinds of systems is independently capable of being effectively deployed as an anomaly detection system. By employing sensor fusion techniques to combine the instrumentation classification approach with the signature matching approach, this provides an intrusion protection system that is capable of detecting both well known and newly developed threats while having a low false positive rate.

SUH et al. (US 20080043739 A1) disclosed a network system using Mobile Internet Protocol (IP). The network system includes a correspondent node for transmitting a packet in which information passing a packet filter rule is included, and a packet filtering apparatus for determining whether an address included in information of the packet received from the correspondent node is identical to a destination address

stored in the packet filter rule, and determining whether to pass the packet according to the determination result.

Friskney et al. (US 20080279196 A1) disclosed enabling differential forwarding in address-based carrier networks such as Ethernet networks. There is described a method of and connection controller for establishing connections (76, 77) in a frame-based communications network comprising nodes (71-75 and 78) such as Ethernet switches. The connections are established by configuring, in various of the nodes, mappings for forwarding data frames, such as Ethernet frames. The mappings are from a combination of a) a destination (or source) address corresponding to a destination (or source) node (73) of the connection and b) an identifier, such as a VLAN tag. The mappings are to selected output ports of the various nodes. By using the combination of destination (or source) address AND identifier, the mappings enable data frames belonging to different connections (76, 77) to be forwarded differentially (ie forwarded on different output ports) at a node (75) despite the different connections having the same destination node. This enables flexibility in routing connections and the ability to perform traffic engineering.

Haswell (US 20090150996 A1) disclosed embedding a programmable packet filter into an application to protect the application against malicious network packets are disclosed. Traditional packet filtering techniques to protect against malicious packets designed to exploit defects in applications, based on external packet filtering devices create a bottleneck in network traffic and present a large overhead cost. In addition, when security vulnerabilities in applications are discovered, traditional application updating methods lack a fast enough turn-around time to protect the application and

users data from attack. These problems can be overcome by embedding a programmable packet filter into the application itself. The application can use the filter to discard malicious network packets. Furthermore, the filter can be updated via configuration files downloaded from the application vendor to update the application's embedded programmable packet filter without having to update the entire program code of the application.

Ahn (US 20110055916 A1) disclosed a method including 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.

Zuk et al. (US 8009566 B2) disclosed inspecting data packets in a computer network. One or more data packets through the network have associated header data and content. One method includes receiving a data packet, examining the data packet to classify the data packet including classifying the data packet using information included in the header and content, determining flow instructions for processing the packet based on both the header information and the content and processing of the packet using the flow instructions.

Jordan (US 8839417 B1) disclosed a system configured to analyze a received network communication; determine, based on information above the data link layer of the received network communication, if the received network communication is to be handled by a service available on a network; and respond affirmatively to a device sending the network communication that the service is available on the network. If it is determined that the service is available on the network, the code is configured to cause a processor to route received network communication to a component within the network that is configured to provide the service. If it is determined that the service is not available on the network, the code is configured to cause a processor to route the received network communication to a predetermined network component configured to analyze and interact with the received network communication and to generate rules based on analysis and interaction with the received network communication.

Bharali et al. (US 20140150051 A1) disclosed receiving a network policy that includes a domain name (e.g., the network policy can include a network security rule that is based on the domain name); and periodically updating Internet Protocol (IP) address information associated with the domain name by performing a Domain Name Server (DNS) query. In some embodiments, dynamic resolution of Fully Qualified Domain Name (FQDN) address objects in policy definitions includes dynamically performing a first local Domain Name Server (DNS) lookup for a first VSYS using a first DNS server on a first domain name for implementing a network policy based on the first domain name; dynamically performing a second local DNS lookup for a second VSYS using a second DNS server on the first domain name for implementing the network policy based on the first domain name; in which the network policy includes a network

security rule that is based on the first domain name, and the network policy includes a network security rule that is based on the second domain name.

However, the prior art of record, taken by itself or in any combination, **do not** anticipate or make obvious the invention of the present application and in particular the claim features listed above.

8. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicants' disclosure.

a. **Xu et al., ("Source Address Filtering Firewall to Defend against Denial of Service Attacks", September 2004, IEEE 60th Vehicular Technology Conference, Vol. 5, pp. 3296-3300)**

b. **Lyon (US 20140245421 A1)**

c. **Sampath et al. (US 8738906 B1)**

d. **Stevens et al. (US 20150135325 A1)**

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kenneth W Chang whose telephone number is (571)270-7530. The examiner can normally be reached on Monday - Friday 9-5pm EST.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on 571-272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see https://ppair-my.uspto.gov/pair/PrivatePair. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/KENNETH W CHANG/
Primary Examiner, Art Unit 2438
UNITED STATES PATENT AND TRADEMARK OFFICE
07.28.2020

Notice of References Cited	Application/Control No. 16/728,766	Applicant(s)/Patent Under Reexamination Rogers et al.	
	Examiner Kenneth W Chang	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-8738906-B1	05-2014	Sampath; Dhananjay	H04N21/643	713/166
*	B	US-20150135325-A1	05-2015	Stevens; Gene	H04L63/1425	726/25
*	C	US-20140245421-A1	08-2014	Lyon; Barrett Gibson	H04L61/2539	726/11
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Xu et al., Source Address Filtering Firewall to Defend against Denial of Service Attacks, September 2004, IEEE 60th Vehicular Technology Conference, Vol. 5, pp. 3296-3300 (Year: 2004)
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/728,766	Rogers et al.
	Examiner	**Art Unit**
	Kenneth W Chang	2438

CPC						
Symbol					**Type**	**Version**
H04L	/	63	/	20	F	2013-01-01
H04L	/	63	/	0236	I	2013-01-01
H04L	/	63	/	0263	I	2013-01-01
H04L	/	63	/	0218	I	2013-01-01
H04L	/	63	/	0209	I	2013-01-01
H04L	/	67	/	02	I	2013-01-01

CPC Combination Sets							
Symbol					**Type**	**Set**	**Ranking**	**Version**
	/		/					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	27	
/KENNETH W CHANG/ Primary Examiner, Art Unit 2438	28 July 2020	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	5

U.S. Patent and Trademark Office

Part of Paper No.: 20200727a

Keysight Technologies Ex. 1002
Page 79 of 460

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/728,766	Rogers et al.
	Examiner	**Art Unit**
	Kenneth W Chang	2438

INTERNATIONAL CLASSIFICATION					
CLAIMED					
H04L	/	29	/	06	

NON-CLAIMED					
	/		/		

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					

NONE (Assistant Examiner) (Date)	**Total Claims Allowed:** 27	
/KENNETH W CHANG/ Primary Examiner, Art Unit 2438 (Primary Examiner) 28 July 2020 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 5

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/728,766	Rogers et al.
	Examiner	**Art Unit**
	Kenneth W Chang	2438

☑ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	27	
/KENNETH W CHANG/ Primary Examiner, Art Unit 2438	28 July 2020	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	5

U.S. Patent and Trademark Office

Part of Paper No.: 20200727a

Keysight Technologies Ex. 1002
Page 81 of 460

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/728,766	Rogers et al.
	Examiner	Art Unit
	Kenneth W Chang	2438

CPC - Searched*		
Symbol	**Date**	**Examiner**
H04L63/20	04/11/2020	KC
H04L63/0209	04/11/2020	KC
H04L63/0218	04/11/2020	KC
H04L63/0236	04/11/2020	KC
H04L67/02	04/11/2020	KC
H04L63/20	07/27/2020	KC
H04L63/0209	07/27/2020	KC
H04L63/0218	07/27/2020	KC
H04L63/0236	07/27/2020	KC
H04L67/02	07/27/2020	KC

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

/KENNETH W CHANG/ Primary Examiner, Art Unit 2438	

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/728,766	Rogers et al.
	Examiner	**Art Unit**
	Kenneth W Chang	2438

Search Notes		
Search Notes	**Date**	**Examiner**
Searched Inventors' Names and Assignee on PE2E DAV and EAST databases.	04/11/2020	KC
Searched IQ IP.com NPL database.	04/11/2020	KC
Completed Limited Classified Search in CPC on EAST USPAT, PGPUB, and EPO databases with Keywords.	04/12/2020	KC
Keywords: (malware or malicious) with (traffic or packet) with (data or information or feedback) and rule with packet with filter$9 with (updat $9)	04/12/2020	KC
Updated Limited Classified Search in CPC on EAST USPAT, PGPUB , and EPO databases with Keywords. See East Search History.	07/27/2020	KC
Keywords: (address with (malicious or malware or blacklist$9) with (traffic or packet$5) with service) same (filter$9)	07/27/2020	KC
Updated NPL search on IEEE Xplore Database online.	07/27/2020	KC
Interference Search Completed on USPAT with claim language search. See EAST SEARCH HISTORY for interference searches.	07/27/2020	KC

/KENNETH W CHANG/ Primary Examiner, Art Unit 2438	

Keysight Technologies Ex. 1002
Page 83 of 460

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/728,766	Rogers et al.
	Examiner	Art Unit
	Kenneth W Chang	2438

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**
	(address AND (malicious or malware or blacklist$9) AND (traffic or packet$5) AND service AND (filter$9) AND (polic$5 or rule)).CLM.	07/27/2020	KC
	(address AND (malicious or malware or blacklist$9) AND (traffic or packet$5) AND service AND (filter$9) AND (polic$5 or rule) AND gateway AND (secure or security)).CLM.	07/27/2020	KC
	(address AND (malicious or malware or blacklist$9) AND (traffic or packet$5) AND service AND (filter$9) AND (polic$5 or rule) AND gateway AND match$9).CLM.	07/27/2020	KC
	(address AND (malicious or malware or blacklist$9) AND (traffic or packet$5) AND service AND (filter$9) AND (polic$5 or rule) AND gateway AND (transform$9 or function)).CLM.	07/27/2020	KC
	(address AND (malicious or malware or blacklist$9) AND (traffic or packet$5) AND service AND (filter$9) AND (polic$5 or rule) AND gateway AND (updat $9)).CLM.	07/27/2020	KC
	(address AND (malicious or malware or blacklist$9) AND (traffic or packet$5) AND service AND (filter$9) AND (polic$5 or rule) AND gateway AND (creat$9 or modif$9 or alter$9)).CLM.	07/27/2020	KC
	(address AND (malicious or malware or blacklist$9) AND (traffic or packet$5) AND service AND (filter$9) AND (polic$5 or rule) AND (third with party)).CLM.	07/27/2020	KC
	(address AND (malicious or malware or blacklist$9) AND (traffic or packet$5) AND service AND (filter$9) AND (polic$5 or rule) AND gateway AND (secure or security) AND protect$9).CLM.	07/27/2020	KC

/KENNETH W CHANG/ Primary Examiner, Art Unit 2438	

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

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. 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	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\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
/KC/	1	20130081102	A1	2013-03-28	Beauvais et al.	
/KC/	2	20120311693	A1	2012-12-06	Horman 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							

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

NON-PATENT LITERATURE DOCUMENTS Remove

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\US

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]
/KC/	1	2020 July 02 - (US) Final Rejection - US App 16/158,868	

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

EXAMINER SIGNATURE

Examiner Signature	/KENNETH W CHANG/	Date Considered	07/27/2020

*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.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L18	1	"20140245421".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/07/27 10:32
L17	1	"20150135325".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/07/27 10:31
L16	3	H04L67/02.CPC. and (address with (malicious or malware or blacklist$9) with (traffic or packet$5) with service) same (filter$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2020/07/27 10:28
L15	16	H04L63/0236.CPC. and (address with (malicious or malware or blacklist$9) with (traffic or packet$5) with service) same (filter$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2020/07/27 10:27
L14	0	H04L63/0218.CPC. and (address with (malicious or malware or blacklist$9) with (traffic or packet$5) with service) same (filter$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2020/07/27 10:27
L13	0	H04L63/0209.CPC. and (address with (malicious or malware or blacklist$9) with (traffic or packet$5) with service) same (filter$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2020/07/27 10:27
L12	67	H04L63/20.CPC. and (address with (malicious or malware or blacklist$9) with (traffic or packet$5) with service) same (filter$9)	US-PGPUB; USP	ADJ	ON	2020/07/27 10:27

			AT; EPO			
L11	5	(address with (malicious or malware or blacklist$9) with (traffic or packet$5) with service) same (filter$9) same (polic$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2020/07/27 10:25
L10	140	(address with (malicious or malware or blacklist$9) with (traffic or packet$5) with service) same (filter$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2020/07/27 10:24
L9	481	(address with (malicious or malware or blacklist$9) with (traffic or packet$5) with service)	US-PGPUB; USPAT; EPO	ADJ	ON	2020/07/27 10:24
L8	69	(malware or malicious) with (service or track$5) with (traffic or informat$9) and rule with packet with filter$9 with (creat$9 or updat$9 or alter$9 or generat$9 or new)	US-PGPUB; USPAT; EPO	ADJ	ON	2020/07/27 09:55
L7	54	(malware or malicious) with (traffic or packet) with (data or information or feedback) and rule with packet with filter$9 with (updat$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2020/07/27 09:54
L6	3,887	H04L63/0263.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/07/27 09:54
L5	40,825	H04L67/02.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/07/27 09:54
L4	4,111	H04L63/0236.CPC.	US-PGPUB; USP	ADJ	ON	2020/07/27 09:54

			AT; EPO			
L3	1,187	H04L63/0218.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/07/27 09:54
L2	2,132	H04L63/0209.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/07/27 09:53
L1	18,377	H04L63/20.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/07/27 09:53
S290	8	H04L63/0209.CPC. AND (firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9)) same polic$9 same (packet or data or datagram or traffic) and (malicious or malware or attack$9 or intrusion or ddos or protect$9) and (server with (external or outside))	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/12 15:00
S289	61	H04L63/20.CPC. AND (firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9)) same polic$9 same (packet or data or datagram or traffic) and (malicious or malware or attack$9 or intrusion or ddos or protect$9) and (server with (external or outside))	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/12 15:00
S288	192	("20080028467" | "20080043739" | "20080072307" | "20080077705" | "20080080493" | "20080086435" | "20080101234" | "20080163333" | "20080201772" | "20080229415" | "20080235755" | "20080279196" | "20080301765" | "20080313738" | "20080320116" | "20090028160" | "20090138938" | "20090144819" | "20090150972" | "20090172800" | "20090222877" | "20090240698" | "20090262723" | "20090262741" | "20090300759" | "20090328219" | "20100011433" | "20100011434" | "20100082811" | "20100095367" | "20100107240" | "20100115621" | "20100132027" | "20100195503" | "20100199346" | "20100202299" | "20100211678" | "20100232445" | "20100242098" | "20100268799" | "20100296441" | "20100303240" | "20110055916" | "20110055923" | "20110088092" | "20110141900" | "20110154470" | "20110185055" | "20110214157" | "20110270956" | "20110277034" | "20120023576" | "20120084866" | "20120106354" |	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/12 14:41

		"20120110656" | "20120113987" | "20120240135" | "20120240185" | "20120264443" | "20120314617" | "20120331543" | "20130007257" | "20130047020" | "20130059527" | "20130061294" | "20130104236" | "20130117852" | "20130139236" | "20130254766" | "20130291100" | "20130305311" | "20140075510" | "20140082204" | "20140082730" | "20140115654" | "20140150051" | "20140201123" | "20140215561" | "20140215574" | "20140245423" | "20140259170" | "20140281030" | "20140283004" | "20140283030" | "20140317397" | "20140317737" | "20140337613" | "20140365372" | "20140366132" | "20150033336" | "20150052601" | "20150106930" | "20150128274" | "20150135325" | "20150207809" | "20150237012" | "20150244734" | "20150256431" | "20150304354" | "20150334125" | "20150341389" | "20150347246" | "20150350229" | "20150372977" | "20150373043" | "20160020968" | "20160028751" | "20160065611" | "20160112443" | "20160119365" | "20160127417" | "20160191558" | "20160205069" | "20160219065" | "20160285706" | "20160294870" | "20160366099" | "20170223046" | "20170272469" | "6098172" | "6147976" | "6226372" | "6279113" | "6317837" | "6484261" | "6611875" | "6662235" | "6678827" | "6826694" | "6907042" | "6971028" | "7089581" | "7095716" | "7107613" | "7143438" | "7152240" | "7185368" | "7215637" | "7225269" | "7227842" | "7237267" | "7263099" | "7296288" | "7299353" | "7331061" | "7478429" | "7499412" | "7539186" | "7610621" | "7684400" | "7710885" | "7721084" | "7792775" | "7814158" | "7814546" | "7818794" | "7849502" | "7913303" | "7954143" | "8004994" | "8009566" | "8037517" | "8042167" | "8117655" | "8156206" | "8176561" | "8219675" | "8271645" | "8306994" | "8307029" | "8331234" | "8422391" | "8495725" | "8510821" | "8726379" | "8789135" | "8806638" | "8832832" | "8856926" | "8935785" | "9094445" | "9124552" | "9137205" | "9154446" | "9160713" | "9172627" | "9419942" | "9531672" | "9634911" | "9686193").PN.				
S287	90	("20010039579" | "20010039624" | "20020016858" | "20020038339" | "20020049899" | "20020083345" | "20020112188" | "20020152209" | "20020164962" | "20020165949" | "20020186683" | "20020198981" | "20030005122" | "20030014665" | "20030018591" | "20030035370" | "20030051026" | "20030088787" | "20030097590" | "20030105976" | "20030120622" | "20030123456" | "20030142681" | "20030145225" | "20030154297" | "20030154399" | "20030188192" | "20030212900" | "20030220940" | "20040010712" | "20040015719" | "20040073655" | "20040088542" | "20040093513" | "20040098511" | "20040114518" | "20040123220" | "20040131056" | "20040148520" | "20040151155" | "20040172529" | "20040172557" | "20040177139" | "20040181690" | "20040193943" | "20040199629" | "20040205360" | "20040250124" |	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/12 14:41

		"20050010765" | "20050024189" | "20050071650" | "20050076227" | "20050108557" | "20050114704" | "20050117576" | "20050125697" | "20050138204" | "20050138353" | "20050141537" | "20050183140" | "20050229246" | "20050249214" | "20050251570" | "20050283823" | "20050286522" | "20060031928" | "20060048142" | "20060053491" | "20060070122" | "20060080733" | "20060085849" | "20060104202" | "20060114899" | "20060133377" | "20060136987" | "20060137009" | "20060146879" | "20060159028" | "20060195896" | "20060212572" | "20060248580" | "20060262798" | "20070056038" | "20070083924" | "20070118894" | "20070147380" | "20070211644" | "20070240208" | "20070291789" | "20080005795").PN.				
S286	1	"20060123481".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 21:16
S285	1	"20090150996".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 21:00
S284	8	(malware or malicious) with (traffic or packet) with (data or information or feedback) same rule with packet with filter$9 with (updat$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 20:40
S283	51	(malware or malicious) with (traffic or packet) with (data or information or feedback) and rule with packet with filter$9 with (updat$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 20:40
S282	67	(malware or malicious) with (service or track$5) with (traffic or informat$9) and rule with packet with filter$9 with (creat$9 or updat$9 or alter$9 or generat$9 or new)	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 17:37
S281	0	(malware or malicious) with (service or track$5) with (traffic or informat$9) same rule with packet with filter$9 with (creat$9 or updat$9 or alter$9 or generat$9 or new)	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 17:36

S280	0	(malware or malicious) with (host) with (track$9) with (service or informat$9) same rule with packet with filter$9 with (creat$9 or updat$9 or alter$9 or generat$9 or new)	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 17:34
S278	0	(malware or malicious) with (track$9) with (service or informat$9) with rule with packet with filter$9 with (creat$9 or updat$9 or alter$9 or generat$9 or new)	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 17:33
S277	0	(malware or malicious) with (host) with (track$9) with (service or informat$9) with rule with packet with filter$9 with (creat$9 or updat$9 or alter$9 or generat$9 or new)	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 17:21
S276	0	(malware or malicious) with (host) with (track$9) with (service or informat$9) with rule with packet with filter$9 with (creat$9 or updat$9 or alter$9 or generat$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 17:21
S275	1	"20070118894".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 16:14
S274	1	"20060059551".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 12:08
S273	1	"20080244726".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 12:06
S272	1	"20030088788".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 12:04

S271	1	"20030118038".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 12:00
S270	1	"20120069749".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 11:58
S269	1	"6230271".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 11:58
S268	1	"20080016550".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 11:27
S267	1	"20110016509".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 11:12
S266	93	(firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9)) same polic$9 same (packet or data or datagram or traffic) and (malicious or malware or attack$9 or intrusion or ddos or protect$9) and (server with (external or outside))	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 11:07
S265	1	"20030154399".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 10:59
S264	1	"20070271605".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 10:52

S263	1	"6400707".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 10:47
S262	39,467	H04L67/02.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 10:45
S261	3,914	H04L63/0236.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 10:45
S260	1,150	H04L63/0218.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 10:45
S259	2,058	H04L63/0209.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 10:45
S258	17,591	H04L63/20.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 10:45
S257	34	(centripetal networks).as.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 10:44
S256	188	(moore adj3 sean).in.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 10:44

S255	607	(rogers adj3 steven).in.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 10:44
S254	4	(10567437 | 10091246 | 9560077 | 9137205).pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/03/20 21:17
S253	29	H04L63/0218.CPC. and (firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9)) same polic$9 and (malicious or malware or attack$9 or intrusion) same (packet$9 or frame or traffic$)	US-PGPUB; USPAT; EPO	ADJ	ON	2019/12/04 15:20
S252	3	(20080040793 | 20130117801 | 7853996).pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/12/04 15:20
S251	196	H04L63/0263.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing)	US-PGPUB; USPAT; EPO	ADJ	ON	2019/12/04 15:17
S250	1,047	(set or list$5) with (addresses) with (ip or internet protocol or source) with (discard$9 or block$6 or drop$5) same (packet) and (forward$9 or allow$8) with (outside or otherwise or address$5) same (packet) with (address$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2019/12/04 15:17
S249	117	(firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9)) same polic$9 and (malicious or malware or attack$9 or intrusion) same (packet$9 or frame or traffic$)	US-PGPUB; USPAT; EPO	ADJ	ON	2019/12/04 15:17
S239	62	("20020083345" | "20020152209" | "20030005122" | "20030014665" | "20030088787" | "20040015719" | "20040114518" | "20040131056" | "20050249214" | "20060031928" | "20070056038" | "20070291789" | "20080028467" | "20080080493" | "20080086435" | "20080101234" | "20080201772" | "20080313738" | "20080320116" | "20090144819" | "20090262723" |	US-PGPUB; USPAT; EPO	ADJ	ON	2019/12/03 17:00

		"20090300759" | "20100115621" | "20100195503" | "20100202299" | "20110214157" | "20120084866" | "20120110656" | "20120240185" | "20130007257" | "20130139236" | "20140082204" | "20140082730" | "20140215561" | "20140337613" | "20150128274" | "20150135325" | "20150207809" | "20150256431" | "20150347246" | "20160028751" | "20160127417" | "20160191558" | "20170223046" | "20170272469" | "6907042" | "6971028" | "7152240" | "7185368" | "7225269" | "7499412" | "7849502" | "8156206" | "8219675" | "8271645" | "8331234" | "8422391" | "8510821" | "9531672" | "9634911" | "9686193").PN.				
S238	37,877	H04L67/02.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/12/03 16:57
S237	3,704	H04L63/0236.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/12/03 16:57
S236	1,116	H04L63/0218.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/12/03 16:57
S235	20	H04L63/0209.CPC. and (firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9)) same polic$9 and (malicious or malware or attack$9 or intrusion) same (packet$9 or frame or traffic$)	US-PGPUB; USPAT; EPO	ADJ	ON	2019/12/03 16:57
S234	16,620	H04L63/20.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/12/03 16:57
S233	1	"20090262741".PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/21 14:06

S232	43	H04L63/0263.CPC. and (firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9)) same polic$9 and (malicious or malware or attack$9 or intrusion) same (packet$9 or frame or traffic$)	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/21 10:32
S231	18	H04L63/0236.CPC. and (firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9)) same polic$9 and (malicious or malware or attack$9 or intrusion) same (packet$9 or frame or traffic$)	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/21 10:31
S230	26	H04L63/0218.CPC. and (firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9)) same polic$9 and (malicious or malware or attack$9 or intrusion) same (packet$9 or frame or traffic$)	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/21 10:31
S229	18	H04L63/0209.CPC. and (firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9)) same polic$9 and (malicious or malware or attack$9 or intrusion) same (packet$9 or frame or traffic$)	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/21 10:31
S228	39	H04L63/20.CPC. and (firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9)) same polic$9 and (malicious or malware or attack$9 or intrusion) same (packet$9 or frame or traffic$)	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/21 10:31
S227	109	(firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9)) same polic$9 and (malicious or malware or attack$9 or intrusion) same (packet$9 or frame or traffic$)	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/21 10:30
S226	15	(firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9)) same polic$9 same (malicious or malware or attack$9 or intrusion) same (packet$9 or frame or traffic$)	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/21 10:17
S225	38	(firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9)) same polic$9 same (malicious or malware or attack$9 or intrusion)	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/21 10:16

S224	454	(firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9)) same polic$9	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/21 10:16
S223	3,300	(firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9 or polic$9))	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/21 10:16
S222	1	"20140090046".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 22:35
S221	1	"20050076227".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 20:34
S220	1	"20120069749".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 20:32
S219	0	(updat$9 with policy with rule with (signat9 or criter$5) same (drop$9)) same packet	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 18:33
S218	2	(updat$9 with policy with rule with (signat9 or criter$5) same (drop$9))	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 18:33
S217	1	(updat$9 with policy with rule with (signat9 or criter$5) with (encapsulat$9 or replac$9 or insert$9))	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 18:32

S216	0	(updat$9 with policy with rule with signat9 with (encapsulat$9 or replac$9 or insert$9)) same (router or gateway)	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 18:32
S215	0	(updat$9 with policy with rule with signat9 with (encapsulat$9 or replac$9 or insert$9))same gateway	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 18:32
S214	35,632	H04L67/02.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 13:52
S213	3,229	H04L63/0263.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 13:52
S212	3,395	H04L63/0236.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 13:52
S211	1,064	H04L63/0218.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 13:52
S210	1,813	H04L63/0209.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 13:52
S209	15,017	H04L63/20.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 13:51

S208	162	(moore adj3 sean).in.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 13:50
S207	569	(rogers adj3 steven).in.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 13:50
S206	23	(centripetal networks).as.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 13:50
S205	3	(10091246 | 9560077 | 9137205).pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/16 14:18
S204	1	"9894051".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2018/05/10 16:43
S203	67	H04L67/02.CPC. and (rule) with (set or group or subset or subgroup) with address$5 same network$9 same (traffic or packet$9) and (filter$9 or firewall or router or rout$9 or intrusion or ids)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/27 13:36
S202	193	H04L63/0263.CPC. and (rule) with (set or group or subset or subgroup) with address$5 same network$9 same (traffic or packet$9) and (filter$9 or firewall or router or rout$9 or intrusion or ids)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/27 13:36
S201	82	H04L63/0236.CPC. and (rule) with (set or group or subset or subgroup) with address$5 same network$9 same (traffic or packet$9) and (filter$9 or firewall or router or rout$9 or intrusion or ids)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/27 13:36

S200	33	H04L63/0218.CPC. and (rule) with (set or group or subset or subgroup) with address$5 same network$9 same (traffic or packet$9) and (filter$9 or firewall or router or rout$9 or intrusion or ids)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/27 13:36
S199	28	H04L63/0209.CPC. and (rule) with (set or group or subset or subgroup) with address$5 same network$9 same (traffic or packet$9) and (filter$9 or firewall or router or rout$9 or intrusion or ids)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/27 13:36
S198	148	H04L63/20.CPC. and (rule) with (set or group or subset or subgroup) with address$5 same network$9 same (traffic or packet$9) and (filter$9 or firewall or router or rout$9 or intrusion or ids)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/27 13:35
S197	1,414	(rule) with (set or group or subset or subgroup) with address$5 same network$9 same (traffic or packet$9) and (filter$9 or firewall or router or rout$9 or intrusion or ids)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/27 13:35
S196	42	H04L63/20.CPC. AND (rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9) and network$9 same (border$5 or boundary or boundaries) and (head or header or heading) and (vlan or virtual$5 local area network or virtual$5 lan)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/27 13:35
S195	1	"8009566" .pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/27 13:34
S194	1	"6279113".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/27 13:33
S193	1	"20140150051".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/27 13:24

S192	1,425	(rule) with (set or group or subset) with address$5 same network$9 same (traffic or packet$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/27 12:21
S191	152	("20010039579" | "20010039624" | "20020016858" | "20020038339" | "20020049899" | "20020164962" | "20020165949" | "20020186683" | "20020198981" | "20030035370" | "20030097590" | "20030105976" | "20030120622" | "20030123456" | "20030142681" | "20030145225" | "20030154297" | "20030154399" | "20030188192" | "20030212900" | "20040010712" | "20040073655" | "20040088542" | "20040093513" | "20040098511" | "20040151155" | "20040177139" | "20040193943" | "20040205360" | "20040250124" | "20050010765" | "20050024189" | "20050114704" | "20050117576" | "20050125697" | "20050138204" | "20050141537" | "20050183140" | "20050229246" | "20050251570" | "20050286522" | "20060048142" | "20060053491" | "20060070122" | "20060104202" | "20060114899" | "20060136987" | "20060137009" | "20060146879" | "20060195896" | "20060212572" | "20060248580" | "20060262798" | "20070083924" | "20070211644" | "20070240208" | "20080005795" | "20080043739" | "20080072307" | "20080077705" | "20080163333" | "20080229415" | "20080235755" | "20080279196" | "20080301765" | "20090138938" | "20090172800" | "20090222877" | "20090240698" | "20090328219" | "20100011433" | "20100011434" | "20100082811" | "20100095367" | "20100107240" | "20100132027" | "20100199346" | "20100211678" | "20100232445" | "20100242098" | "20100268799" | "20100296441" | "20100303240" | "20110055916" | "20110055923" | "20110088092" | "20110141900" | "20110185055" | "20110270956" | "20120023576" | "20120106354" | "20120113987" | "20120240135" | "20120264443" | "20120314617" | "20120331543" | "20130047020" | "20130059527" | "20130061294" | "20130117852" | "20130254766" | "20130305311" | "20140075510" | "20140115654" | "20140201123" | "20140215574" | "20140281030" | "20140283004" | "20140283030" | "20140366132" | "20150237012" | "20150304354" | "20150334125" | "6098172" | "6147976" | "6226372" | "6317837" | "6484261" | "6611875" | "6662235" | "7089581" | "7107613" | "7215637" | "7227842" | "7237267" | "7263099" | "7299353" | "7331061" | "7478429" | "7539186" | "7610621" | "7684400" | "7710885" | "7721084" | "7818794" | "7954143" | "8004994" | "8037517" | "8042167" | "8117655" | "8176561" | "8306994" | "8495725" | "8726379" | "8806638" | "8856926" | "8935785" | "9094445" | "9124552" | "9137205" | "9154446" | "9160713").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/26 22:49

S190	458	(rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9) and network$9 same (border$5 or boundary or boundaries) and (head or header or heading) and (vlan or virtual$5 local area network or virtual$5 lan)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/26 20:12
S189	28,348	H04L67/02.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/26 20:12
S188	2,517	H04L63/0263.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/26 20:12
S187	2,500	H04L63/0236.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/26 20:12
S186	893	H04L63/0218.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/26 20:11
S185	1,445	H04L63/0209.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/26 20:11
S184	11,470	H04L63/20.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/26 20:11
S183	16	(centripetal networks).as.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/26 20:11

S182	128	(moore adj3 sean).in.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/26 20:11
S181	541	(rogers adj3 steven).in.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/26 20:11
S180	2	(9560077 | 9137205).PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/26 20:03
S171	3	(6147976 | 9154446 | 7610621).pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/09/22 15:55
S170	16	H04L63/0218.CPC. AND rule and (drop$5 or discard$5) with (packet or flow or flood or frame) same (switch or router or hub) and (lan or local area network) AND (zone or edge or boundary)	US-PGPUB; USPAT; EPO	ADJ	ON	2016/09/22 15:48
S169	189	H04L63/0236.CPC. AND rule and (drop$5 or discard$5) with (packet or flow or flood or frame) same (switch or router or hub) and (lan or local area network) AND (zone or edge or boundary)	US-PGPUB; USPAT; EPO	ADJ	ON	2016/09/22 15:48
S168	27	H04L63/0209.CPC. AND rule and (drop$5 or discard$5) with (packet or flow or flood or frame) same (switch or router or hub) and (lan or local area network) AND (zone or edge or boundary)	US-PGPUB; USPAT; EPO	ADJ	ON	2016/09/22 15:48
S167	210	H04L63/20.CPC. AND rule and (drop$5 or discard$5) with (packet or flow or flood or frame) same (switch or router or hub) and (lan or local area network) AND (zone or edge or boundary)	US-PGPUB; USPAT; EPO	ADJ	ON	2016/09/22 15:48

S166	780	H04L63/0218.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/09/22 15:47
S165	2,077	H04L63/0236.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/09/22 15:47
S164	22,610	H04L67/02.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/09/22 15:47
S163	1,249	H04L63/0209.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/09/22 15:47
S162	9,210	H04L63/20.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/09/22 15:47
S161	4,596	rule and (drop$5 or discard$5) with (packet or flow or flood or frame) same (switch or router or hub) and (lan or local area network) AND (zone or edge or boundary)	US-PGPUB; USPAT; EPO	OR	ON	2016/09/22 15:46
S160	146	("20030142681" | "20030212900" | "20050117576" | "20070083924" | "20080005795" | "20100082811" | "20110055916" | "20120314617" | "20130059527" | "8806638" | "20110185055" | "20120331543" | "20010039624" | "20070240208" | "6317837" | "20020016858" | "20060262798" | "20050251570" | "20150304354" | "7237267" | "20050010765" | "20140115654" | "7263099" | "20100095367" | "8176561" | "20050138204" | "20060212572" | "20100211678" | "20100296441" | "7539186" | "7684400" | "20060146879" | "8306994" | "20080043739" | "20020198981" | "20050286522" | "20080077705" | "20100303240" | "20140281030" | "7954143" | "20040177139" | "20040205360" | "20140283004" | "20150237012" | "7107613" | "7237267" | "7331061" | "8495725" | "20060053491" | "20120023576" |	US-PGPUB; USPAT; EPO	OR	ON	2016/09/22 15:29

		"20130305311" | "20060248580" | "20090328219" | "20110088092" | "20120113987" | "8935785" | "20030154297" | "20020049899" | "20030035370" | "9137205" | "20040193943" | "20040205360" | "20050010765" | "20050114704" | "20140215574" | "20140283004" | "20140283030" | "7299353" | "20050114704" | "20050183140" | "20060104202" | "20060212572" | "20090138938" | "20140201123" | "6098172" | "7089581" | "20040093513" | "7215637" | "20030145225" | "20060048142" | "20060195896" | "20120264443" | "7818794" | "20140366132" | "20020038339" | "20050183140" | "20050229246" | "20060212572" | "20070083924" | "20080229415" | "20080301765" | "20100199346" | "20150237012" | "7089581" | "7263099" | "9124552" | "9160713" | "20020038339" | "20040010712" | "20040088542" | "20050251570" | "20060070122" | "20100199346" | "20110055923" | "6484261" | "7299353" | "20090240698" | "20110185055" | "20120106354" | "20140075510" | "20050141537" | "20080072307" | "20090172800" | "20100132027" | "6226372" | "20060114899" | "20130061294" | "8726379" | "20060048142" | "20060070122" | "6098172" | "7107613" | "20050286522" | "20140281030" | "20150304354" | "7227842" | "7954143" | "20020186683" | "20030154399" | "20040098511" | "20100011434" | "7478429" | "8004994" | "20030097590" | "20030123456" | "20100242098" | "20020165949" | "20040073655" | "20090138938" | "20100268799" | "20140201123" | "6484261" | "7227842" | "7331061" | "8042167" | "8495725" | "9094445" | "20040193943" | "20050229246" | "20080229415" | "20140283030" | "8037517" | "9124552" | "20080163333" | "20090222877" | "20100107240" | "20130117852" | "8117655" | "20030188192" | "20040088542" | "20040151155" | "20080235755" | "20110270956" | "7710885" | "7721084" | "20110055916" | "20040177139" | "20060104202" | "20100011433" | "6662235" | "20020165949" | "20020198981" | "20050125697" | "20060048142" | "20100303240" | "9094445" | "9160713" | "20010039579" | "20040250124" | "20130047020" | "20120240135" | "6611875" | "8856926" | "20130254766" | "20060136987" | "20080279196" | "20030120622" | "20040010712" | "20040088542" | "20050125697" | "20110055923" | "20140115654" | "8037517" | "20030120622" | "20040073655" | "20070083924" | "20080077705" | "20080301765" | "20100011433" | "20100268799" | "20140215574" | "6662235" | "8042167" | "20030105976" | "20060137009" | "20070211644" | "20100232445" | "20150334125").PN.				
S159	100	(US-6137792-$ or US-6055236-$ or US-5706348-$ or US-5710760-$ or US-5805705-$ or US-5987520-$ or US-5991401-$ or US-6011910-$ or US-6026085-$ or US-6147987-$ or US-6233232-$ or US-4774658-$ or US-4799153-$ or US-4901348-$ or US-4965804-$ or US-5247513-$ or US-5251203-$ or US-5280529-$ or US-5442708-$ or US-5444782-$ or US-5485455-$	USPAT	OR	ON	2016/01/06 13:46

		or US-5490252-$ or US-5491694-$ or US-5521910-$ or US-5615340-$ or US-5640456-$).did. or (US-5642421-$ or US-5657452-$ or US-5684800-$ or US-5729594-$ or US-5737318-$ or US-5751952-$ or US-5768525-$ or US-5781550-$ or US-5790546-$ or US-5796942-$ or US-5799285-$ or US-5828846-$ or US-5864683-$ or US-5896499-$ or US-5913037-$ or US-5935249-$ or US-5946308-$ or US-5950172-$ or US-5953337-$ or US-6009528-$ or US-6035405-$ or US-6070243-$ or US-6081524-$ or US-6084858-$ or US-6098173-$ or US-6101539-$ or US-6101170-$).did. or (US-6118775-$ or US-6141755-$ or US-6148402-$ or US-6147995-$ or US-6167052-$ or US-6172991-$ or US-6188671-$ or US-6195705-$ or US-6199113-$ or US-6202081-$ or US-6230002-$ or US-6230271-$ or US-6249519-$ or US-4332980-$ or US-4445214-$ or US-4509073-$ or US-4768204-$ or US-4771422-$ or US-4787082-$ or US-4802220-$ or US-4823389-$ or US-4866770-$ or US-4872160-$ or US-4896319-$ or US-4922486-$ or US-4985895-$ or US-5048087-$).did. or (US-5029207-$ or US-5220501-$ or US-5228083-$ or US-5235644-$ or US-5237610-$ or US-5247380-$ or US-5261044-$ or US-5261059-$ or US-5268962-$ or US-5282244-$ or US-5295244-$ or US-5303302-$ or US-5303303-$ or US-5311593-$ or US-5313465-$ or US-5319712-$ or US-5351287-$ or US-5353353-$ or US-5386471-$ or US-5394469-$).did.				
S158	254	(encapsul$9) with (packet) with (header or heading) with (address) with (destination) with (different or new or alternate)	US-PGPUB; USPAT; EPO	OR	ON	2016/01/06 11:55
S157	64	("20030142681" | "20030212900" | "20050117576" | "20070083924" | "20080005795" | "20100082811" | "20110055916" | "20120314617" | "20130059527" | "8806638" | "20110185055" | "20120331543" | "20010039624" | "20070240208" | "6317837" | "20050138204" | "20060212572" | "20100211678" | "20100296441" | "7539186" | "7684400" | "20060146879" | "8306994" | "20060248580" | "20090328219" | "20110088092" | "20120113987" | "8935785" | "20030154297" | "20020049899" | "20030035370" | "9137205" | "20030145225" | "20060048142" | "20060195896" | "20120264443" | "7818794" | "20140366132" | "20050141537" | "20080072307" | "20090172800" | "20100132027" | "6226372" | "20060114899" | "20130061294" | "8726379" | "20100011434" | "7478429" | "8004994" | "20030097590" | "20030123456" | "20100242098" | "20030188192" | "20040088542" | "20040151155" | "20080235755" | "20110270956" | "7710885" | "7721084" | "20120240135" | "6611875" | "8856926" | "20130254766" | "20060136987").PN.	US-PGPUB; USPAT; EPO	OR	ON	2016/01/06 10:02
S156	1	"20080298373".pn.	US-PGPUB;	ADJ	ON	2016/01/05 14:25

			USPAT; EPO			
S155	1	"20060262798".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/01/05 14:20
S154	98	(vlan or virtual$5 lan) same different$5 with (rout$9) same (destination) with (address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service)	US-PGPUB; USPAT; EPO	ADJ	ON	2016/01/05 14:20
S153	157	(vlan or virtual$5 lan) same different$5 with (rout$9) same (destination) with (address)	US-PGPUB; USPAT; EPO	ADJ	ON	2016/01/05 14:07
S152	456	(vlan or virtual$5 lan) same (rout$9) same (destination) with (address) same different	US-PGPUB; USPAT; EPO	ADJ	ON	2016/01/05 14:07
S151	2,204	(vlan or virtual$5 lan) same (rout$9) same (destination) same (address)	US-PGPUB; USPAT; EPO	ADJ	ON	2016/01/05 14:07
S150	1	"20110055916".pn.	US-PGPUB; USPAT; EPO	OR	ON	2016/01/05 10:22
S148	1	"20080043739".pn.	US-PGPUB; USPAT; EPO	OR	ON	2016/01/05 10:20
S147	1	"9137205".pn.	US-PGPUB; USP	ADJ	ON	2016/01/04 16:47

			AT; EPO			
S145	1	"9137205".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:59
S144	176	H04L63/20.CPC. and (rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9) and network$9 same (border$5 or boundary or boundaries) and (head or header or heading)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:52
S143	43	H04L63/0263.CPC. and (rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9) and network$9 same (border$5 or boundary or boundaries) and (head or header or heading)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:52
S142	28	H04L63/0218.CPC. and (rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9) and network$9 same (border$5 or boundary or boundaries) and (head or header or heading)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:52
S141	12	H04L67/02.CPC. and (rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9) and network$9 same (border$5 or boundary or boundaries) and (head or header or heading) and (vlan or virtual$5 local area network or virtual$5 lan)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:52
S140	6	H04L63/0236.CPC. and (rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9) and network$9 same (border$5 or boundary or boundaries) and (head or header or heading) and (vlan or virtual$5 local area network or virtual$5 lan)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:52
S139	4	H04L63/0218.CPC. and (rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9)	US-PGPUB; USP	ADJ	ON	2015/12/30 15:51

		and network$9 same (border$5 or boundary or boundaries) and (head or header or heading) and (vlan or virtual$5 local area network or virtual$5 lan)	AT; EPO			
S138	12	H04L63/02.CPC. AND (rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9) and network$9 same (border$5 or boundary or boundaries) and (head or header or heading) and (vlan or virtual$5 local area network or virtual$5 lan)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:51
S137	29	H04L63/20.CPC. AND (rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9) and network$9 same (border$5 or boundary or boundaries) and (head or header or heading) and (vlan or virtual$5 local area network or virtual$5 lan)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:51
S136	314	(rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9) and network$9 same (border$5 or boundary or boundaries) and (head or header or heading) and (vlan or virtual$5 local area network or virtual$5 lan) and (rout$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:51
S135	314	(rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9) and network$9 same (border$5 or boundary or boundaries) and (head or header or heading) and (vlan or virtual$5 local area network or virtual$5 lan)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:51
S134	1,264	(rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9) and network$9 same (border$5 or boundary or boundaries) and (head or header or heading)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:49
S133	1,418	(rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9) and network$9 same (border$5 or boundary or boundaries)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:48

S132	1,418	(rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9) and network$9 same (border or boundary or boundaries)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:48
S131	3,288	(rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:48
S130	3,294	(rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip or internet protocol) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:47
S129	19,319	(rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip or internet protocol) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:47
S128	31,220	(rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip or internet protocol) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:47
S127	9	(centripetal networks).as.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:45
S126	110	(moore adj3 sean).in.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:45
S125	488	(rogers adj3 steven).in.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:45

S124	18,904	H04L67/02.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:44
S123	7,270	H04L63/20.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:44
S122	1,626	H04L63/0236.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:44
S121	1,853	H04L63/0263.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:44
S120	720	H04L63/0218.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:44
S119	35	H04L63/02.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing or rout$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:44
S118	123	H04L63/20.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing or rout$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:44
S117	8	("20020049899" | "20060136987" | "20060146879" | "20070240208" | "20100242098" | "20130061294" | "6317837" | "8306994").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/07/30 16:25

S116	6	("20030154297" | "20060114899" | "20110185055" | "20120331543" | "20130254766" | "8004994").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/07/30 16:25
S115	3	("7478429" | "7818794" | "8935785").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/07/22 10:50
S112	34	H04L63/20.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing or rout$9) and (edge or boundary or boundaries or border$5) with network	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 17:38
S111	51	H04L63/20.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing or rout$9) and (edge or boundary or boundaries or border$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 17:38
S110	96	H04L63/20.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing or rout$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 17:37
S109	8	H04L63/0218.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing or encapsul$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 17:36
S108	12	(US-20060212572-$ or US-20030145225-$ or US-20060048142-$ or US-20010039624-$ or US-20050138204-$ or US-20100296441-$ or US-20080072307-$ or US-20050141537-$ or US-20030142681-$ or US-20100082811-$ or US-20030035370-$ or US-20110088092-$).did.	US-PGPUB	ADJ	ON	2015/03/26 17:35
S107	6	("20030097590" | "20090328219" | "20120240135" | "20120314617" | "6611875" | "8806638").PN.	US-PGPUB;	ADJ	ON	2015/03/26 14:52

			USPAT; EPO			
S90	96	H04L63/20.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing or rout$9 or encapsul$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 12:26
S88	8	H04L63/0218.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing or rout$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 12:22
S87	67	H04L63/0263.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing or rout$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 12:22
S86	67	H04L63/0263.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 12:11
S85	96	H04L63/20.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 12:11
S84	8	H04L63/0218.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 12:11
S83	1,680	H04L63/0263.CPC.	US-PGPUB; USP	ADJ	ON	2015/03/26 12:04

			AT; EPO			
S82	5,918	H04L63/20.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 12:04
S81	655	H04L63/0218.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 12:04
S80	6	("20030097590" | "20090328219" | "20120240135" | "20120314617" | "6611875" | "8806638").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/14 21:26
S79	34	(SIP or session initiat$9 protocol) with (URI or uniform resourse) with (header or heading) same (network address$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/14 21:20
S78	1,202	(SIP or session initiat$9 protocol) with (URI or uniform resourse) with (header or heading)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/14 21:20
S77	1,806	(SIP or session initiat$9 protocol) same (URI or uniform resourse) same (header or heading)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/14 21:19
S76	114	(network with transparent$5 with layer) same address$9 same (link$9) and (secure or security or attack$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 14:01
S75	171	(network with transparent$5 with layer) same address$9 same (link$9)	US-PGPUB; USP	ADJ	ON	2015/02/24 14:00

			AT; EPO			
S74	539	(network with transparent$5 with layer) same address$9	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 14:00
S73	2	("20080005795" | "20090172800").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 13:49
S72	3	("7539186" | "7710885" | "8856926").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 13:48
S71	66	H04L63/0263.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 11:54
S70	88	H04L63/20.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 11:54
S69	8	H04L63/0218.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 11:54
S68	1,654	H04L63/0263.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 11:54

S67	5,709	H04L63/20.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 11:54
S66	647	H04L63/0218.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 11:53
S65	1	"20140115654".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 11:53
S64	26	713/1,100,150,151,152,153,154,155,166,167,168.CCLS. AND S61	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 02:26
S63	54	709/201,203,217,218,219,220,223,224,225,226,227,228,229,230,231,238,239,240,242,244,245.CCLS. AND S61	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 02:26
S62	31	726/3,6,11,12,13,14,15,16,17,22,23,24,25.CCLS. AND S61	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 02:26
S61	198	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing) same (ipsec or ip security or internet protocol security)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 02:26
S60	24,976	713/1,100,150,151,152,153,154,155,166,167,168.CCLS.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 02:26

S59	125,386	709/201,203,217,218,219,220,223,224,225,226,227,228,229,230,231,238,239,240,242,244,245.CCLS.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 02:26
S58	26,093	726/3,6,11,12,13,14,15,16,17,22,23,24,25.CCLS.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 02:24
S57	1	"20030035370".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 01:42
S56	1	"20050135375".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 01:39
S55	1	"20110088092".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 00:40
S54	69	(spoof$5) with (address$5) with (network or source) with (policy or policies or rule)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 00:28
S53	209	(spoof$5) with (address$5) with (network or source) same (policy or policies or rule)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 00:28
S52	1	"20100082811".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 00:08

S51	1	"20080279200".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 23:51
S50	5	(blacklist$5 or black list$9) with (addresses) with (paid or pay)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 23:46
S49	5	(blacklist$5 or black list$9) with (addresses) with (provider) with (subscription or subscribing or subscriber)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 23:42
S48	55	(blacklist$5 or black list$9) with (addresses) with (provider) with (service)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 23:41
S47	15	(blacklist$5 or black list$9) with (addresses) with (subscription or subscriber or subscribing) with (service)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 23:38
S46	222	(blacklist$5 or black list$9) with (addresses) same (subscription or subscriber or subscribing or customer)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 23:38
S45	2	(blacklist$5 or black list$9) with (addresses) with (discard$9 or block$6 or drop$5) with (packet) same (subscription or subscriber or subscribing or customer)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 23:38
S44	3	(differentiat$10 service code point select$5 or dscp select$5 or Diff-Serv Code Point) same (header or heading) same (traffic or packet) same (policy or policies or rule)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 22:48

S43	26	(differentiat$10 service code point select$5 or dscp select$5 or Diff-Serv Code Point) same (header or heading) same (traffic or packet)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 22:47
S42	10	(differentiat$10 service code point select$5 or dscp select$5) same (header or heading) same (traffic or packet)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 22:47
S41	34	(forward$9) with (packet) same (queue or group or buffer$5) same (priority) same (faster or higher) same (policy or policies or whitelist$5 or white list$8)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 21:56
S40	11	(discard$10 or block$5 or drop$5) and (forward$9 or allow$8) with (packet) with (address$5) same (policy or policies or whitelist$5 or white list$8) same (voip or voice over ip or voice over internet protocol) same (call or session or traffic or connection)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 20:32
S39	12	(discard$10 or block$5 or drop$5) and (forward$9 or allow$8) with (packet) with (address$5) same (policy or policies or whitelist$5 or white list$8) same (voip or voice over ip or voice over internet protocol)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 20:32
S38	223	(discard$10 or block$5 or drop$5) and (forward$9 or allow$8) with (packet) with (address$5) same (policy or policies or whitelist$5 or white list$8) and (voip or voice over ip or voice over internet protocol)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 20:31
S37	21	(discard$10 or block$5 or drop$5) and (forward$9 or allow$8) with (packet) with (address$5) with (whitelist$9 or white list$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 20:07
S36	5	(discard$10 or block$5 or drop$5) and (forward$9 or allow$8) with (packet) with (address$5) with (whitelist$9 or white list$5) with (only)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 20:07

S35	5	(addresses) with (ip or internet protocol or source) with (discard$9 or block$6 or drop$5) with (packet) and (forward$9 or allow$8) with (packet) with (address$5) with (whitelist$9 or white list$5) with (only)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 20:05
S34	15	(addresses) with (ip or internet protocol or source) with (discard$9 or block$6 or drop$5) with (packet) and (forward$9 or allow$8) with (outside or otherwise or address$5) with (packet) with (address$5) with (whitelist$9 or white list$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 20:04
S33	12	(blacklist$5 or black list$9) with (addresses) with (ip or internet protocol or source) with (discard$9 or block$6 or drop$5) with (packet) and (forward$9 or allow$8) with (outside or otherwise or address$5) with (packet) with (address$5) with (blacklist$5 or black list$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 18:28
S32	19	(blacklist$5 or black list$9) with (addresses) with (ip or internet protocol or source) with (discard$9 or block$6 or drop$5) with (packet) and (forward$9 or allow$8) with (outside or otherwise or address$5) with (packet) with (address$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 18:28
S31	1	(blacklist$5 or black list$5) with (address$9) with increas$9 with (policy or policies)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 18:26
S30	546	(set or list$5) with (addresses) with (ip or internet protocol or source) with (discard$9 or block$6 or drop$5) with (packet) and (forward$9 or allow$8) with (outside or otherwise or address$5) with (packet) with (address$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 18:24
S29	705	(set or list$5) with (addresses) with (ip or internet protocol or source) with (discard$9 or block$6 or drop$5) same (packet) and (forward$9 or allow$8) with (outside or otherwise or address$5) same (packet) with (address$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 18:24
S28	1,857	(set or list$5) with (addresses) with (ip or internet protocol or source) same (discard$9 or block$6 or drop$5) same (packet) and (forward$9 or allow$8) with (outside or otherwise or address$5) same (packet) same (address$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 18:24

S27	8,993	(set or list$5) with (addresses) with (ip or internet protocol or source) same (discard$9 or block$6 or drop$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 18:23
S26	74	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (function or algorithm or filter$9 or processing) same (ipsec or ip security or internet protocol security) and (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) same (policy or policies) and (address$10) with (source or destination or network or ip or internet protocol)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 15:35
S25	9	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (function or algorithm or filter$9 or processing) same (ipsec or ip security or internet protocol security) and (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) same (policy or policies) and (pipelin$5 or parallel$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 15:25
S24	28	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (function or algorithm or filter$9 or processing) same (ipsec or ip security or internet protocol security) and (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) same (policy or policies)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 15:25
S23	198	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing) same (ipsec or ip security or internet protocol security)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 15:24
S22	253	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing) and (ipsec or ip security or internet protocol security)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 15:23
S21	252	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing) and (ipsec or ip security)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 15:23

S20	534	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:19
S19	534	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:18
S18	551	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:18
S17	570	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:18
S16	1,430	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) and (security or secure or protect$9 or ids or intrusion or dos or denial of service)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:17
S15	3,295	(gateway) same (policy or policies) same (packet or traffic) and (rule) and (address$10) with (source or destination or network or ip or internet protocol) and (security or secure or protect$9 or ids or intrusion or dos or denial of service)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:16
S14	3,686	(gateway) same (policy or policies) same (packet or traffic) and (rule) and (address$10) with (source or destination or network or ip or internet protocol)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:15
S13	4,415	(gateway) same (policy or policies) same (packet or traffic) and (rule)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:14

S12	7	("20120113987" | "20060195896" | "7684400" | "20060248580" | "20110055916" | "0000000" | "20110270956" | "20130059527" | "20100011434" | "20120264443" | "6226372" | "20040151155" | "20030212900" | "20050117576" | "20060048142" | "20030188192" | "7721084" | "20030123456" | "20070083924" | "20100211678").PN. and (gateway) and (policy or policies)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:12
S11	17	S7 and (gateway) and (policy or policies)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:05
S10	17	S6 and (gateway) and (policy or policies)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:05
S9	7	S8 and (gateway) and (policy or policies)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:03
S8	20	("20050071655" | "20040098618" | "20090038008" | "7975059" | "6715084" | "20060143709" | "20010020255" | "20020066034" | "20040148520" | "20060143688" | "20090037682" | "20120167120" | "20020078382" | "20040128543" | "20020162026" | "20040044912" | "8214900" | "20020083175" | "20030145225" | "20030204632").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:01
S7	54	("20060173992" | "20030084329" | "20030035370" | "20010042200" | "20020133721" | "20030023733" | "20060095965" | "20060230444" | "20020073155" | "20030233328" | "20060212524" | "20070180510" | "7536715" | "20060212572" | "20020198956" | "20040199793" | "20030126468" | "20050050338" | "20040073800" | "20060050719" | "20050262556" | "20040049574" | "20030101260" | "20020198956" | "20030035370" | "20040190522" | "20070157316" | "20050182950" | "20020073337" | "20030145225" | "20040117624" | "20040128538" | "20040148520" | "20070056030" | "20040004941" | "20030061514" | "20030014665" | "20060193470" | "20080176536" | "7409712" | "20020133721" | "20020166063" | "20030204632" | "20060137012" | "7574740" | "20050086502" | "7331060" | "20030023733" | "20050278415" | "20020178378" | "20030101260" | "20070180511" | "20020162026" | "20050037733" | "20050039104" | "7702739" | "20010042200" | "20020073337" | "20030145225" | "20040117624" | "20050180416" | "20020083175" | "20060048142").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/18 23:56

S6	53	("20060173992" | "20030084329" | "20030035370" | "20040128538" | "20010042200" | "20060230444" | "20020073155" | "20030233328" | "20060212524" | "20070180510" | "7536715" | "20060212572" | "20020178378" | "20040199793" | "20030126468" | "20050050338" | "20060095965" | "20060050719" | "20050262556" | "20040049574" | "20030101260" | "20040073800" | "20020198956" | "20040190522" | "20070157316" | "20050182950" | "20040117624" | "20040148520" | "20070056030" | "20040004941" | "20030061514" | "20030014665" | "20060193470" | "20080176536" | "7409712" | "20020133721" | "20020166063" | "20030204632" | "20060137012" | "7574740" | "20050086502" | "7331060" | "20030023733" | "20070180511" | "20020162026" | "20050037733" | "20050039104" | "7702739" | "20020073337" | "20030145225" | "20050180416" | "20020083175" | "20060048142").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/18 23:55
S5	3	(centripetal networks).as.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/18 14:50
S4	95	(moore adj3 sean).in.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/18 14:49
S3	443	(rogers adj3 steven).in.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/18 14:49
S2	5,511	726/1.CCLS.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/18 14:49
S1	19	("20120113987" | "20060195896" | "7684400" | "20060248580" | "20110055916" | "0000000" | "20110270956" | "20130059527" | "20100011434" | "20120264443" | "6226372" | "20040151155" | "20030212900" | "20050117576" | "20060048142" | "20030188192" | "7721084" | "20030123456" | "20070083924" | "20100211678").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/18 14:49

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L26	3	(address AND (malicious or malware or blacklist$9) AND (traffic or packet$5) AND service AND (filter$9) AND (polic$5 or rule) AND gateway AND (secure or security) AND protect$9).CLM.	USPAT	ADJ	ON	2020/07/27 10:36
L25	1	(address AND (malicious or malware or blacklist$9) AND (traffic or packet$5) AND service AND (filter$9) AND (polic$5 or rule) AND (third with party)).CLM.	USPAT	ADJ	ON	2020/07/27 10:35
L24	3	(address AND (malicious or malware or blacklist$9) AND (traffic or packet$5) AND service AND (filter$9) AND (polic$5 or rule) AND gateway AND (creat$9 or modif$9 or alter$9)).CLM.	USPAT	ADJ	ON	2020/07/27 10:35
L23	3	(address AND (malicious or malware or blacklist$9) AND (traffic or packet$5) AND service AND (filter$9) AND (polic$5 or rule) AND gateway AND (updat$9)).CLM.	USPAT	ADJ	ON	2020/07/27 10:35
L22	1	(address AND (malicious or malware or blacklist$9) AND (traffic or packet$5) AND service AND (filter$9) AND (polic$5 or rule) AND gateway AND (transform$9 or function)).CLM.	USPAT	ADJ	ON	2020/07/27 10:34
L21	1	(address AND (malicious or malware or blacklist$9) AND (traffic or packet$5) AND service AND (filter$9) AND (polic$5 or rule) AND gateway AND match$9).CLM.	USPAT	ADJ	ON	2020/07/27 10:34
L20	3	(address AND (malicious or malware or blacklist$9) AND (traffic or packet$5) AND service AND (filter$9) AND (polic$5 or rule) AND gateway AND (secure or security)).CLM.	USPAT	ADJ	ON	2020/07/27 10:34
L19	18	(address AND (malicious or malware or blacklist$9) AND (traffic or packet$5) AND service AND (filter$9) AND (polic$5 or rule)).CLM.	USPAT	ADJ	ON	2020/07/27 10:33
S248	3	((boundary or edge or border$5) AND (gateway) AND (host) AND (function) AND rule AND LAN).CLM.	US-PGPUB; USPAT	ADJ	ON	2019/12/03 17:08
S247	2	((boundary or edge or border$5) AND (gateway) AND (host) AND (function) AND rule AND matrix).CLM.	US-PGPUB; USPAT	ADJ	ON	2019/12/03 17:08
S246	12	((boundary or edge or border$5) AND (gateway) AND (host) AND (function) AND rule AND switch$9).CLM.	US-PGPUB; USPAT	ADJ	ON	2019/12/03 17:08

S245	6	((boundary or edge or border$5) AND (gateway) AND (host) AND (function) AND (rule) AND address AND destin$9).CLM.	US-PGPUB; USPAT	ADJ	ON	2019/12/03 17:08
S244	27	((boundary or edge or border$5) AND (gateway) AND (host) AND (function) AND rule).CLM.	US-PGPUB; USPAT	ADJ	ON	2019/12/03 17:07
S242	16	((boundary or edge or border$5) AND (gateway) AND (lan or local area network) AND (switch$9) AND (drop$9 or discard$9)).CLM.	US-PGPUB; USPAT	ADJ	ON	2019/12/03 17:06
S241	6	((boundary or edge or border$5) AND (matrix) AND (lan or local area network) AND (switch$9) AND (drop$9) AND (drop$9 or discard$9)).CLM.	US-PGPUB; USPAT	ADJ	ON	2019/12/03 17:06
S240	2	((boundary or edge) AND (matrix) AND (lan or local area network) AND (switch$9) AND (drop$9) AND (drop$9 or discard$9) AND (protect$9)).CLM.	US-PGPUB; USPAT	ADJ	ON	2019/12/03 17:05
S179	0	((boundary or edge) AND (matrix) AND (lan or local area network) AND (switch$9) AND (drop$9 or discard$9 or filter$9) AND (protect$9) AND (criteria or condition) AND (adapter or interface) AND address).CLM.	US-PGPUB; USPAT	ADJ	ON	2016/09/22 16:28
S178	0	((boundary or edge) AND (matrix) AND (lan or local area network) AND (switch$9) AND (drop$9 or discard$9) AND (protect$9) AND (criteria or condition) AND (adapter or interface) AND address).CLM.	US-PGPUB; USPAT	ADJ	ON	2016/09/22 16:28
S177	0	((boundary or edge) AND (matrix) AND (lan or local area network) AND (switch$9) AND (drop$9) AND (drop$9 or discard$9) AND (protect$9) AND (criteria or condition) AND (interface) AND address).CLM.	US-PGPUB; USPAT	ADJ	ON	2016/09/22 16:28
S176	0	((boundary or edge) AND (matrix) AND (lan or local area network) AND (switch$9) AND (drop$9) AND (drop$9 or discard$9) AND (protect$9) AND (criteria or condition) AND host).CLM.	US-PGPUB; USPAT	ADJ	ON	2016/09/22 16:27
S175	0	((boundary or edge) AND (matrix) AND (lan or local area network) AND (switch$9) AND (drop$9) AND (drop$9 or discard$9) AND (protect$9) AND (criteria or condition)).CLM.	US-PGPUB; USPAT	ADJ	ON	2016/09/22 16:27
S174	0	((boundary or edge) AND (matrix) AND (lan or local area network) AND (switch$9) AND (drop$9) AND (drop$9 or discard$9) AND (protect$9)).CLM.	US-PGPUB; USPAT	ADJ	ON	2016/09/22 16:08

S173	4	((boundary or edge) AND (matrix) AND (lan or local area network) AND (switch$9) AND (drop$9) AND (drop$9 or discard$9)).CLM.	US-PGPUB; USPAT	ADJ	ON	2016/09/22 15:14
S172	13	((gateway) AND (policy or policies) AND (packet or traffic or frame) AND (rule) AND (address$10) AND (source or destination or ip or internet protocol) AND (security or secure or protect$9 or ids or intrusion or dos or denial of service) AND (server or manager or managing or supervis$9) AND (set or list) AND (function or algorithm or filter$9 or processing) AND (forward$9 or drop$9) AND network$9 AND (set or list$9)).CLM.	US-PGPUB; USPAT	ADJ	ON	2016/09/22 14:42
S114	4	((gateway) AND (policy or policies) AND (packet or traffic or frame) AND (rule) AND (boundary or boundaries or edge or border$5) AND (rule) AND (drop$9 or discard$9)).CLM.	US-PGPUB; USPAT	ADJ	ON	2015/03/26 17:27
S113	1	((gateway) AND (policy or policies) AND (packet or traffic or frame) AND (rule) AND (boundary or boundaries or edge or border$5) AND (rule) AND (drop$9 or discard$9) AND (first) AND (second)).CLM.	US-PGPUB; USPAT	ADJ	ON	2015/03/26 17:17
S106	1	((gateway) AND (policy or policies) AND (packet or traffic or frame) AND (rule) AND (address$10) AND (source or destination or ip or internet protocol) AND (security or secure or protect$9 or ids or intrusion or dos or denial of service) AND (server or manager or managing or supervis$9) AND (encapsu$9) AND (routing or route or routed) AND protect$9 AND network$9 AND (URI or uniform resource)).CLM.	US-PGPUB; USPAT	ADJ	ON	2015/03/26 12:34
S102	1	((gateway) AND (policy or policies) AND (packet or traffic or frame) AND (rule) AND (address$10) AND (source or destination or ip or internet protocol) AND (security or secure or protect$9 or ids or intrusion or dos or denial of service) AND (server or manager or managing or supervis$9) AND (encapsu$9) AND (routing or route or routed) AND network$9 AND (URI or uniform resource)).CLM.	US-PGPUB; USPAT	ADJ	ON	2015/03/26 12:27
S101	1	((gateway) AND (policy or policies) AND (packet or traffic or frame) AND (rule) AND (address$10) AND (source or destination or ip or internet protocol) AND (security or secure or protect$9 or ids or intrusion or dos or denial of service) AND (server or manager or managing or supervis$9) AND (encapsu$9) AND (routing or route or routed) AND	US-PGPUB; USPAT	ADJ	ON	2015/03/26 12:27

		network$9 AND (SIP or session initia$9 protocol)).CLM.				
S100	1	((gateway) AND (policy or policies) AND (packet or traffic or frame) AND (rule) AND (address$10) AND (source or destination or ip or internet protocol) AND (security or secure or protect$9 or ids or intrusion or dos or denial of service) AND (server or manager or managing or supervis$9) AND (set or list) AND (encapsu$9) AND (routing or route or routed) AND network$9 AND (SIP or session initia$9 protocol)).CLM.	US-PGPUB; USPAT	ADJ	ON	2015/03/26 12:26
S99	2	((gateway) AND (policy or policies) AND (packet or traffic or frame) AND (rule) AND (address$10) AND (source or destination or ip or internet protocol) AND (security or secure or protect$9 or ids or intrusion or dos or denial of service) AND (server or manager or managing or supervis$9) AND (set or list) AND (function or algorithm or filter$9 or processing) AND (routing or route or routed) AND network$9 AND (SIP or session initia$9 protocol)).CLM.	US-PGPUB; USPAT	ADJ	ON	2015/03/26 12:23
S97	3	((gateway) AND (policy or policies) AND (packet or traffic or frame) AND (rule) AND (address$10) AND (source or destination or ip or internet protocol) AND (security or secure or protect$9 or ids or intrusion or dos or denial of service) AND (server or manager or managing or supervis$9) AND (set or list) AND (function or algorithm or filter$9 or processing) AND (forward$9 or drop$9) AND network$9 AND dynamic$9).CLM.	US-PGPUB; USPAT	ADJ	ON	2015/03/26 12:17
S96	9	((gateway) AND (policy or policies) AND (packet or traffic or frame) AND (rule) AND (address$10) AND (source or destination or ip or internet protocol) AND (security or secure or protect$9 or ids or intrusion or dos or denial of service) AND (server or manager or managing or supervis$9) AND (set or list) AND (function or algorithm or filter$9 or processing) AND (forward$9 or drop$9) AND network$9 AND (set or list$9 or group$9 or subset)).CLM.	US-PGPUB; USPAT	ADJ	ON	2015/03/26 12:16
S95	9	((gateway) AND (policy or policies) AND (packet or traffic or frame) AND (rule) AND (address$10) AND (source or destination or ip or internet protocol) AND (security or secure or protect$9 or ids or intrusion or dos or denial of service) AND (server or manager or managing or supervis$9) AND (set or list) AND	US-PGPUB; USPAT	ADJ	ON	2015/03/26 12:16

		(function or algorithm or filter$9 or processing) AND (forward$9 or drop$9) AND network$9 AND (set or list$9)).CLM.				

7/27/2020 10:37:46 AM
C:\Users\kchang3\Documents\EAST\Workspaces\16728766_CON4.wsp

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

BIB DATA SHEET

CONFIRMATION NO. 8018

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
16/728,766	12/27/2019	726	2438	007742.00151\US

APPLICANTS

Centripetal Networks, Inc., Portsmouth, NH;

INVENTORS

Steven Rogers, Leesburg, VA;
Sean Moore, Hollis, NH;

**** CONTINUING DATA ***************************

This application is a CON of 16/111,524 08/24/2018 PAT 10567437
which is a CON of 15/413,834 01/24/2017 PAT 10091246
which is a CON of 14/698,560 04/28/2015 PAT 9560077
which is a CON of 13/657,010 10/22/2012 PAT 9137205

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
01/21/2020

Foreign Priority claimed	❑ Yes ☑ No	❑ Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
35 USC 119(a-d) conditions met	❑ Yes ☑ No		VA	10	27	4
Verified and Acknowledged	/KENNETH W CHANG/ Examiner's Signature	Initials				

ADDRESS

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

TITLE

METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK

FILING FEE RECEIVED		
1365	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	❑ All Fees ❑ 1.16 Fees (Filing) ❑ 1.17 Fees (Processing Ext. of time) ❑ 1.18 Fees (Issue) ❑ Other _____ ❑ Credit

IEEE.org IEEE Xplore IEEE-SA IEEE Spectrum More Sites Cart (1) Create Account Persor

Browse My Settings Help Access provided by: United States Patent and Trademark Office Sign Out

Access provided by: United States Patent and Trademark Office Sign Out

All

Search within results Download PDFs | Per Page: Per Page 25 | Export | Alert Set Search Alerts | Search History

Showing 1-13 of 13 for **packet filtering network address service malicious**

Filters Applied: 2004 - 2011

Conferences (12) Courses (1)

Filter Alert Set Search Alerts | sort: Sort Relevance

Show

- All Results
- My Subscribed Content
- Open Access

Year

Single Year | Range

2004 2004 2011 2011

From 2004 To 2011

Author

Affiliation

Publication Title

Publisher

Conference Location

Publication Topics

Mitigating Distributed Denial-of-Service Attacks: Application-Defense and Network-Defense Methods
Zhang Fu
2011 Seventh European Conference on Computer Network Defense
Year: 2011 | Conference Paper | Publisher: IEEE
Abstract (87 Kb)

Mitigating Distributed Denial-of-Service Attacks: Application-Defense and Network-Defense Methods

Zhang Fu
2011 Seventh European Conference on Computer Network Defense
Year: 2011 | Conference Paper | Publisher: IEEE

Empirical Study of Tolerating Denial-of-Service Attacks with the Fosel Architecture
Hakem Beitollahi ; Geert Deconinck
2009 Eighth IEEE International Symposium on Network Computing and Applications
Year: 2009 | Conference Paper | Publisher: IEEE
Cited by: Papers (2)
Abstract (371 Kb)

Empirical Study of Tolerating Denial-of-Service Attacks with the Fosel Architecture

Hakem Beitollahi | Geert Deconinck
2009 Eighth IEEE International Symposium on Network Computing and Applications
Year: 2009 | Conference Paper | Publisher: IEEE

A Hash-Based Path Identification Scheme for DDoS Attacks Defense
Guang Jin ; Fei Zhang ; Yuan Li ; Honghao Zhang ; Jiangbo Qian
2009 Ninth IEEE International Conference on Computer and Information Technology
Year: 2009 | Volume: 2 | Conference Paper | Publisher: IEEE
Cited by: Papers (1)
Abstract (296 Kb)

JXCDC Call for Papers IEEE Submit a Paper

IEEE Authors: Increase Your Research Impact Add executable code to your research articles Promote your code

CO CODE OCEAN IEEE

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 NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/728,766	12/27/2019	Steven Rogers	007742.00151\US	8018

22907 7590 07/17/2020
BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

EXAMINER
CHANG, KENNETH W

ART UNIT	PAPER NUMBER
2438	

NOTIFICATION DATE	DELIVERY MODE
07/17/2020	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

GPD@bannerwitcoff.com
eofficeaction@bannerwitcoff.com

Applicant-Initiated Interview Summary	**Application No.** 16/728,766	**Applicant(s)** Rogers et al.	
	Examiner Kenneth W Chang	**Art Unit** 2438	**AIA (FITF) Status** No

All participants (applicant, applicants representative, PTO personnel):

(1) Kenneth W. Chang.

(2) Scott Kelly.

(3) Kirk Sigmon.

(4) _____.

Date of Interview: 14 July 2020.

Type: ☑ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☑ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☑103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: 1.

Identification of prior art discussed: Javala and Bhatnagar.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

The Examiner conducted a telephone conference with applicants' attorneys of record Scott Kelly (Reg. No. 65,121) and Kirk Sigmon (Reg. No. 76,326) to discuss the claims. Attorney Kelly distinguished the claimed invention from the prior art, and the Examiner gave suggestions to clarify the claim language. Attorney Sigmon discussed possible amendments to the claims to overcome the Bhatnagar reference..

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/KENNETH W CHANG/ Primary Examiner, Art Unit 2438	

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiners responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicants correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,-
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
(The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicants record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiners version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, Interview Record OK on the paper recording the substance of the interview along with the date and the examiners initials.

Docket No.: 007742.00151\US
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Steven Rogers et al.

Application No.: 16/728,766 Confirmation No.: 8018

Filed: December 27, 2019 Art Unit: 2438

For: METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK Examiner: K. W. Chang

AMENDMENT IN RESPONSE TO NON-FINAL OFFICE ACTION UNDER 37 C.F.R. § 1.111

MS Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

INTRODUCTORY COMMENTS

In response to the Office Action dated April 16, 2020, please amend the above-identified U.S. patent application as follows:

Amendments to the Claims begin on page 2.

Remarks begin on page 11.

If any fees are required or if an overpayment has been made, the Commissioner is authorized to charge or credit the undersigned's Deposit Account No. 19-0733, accordingly.

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A method of filtering packets at a packet security gateway, of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway and one or more networks other than the network protected by the packet security gateway, the method comprising:

receiving, by the packet security gateway and from a security policy management server external from the network protected by the packet security gateway, a dynamic security policy comprising a first set of packet filtering rules to be applied to all network traffic traversing the boundary, wherein:

each packet filtering rule of the first set of packet filtering rules comprises at least one packet matching criterion and a corresponding packet transformation function, and

one or more first packet filtering rules of the first set of packet filtering rules comprise packet matching criteria corresponding to one or more network addresses and were automatically created or altered by the security policy management server based on aggregated malicious traffic information, received from at least one third party malicious host tracker service located in the one or more networks other than the network protected by the packet security gateway, that comprises network addresses that have been determined, by the at least one third party malicious host tracker service, to be associated with malicious network traffic;

performing, on a packet by packet basis, packet filtering on a first portion of packets corresponding to network traffic traversing the boundary via the packet security gateway based on the first set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets;

receiving, by the packet security gateway and after performing packet filtering on the first portion of the packets, an updated second set of packet filtering rules for the

dynamic security policy from the security policy management server, wherein the updated second set of packet filtering rules comprises an update to the one or more first packet filtering rules created or altered by the security policy management server based on updated malicious traffic information received from the at least one third party malicious host tracker service; and

performing, on a packet by packet basis, packet filtering on a second portion of the packets corresponding to network traffic traversing the boundary via the packet security gateway based on the updated second set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the second set of packet filtering rules on the second portion of packets.

2. (Currently Amended) The method of claim 1, wherein the at least one packet matching criterion corresponding to the one or more first packet filtering rules automatically created or altered by the security policy management server comprises at least one of the one or more network addresses ~~indicated by the malicious traffic information~~.

3. (Currently Amended) The method of claim 1, wherein the at least one third party malicious host tracker service comprises a subscription service that aggregates information associated with malicious network traffic.

4. (Currently Amended) The method of claim 1, wherein the ~~malicious traffic information comprises a list of~~one or more network addresses were associated, by a subscription service, with malicious network traffic~~known to be associated with malicious network traffic~~.

5. (Original) The method of claim 1, wherein at least one packet transformation function comprises a network protective action.

6. (Original) The method of claim 1, further comprising:

receiving, by the packet security gateway, packets in a network layer transparent manner using an interface that is not addressed at the network layer; and

performing the at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets at the network layer.

7. (Original) The method of claim 1, wherein one or more packet filtering rules of the first set of packet filtering rules specify a packet transformation function other than forwarding or dropping the corresponding packets.

8. (Currently Amended) A packet security gateway, of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway and one or more networks other than the network protected by the packet security gateway, comprising:

one or more processors; and

memory storing instructions that, when executed by the one or more processors, cause the packet security gateway to:

receive, from a security policy management server external from the network protected by the packet security gateway, a dynamic security policy comprising a first set of packet filtering rules to be applied to all network traffic traversing the boundary, wherein:

each packet filtering rule of the first set of packet filtering rules comprises at least one packet matching criterion and a corresponding packet transformation function, and

one or more first packet filtering rules of the first set of packet filtering rules comprise packet matching criteria corresponding to one or more network addresses and were automatically created or altered by the security policy management server based on aggregated malicious traffic information, received from at least one third party malicious host tracker service located in the one or more networks other than the network protected by the packet security gateway, that comprises network addresses that have been determined, by the at least one

third party malicious host tracker service, to be associated with malicious network traffic;

perform, on a packet by packet basis, packet filtering on a first portion of packets corresponding to network traffic traversing the boundary via the packet security gateway based on the first set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets;

receive, after performing packet filtering on the first portion of the packets, an updated second set of packet filtering rules for the dynamic security policy from the security policy management server, wherein the updated second set of packet filtering rules comprises an update to the one or more first packet filtering rules created or altered by the security policy management server based on updated malicious traffic information received from the at least one third party malicious host tracker service; and

perform, on a packet by packet basis, packet filtering on a second portion of the packets corresponding to network traffic traversing the boundary via the packet security gateway based on the updated second set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the second set of packet filtering rules on the second portion of packets.

9. (Currently Amended) The packet security gateway of claim 8, wherein the at least one packet matching criterion corresponding to the one or more first packet filtering rules automatically created or altered by the security policy management server comprises at least one of the one or more network addresses ~~indicated by the malicious traffic information~~.

10. (Currently Amended) The packet security gateway of claim 8, wherein the at least one third party malicious host tracker service comprises a subscription service that aggregates information associated with malicious network traffic.

11. (Currently Amended) The packet security gateway of claim 8, wherein the ~~malicious traffic information comprises a list of~~one or more network addresses were associated, by a

subscription service, with malicious network traffic~~known to be associated with malicious network traffic~~.

12. (Original) The packet security gateway of claim 8, wherein at least one packet transformation function comprises a network protective action.

13. (Original) The packet security gateway of claim 8, wherein the instructions further cause the packet security gateway to:

receive packets in a network layer transparent manner using an interface that is not addressed at the network layer; and

perform the at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets at the network layer.

14. (Original) The packet security gateway of claim 8, wherein one or more packet filtering rules of the first set of packet filtering rules specify a packet transformation function other than forwarding or dropping the corresponding packets.

15. (Currently Amended) One or more non-transitory computer readable media storing instructions that, when executed by at least one processor, cause a packet security gateway, of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway and one or more networks other than the network protected by the packet security gateway, to perform steps comprising:

receiving, from a security policy management server external from the network protected by the packet security gateway, a dynamic security policy comprising a first set of packet filtering rules to be applied to all network traffic traversing the boundary, wherein:

each packet filtering rule of the first set of packet filtering rules comprises at least one packet matching criterion and a corresponding packet transformation function, and

one or more first packet filtering rules of the first set of packet filtering rules comprise packet matching criteria corresponding to one or more network addresses and were automatically created or altered by the security policy management server based on aggregated malicious traffic information, received from at least one third party malicious host tracker service located in the one or more networks other than the network protected by the packet security gateway, that comprises network addresses that have been determined, by the at least one third party malicious host tracker service, to be associated with malicious network traffic;

performing, on a packet by packet basis, packet filtering on a first portion of packets corresponding to network traffic traversing the boundary via the packet security gateway based on the first set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets;

receiving, after performing packet filtering on the first portion of the packets, an updated second set of packet filtering rules for the dynamic security policy from the security policy management server, wherein the updated second set of packet filtering rules comprises an update to the one or more first packet filtering rules created or altered by the security policy management server based on updated malicious traffic information received from the at least one third party malicious host tracker service; and

performing, on a packet by packet basis, packet filtering on a second portion of the packets corresponding to network traffic traversing the boundary via the packet security gateway based on the updated second set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the second set of packet filtering rules on the second portion of packets.

16. (Currently Amended) The computer readable media of claim 15, wherein the at least one packet matching criterion corresponding to the one or more first packet filtering rules automatically created or altered by the security policy management server comprises at least one of the one or more network addresses ~~indicated by the malicious traffic information~~.

17. (Currently Amended) The computer readable media of claim 15, wherein the at least one third party malicious host tracker service comprises a subscription service that aggregates information associated with malicious network traffic, and wherein the ~~malicious traffic information comprises a list of~~one or more network addresses were associated, by a subscription service, with malicious network traffic~~known to be associated with malicious network traffic~~.

18. (Original) The computer readable media of claim 15, wherein at least one packet transformation function comprises a network protective action.

19. (Original) The computer readable media of claim 15, further comprising:

receiving, by the packet security gateway, packets in a network layer transparent manner using an interface that is not addressed at the network layer; and

performing the at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets at the network layer.

20. (Original) The computer readable media of claim 15, wherein one or more packet filtering rules of the first set of packet filtering rules specify a packet transformation function other than forwarding or dropping the corresponding packets.

21. (Currently Amended) A method of filtering packets at a packet security gateway configured for protection of a network and associated with a security policy management server external from the network, the method comprising:

receiving, by the packet security gateway, a dynamic security policy comprising a first set of packet filtering rules from the security policy management server, wherein each packet filtering rule of the first set of packet filtering rules comprises at least one packet matching criterion and a corresponding packet transformation function, and wherein one or more first packet filtering rules of the first set of packet filtering rules comprise packet matching criteria corresponding to one or more network addresses and

were automatically created or altered by the security policy management server based on aggregated malicious traffic information, received from at least one third party malicious host tracker service located in the one or more networks other than the network protected by the packet security gateway, that comprises network addresses that have been determined, by the at least one third party malicious host tracker service, to be associated with malicious network traffic;

performing, on a packet by packet basis, packet filtering on a first portion of packets associated with the network protected by the packet security gateway based on the first set of packet filtering rules by performing at least one of multiple packet transformation functions specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets;

receiving, by the packet security gateway and after performing packet filtering on the first portion of the packets, an updated second set of packet filtering rules for the dynamic security policy from the security policy management server, wherein the updated second set of packet filtering rules comprises an update to the one or more first packet filtering rules created or altered by the security policy management server based on updated malicious traffic information received from the at least one third party malicious host tracker service; and

performing, on a packet by packet basis, packet filtering on a second portion of the packets associated with the network protected by the packet security gateway based on the updated second set of packet filtering rules.

22. (Currently Amended) The method of claim 21, wherein the at least one packet matching criterion corresponding to the one or more first packet filtering rules automatically created or altered by the security policy management server comprises at least one of the one or more network addresses ~~indicated by the malicious traffic information~~.

23. (Currently Amended) The method of claim 21, wherein the at least one third party malicious host tracker service comprises a subscription service that aggregates information associated with malicious network traffic.

24. (Currently Amended) The method of claim 21, wherein the ~~malicious traffic information comprises a list of~~one or more network addresses were associated, by a subscription service, with malicious network traffic~~known to be associated with malicious network traffic~~.

25. (Original) The method of claim 21, wherein at least one packet transformation function comprises a network protective action.

26. (Original) The method of claim 21, further comprising:

receiving, by the packet security gateway, packets in a network layer transparent manner using an interface that is not addressed at the network layer; and

performing the at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets at the network layer.

27. (Original) The method of claim 21, wherein one or more packet filtering rules of the first set of packet filtering rules specify a packet transformation function other than forwarding or dropping the corresponding packets.

REMARKS

The Office Action of April 16, 2020, (the "Action") has been carefully reviewed and these remarks are responsive thereto. Claims 1–4, 8–11, 15–17, and 21–24 have been amended. No new matter has been added. Claims 1–27 are therefore pending, with claims 1, 8, 15, and 21 being independent. Reconsideration and allowance of the instant application are respectfully requested.

STATEMENT OF SUBSTANCE OF EXAMINER INTERVIEW

Applicant thanks Examiner Chang for the interview on July 14, 2020. During that interview, the 35 U.S.C. § 103 rejections were discussed. No agreement was reached.

REJECTIONS UNDER 35 U.S.C. § 103

Claims 1–3, 5, 7–10, 12, 14–16, 18, 20–23, 25, and 27 stand rejected under 35 U.S.C. § 103 for allegedly being unpatentable over, U.S. Pub. No. 2003/0118038 to Jalava *et al.* ("Jalava") in view of U.S. Pub. No. 2006/0123481 to Bhatnagar *et al.* ("Bhatnagar").

Claims 4, 11, 17, and 24 stand rejected under 35 U.S.C. § 103 for allegedly being unpatentable over Jalava, Bhatnagar, and U.S. Pub. No. 2010/0082811 to Van Der Merwe *et al.* ("Van Der Merwe").

Claims 6, 13, 19, and 26 stand rejected under 35 U.S.C. § 103 for allegedly being unpatentable over Jalava and Bhatnagar, further in view of U.S. Pub. No. 2009/0262741 to Jungck *et al.* ("Jungck").

Claim 1 and Claims Depending Therefrom

Claim 1 has been amended to recite, *inter alia*:

> *receiving, by the packet security gateway and from a security policy management server external from the network protected by the packet security gateway, a dynamic security policy comprising a first set of packet filtering rules to be applied to all network traffic traversing the boundary, wherein:*
>
> *each packet filtering rule of the first set of packet filtering rules comprises at least one packet matching criterion and a corresponding packet transformation function, and*
>
> *one or more first packet filtering rules of the first set of packet filtering rules comprise packet matching criteria corresponding to one or more network addresses and were automatically created or altered by the*

security policy management server based on aggregated malicious traffic information, received from at least one third party malicious host tracker service located in the one or more networks other than the network protected by the packet security gateway, that comprises network addresses that have been determined, by the at least one third party malicious host tracker service, to be associated with malicious network traffic;

None of the cited references teach, disclose, or otherwise suggest at least these features for at least the following reasons.

None of the cited references teach, disclose, or otherwise suggest "*receiving, by the packet security gateway and from a security policy management server external from the network protected by the packet security gateway, a dynamic security policy comprising a first set of packet filtering rules to be applied to all network traffic traversing the boundary, wherein: each packet filtering rule of the first set of packet filtering rules comprises at least one packet matching criterion and a corresponding packet transformation function, and one or more first packet filtering rules of the first set of packet filtering rules comprise packet matching criteria corresponding to one or more network addresses and were automatically created or altered by the security policy management server based on aggregated malicious traffic information, received from at least one third party malicious host tracker service located in the one or more networks other than the network protected by the packet security gateway, that comprises network addresses that have been determined, by the at least one third party malicious host tracker service, to be associated with malicious network traffic*." The Action, on page 7, concedes that Jalava "does not specifically disclose . . . packet filtering rules created or altered by [a] management server based on updated malicious traffic information received from a malicious host tracker service." To remedy this deficiency, the Action cites Bhatnagar, asserting (on page 7 of the Action) that Bhatnagar "create[]s updated filter rules by filter generation service based on translating malicious traffic patterns received from the security service [0022]; [0024]." Bhatnagar describes that "network elements" may be "updated with patterns associated with malicious code, so that malicious code may be detected and blocked at the network level." (Bhatnagar, Abstract). Such patterns are "malicious code definitions" which may be "update[d] . . . daily or several times per

day." (*Id.*, para. 0007). Bhatnagar explains that "a security service 30," such as "Symantec™ and MacAfee™," "provides updates 32 as new threats are identified on the network." (*Id.,* para. 0022). Bhatnagar elaborates:

> When a new threat is identified, the security service 30 will obtain a signature of the threat from the agents (not shown) and generate a pattern that may be used by the network elements 12, 14, to identify the threat. Pattern generation of this sort is currently done by security services, for example, in connection with providing updates to security software 24, and the invention is not limited to a particular manner of generating these types of updates.

(*Id.*). But Bhatnagar fails to teach, disclose, or otherwise suggest "*receiving . . . a dynamic security policy comprising a first set of packet filtering rules to be applied to all network traffic traversing the boundary, wherein: . . . one or more first packet filtering rules of the first set of packet filtering rules comprise packet matching criteria corresponding to one or more network addresses and were automatically created or altered by the security policy management server based on aggregated malicious traffic information, received from at least one third party malicious host tracker service located in the one or more networks other than the network protected by the packet security gateway, that comprises network addresses that have been determined, by the at least one third party malicious host tracker service, to be associated with malicious network traffic.*" First, Bhatnagar's "pattern[s]" are not "*one or more first packet filtering rules"* that "*comprise packet matching criteria corresponding to one or more network addresses,"* but instead are "malicious code definitions." (*Id.,* para. 0007). Such patterns are used, by the network element or other devices, to later generate rules to detect those code threats. (*Id.,* paras. 0023–0024). In other words, Bhatnagar discusses code signatures, but not "*one or more first packet filtering rules*" that "*were automatically created or altered by the security policy management server.*" Second, even assuming that Bhatnagar did disclose "packet filtering rules created or altered by [a] management server" (not conceded by Applicant), Bhatnagar does not teach, disclose, or otherwise suggest that such rules were "*were automatically created or altered by the security policy management server based on aggregated malicious traffic information, received from at least one third party malicious host tracker service located in the one or more networks other than the network protected by the packet security gateway, that comprises network addresses that have been determined, by the at least one third party malicious host tracker service, to be associated with malicious network traffic.*" For instance, Bhatnagar does not teach "*aggregated malicious traffic information.*" And,

in any event, such information does not comprise "*network addresses that have been determined, by the at least one third party malicious host tracker service, to be associated with malicious network traffic*."

Accordingly, claim 1 is in a condition for allowance. Independent claims 8, 15, and 21 have been similarly amended and are allowable for similar reasons. Claims 2–7, 9–14, 16–20, and 22–27 depend from independent claims 1, 8, 15, and 21 and are allowable for similar reasons, and also because of their respective novel features.

As one example of how the dependent claims define over the cited references, claim 2 has been amended to recite "*wherein the at least one packet matching criterion corresponding to the one or more first packet filtering rules automatically created or altered by the security policy management server comprises at least one of the one or more network addresses*." As indicated above, page 7 of the Action concedes that Jalava "does not specifically disclose . . . packet filtering rules created or altered by [a] management server based on updated malicious traffic information received from a malicious host tracker service." To remedy this deficiency, the Action cites Bhatnagar. The Action seems to assert that Bhatnagar teaches "*malicious traffic information*" through its patterns; that is, "malicious code definitions." (*Id.,* para. 0007). But Bhatnagar does not indicate that such patterns "*comprise[] network addresses that have been determined, by the at least one third party malicious host tracker service, to be associated with malicious network traffic.*" Claims 9, 16, and 22 are allowable for similar reasons.

As another example of how the dependent claims define over the cited references, claim 3 recites "*wherein the at least one third party malicious host tracker service comprises a subscription service that aggregates information associated with malicious network traffic.*" Bhatnagar's "security service 30 will obtain a signature of the threat from the agents (not shown) and generate a pattern that may be used by the network elements." (*Id.,* para. 0022). Regardless of whether Bhatnagar's "security service 30" or its "agents" are analogized as the "*subscription service,*" neither "*aggregate[] information associated with malicious network traffic.*" To the contrary, they receive a signature, generate a pattern, and (ultimately) generate a rule based on those patterns. Claims 10, 17, 23 are allowable for similar reasons.

As yet another example of how the dependent claims define over the cited references, claim 4 has been amended to recite "*wherein the one or more network addresses were associated, by a*

subscription service, with malicious network traffic." The Action seems to assert that Bhatnagar teaches "*malicious traffic information"* through its patterns; that is, "malicious code definitions." (*Id.,* para. 0007). But Bhatnagar's patterns are not "*malicious traffic information"* comprising "*one or more network addresses"* that "*were associated, by a subscription service, with malicious network traffic."* Claims 11, 17, 24 are allowable for similar reasons.

CONCLUSION

All issues having been addressed, Applicant respectfully submits that the instant application is in condition for allowance, and respectfully solicits prompt notification of the same. However, if for any reason the Examiner believes the application is not in condition for allowance or there are any questions, the Examiner is requested to contact the undersigned at (202) 824-3158.

Dated: July 16, 2020

Respectfully submitted,

By: */Kirk A. Sigmon/*
Kirk A. Sigmon
Registration No.: 76,326

BANNER & WITCOFF, LTD.
1100 13th St. NW
STE 1200
Washington, DC 20005
(202) 824-3000

Electronic Acknowledgement Receipt

EFS ID:	40018483
Application Number:	16728766
International Application Number:	
Confirmation Number:	8018
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	Kirk Allen Sigmon/MARIAMA SEASAY
Filer Authorized By:	Kirk Allen Sigmon
Attorney Docket Number:	007742.00151\US
Receipt Date:	16-JUL-2020
Filing Date:	27-DEC-2019
Time Stamp:	12:06:18
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		USAN_16_728766_Response_to_Non-Final_Office_Action_-_007742_20641023.pdf	73167 7efc174977020725cccde90bfe8aaa806e5bd49a	yes	16

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	10
	Applicant Arguments/Remarks Made in an Amendment	11	16
Warnings:			
Information:			
	Total Files Size (in bytes):	73167	

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/SB/06 (09-11)
Approved for use through 1/31/2014. 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.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 16/728,766	Filing Date 12/27/2019	☐ To be Mailed

ENTITY: ☐ LARGE ☑ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $50 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $230 =	
☐ 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).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	07/16/2020	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 27	Minus	** 27	= 0		x $50 =	0
	Independent (37 CFR 1.16(h))	* 4	Minus	*** 4	= 0		x $230 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=		x $0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $0 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	SLIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/SHANDA E ROSS/
*** 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 number found in the appropriate box in column 1.	

This collection of information is required by 37 CFR 1.16. 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 12 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.

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. 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	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\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	20130081102	A1	2013-03-28	Beauvais et al.	
	2	20120311693	A1	2012-12-06	Horman 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							

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

NON-PATENT LITERATURE DOCUMENTS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\US

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]
	1	2020 July 02 - (US) Final Rejection - US App 16/158,868	

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	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\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	/Kirk A. Sigmon/	Date (YYYY-MM-DD)	2020-07-10
Name/Print	Kirk A. Sigmon	Registration Number	76,326

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 Patent Application Fee Transmittal

Application Number:	16728766
Filing Date:	27-Dec-2019
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Filer:	Kirk Allen Sigmon/Niki Rollhauser
Attorney Docket Number:	007742.00151\US

Filed as Small 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:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
SUBMISSION- INFORMATION DISCLOSURE STMT	2806	1	120	120
		Total in USD ($)		**120**

Electronic Acknowledgement Receipt

EFS ID:	39964004
Application Number:	16728766
International Application Number:	
Confirmation Number:	8018
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	Kirk Allen Sigmon/Niki Rollhauser
Filer Authorized By:	Kirk Allen Sigmon
Attorney Docket Number:	007742.00151\US
Receipt Date:	10-JUL-2020
Filing Date:	27-DEC-2019
Time Stamp:	10:23:00
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$120
RAM confirmation Number	E202070A23161051
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	Information_Disclosure_Statement_007742_00151.PDF	1034234 8c65cb1c86a8f1126010d1d864eabf7b800d4f94	no	4
Warnings:					
Information:					
2	Non Patent Literature	Final_Rejection.PDF	952926 50d35411372d73e9d34507a01013e31c66385124	no	25
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30673 b79e59c5b7249022f6f02ae5759764d8c7155346	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	2017833		

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
16/728,766	12/27/2019	Steven Rogers	007742.00151\US

CONFIRMATION NO. 8018

PUBLICATION NOTICE

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

OC000000116642993

Title:METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK

Publication No.US-2020-0137121-A1
Publication Date:04/30/2020

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Public Records Division. The Public Records Division can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Public Records Division, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently https://portal.uspto.gov/pair/PublicPair. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

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 NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/728,766	12/27/2019	Steven Rogers	007742.00151\US	8018

22907 7590 04/16/2020

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

EXAMINER
CHANG, KENNETH W

ART UNIT	PAPER NUMBER
2438	

NOTIFICATION DATE	DELIVERY MODE
04/16/2020	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

GPD@bannerwitcoff.com
eofficeaction@bannerwitcoff.com

Office Action Summary	Application No. 16/728,766	Applicant(s) Rogers et al.	
	Examiner Kenneth W Chang	Art Unit 2438	AIA (FITF) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 12/27/2019.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL.** 2b) ☑ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-27 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-27 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☑ The drawing(s) filed on 12/27/2019 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☑ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

DETAILED ACTION

1. This first non-final action is in response to applicants' original filing on 12/27/2019. **Claims 1-27** are currently pending and have been considered as follows.

Notice of Pre-AIA or AIA Status

2. The present application is being examined under the **pre-AIA** first to invent provisions.

3. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

Drawings

4. The drawings filed on 12/27/2019 are accepted.

Information Disclosure Statement

5. The information disclosure statements (IDS) submitted on 03/25/2020 and 04/07/2020 have been placed in the application file, and the information referred therein has been considered as to the merits.

Claim Rejections - 35 USC § 103

6. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. This application currently names joint inventors. In considering patentability of the claims under pre-AIA 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of pre-AIA 35 U.S.C. 103(c) and potential pre-AIA 35 U.S.C. 102(e), (f) or (g) prior art under pre-AIA 35 U.S.C. 103(a).

8. **Claims 1-3, 5, 7-10, 12, 14-16, 18, 20-23, 25, and 27** are rejected under pre-AIA 35 U.S.C. 103(a) as being as being unpatentable over Jalava et al. (US 20030118038 A1, hereinafter **Jalava**) in view of Bhatnagar et al. (US 20060123481 A1, hereinafter **Bhatnagar**).

As to Claim 1:

Jalava discloses a method of filtering packets at a packet security gateway **(e.g. Jalava "A personalized firewall or other network gateway is provided by a method of matching a data packet to a rule in a network gateway having a rule base. One or more identification values are determined (302) on the basis of the data packet and property value(s) associated with said one or more identification values are queried (304) and received from a property server. The property value(s) describe for example allowed connections and services for an entity associated with the identification value(s). The property value(s) are compared (306) to at least one rule in the rule base, said at least one rule comprising property value(s) and an action, and the action defined in said at least one rule is taken (310), if said**

property value(s) of the rule match corresponding property value(s) associated with said one or more identification values" [Abstract]), of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway and one or more networks other than the network protected by the packet security gateway **(e.g. Jalava "As already described above, the firewall 23 and 31 are gateways which operate at the same time as a connector and a separator between the networks in a sense that the firewalls keep track of the traffic that passes through them from one network to another and restrict connections and packets that are defined as unwanted by the administrators of the systems" [0049]; Fig. 2A; [0044])**, the method comprising:

- receiving, by the packet security gateway and from a security policy management server external from the network protected by the packet security gateway **(e.g. Jalava management server 25 is remotely connected to the firewall over the public network and sends firewall rules to the firewall for execution [0044]; Fig. 2A)**, a dynamic security policy comprising a first set of packet filtering rules to be applied to all network traffic traversing the boundary **(e.g. Jalava rules for firewall [0041]; [0044]; [0045]; [0049]; [0050])**, wherein:
- each packet filtering rule of the first set of packet filtering rules comprises at least one packet matching criterion and a corresponding packet transformation function **(e.g. Jalava "it is detected, if a data packet, which has been received, is compared to a rule containing property values (that is, requiring the use of property values for match process)… One or more identification values are determined on the basis of the data packet (step**

302) and property value(s) associated with the identification value(s) are queried and received (step 304). In practice, the property values are stored in the firewall for future use after receiving them. If the property values are already stored, they do not need to be queried again. Then the property value(s) are compared to a rule, which includes property value(s) and an action, in step 306. If the property value(s) of the rule match corresponding property value(s) associated with the identification value(s), the action defined in the rule is taken (steps 308 and 310). If the property value(s) of the rule do not match corresponding property value(s) associated with the identification value(s), the next rule of the rule base is processed in step 312" [0050]), and

- one or more first packet filtering rules of the first set of packet filtering rules were automatically created or altered by the security policy management server **(e.g. Jalava "firewall configuration (the rules), which may include also VPN configuration, is defined in the management system" [0044])**;
- performing, on a packet by packet basis, packet filtering on a first portion of packets corresponding to network traffic traversing the boundary via the packet security gateway based on the first set of packet filtering rules by performing at least one packet transformation function **(e.g. Jalava "In a firewall, the action is typically deny or allow, which means the data packet is discarded or allowed to proceed, correspondingly" [0003]; [0004]; [0017]; [0049])** specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets **(e.g. "The property value(s) are compared (306)**

to at least one rule in the rule base, said at least one rule comprising property value(s) and an action, and the action defined in said at least one rule is taken (310), if said property value(s) of the rule match corresponding property value(s) associated with said one or more identification values" [Abstract]; [0017]; [0049]);

- receiving, by the packet security gateway and after performing packet filtering on the first portion of the packets, an updated second set of packet filtering rules for the dynamic security policy from the security policy management server, wherein the updated second set of packet filtering rules comprises an update to the one or more first packet filtering rules **(e.g. Jalava "the network gateway requests to be notified, if the property value(s) stored in the network gateway in step 504 are updated in the property server. At this point such a request needs to be stored in the property server with reference to the corresponding property value--identification value combination (not shown in the Figure). In step 602, a notification comprising updated property value(s) and associated identification value(s) are received. The old property value(s) in the network gateway are then replaced with the corresponding updated property value(s) in step 604" [0065]; [0066]; [0069])**; and
- performing, on a packet by packet basis, packet filtering on a second portion of the packets corresponding to network traffic traversing the boundary via the packet security gateway based on the updated second set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the second set of packet filtering rules on the

second portion of packets **(e.g. Jalava "When the firewall has compared a data packet to N first rules and none of them has matched the data packet, it is required to find out the property values associated with the source of the data packet. The firewall queries the property values from the property server by the source IP address 10.1.1.7 and receives the sequence of 101100 mentioned above" [0057]; [0050]; [0017]; [0049])**;

But **Jalava** does not specifically disclose:

- packet filtering rules created or altered by [a] management server based on updated malicious traffic information received from a malicious host tracker service.

However, the analogous art **Bhatnagar** does disclose packet filtering rules created *or* altered by [a] management server based on updated malicious traffic information received from a malicious host tracker service **(e.g. Bhatnagar create updated filter rules by filter generation service based on translating malicious traffic patterns received from the security service [0022]; [0024])**. **Jalava** and **Bhatnagar** are analogous art because they are from the same field of endeavor in network packet filtering.

- (e.g. see **Bhatnagar**, "In the example shown in FIG. 1, a security service 30 provides updates 32 as new threats are identified on the network… When a new threat is identified, the security service 30 will obtain a signature of the threat from the agents (not shown) and generate a pattern that may be used by the network elements 12, 14, to identify the threat. Pattern generation of this sort is currently done by security services, for example, in connection with providing

updates to security software 24, and the invention is not limited to a particular manner of generating these types of updates" **[0022]**; see also "the patterns generated by the security service may be sent to a network management station 34. The network management station may then pass the patterns to a filter generation service 36 configured to create filter rules specific to the different types of network elements on the network 10. The filter generation service 36, in this alternate embodiment, is configured to translate the pattern received from the security service 30 via update 32 into filter rules 38 that are transmitted to the network elements and used by the network elements 12, 14 to filter traffic on the network. In either embodiment, the filter rules will be installed into the forwarding planes of the network elements configured to act as detection points 28, so that traffic matching the patterns will be removed from the network. By continually updating the detection points 28 in real time as threats are discovered, it is possible to immunize the network against outbreaks of malicious code to reduce the chance that malicious code will reach the customer equipment" **[0024]**; "When a pattern match is found, the traffic may be discarded or, alternatively, additional remedial action may be taken such as to trace the traffic backwards through the network toward the source. Tracing the traffic backwards through the network may enable the source of the traffic to be identified" **[0028]**).

At the time of applicants' invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Jalava** and **Bhatnagar** before him or her, to modify the system and method of **Jalava** with the teachings of **Bhatnagar** to include *packet filtering rules created or altered by [a] management server based on updated malicious*

traffic information received from a malicious host tracker service as claimed because **Jalava**'s system and method provides a management server that remotely connects to firewalls/gateways at protected networks to provide packet filtering rules and updates **(Jalava [Abstract]-[0069])** which could be based on received malicious traffic patterns sent from a security service **(Bhatnagar [0022]; [0024]; [0028])**. The suggestion/motivation for doing so would have been to stop malicious code that spans multiple packets at the network level so that new security threats may be neutralized quickly once discovered **(Bhatnagar [0026]; [0027])**. Therefore, it would have been obvious to combine **Jalava** and **Bhatnagar** to obtain the invention as specified in the instant claim(s).

As to Claim 2:

Jalava in view of **Bhatnagar** discloses the method of claim 1, wherein the at least one packet matching criterion corresponding to the one or more first packet filtering rules automatically created or altered by the security policy management server comprises at least one network address indicated by the malicious traffic information **(e.g. Jalava "a characterizing value may be for example a header field value, a payload field value, an IP address (source or destination), port number (source or destination)" [0019]; [0020]; [0052]; [0057]; [0058])**.

As to Claim 3:

Jalava in view of **Bhatnagar** discloses the method of claim 1, wherein the malicious host tracker service comprises a subscription service that aggregates information associated with malicious network traffic **(e.g. Bhatnagar security service provides updates to subscribers, such companies as Symantec and MacAfee have security**

agents in millions of machines that detect viruses and other malicious code and generate threat patterns [0022]; [0018]; [0019]). The Examiner supplies the same rationale for the combination of references **Jalava** and **Bhatnagar** as in Claim 1 above.

As to Claim 5:

Jalava in view of **Bhatnagar** discloses the method of claim 1, wherein at least one packet transformation function comprises a network protective action **(e.g. Jalava "In a firewall, the action is typically deny or allow, which means the data packet is discarded or allowed to proceed, correspondingly" [0003])**.

As to Claim 7:

Jalava in view of **Bhatnagar** discloses the method of claim 1, wherein one or more packet filtering rules of the first set of packet filtering rules specify a packet transformation function **(e.g. Bhatnagar "additional remedial action may be taken such as to trace the traffic backwards through the network toward the source. Tracing the traffic backwards through the network may enable the source of the traffic to be identified, so that the edge network element connected to the source may cause the port over which the source connects to the network to be shut down" [0028])** other than forwarding or dropping the corresponding packets. The Examiner supplies the same rationale for the combination of references **Jalava** and **Bhatnagar** as in Claim 1 above.

As to Claim 8:

Jalava discloses a packet security gateway **(e.g. Jalava "A personalized firewall or other network gateway is provided by a method of matching a data packet to a rule in a network gateway having a rule base. One or more identification values**

are determined (302) on the basis of the data packet and property value(s) associated with said one or more identification values are queried (304) and received from a property server. The property value(s) describe for example allowed connections and services for an entity associated with the identification value(s). The property value(s) are compared (306) to at least one rule in the rule base, said at least one rule comprising property value(s) and an action, and the action defined in said at least one rule is taken (310), if said property value(s) of the rule match corresponding property value(s) associated with said one or more identification values" [Abstract]), of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway and one or more networks other than the network protected by the packet security gateway **(e.g. Jalava "As already described above, the firewall 23 and 31 are gateways which operate at the same time as a connector and a separator between the networks in a sense that the firewalls keep track of the traffic that passes through them from one network to another and restrict connections and packets that are defined as unwanted by the administrators of the systems" [0049]; Fig. 2A; [0044])**, comprising:

- one or more processors **(e.g. Jalava machine/computer [0002])**; and
- memory storing instructions **(e.g. Jalava memory [Claim 19]; computer-readable medium containing computer software [Claim 21])** that, when executed by the one or more processors, cause the packet security gateway to:
- receive, from a security policy management server external from the network protected by the packet security gateway **(e.g. Jalava management server 25**

is remotely connected to the firewall over the public network and sends firewall rules to the firewall for execution [0044]; Fig. 2A), a dynamic security policy comprising a first set of packet filtering rules to be applied to all network traffic traversing the boundary **(e.g. Jalava rules for firewall [0041]; [0044]; [0045]; [0049]; [0050])**, wherein:

- each packet filtering rule of the first set of packet filtering rules comprises at least one packet matching criterion and a corresponding packet transformation function **(e.g. Jalava "it is detected, if a data packet, which has been received, is compared to a rule containing property values (that is, requiring the use of property values for match process)… One or more identification values are determined on the basis of the data packet (step 302) and property value(s) associated with the identification value(s) are queried and received (step 304). In practice, the property values are stored in the firewall for future use after receiving them. If the property values are already stored, they do not need to be queried again. Then the property value(s) are compared to a rule, which includes property value(s) and an action, in step 306. If the property value(s) of the rule match corresponding property value(s) associated with the identification value(s), the action defined in the rule is taken (steps 308 and 310). If the property value(s) of the rule do not match corresponding property value(s) associated with the identification value(s), the next rule of the rule base is processed in step 312" [0050])**, and

- one or more first packet filtering rules of the first set of packet filtering rules were automatically created or altered by the security policy management server **(e.g. Jalava "firewall configuration (the rules), which may include also VPN configuration, is defined in the management system" [0044])**;
- perform, on a packet by packet basis, packet filtering on a first portion of packets corresponding to network traffic traversing the boundary via the packet security gateway based on the first set of packet filtering rules by performing at least one packet transformation function **(e.g. Jalava "In a firewall, the action is typically deny or allow, which means the data packet is discarded or allowed to proceed, correspondingly" [0003]; [0004]; [0017]; [0049])** specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets **(e.g. "The property value(s) are compared (306) to at least one rule in the rule base, said at least one rule comprising property value(s) and an action, and the action defined in said at least one rule is taken (310), if said property value(s) of the rule match corresponding property value(s) associated with said one or more identification values" [Abstract]; [0017]; [0049])**;
- receive, after performing packet filtering on the first portion of the packets, an updated second set of packet filtering rules for the dynamic security policy from the security policy management server, wherein the updated second set of packet filtering rules comprises an update to the one or more first packet filtering rules **(e.g. Jalava "the network gateway requests to be notified, if the property value(s) stored in the network gateway in step 504 are updated in**

the property server. At this point such a request needs to be stored in the property server with reference to the corresponding property value--identification value combination (not shown in the Figure). In step 602, a notification comprising updated property value(s) and associated identification value(s) are received. The old property value(s) in the network gateway are then replaced with the corresponding updated property value(s) in step 604" [0065]; [0066]; [0069]); and

- perform, on a packet by packet basis, packet filtering on a second portion of the packets corresponding to network traffic traversing the boundary via the packet security gateway based on the updated second set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the second set of packet filtering rules on the second portion of packets **(e.g. Jalava "When the firewall has compared a data packet to N first rules and none of them has matched the data packet, it is required to find out the property values associated with the source of the data packet. The firewall queries the property values from the property server by the source IP address 10.1.1.7 and receives the sequence of 101100 mentioned above" [0057]; [0050]; [0017]; [0049])**;

But **Jalava** does not specifically disclose:

- packet filtering rules created or altered by [a] management server based on updated malicious traffic information received from a malicious host tracker service.

However, the analogous art **Bhatnagar** does disclose packet filtering rules created *or* altered by [a] management server based on updated malicious traffic information received from a malicious host tracker service **(e.g. Bhatnagar create updated filter rules by filter generation service based on translating malicious traffic patterns received from the security service [0022]; [0024])**. **Jalava** and **Bhatnagar** are analogous art because they are from the same field of endeavor in network packet filtering.

- (e.g. see **Bhatnagar**, "In the example shown in FIG. 1, a security service 30 provides updates 32 as new threats are identified on the network… When a new threat is identified, the security service 30 will obtain a signature of the threat from the agents (not shown) and generate a pattern that may be used by the network elements 12, 14, to identify the threat. Pattern generation of this sort is currently done by security services, for example, in connection with providing updates to security software 24, and the invention is not limited to a particular manner of generating these types of updates" **[0022]**; see also "the patterns generated by the security service may be sent to a network management station 34. The network management station may then pass the patterns to a filter generation service 36 configured to create filter rules specific to the different types of network elements on the network 10. The filter generation service 36, in this alternate embodiment, is configured to translate the pattern received from the security service 30 via update 32 into filter rules 38 that are transmitted to the network elements and used by the network elements 12, 14 to filter traffic on the network. In either embodiment, the filter rules will be installed into the forwarding

planes of the network elements configured to act as detection points 28, so that traffic matching the patterns will be removed from the network. By continually updating the detection points 28 in real time as threats are discovered, it is possible to immunize the network against outbreaks of malicious code to reduce the chance that malicious code will reach the customer equipment" **[0024]**; "When a pattern match is found, the traffic may be discarded or, alternatively, additional remedial action may be taken such as to trace the traffic backwards through the network toward the source. Tracing the traffic backwards through the network may enable the source of the traffic to be identified" **[0028]**).

At the time of applicants' invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Jalava** and **Bhatnagar** before him or her, to modify the system and method of **Jalava** with the teachings of **Bhatnagar** to include *packet filtering rules created or altered by [a] management server based on updated malicious traffic information received from a malicious host tracker service* as claimed because **Jalava**'s system and method provides a management server that remotely connects to firewalls/gateways at protected networks to provide packet filtering rules and updates **(Jalava [Abstract]-[0069])** which could be based on received malicious traffic patterns sent from a security service **(Bhatnagar [0022]; [0024]; [0028])**. The suggestion/motivation for doing so would have been to stop malicious code that spans multiple packets at the network level so that new security threats may be neutralized quickly once discovered **(Bhatnagar [0026]; [0027])**. Therefore, it would have been obvious to combine **Jalava** and **Bhatnagar** to obtain the invention as specified in the instant claim(s).

As to Claim 9:

Jalava in view of **Bhatnagar** discloses the packet security gateway of claim 8, wherein the at least one packet matching criterion corresponding to the one or more first packet filtering rules automatically created or altered by the security policy management server comprises at least one network address indicated by the malicious traffic information **(e.g. Jalava "a characterizing value may be for example a header field value, a payload field value, an IP address (source or destination), port number (source or destination)" [0019]; [0020]; [0052]; [0057]; [0058])**.

As to Claim 10:

Jalava in view of **Bhatnagar** discloses the packet security gateway of claim 8, wherein the malicious host tracker service comprises a subscription service that aggregates information associated with malicious network traffic **(e.g. Bhatnagar security service provides updates to subscribers, such companies as Symantec and MacAfee have security agents in millions of machines that detect viruses and other malicious code and generate threat patterns [0022]; [0018]; [0019])**. The Examiner supplies the same rationale for the combination of references **Jalava** and **Bhatnagar** as in Claim 8 above.

As to Claim 12:

Jalava in view of **Bhatnagar** discloses the packet security gateway of claim 8, wherein at least one packet transformation function comprises a network protective action **(e.g. Jalava "In a firewall, the action is typically deny or allow, which means the data packet is discarded or allowed to proceed, correspondingly" [0003])**.

As to Claim 14:

Jalava in view of **Bhatnagar** discloses the packet security gateway of claim 8, wherein one or more packet filtering rules of the first set of packet filtering rules specify a packet transformation function **(e.g. Bhatnagar "additional remedial action may be taken such as to trace the traffic backwards through the network toward the source. Tracing the traffic backwards through the network may enable the source of the traffic to be identified, so that the edge network element connected to the source may cause the port over which the source connects to the network to be shut down" [0028])** other than forwarding or dropping the corresponding packets. The Examiner supplies the same rationale for the combination of references **Jalava** and **Bhatnagar** as in Claim 8 above.

As to Claim 15:

Jalava discloses one or more non-transitory computer readable media storing instructions **(e.g. Jalava memory [Claim 19]; computer-readable medium containing computer software [Claim 21])** that, when executed by at least one processor, cause a packet security gateway **(e.g. Jalava "A personalized firewall or other network gateway is provided by a method of matching a data packet to a rule in a network gateway having a rule base. One or more identification values are determined (302) on the basis of the data packet and property value(s) associated with said one or more identification values are queried (304) and received from a property server. The property value(s) describe for example allowed connections and services for an entity associated with the identification value(s). The property value(s) are compared (306) to at least one rule in the rule base, said at least one rule comprising property value(s) and an action, and the**

action defined in said at least one rule is taken (310), if said property value(s) of the rule match corresponding property value(s) associated with said one or more identification values" [Abstract]), of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway and one or more networks other than the network protected by the packet security gateway **(e.g. Jalava "As already described above, the firewall 23 and 31 are gateways which operate at the same time as a connector and a separator between the networks in a sense that the firewalls keep track of the traffic that passes through them from one network to another and restrict connections and packets that are defined as unwanted by the administrators of the systems" [0049]; Fig. 2A; [0044])**, to perform steps comprising:

- receiving, from a security policy management server external from the network protected by the packet security gateway **(e.g. Jalava management server 25 is remotely connected to the firewall over the public network and sends firewall rules to the firewall for execution [0044]; Fig. 2A)**, a dynamic security policy comprising a first set of packet filtering rules to be applied to all network traffic traversing the boundary **(e.g. Jalava rules for firewall [0041]; [0044]; [0045]; [0049]; [0050])**, wherein:
- each packet filtering rule of the first set of packet filtering rules comprises at least one packet matching criterion and a corresponding packet transformation function **(e.g. Jalava "it is detected, if a data packet, which has been received, is compared to a rule containing property values (that is, requiring the use of property values for match process)… One or more**

identification values are determined on the basis of the data packet (step 302) and property value(s) associated with the identification value(s) are queried and received (step 304). In practice, the property values are stored in the firewall for future use after receiving them. If the property values are already stored, they do not need to be queried again. Then the property value(s) are compared to a rule, which includes property value(s) and an action, in step 306. If the property value(s) of the rule match corresponding property value(s) associated with the identification value(s), the action defined in the rule is taken (steps 308 and 310). If the property value(s) of the rule do not match corresponding property value(s) associated with the identification value(s), the next rule of the rule base is processed in step 312" [0050]), and

- one or more first packet filtering rules of the first set of packet filtering rules were automatically created or altered by the security policy management server **(e.g. Jalava "firewall configuration (the rules), which may include also VPN configuration, is defined in the management system" [0044])**;
- performing, on a packet by packet basis, packet filtering on a first portion of packets corresponding to network traffic traversing the boundary via the packet security gateway based on the first set of packet filtering rules by performing at least one packet transformation function **(e.g. Jalava "In a firewall, the action is typically deny or allow, which means the data packet is discarded or allowed to proceed, correspondingly" [0003]; [0004]; [0017]; [0049])** specified by at least one packet filtering rule of the first set of packet filtering rules

on the first portion of packets **(e.g. "The property value(s) are compared (306) to at least one rule in the rule base, said at least one rule comprising property value(s) and an action, and the action defined in said at least one rule is taken (310), if said property value(s) of the rule match corresponding property value(s) associated with said one or more identification values" [Abstract]; [0017]; [0049])**;

- receiving, after performing packet filtering on the first portion of the packets, an updated second set of packet filtering rules for the dynamic security policy from the security policy management server, wherein the updated second set of packet filtering rules comprises an update to the one or more first packet filtering rules **(e.g. Jalava "the network gateway requests to be notified, if the property value(s) stored in the network gateway in step 504 are updated in the property server. At this point such a request needs to be stored in the property server with reference to the corresponding property value--identification value combination (not shown in the Figure). In step 602, a notification comprising updated property value(s) and associated identification value(s) are received. The old property value(s) in the network gateway are then replaced with the corresponding updated property value(s) in step 604" [0065]; [0066]; [0069])**; and
- performing, on a packet by packet basis, packet filtering on a second portion of the packets corresponding to network traffic traversing the boundary via the packet security gateway based on the updated second set of packet filtering rules by performing at least one packet transformation function specified by at

least one packet filtering rule of the second set of packet filtering rules on the second portion of packets **(e.g. Jalava "When the firewall has compared a data packet to N first rules and none of them has matched the data packet, it is required to find out the property values associated with the source of the data packet. The firewall queries the property values from the property server by the source IP address 10.1.1.7 and receives the sequence of 101100 mentioned above" [0057]; [0050])**;

But **Jalava** does not specifically disclose:

- packet filtering rules created or altered by [a] management server based on updated malicious traffic information received from a malicious host tracker service.

However, the analogous art **Bhatnagar** does disclose packet filtering rules created *or* altered by [a] management server based on updated malicious traffic information received from a malicious host tracker service **(e.g. Bhatnagar create updated filter rules by filter generation service based on translating malicious traffic patterns received from the security service [0022]; [0024])**. **Jalava** and **Bhatnagar** are analogous art because they are from the same field of endeavor in network packet filtering.

- (e.g. see **Bhatnagar**, "In the example shown in FIG. 1, a security service 30 provides updates 32 as new threats are identified on the network… When a new threat is identified, the security service 30 will obtain a signature of the threat from the agents (not shown) and generate a pattern that may be used by the network elements 12, 14, to identify the threat. Pattern generation of this sort is

currently done by security services, for example, in connection with providing updates to security software 24, and the invention is not limited to a particular manner of generating these types of updates" **[0022]**; see also "the patterns generated by the security service may be sent to a network management station 34. The network management station may then pass the patterns to a filter generation service 36 configured to create filter rules specific to the different types of network elements on the network 10. The filter generation service 36, in this alternate embodiment, is configured to translate the pattern received from the security service 30 via update 32 into filter rules 38 that are transmitted to the network elements and used by the network elements 12, 14 to filter traffic on the network. In either embodiment, the filter rules will be installed into the forwarding planes of the network elements configured to act as detection points 28, so that traffic matching the patterns will be removed from the network. By continually updating the detection points 28 in real time as threats are discovered, it is possible to immunize the network against outbreaks of malicious code to reduce the chance that malicious code will reach the customer equipment" **[0024]**; "When a pattern match is found, the traffic may be discarded or, alternatively, additional remedial action may be taken such as to trace the traffic backwards through the network toward the source. Tracing the traffic backwards through the network may enable the source of the traffic to be identified" **[0028]**).

At the time of applicants' invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Jalava** and **Bhatnagar** before him or her, to modify the system and method of **Jalava** with the teachings of **Bhatnagar** to include *packet*

filtering rules created or altered by [a] management server based on updated malicious traffic information received from a malicious host tracker service as claimed because **Jalava**'s system and method provides a management server that remotely connects to firewalls/gateways at protected networks to provide packet filtering rules and updates **(Jalava [Abstract]-[0069])** which could be based on received malicious traffic patterns sent from a security service **(Bhatnagar [0022]; [0024]; [0028])**. The suggestion/motivation for doing so would have been to stop malicious code that spans multiple packets at the network level so that new security threats may be neutralized quickly once discovered **(Bhatnagar [0026]; [0027])**. Therefore, it would have been obvious to combine **Jalava** and **Bhatnagar** to obtain the invention as specified in the instant claim(s).

As to Claim 16:

Jalava in view of **Bhatnagar** discloses the computer readable media of claim 15, wherein the at least one packet matching criterion corresponding to the one or more first packet filtering rules automatically created or altered by the security policy management server comprises at least one network address indicated by the malicious traffic information **(e.g. Jalava "a characterizing value may be for example a header field value, a payload field value, an IP address (source or destination), port number (source or destination)" [0019]; [0020]; [0052]; [0057]; [0058])**.

As to Claim 18:

Jalava in view of **Bhatnagar** discloses the computer readable media of claim 15, wherein at least one packet transformation function comprises a network protective

action **(e.g. Jalava "In a firewall, the action is typically deny or allow, which means the data packet is discarded or allowed to proceed, correspondingly" [0003])**.

As to Claim 20:

Jalava in view of **Bhatnagar** discloses the computer readable media of claim 15, wherein one or more packet filtering rules of the first set of packet filtering rules specify a packet transformation function **(e.g. Bhatnagar "additional remedial action may be taken such as to trace the traffic backwards through the network toward the source. Tracing the traffic backwards through the network may enable the source of the traffic to be identified, so that the edge network element connected to the source may cause the port over which the source connects to the network to be shut down" [0028])** other than forwarding or dropping the corresponding packets. The Examiner supplies the same rationale for the combination of references **Jalava** and **Bhatnagar** as in Claim 15 above.

As to Claim 21:

Jalava discloses a method of filtering packets at a packet security gateway configured for protection of a network **(e.g. Jalava "A personalized firewall or other network gateway is provided by a method of matching a data packet to a rule in a network gateway having a rule base. One or more identification values are determined (302) on the basis of the data packet and property value(s) associated with said one or more identification values are queried (304) and received from a property server. The property value(s) describe for example allowed connections and**

services for an entity associated with the identification value(s). The property value(s) are compared (306) to at least one rule in the rule base, said at least one rule comprising property value(s) and an action, and the action defined in said at least one rule is taken (310), if said property value(s) of the rule match corresponding property value(s) associated with said one or more identification values" [Abstract]) and associated with a security policy management server external from the network **(e.g. Jalava management server 25 is remotely connected to the firewall over the public network and sends firewall rules to the firewall for execution [0044]; Fig. 2A)**, the method comprising:

- receiving, by the packet security gateway **(e.g. Jalava management server sends firewall rules to the firewall for execution [0044]; Fig. 2A)**, a dynamic security policy comprising a first set of packet filtering rules from the security policy management server **(e.g. Jalava rules for firewall [0041]; [0044]; [0045]; [0049]; [0050])**, wherein each packet filtering rule of the first set of packet filtering rules comprises at least one packet matching criterion and a corresponding packet transformation function **(e.g. Jalava "it is detected, if a data packet, which has been received, is compared to a rule containing property values (that is, requiring the use of property values for match process)… One or more identification values are determined on the basis of the data packet (step 302) and property value(s) associated with the identification value(s) are queried and received (step 304). In practice, the property values are stored in the firewall for future use after receiving them. If the property values are already stored, they do not need to be**

queried again. Then the property value(s) are compared to a rule, which includes property value(s) and an action, in step 306. If the property value(s) of the rule match corresponding property value(s) associated with the identification value(s), the action defined in the rule is taken (steps 308 and 310). If the property value(s) of the rule do not match corresponding property value(s) associated with the identification value(s), the next rule of the rule base is processed in step 312" [0050]), and wherein one or more first packet filtering rules of the first set of packet filtering rules were automatically created or altered by the security policy management server **(e.g. Jalava "firewall configuration (the rules), which may include also VPN configuration, is defined in the management system" [0044])**;

- performing, on a packet by packet basis, packet filtering on a first portion of packets corresponding to network traffic traversing the boundary via the packet security gateway based on the first set of packet filtering rules by performing at least one of multiple packet transformation functions **(e.g. Jalava "In a firewall, the action is typically deny or allow, which means the data packet is discarded or allowed to proceed, correspondingly" [0003]; [0004]; [0017]; [0049])** specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets **(e.g. "The property value(s) are compared (306) to at least one rule in the rule base, said at least one rule comprising property value(s) and an action, and the action defined in said at least one rule is taken (310), if said property value(s) of the rule match**

corresponding property value(s) associated with said one or more identification values" [Abstract]; [0017]; [0049]);

- receiving, by the packet security gateway and after performing packet filtering on the first portion of the packets, an updated second set of packet filtering rules for the dynamic security policy from the security policy management server, wherein the updated second set of packet filtering rules comprises an update to the one or more first packet filtering rules **(e.g. Jalava "the network gateway requests to be notified, if the property value(s) stored in the network gateway in step 504 are updated in the property server. At this point such a request needs to be stored in the property server with reference to the corresponding property value--identification value combination (not shown in the Figure). In step 602, a notification comprising updated property value(s) and associated identification value(s) are received. The old property value(s) in the network gateway are then replaced with the corresponding updated property value(s) in step 604" [0065]; [0066]; [0069])**; and
- performing, on a packet by packet basis, packet filtering on a second portion of the packets associated with the network protected by the packet security gateway based on the updated second set of packet filtering rules **(e.g. Jalava "When the firewall has compared a data packet to N first rules and none of them has matched the data packet, it is required to find out the property values associated with the source of the data packet. The firewall queries the property values from the property server by the source IP address**

10.1.1.7 and receives the sequence of 101100 mentioned above" [0057]; [0050]);

But **Jalava** does not specifically disclose:

- packet filtering rules created or altered by [a] management server based on updated malicious traffic information received from a malicious host tracker service.

However, the analogous art **Bhatnagar** does disclose packet filtering rules created *or* altered by [a] management server based on updated malicious traffic information received from a malicious host tracker service **(e.g. Bhatnagar create updated filter rules by filter generation service based on translating malicious traffic patterns received from the security service [0022]; [0024])**. **Jalava** and **Bhatnagar** are analogous art because they are from the same field of endeavor in network packet filtering.

- (e.g. see **Bhatnagar**, "In the example shown in FIG. 1, a security service 30 provides updates 32 as new threats are identified on the network… When a new threat is identified, the security service 30 will obtain a signature of the threat from the agents (not shown) and generate a pattern that may be used by the network elements 12, 14, to identify the threat. Pattern generation of this sort is currently done by security services, for example, in connection with providing updates to security software 24, and the invention is not limited to a particular manner of generating these types of updates" **[0022]**; see also "the patterns generated by the security service may be sent to a network management station 34. The network management station may then pass the patterns to a filter

generation service 36 configured to create filter rules specific to the different types of network elements on the network 10. The filter generation service 36, in this alternate embodiment, is configured to translate the pattern received from the security service 30 via update 32 into filter rules 38 that are transmitted to the network elements and used by the network elements 12, 14 to filter traffic on the network. In either embodiment, the filter rules will be installed into the forwarding planes of the network elements configured to act as detection points 28, so that traffic matching the patterns will be removed from the network. By continually updating the detection points 28 in real time as threats are discovered, it is possible to immunize the network against outbreaks of malicious code to reduce the chance that malicious code will reach the customer equipment" **[0024]**; "When a pattern match is found, the traffic may be discarded or, alternatively, additional remedial action may be taken such as to trace the traffic backwards through the network toward the source. Tracing the traffic backwards through the network may enable the source of the traffic to be identified" **[0028]**).

At the time of applicants' invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Jalava** and **Bhatnagar** before him or her, to modify the system and method of **Jalava** with the teachings of **Bhatnagar** to include *packet filtering rules created or altered by [a] management server based on updated malicious traffic information received from a malicious host tracker service* as claimed because **Jalava**'s system and method provides a management server that remotely connects to firewalls/gateways at protected networks to provide packet filtering rules and updates **(Jalava [Abstract]-[0069])** which could be based on received malicious traffic patterns

sent from a security service **(Bhatnagar [0022]; [0024]; [0028])**. The suggestion/motivation for doing so would have been to stop malicious code that spans multiple packets at the network level so that new security threats may be neutralized quickly once discovered **(Bhatnagar [0026]; [0027])**. Therefore, it would have been obvious to combine **Jalava** and **Bhatnagar** to obtain the invention as specified in the instant claim(s).

As to Claim 22:

Jalava in view of **Bhatnagar** discloses the method of claim 21, wherein the at least one packet matching criterion corresponding to the one or more first packet filtering rules automatically created or altered by the security policy management server comprises at least one network address indicated by the malicious traffic information **(e.g. Jalava "a characterizing value may be for example a header field value, a payload field value, an IP address (source or destination), port number (source or destination)" [0019]; [0020]; [0052]; [0057]; [0058])**.

As to Claim 23:

Jalava in view of **Bhatnagar** discloses the method of claim 21, wherein the malicious host tracker service comprises a subscription service that aggregates information associated with malicious network traffic **(e.g. Bhatnagar security service provides updates to subscribers, such companies as Symantec and MacAfee have security agents in millions of machines that detect viruses and other malicious code and generate threat patterns [0022]; [0018]; [0019])**. The Examiner supplies the same rationale for the combination of references **Jalava** and **Bhatnagar** as in Claim 21 above.

As to Claim 25:

Jalava in view of **Bhatnagar** discloses the method of claim 21, wherein at least one packet transformation function comprises a network protective action **(e.g. Jalava "In a firewall, the action is typically deny or allow, which means the data packet is discarded or allowed to proceed, correspondingly" [0003])**.

As to Claim 27:

Jalava in view of **Bhatnagar** discloses the method of claim 21, wherein one or more packet filtering rules of the first set of packet filtering rules specify a packet transformation function **(e.g. Bhatnagar "additional remedial action may be taken such as to trace the traffic backwards through the network toward the source. Tracing the traffic backwards through the network may enable the source of the traffic to be identified, so that the edge network element connected to the source may cause the port over which the source connects to the network to be shut down" [0028])** other than forwarding or dropping the corresponding packets. The Examiner supplies the same rationale for the combination of references **Jalava** and **Bhatnagar** as in Claim 21 above.

9. **Claims 4, 11, 17, and 24** are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over **Jalava** in view of **Bhatnagar** as applied to Claims 1, 8, 15, and 21 above, and further in view of Van Der Merwe et al. (US 20100082811 A1, IDS submitted 03/25/2020, hereinafter **Van Der Merwe**).

As to Claim 4:

Jalava in view of **Bhatnagar** discloses the method of claim 1, but does not specifically disclose:

- wherein the malicious traffic information comprises a list of network addresses known to be associated with malicious network traffic.

However, the analogous art **Van Der Merwe** does disclose wherein the malicious traffic information comprises a list of network addresses known to be associated with malicious network traffic **(e.g. Van Der Merwe blacklist generated from received malicious network sources [0042]; [0043]; addresses of sources of unwanted data traffic [0003]; [0005]; unwanted traffic sources [0006]; malicious traffic source [0043]; [0028]; raw blacklists acquired from reputation systems [0030])**. **Jalava**, **Bhatnagar**, and **Van Der Merwe** are analogous art because they are from the same field of endeavor in coordinated processing of network packets.

- (e.g. see **Van Der Merwe**, "Blacklists may be derived, for example, from e-mail spam logs, firewall logs, databases from anti-spyware software, and databases from anti-virus software. Blacklists may also contain user-specified entries" **[0022]**; see also "Herein, a customer refers to an end-user of network services. A customer, for example, may operate user system US1 150. A user system operated by a customer is also referred to as a customer user system" **[0028]**; see also "In FIG. 2(a), a set of raw blacklists 202 is acquired from reputation systems RS1 130-RS3 134 as input to traffic filter system TFS 140. Additional raw blacklists may also be inputted by the network administrator. A raw blacklist refers to a blacklist which has not been processed by traffic filter system 140. In step 204, TFS 140 consolidates the multiple raw blacklists into a single list of unwanted traffic sources, referred to herein as a consolidated raw blacklist" **[0030]**; see also "FIG. 2(c) shows a flowchart of steps for generating a customer

> blacklist for a specific customer. Network blacklist 216 and a customer whitelist 234 (for a specific customer) are acquired as input into TFS 140… In general, since customer whitelist 234 may be different for different specific customers, customer blacklist 248 may be different for different specific customers. A customer blacklist is associated with a customer system" **[0042]**; see also "For example, network blacklist 216 may be updated in response to a network attack by a malicious traffic source" **[0043]**).

At the time of applicants' invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Jalava**, **Bhatnagar**, and **Van Der Merwe** before him or her, to modify the combination of **Jalava** and **Bhatnagar** with the teachings of **Van Der Merwe** to include *wherein the malicious traffic information comprises a list of network addresses known to be associated with malicious network traffic* as claimed because **Jalava**'s system and method provides a management server that remotely connects to firewalls/gateways at protected networks to provide packet filtering rules and updates **(Jalava [Abstract]-[0069])** which could be based on received malicious traffic patterns **(Bhatnagar [0022]; [0024]; [0028])** that comprise generated blacklists of malicious traffic sources for network service customers **(Van Der Merwe [0022]; [0028]; [0030]; [0042]; [0043])**. The suggestion/motivation for doing so would have been to provide a customer specific blacklist that is different for specific customers **(Van Der Merwe [0004]; [0042])**. Therefore, it would have been obvious to combine **Jalava**, **Bhatnagar**, and **Van Der Merwe** to obtain the invention as specified in the instant claim(s).

As to Claim 11:

Jalava in view of **Bhatnagar** discloses the packet security gateway of claim 8, but does not specifically disclose:

- wherein the malicious traffic information comprises a list of network addresses known to be associated with malicious network traffic.

However, the analogous art **Van Der Merwe** does disclose wherein the malicious traffic information comprises a list of network addresses known to be associated with malicious network traffic **(e.g. Van Der Merwe blacklist generated from received malicious network sources [0042]; [0043]; addresses of sources of unwanted data traffic [0003]; [0005]; unwanted traffic sources [0006]; malicious traffic source [0043]; [0028]; raw blacklists acquired from reputation systems [0030])**. **Jalava**, **Bhatnagar**, and **Van Der Merwe** are analogous art because they are from the same field of endeavor in coordinated processing of network packets.

- (e.g. see **Van Der Merwe**, "Blacklists may be derived, for example, from e-mail spam logs, firewall logs, databases from anti-spyware software, and databases from anti-virus software. Blacklists may also contain user-specified entries" **[0022]**; see also "Herein, a customer refers to an end-user of network services. A customer, for example, may operate user system US1 150. A user system operated by a customer is also referred to as a customer user system" **[0028]**; see also "In FIG. 2(a), a set of raw blacklists 202 is acquired from reputation systems RS1 130-RS3 134 as input to traffic filter system TFS 140. Additional raw blacklists may also be inputted by the network administrator. A raw blacklist refers to a blacklist which has not been processed by traffic filter system 140. In

> step 204, TFS 140 consolidates the multiple raw blacklists into a single list of unwanted traffic sources, referred to herein as a consolidated raw blacklist" **[0030]**; see also "FIG. 2(c) shows a flowchart of steps for generating a customer blacklist for a specific customer. Network blacklist 216 and a customer whitelist 234 (for a specific customer) are acquired as input into TFS 140... In general, since customer whitelist 234 may be different for different specific customers, customer blacklist 248 may be different for different specific customers. A customer blacklist is associated with a customer system" **[0042]**; see also "For example, network blacklist 216 may be updated in response to a network attack by a malicious traffic source" **[0043]**).

At the time of applicants' invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Jalava**, **Bhatnagar**, and **Van Der Merwe** before him or her, to modify the combination of **Jalava** and **Bhatnagar** with the teachings of **Van Der Merwe** to include *wherein the malicious traffic information comprises a list of network addresses known to be associated with malicious network traffic* as claimed because **Jalava**'s system and method provides a management server that remotely connects to firewalls/gateways at protected networks to provide packet filtering rules and updates **(Jalava [Abstract]-[0069])** which could be based on received malicious traffic patterns **(Bhatnagar [0022]; [0024]; [0028])** that comprise generated blacklists of malicious traffic sources for network service customers **(Van Der Merwe [0022]; [0028]; [0030]; [0042]; [0043])**. The suggestion/motivation for doing so would have been to provide a customer specific blacklist that is different for specific customers **(Van Der Merwe**

[0004]; [0042]). Therefore, it would have been obvious to combine **Jalava**, **Bhatnagar**, and **Van Der Merwe** to obtain the invention as specified in the instant claim(s).

As to Claim 17:

Jalava in view of **Bhatnagar** discloses the computer readable media of claim 15, wherein the malicious host tracker service comprises a subscription service that aggregates information associated with malicious network traffic **(e.g. Bhatnagar security service provides updates to subscribers, such companies as Symantec and MacAfee have security agents in millions of machines that detect viruses and other malicious code and generate threat patterns [0022]; [0018]; [0019])**, but does not specifically disclose:

- wherein the malicious traffic information comprises a list of network addresses known to be associated with malicious network traffic.

However, the analogous art **Van Der Merwe** does disclose wherein the malicious traffic information comprises a list of network addresses known to be associated with malicious network traffic **(e.g. Van Der Merwe blacklist generated from received malicious network sources [0042]; [0043]; addresses of sources of unwanted data traffic [0003]; [0005]; unwanted traffic sources [0006]; malicious traffic source [0043]; [0028]; raw blacklists acquired from reputation systems [0030])**. **Jalava**, **Bhatnagar**, and **Van Der Merwe** are analogous art because they are from the same field of endeavor in coordinated processing of network packets.

- (e.g. see **Van Der Merwe**, "Blacklists may be derived, for example, from e-mail spam logs, firewall logs, databases from anti-spyware software, and databases from anti-virus software. Blacklists may also contain user-specified entries"

[0022]; see also "Herein, a customer refers to an end-user of network services. A customer, for example, may operate user system US1 150. A user system operated by a customer is also referred to as a customer user system" **[0028]**; see also "In FIG. 2(a), a set of raw blacklists 202 is acquired from reputation systems RS1 130-RS3 134 as input to traffic filter system TFS 140. Additional raw blacklists may also be inputted by the network administrator. A raw blacklist refers to a blacklist which has not been processed by traffic filter system 140. In step 204, TFS 140 consolidates the multiple raw blacklists into a single list of unwanted traffic sources, referred to herein as a consolidated raw blacklist" **[0030]**; see also "FIG. 2(c) shows a flowchart of steps for generating a customer blacklist for a specific customer. Network blacklist 216 and a customer whitelist 234 (for a specific customer) are acquired as input into TFS 140… In general, since customer whitelist 234 may be different for different specific customers, customer blacklist 248 may be different for different specific customers. A customer blacklist is associated with a customer system" **[0042]**; see also "For example, network blacklist 216 may be updated in response to a network attack by a malicious traffic source" **[0043]**).

At the time of applicants' invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Jalava**, **Bhatnagar**, and **Van Der Merwe** before him or her, to modify the combination of **Jalava** and **Bhatnagar** with the teachings of **Van Der Merwe** to include *wherein the malicious traffic information comprises a list of network addresses known to be associated with malicious network traffic* as claimed because **Jalava**'s system and method provides a management server that remotely connects to

firewalls/gateways at protected networks to provide packet filtering rules and updates **(Jalava [Abstract]-[0069])** which could be based on received malicious traffic patterns **(Bhatnagar [0022]; [0024]; [0028])** that comprise generated blacklists of malicious traffic sources for network service customers **(Van Der Merwe [0022]; [0028]; [0030]; [0042]; [0043])**. The suggestion/motivation for doing so would have been to provide a customer specific blacklist that is different for specific customers **(Van Der Merwe [0004]; [0042])**. Therefore, it would have been obvious to combine **Jalava**, **Bhatnagar**, and **Van Der Merwe** to obtain the invention as specified in the instant claim(s).

As to Claim 24:

Jalava in view of **Bhatnagar** discloses the method of claim 21, but does not specifically disclose:

- wherein the malicious traffic information comprises a list of network addresses known to be associated with malicious network traffic.

However, the analogous art **Van Der Merwe** does disclose wherein the malicious traffic information comprises a list of network addresses known to be associated with malicious network traffic **(e.g. Van Der Merwe blacklist generated from received malicious network sources [0042]; [0043]; addresses of sources of unwanted data traffic [0003]; [0005]; unwanted traffic sources [0006]; malicious traffic source [0043]; [0028]; raw blacklists acquired from reputation systems [0030])**. **Jalava**, **Bhatnagar**, and **Van Der Merwe** are analogous art because they are from the same field of endeavor in coordinated processing of network packets.

- (e.g. see **Van Der Merwe**, “Blacklists may be derived, for example, from e-mail spam logs, firewall logs, databases from anti-spyware software, and databases

from anti-virus software. Blacklists may also contain user-specified entries" **[0022]**; see also "Herein, a customer refers to an end-user of network services. A customer, for example, may operate user system US1 150. A user system operated by a customer is also referred to as a customer user system" **[0028]**; see also "In FIG. 2(a), a set of raw blacklists 202 is acquired from reputation systems RS1 130-RS3 134 as input to traffic filter system TFS 140. Additional raw blacklists may also be inputted by the network administrator. A raw blacklist refers to a blacklist which has not been processed by traffic filter system 140. In step 204, TFS 140 consolidates the multiple raw blacklists into a single list of unwanted traffic sources, referred to herein as a consolidated raw blacklist" **[0030]**; see also "FIG. 2(c) shows a flowchart of steps for generating a customer blacklist for a specific customer. Network blacklist 216 and a customer whitelist 234 (for a specific customer) are acquired as input into TFS 140… In general, since customer whitelist 234 may be different for different specific customers, customer blacklist 248 may be different for different specific customers. A customer blacklist is associated with a customer system" **[0042]**; see also "For example, network blacklist 216 may be updated in response to a network attack by a malicious traffic source" **[0043]**).

At the time of applicants' invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Jalava**, **Bhatnagar**, and **Van Der Merwe** before him or her, to modify the combination of **Jalava** and **Bhatnagar** with the teachings of **Van Der Merwe** to include *wherein the malicious traffic information comprises a list of network addresses known to be associated with malicious network traffic* as claimed because

Jalava's system and method provides a management server that remotely connects to firewalls/gateways at protected networks to provide packet filtering rules and updates **(Jalava [Abstract]-[0069])** which could be based on received malicious traffic patterns **(Bhatnagar [0022]; [0024]; [0028])** that comprise generated blacklists of malicious traffic sources for network service customers **(Van Der Merwe [0022]; [0028]; [0030]; [0042]; [0043])**. The suggestion/motivation for doing so would have been to provide a customer specific blacklist that is different for specific customers **(Van Der Merwe [0004]; [0042])**. Therefore, it would have been obvious to combine **Jalava**, **Bhatnagar**, and **Van Der Merwe** to obtain the invention as specified in the instant claim(s).

10. **Claims 6, 13, 19, and 26** are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over **Jalava** in view of **Bhatnagar** as applied to Claims 1, 8, 15, and 21 above, and further in view of Jungck et al. (US 20090262741 A1, IDS submitted 03/25/2020, hereinafter **Jungck**).

As to Claim 6:

Jalava in view of **Bhatnagar** discloses the method of claim 1, further comprising: performing the at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets at the network layer **(e.g. Jalava "In a firewall, the action is typically deny or allow, which means the data packet is discarded or allowed to proceed, correspondingly" [0003]; [0004]; "The property value(s) are compared (306) to at least one rule in the rule base, said at least one rule comprising property value(s) and an action, and the action defined in said at least one rule is taken (310), if said property value(s) of the rule match corresponding property value(s)**

associated with said one or more identification values" [Abstract]; [0017]; [0049]), but does not specifically disclose:

- receiving, by the packet security gateway, packets in a network layer transparent manner using an interface that is not addressed at the network layer.

However, the analogous art **Jungck** does disclose receiving, by the packet security gateway, packets in a network layer transparent manner using an interface that is not addressed at the network layer **(e.g. Jungck the edge server "effectively needs no address because it intercepts the necessary network traffic" [0098]; [0108]; [0159]-[0165]; devices may be selectively transparent to the network [0126]-[0128]; [0153])**. **Jalava**, **Bhatnagar**, and **Jungck** are analogous art because they are from the same field of endeavor in coordinated processing of network packets.

- (e.g. see **Jungck**, "A major distinction between the edge server 502 and a proxy server is that there is no one address of the edge server 502. The edge server 502 effectively needs no address because it intercepts the necessary network traffic. Therefore, clients 102, 104 do not need to know of the existence of the edge server 502 and can operate as they normally do, making content requests of servers 108" **[0098]**; see also "the edge server 602 is further capable of intercepting data traffic at the packet level based on the source or destination IP address contained within the packets flowing past the edge server 602. In this way, the edge server 602 is able to provide complete isolation of its subscribing servers 108, 110" **[0108]**; **[0128]; [0153]; [0159]-[0165]**).

At the time of applicants' invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Jalava**, **Bhatnagar**, and **Jungck** before him or her, to

modify the combination of **Jalava** and **Bhatnagar** with the teachings of **Jungck** to include *receiving, by the packet security gateway, packets in a network layer transparent manner using an interface that is not addressed at the network layer* as claimed because **Jalava**'s system and method provides a management server that remotely connects to firewalls/gateways at protected networks which provide packet filtering on all traffic that passes through one network to another **(Jalava [Abstract]-[0069])** where packets could be intercepted transparently by an edge routing device with no network address **(Jungck [0098]; [0108]; [0126]-[0128]; [0153]; [0159]-[0165])**. The suggestion/motivation for doing so would have been to allow for early and reliable packet interception and further ensures some measure of reliability in determining the origination of a particular packet **(Jungck [0121])**. Therefore, it would have been obvious to combine **Jalava**, **Bhatnagar**, and **Jungck** to obtain the invention as specified in the instant claim(s).

As to Claim 13:

Jalava in view of **Bhatnagar** discloses the packet security gateway of claim 8, wherein the instructions further cause the packet security gateway to: perform the at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets at the network layer **(e.g. Jalava "In a firewall, the action is typically deny or allow, which means the data packet is discarded or allowed to proceed, correspondingly" [0003]; [0004]; "The property value(s) are compared (306) to at least one rule in the rule base, said at least one rule comprising property value(s) and an action, and the action defined in said at least one rule is taken (310), if said property value(s) of the rule match**

corresponding property value(s) associated with said one or more identification values" [Abstract]; [0017]; [0049]), but does not specifically disclose:

- receive packets in a network layer transparent manner using an interface that is not addressed at the network layer.

However, the analogous art **Jungck** does disclose receive packets in a network layer transparent manner using an interface that is not addressed at the network layer **(e.g. Jungck the edge server "effectively needs no address because it intercepts the necessary network traffic" [0098]; [0108]; [0159]-[0165]; devices may be selectively transparent to the network [0126]-[0128]; [0153])**. **Jalava**, **Bhatnagar**, and **Jungck** are analogous art because they are from the same field of endeavor in coordinated processing of network packets.

- (e.g. see **Jungck**, "A major distinction between the edge server 502 and a proxy server is that there is no one address of the edge server 502. The edge server 502 effectively needs no address because it intercepts the necessary network traffic. Therefore, clients 102, 104 do not need to know of the existence of the edge server 502 and can operate as they normally do, making content requests of servers 108" **[0098]**; see also "the edge server 602 is further capable of intercepting data traffic at the packet level based on the source or destination IP address contained within the packets flowing past the edge server 602. In this way, the edge server 602 is able to provide complete isolation of its subscribing servers 108, 110" **[0108]**; **[0128]; [0153]; [0159]-[0165]**).

At the time of applicants' invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Jalava**, **Bhatnagar**, and **Jungck** before him or her, to

modify the combination of **Jalava** and **Bhatnagar** with the teachings of **Jungck** to include *receive packets in a network layer transparent manner using an interface that is not addressed at the network layer* as claimed because **Jalava**'s system and method provides a management server that remotely connects to firewalls/gateways at protected networks which provide packet filtering on all traffic that passes through one network to another **(Jalava [Abstract]-[0069])** where packets could be intercepted transparently by an edge routing device with no network address **(Jungck [0098]; [0108]; [0126]-[0128]; [0153]; [0159]-[0165])**. The suggestion/motivation for doing so would have been to allow for early and reliable packet interception and further ensures some measure of reliability in determining the origination of a particular packet **(Jungck [0121])**. Therefore, it would have been obvious to combine **Jalava**, **Bhatnagar**, and **Jungck** to obtain the invention as specified in the instant claim(s).

As to Claim 19:

Jalava in view of **Bhatnagar** discloses the computer readable media of claim 15, further comprising: performing the at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets at the network layer **(e.g. Jalava "In a firewall, the action is typically deny or allow, which means the data packet is discarded or allowed to proceed, correspondingly" [0003]; [0004]; "The property value(s) are compared (306) to at least one rule in the rule base, said at least one rule comprising property value(s) and an action, and the action defined in said at least one rule is taken (310), if said property value(s) of the rule match corresponding property value(s)**

associated with said one or more identification values" [Abstract]; [0017]; [0049]), but does not specifically disclose:

- receiving, by the packet security gateway, packets in a network layer transparent manner using an interface that is not addressed at the network layer.

However, the analogous art **Jungck** does disclose receiving, by the packet security gateway, packets in a network layer transparent manner using an interface that is not addressed at the network layer **(e.g. Jungck the edge server "effectively needs no address because it intercepts the necessary network traffic" [0098]; [0108]; [0159]-[0165]; devices may be selectively transparent to the network [0126]-[0128]; [0153])**. **Jalava**, **Bhatnagar**, and **Jungck** are analogous art because they are from the same field of endeavor in coordinated processing of network packets.

- (e.g. see **Jungck**, "A major distinction between the edge server 502 and a proxy server is that there is no one address of the edge server 502. The edge server 502 effectively needs no address because it intercepts the necessary network traffic. Therefore, clients 102, 104 do not need to know of the existence of the edge server 502 and can operate as they normally do, making content requests of servers 108" **[0098]**; see also "the edge server 602 is further capable of intercepting data traffic at the packet level based on the source or destination IP address contained within the packets flowing past the edge server 602. In this way, the edge server 602 is able to provide complete isolation of its subscribing servers 108, 110" **[0108]**; **[0128]; [0153]; [0159]-[0165]**).

At the time of applicants' invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Jalava**, **Bhatnagar**, and **Jungck** before him or her, to

modify the combination of **Jalava** and **Bhatnagar** with the teachings of **Jungck** to include *receiving, by the packet security gateway, packets in a network layer transparent manner using an interface that is not addressed at the network layer* as claimed because **Jalava**'s system and method provides a management server that remotely connects to firewalls/gateways at protected networks which provide packet filtering on all traffic that passes through one network to another **(Jalava [Abstract]-[0069])** where packets could be intercepted transparently by an edge routing device with no network address **(Jungck [0098]; [0108]; [0126]-[0128]; [0153]; [0159]-[0165])**. The suggestion/motivation for doing so would have been to allow for early and reliable packet interception and further ensures some measure of reliability in determining the origination of a particular packet **(Jungck [0121])**. Therefore, it would have been obvious to combine **Jalava**, **Bhatnagar**, and **Jungck** to obtain the invention as specified in the instant claim(s).

As to Claim 26:

Jalava in view of **Bhatnagar** discloses the method of claim 21, further comprising: performing the at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets at the network layer **(e.g. Jalava "In a firewall, the action is typically deny or allow, which means the data packet is discarded or allowed to proceed, correspondingly" [0003]; [0004]; "The property value(s) are compared (306) to at least one rule in the rule base, said at least one rule comprising property value(s) and an action, and the action defined in said at least one rule is taken (310), if said property value(s) of the rule match corresponding property value(s)**

associated with said one or more identification values" [Abstract]; [0017]; [0049]), but does not specifically disclose:

- receiving, by the packet security gateway, packets in a network layer transparent manner using an interface that is not addressed at the network layer.

However, the analogous art **Jungck** does disclose receiving, by the packet security gateway, packets in a network layer transparent manner using an interface that is not addressed at the network layer **(e.g. Jungck the edge server "effectively needs no address because it intercepts the necessary network traffic" [0098]; [0108]; [0159]-[0165]; devices may be selectively transparent to the network [0126]-[0128]; [0153])**. **Jalava**, **Bhatnagar**, and **Jungck** are analogous art because they are from the same field of endeavor in coordinated processing of network packets.

- (e.g. see **Jungck**, "A major distinction between the edge server 502 and a proxy server is that there is no one address of the edge server 502. The edge server 502 effectively needs no address because it intercepts the necessary network traffic. Therefore, clients 102, 104 do not need to know of the existence of the edge server 502 and can operate as they normally do, making content requests of servers 108" **[0098]**; see also "the edge server 602 is further capable of intercepting data traffic at the packet level based on the source or destination IP address contained within the packets flowing past the edge server 602. In this way, the edge server 602 is able to provide complete isolation of its subscribing servers 108, 110" **[0108]**; **[0128]; [0153]; [0159]-[0165]**).

At the time of applicants' invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Jalava**, **Bhatnagar**, and **Jungck** before him or her, to

modify the combination of **Jalava** and **Bhatnagar** with the teachings of **Jungck** to include *receiving, by the packet security gateway, packets in a network layer transparent manner using an interface that is not addressed at the network layer* as claimed because **Jalava**'s system and method provides a management server that remotely connects to firewalls/gateways at protected networks which provide packet filtering on all traffic that passes through one network to another **(Jalava [Abstract]-[0069])** where packets could be intercepted transparently by an edge routing device with no network address **(Jungck [0098]; [0108]; [0126]-[0128]; [0153]; [0159]-[0165])**. The suggestion/motivation for doing so would have been to allow for early and reliable packet interception and further ensures some measure of reliability in determining the origination of a particular packet **(Jungck [0121])**. Therefore, it would have been obvious to combine **Jalava**, **Bhatnagar**, and **Jungck** to obtain the invention as specified in the instant claim(s).

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicants' disclosure.

a. **Baum et al. (US 6400707 B1)**

b. **Haswell (US 20090150996 A1)**

c. **Jordan (US 8839417 B1)**

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kenneth W Chang whose telephone number is (571)270-7530. The examiner can normally be reached on Monday - Friday 9-5pm EST.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on 571-272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see https://ppair-my.uspto.gov/pair/PrivatePair. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/KENNETH W CHANG/
Primary Examiner, Art Unit 2438
UNITED STATES PATENT AND TRADEMARK OFFICE
04/12/2020

Notice of References Cited	Application/Control No. 16/728,766	Applicant(s)/Patent Under Reexamination Rogers et al.	
	Examiner Kenneth W Chang	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-6400707-B1	06-2002	Baum; Robert T.	H04L63/0263	370/352
*	B	US-20030118038-A1	06-2003	Jalava, Mika	H04L63/0263	370/401
*	C	US-8839417-B1	09-2014	Jordan; Christopher J.	H04L63/0227	726/22
*	D	US-20090150996-A1	06-2009	Haswell; Jonathan	G06F21/554	726/22
*	E	US-20060123481-A1	06-2006	Bhatnagar; Atul	H04L63/0236	726/24
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/728,766	Rogers et al.
	Examiner	Art Unit
	Kenneth W Chang	2438

CPC - Searched*		
Symbol	**Date**	**Examiner**
H04L63/20	04/11/2020	KC
H04L63/0209	04/11/2020	KC
H04L63/0218	04/11/2020	KC
H04L63/0236	04/11/2020	KC
H04L67/02	04/11/2020	KC

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	**Date**	**Examiner**
Searched Inventors' Names and Assignee on PE2E DAV and EAST databases.	04/11/2020	KC
Searched IQ IP.com NPL database.	04/11/2020	KC
Completed Limited Classified Search in CPC on EAST USPAT, PGPUB, and EPO databases with Keywords.	04/12/2020	KC
Keywords: (malware or malicious) with (traffic or packet) with (data or information or feedback) and rule with packet with filter$9 with (updat $9)	04/12/2020	KC

/KENNETH W CHANG/ Primary Examiner, Art Unit 2438	

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/728,766	Rogers et al.
	Examiner	Art Unit
	Kenneth W Chang	2438

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/KENNETH W CHANG/ Primary Examiner, Art Unit 2438	

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/728,766	Rogers et al.
	Examiner	**Art Unit**
	Kenneth W Chang	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/12/2020								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								
	23	✓								
	24	✓								
	25	✓								
	26	✓								
	27	✓								

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

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. 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	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\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]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\US

/KC/	1	2020 Feb 11 (US) Final Written Decision Determining All Challenged Claims Unpatentable of U.S. Patent 9,137,205 B2 - IPR 2018-01444
	2	2020 Feb 11 (US) Final Written Decision Determining All Challenged Claims Unpatentable of U.S. Patent 9,137,205 B2 - IPR 2018-01443
	3	2020 Mar 19 (US) Final Written Decision Determining All Challenged Claims Unpatentable of U.S. Patent 9,565,213 B2 - IPR 2018-01512
	4	2020 Jan 23 (US) Final Written Decision Determining All Challenged Claims Unpatentable of U.S. Patent 9,565,213 B2 - IPR 2018-01386
	5	2020 Mar 31 (US) Final Written Decision Determining All Challenged Claims Unpatentable of U.S. Patent 9,560,077 B2 - IPR 2018-01513

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

EXAMINER SIGNATURE

Examiner Signature	/KENNETH W CHANG/	Date Considered	04/12/2020

*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.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L4	8	H04L63/0209.CPC. AND (firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9)) same polic$9 same (packet or data or datagram or traffic) and (malicious or malware or attack$9 or intrusion or ddos or protect$9) and (server with (external or outside))	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/12 15:00
L3	61	H04L63/20.CPC. AND (firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9)) same polic$9 same (packet or data or datagram or traffic) and (malicious or malware or attack$9 or intrusion or ddos or protect$9) and (server with (external or outside))	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/12 15:00
L2	192	("20080028467" | "20080043739" | "20080072307" | "20080077705" | "20080080493" | "20080086435" | "20080101234" | "20080163333" | "20080201772" | "20080229415" | "20080235755" | "20080279196" | "20080301765" | "20080313738" | "20080320116" | "20090028160" | "20090138938" | "20090144819" | "20090150972" | "20090172800" | "20090222877" | "20090240698" | "20090262723" | "20090262741" | "20090300759" | "20090328219" | "20100011433" | "20100011434" | "20100082811" | "20100095367" | "20100107240" | "20100115621" | "20100132027" | "20100195503" | "20100199346" | "20100202299" | "20100211678" | "20100232445" | "20100242098" | "20100268799" | "20100296441" | "20100303240" | "20110055916" | "20110055923" | "20110088092" | "20110141900" | "20110154470" | "20110185055" | "20110214157" | "20110270956" | "20110277034" | "20120023576" | "20120084866" | "20120106354" | "20120110656" | "20120113987" | "20120240135" | "20120240185" | "20120264443" | "20120314617" | "20120331543" | "20130007257" | "20130047020" | "20130059527" | "20130061294" | "20130104236" | "20130117852" | "20130139236" | "20130254766" | "20130291100" | "20130305311" | "20140075510" | "20140082204" | "20140082730" | "20140115654" | "20140150051" | "20140201123" | "20140215561" |	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/12 14:41

		"20140215574" | "20140245423" | "20140259170" | "20140281030" | "20140283004" | "20140283030" | "20140317397" | "20140317737" | "20140337613" | "20140365372" | "20140366132" | "20150033336" | "20150052601" | "20150106930" | "20150128274" | "20150135325" | "20150207809" | "20150237012" | "20150244734" | "20150256431" | "20150304354" | "20150334125" | "20150341389" | "20150347246" | "20150350229" | "20150372977" | "20150373043" | "20160020968" | "20160028751" | "20160065611" | "20160112443" | "20160119365" | "20160127417" | "20160191558" | "20160205069" | "20160219065" | "20160285706" | "20160294870" | "20160366099" | "20170223046" | "20170272469" | "6098172" | "6147976" | "6226372" | "6279113" | "6317837" | "6484261" | "6611875" | "6662235" | "6678827" | "6826694" | "6907042" | "6971028" | "7089581" | "7095716" | "7107613" | "7143438" | "7152240" | "7185368" | "7215637" | "7225269" | "7227842" | "7237267" | "7263099" | "7296288" | "7299353" | "7331061" | "7478429" | "7499412" | "7539186" | "7610621" | "7684400" | "7710885" | "7721084" | "7792775" | "7814158" | "7814546" | "7818794" | "7849502" | "7913303" | "7954143" | "8004994" | "8009566" | "8037517" | "8042167" | "8117655" | "8156206" | "8176561" | "8219675" | "8271645" | "8306994" | "8307029" | "8331234" | "8422391" | "8495725" | "8510821" | "8726379" | "8789135" | "8806638" | "8832832" | "8856926" | "8935785" | "9094445" | "9124552" | "9137205" | "9154446" | "9160713" | "9172627" | "9419942" | "9531672" | "9634911" | "9686193").PN.				
L1	90	("20010039579" | "20010039624" | "20020016858" | "20020038339" | "20020049899" | "20020083345" | "20020112188" | "20020152209" | "20020164962" | "20020165949" | "20020186683" | "20020198981" | "20030005122" | "20030014665" | "20030018591" | "20030035370" | "20030051026" | "20030088787" | "20030097590" | "20030105976" | "20030120622" | "20030123456" | "20030142681" | "20030145225" | "20030154297" | "20030154399" | "20030188192" | "20030212900" | "20030220940" | "20040010712" | "20040015719" | "20040073655" | "20040088542" | "20040093513" | "20040098511" | "20040114518" | "20040123220" | "20040131056" | "20040148520" | "20040151155" | "20040172529" | "20040172557" | "20040177139" | "20040181690" | "20040193943" | "20040199629" | "20040205360" | "20040250124" | "20050010765" | "20050024189" | "20050071650" | "20050076227" | "20050108557" | "20050114704" | "20050117576" | "20050125697" | "20050138204" | "20050138353" | "20050141537" | "20050183140" |	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/12 14:41

		"20050229246" | "20050249214" | "20050251570" | "20050283823" | "20050286522" | "20060031928" | "20060048142" | "20060053491" | "20060070122" | "20060080733" | "20060085849" | "20060104202" | "20060114899" | "20060133377" | "20060136987" | "20060137009" | "20060146879" | "20060159028" | "20060195896" | "20060212572" | "20060248580" | "20060262798" | "20070056038" | "20070083924" | "20070118894" | "20070147380" | "20070211644" | "20070240208" | "20070291789" | "20080005795").PN.				
S286	1	"20060123481".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 21:16
S285	1	"20090150996".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 21:00
S284	8	(malware or malicious) with (traffic or packet) with (data or information or feedback) same rule with packet with filter$9 with (updat$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 20:40
S283	51	(malware or malicious) with (traffic or packet) with (data or information or feedback) and rule with packet with filter$9 with (updat$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 20:40
S282	67	(malware or malicious) with (service or track$5) with (traffic or informat$9) and rule with packet with filter$9 with (creat$9 or updat$9 or alter$9 or generat$9 or new)	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 17:37

S281	0	(malware or malicious) with (service or track$5) with (traffic or informat$9) same rule with packet with filter$9 with (creat$9 or updat$9 or alter$9 or generat$9 or new)	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 17:36
S280	0	(malware or malicious) with (host) with (track$9) with (service or informat$9) same rule with packet with filter$9 with (creat$9 or updat$9 or alter$9 or generat$9 or new)	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 17:34
S278	0	(malware or malicious) with (track$9) with (service or informat$9) with rule with packet with filter$9 with (creat$9 or updat$9 or alter$9 or generat$9 or new)	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 17:33
S277	0	(malware or malicious) with (host) with (track$9) with (service or informat$9) with rule with packet with filter$9 with (creat$9 or updat$9 or alter$9 or generat$9 or new)	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 17:21
S276	0	(malware or malicious) with (host) with (track$9) with (service or informat$9) with rule with packet with filter$9 with (creat$9 or updat$9 or alter$9 or generat$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 17:21
S275	1	"20070118894".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 16:14
S274	1	"20060059551".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 12:08

S273	1	"20080244726".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 12:06
S272	1	"20030088788".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 12:04
S271	1	"20030118038".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 12:00
S270	1	"20120069749".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 11:58
S269	1	"6230271".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 11:58
S268	1	"20080016550".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 11:27
S267	1	"20110016509".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 11:12

S266	93	(firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9)) same polic$9 same (packet or data or datagram or traffic) and (malicious or malware or attack$9 or intrusion or ddos or protect$9) and (server with (external or outside))	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 11:07
S265	1	"20030154399".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 10:59
S264	1	"20070271605".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 10:52
S263	1	"6400707".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 10:47
S262	39467	H04L67/02.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 10:45
S261	3914	H04L63/0236.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 10:45
S260	1150	H04L63/0218.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 10:45

S259	2058	H04L63/0209.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 10:45
S258	17591	H04L63/20.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 10:45
S257	34	(centripetal networks).as.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 10:44
S256	188	(moore adj3 sean).in.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 10:44
S255	607	(rogers adj3 steven).in.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/04/11 10:44
S254	4	(10567437 | 10091246 | 9560077 | 9137205).pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2020/03/20 21:17
S253	29	H04L63/0218.CPC. and (firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9)) same polic$9 and (malicious or malware or attack$9 or intrusion) same (packet$9 or frame or traffic$)	US-PGPUB; USPAT; EPO	ADJ	ON	2019/12/04 15:20

S252	3	(20080040793 | 20130117801 | 7853996).pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/12/04 15:20
S251	196	H04L63/0263.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing)	US-PGPUB; USPAT; EPO	ADJ	ON	2019/12/04 15:17
S250	1047	(set or list$5) with (addresses) with (ip or internet protocol or source) with (discard$9 or block$6 or drop$5) same (packet) and (forward$9 or allow$8) with (outside or otherwise or address$5) same (packet) with (address$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2019/12/04 15:17
S249	117	(firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9)) same polic$9 and (malicious or malware or attack$9 or intrusion) same (packet$9 or frame or traffic$)	US-PGPUB; USPAT; EPO	ADJ	ON	2019/12/04 15:17
S239	62	("20020083345" | "20020152209" | "20030005122" | "20030014665" | "20030088787" | "20040015719" | "20040114518" | "20040131056" | "20050249214" | "20060031928" | "20070056038" | "20070291789" | "20080028467" | "20080080493" | "20080086435" | "20080101234" | "20080201772" | "20080313738" | "20080320116" | "20090144819" | "20090262723" | "20090300759" | "20100115621" | "20100195503" | "20100202299" | "20110214157" | "20120084866" | "20120110656" | "20120240185" | "20130007257" | "20130139236" | "20140082204" | "20140082730" | "20140215561" | "20140337613" | "20150128274" | "20150135325" | "20150207809" | "20150256431" | "20150347246" | "20160028751" | "20160127417" | "20160191558" | "20170223046" | "20170272469" | "6907042" | "6971028" | "7152240" | "7185368" | "7225269" | "7499412" | "7849502" | "8156206" | "8219675" | "8271645" | "8331234" | "8422391" | "8510821" | "9531672" | "9634911" | "9686193").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/12/03 17:00

S238	37877	H04L67/02.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/12/03 16:57
S237	3704	H04L63/0236.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/12/03 16:57
S236	1116	H04L63/0218.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/12/03 16:57
S235	20	H04L63/0209.CPC. and (firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9)) same polic$9 and (malicious or malware or attack$9 or intrusion) same (packet$9 or frame or traffic$)	US-PGPUB; USPAT; EPO	ADJ	ON	2019/12/03 16:57
S234	16620	H04L63/20.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/12/03 16:57
S233	1	"20090262741".PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/21 14:06
S232	43	H04L63/0263.CPC. and (firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9)) same polic$9 and (malicious or malware or attack$9 or intrusion) same (packet$9 or frame or traffic$)	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/21 10:32

S231	18	H04L63/0236.CPC. and (firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9)) same polic$9 and (malicious or malware or attack$9 or intrusion) same (packet$9 or frame or traffic$)	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/21 10:31
S230	26	H04L63/0218.CPC. and (firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9)) same polic$9 and (malicious or malware or attack$9 or intrusion) same (packet$9 or frame or traffic$)	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/21 10:31
S229	18	H04L63/0209.CPC. and (firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9)) same polic$9 and (malicious or malware or attack$9 or intrusion) same (packet$9 or frame or traffic$)	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/21 10:31
S228	39	H04L63/20.CPC. and (firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9)) same polic$9 and (malicious or malware or attack$9 or intrusion) same (packet$9 or frame or traffic$)	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/21 10:31
S227	109	(firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9)) same polic$9 and (malicious or malware or attack$9 or intrusion) same (packet$9 or frame or traffic$)	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/21 10:30
S226	15	(firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9)) same polic$9 same (malicious or malware or attack$9 or intrusion) same (packet$9 or frame or traffic$)	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/21 10:17
S225	38	(firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9)) same polic$9 same (malicious or malware or attack$9 or intrusion)	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/21 10:16

S224	454	(firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9)) same polic$9	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/21 10:16
S223	3300	(firewall or gateway or router) with ((updat$9 or new or modif$9) adj3 (rule or filter$9 or polic$9))	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/21 10:16
S222	1	"20140090046".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 22:35
S221	1	"20050076227".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 20:34
S220	1	"20120069749".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 20:32
S219	0	(updat$9 with policy with rule with (signat9 or criter$5) same (drop$9)) same packet	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 18:33
S218	2	(updat$9 with policy with rule with (signat9 or criter$5) same (drop$9))	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 18:33

S217	1	(updat$9 with policy with rule with (signat9 or criter$5) with (encapsulat$9 or replac$9 or insert$9))	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 18:32
S216	0	(updat$9 with policy with rule with signat9 with (encapsulat$9 or replac$9 or insert$9)) same (router or gateway)	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 18:32
S215	0	(updat$9 with policy with rule with signat9 with (encapsulat$9 or replac$9 or insert$9))same gateway	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 18:32
S214	35632	H04L67/02.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 13:52
S213	3229	H04L63/0263.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 13:52
S212	3395	H04L63/0236.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 13:52
S211	1064	H04L63/0218.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 13:52

S210	1813	H04L63/0209.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 13:52
S209	15017	H04L63/20.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 13:51
S208	162	(moore adj3 sean).in.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 13:50
S207	569	(rogers adj3 steven).in.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 13:50
S206	23	(centripetal networks).as.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/20 13:50
S205	3	(10091246 | 9560077 | 9137205).pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2019/05/16 14:18
S204	1	"9894051".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2018/05/10 16:43

S203	67	H04L67/02.CPC. and (rule) with (set or group or subset or subgroup) with address$5 same network$9 same (traffic or packet$9) and (filter$9 or firewall or router or rout$9 or intrusion or ids)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/27 13:36
S202	193	H04L63/0263.CPC. and (rule) with (set or group or subset or subgroup) with address$5 same network$9 same (traffic or packet$9) and (filter$9 or firewall or router or rout$9 or intrusion or ids)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/27 13:36
S201	82	H04L63/0236.CPC. and (rule) with (set or group or subset or subgroup) with address$5 same network$9 same (traffic or packet$9) and (filter$9 or firewall or router or rout$9 or intrusion or ids)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/27 13:36
S200	33	H04L63/0218.CPC. and (rule) with (set or group or subset or subgroup) with address$5 same network$9 same (traffic or packet$9) and (filter$9 or firewall or router or rout$9 or intrusion or ids)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/27 13:36
S199	28	H04L63/0209.CPC. and (rule) with (set or group or subset or subgroup) with address$5 same network$9 same (traffic or packet$9) and (filter$9 or firewall or router or rout$9 or intrusion or ids)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/27 13:36
S198	148	H04L63/20.CPC. and (rule) with (set or group or subset or subgroup) with address$5 same network$9 same (traffic or packet$9) and (filter$9 or firewall or router or rout$9 or intrusion or ids)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/27 13:35
S197	1414	(rule) with (set or group or subset or subgroup) with address$5 same network$9 same (traffic or packet$9) and (filter$9 or firewall or router or rout$9 or intrusion or ids)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/27 13:35

S196	42	H04L63/20.CPC. AND (rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9) and network$9 same (border$5 or boundary or boundaries) and (head or header or heading) and (vlan or virtual$5 local area network or virtual$5 lan)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/27 13:35
S195	1	"8009566" .pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/27 13:34
S194	1	"6279113".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/27 13:33
S193	1	"20140150051".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/27 13:24
S192	1425	(rule) with (set or group or subset) with address$5 same network$9 same (traffic or packet$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/27 12:21
S191	152	("20010039579" | "20010039624" | "20020016858" | "20020038339" | "20020049899" | "20020164962" | "20020165949" | "20020186683" | "20020198981" | "20030035370" | "20030097590" | "20030105976" | "20030120622" | "20030123456" | "20030142681" | "20030145225" | "20030154297" | "20030154399" | "20030188192" | "20030212900" | "20040010712" | "20040073655" | "20040088542" | "20040093513" | "20040098511" | "20040151155" | "20040177139" | "20040193943" | "20040205360" | "20040250124" | "20050010765" | "20050024189" | "20050114704" | "20050117576" | "20050125697" | "20050138204" |	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/26 22:49

		"20050141537" | "20050183140" | "20050229246" | "20050251570" | "20050286522" | "20060048142" | "20060053491" | "20060070122" | "20060104202" | "20060114899" | "20060136987" | "20060137009" | "20060146879" | "20060195896" | "20060212572" | "20060248580" | "20060262798" | "20070083924" | "20070211644" | "20070240208" | "20080005795" | "20080043739" | "20080072307" | "20080077705" | "20080163333" | "20080229415" | "20080235755" | "20080279196" | "20080301765" | "20090138938" | "20090172800" | "20090222877" | "20090240698" | "20090328219" | "20100011433" | "20100011434" | "20100082811" | "20100095367" | "20100107240" | "20100132027" | "20100199346" | "20100211678" | "20100232445" | "20100242098" | "20100268799" | "20100296441" | "20100303240" | "20110055916" | "20110055923" | "20110088092" | "20110141900" | "20110185055" | "20110270956" | "20120023576" | "20120106354" | "20120113987" | "20120240135" | "20120264443" | "20120314617" | "20120331543" | "20130047020" | "20130059527" | "20130061294" | "20130117852" | "20130254766" | "20130305311" | "20140075510" | "20140115654" | "20140201123" | "20140215574" | "20140281030" | "20140283004" | "20140283030" | "20140366132" | "20150237012" | "20150304354" | "20150334125" | "6098172" | "6147976" | "6226372" | "6317837" | "6484261" | "6611875" | "6662235" | "7089581" | "7107613" | "7215637" | "7227842" | "7237267" | "7263099" | "7299353" | "7331061" | "7478429" | "7539186" | "7610621" | "7684400" | "7710885" | "7721084" | "7818794" | "7954143" | "8004994" | "8037517" | "8042167" | "8117655" | "8176561" | "8306994" | "8495725" | "8726379" | "8806638" | "8856926" | "8935785" | "9094445" | "9124552" | "9137205" | "9154446" | "9160713").PN.				
S190	458	(rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9) and network$9 same (border$5 or boundary or boundaries) and (head or header or heading) and (vlan or virtual$5 local area network or virtual$5 lan)	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/26 20:12
S189	28348	H04L67/02.CPC.	US-PGPUB; USP	ADJ	ON	2017/10/26 20:12

			AT; EPO			
S188	2517	H04L63/0263.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/26 20:12
S187	2500	H04L63/0236.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/26 20:12
S186	893	H04L63/0218.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/26 20:11
S185	1445	H04L63/0209.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/26 20:11
S184	11470	H04L63/20.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/26 20:11
S183	16	(centripetal networks).as.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/26 20:11
S182	128	(moore adj3 sean).in.	US-PGPUB; USP	ADJ	ON	2017/10/26 20:11

			AT; EPO			
S181	541	(rogers adj3 steven).in.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/26 20:11
S180	2	(9560077 | 9137205).PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2017/10/26 20:03
S171	3	(6147976 | 9154446 | 7610621).pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/09/22 15:55
S170	16	H04L63/0218.CPC. AND rule and (drop$5 or discard$5) with (packet or flow or flood or frame) same (switch or router or hub) and (lan or local area network) AND (zone or edge or boundary)	US-PGPUB; USPAT; EPO	ADJ	ON	2016/09/22 15:48
S169	189	H04L63/0236.CPC. AND rule and (drop$5 or discard$5) with (packet or flow or flood or frame) same (switch or router or hub) and (lan or local area network) AND (zone or edge or boundary)	US-PGPUB; USPAT; EPO	ADJ	ON	2016/09/22 15:48
S168	27	H04L63/0209.CPC. AND rule and (drop$5 or discard$5) with (packet or flow or flood or frame) same (switch or router or hub) and (lan or local area network) AND (zone or edge or boundary)	US-PGPUB; USPAT; EPO	ADJ	ON	2016/09/22 15:48
S167	210	H04L63/20.CPC. AND rule and (drop$5 or discard$5) with (packet or flow or flood or frame) same (switch or router or hub) and (lan or local area network) AND (zone or edge or boundary)	US-PGPUB; USP	ADJ	ON	2016/09/22 15:48

			AT; EPO			
S166	780	H04L63/0218.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/09/22 15:47
S165	2077	H04L63/0236.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/09/22 15:47
S164	22610	H04L67/02.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/09/22 15:47
S163	1249	H04L63/0209.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/09/22 15:47
S162	9210	H04L63/20.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/09/22 15:47
S161	4596	rule and (drop$5 or discard$5) with (packet or flow or flood or frame) same (switch or router or hub) and (lan or local area network) AND (zone or edge or boundary)	US-PGPUB; USPAT; EPO	OR	ON	2016/09/22 15:46
S160	146	("20030142681" | "20030212900" | "20050117576" | "20070083924" | "20080005795" | "20100082811" | "20110055916" | "20120314617" | "20130059527" | "8806638" | "20110185055" | "20120331543" | "20010039624" |	US-PGPUB; USP	OR	ON	2016/09/22 15:29

		"20070240208" | "6317837" | "20020016858" | "20060262798" | "20050251570" | "20150304354" | "7237267" | "20050010765" | "20140115654" | "7263099" | "20100095367" | "8176561" | "20050138204" | "20060212572" | "20100211678" | "20100296441" | "7539186" | "7684400" | "20060146879" | "8306994" | "20080043739" | "20020198981" | "20050286522" | "20080077705" | "20100303240" | "20140281030" | "7954143" | "20040177139" | "20040205360" | "20140283004" | "20150237012" | "7107613" | "7237267" | "7331061" | "8495725" | "20060053491" | "20120023576" | "20130305311" | "20060248580" | "20090328219" | "20110088092" | "20120113987" | "8935785" | "20030154297" | "20020049899" | "20030035370" | "9137205" | "20040193943" | "20040205360" | "20050010765" | "20050114704" | "20140215574" | "20140283004" | "20140283030" | "7299353" | "20050114704" | "20050183140" | "20060104202" | "20060212572" | "20090138938" | "20140201123" | "6098172" | "7089581" | "20040093513" | "7215637" | "20030145225" | "20060048142" | "20060195896" | "20120264443" | "7818794" | "20140366132" | "20020038339" | "20050183140" | "20050229246" | "20060212572" | "20070083924" | "20080229415" | "20080301765" | "20100199346" | "20150237012" | "7089581" | "7263099" | "9124552" | "9160713" | "20020038339" | "20040010712" | "20040088542" | "20050251570" | "20060070122" | "20100199346" | "20110055923" | "6484261" | "7299353" | "20090240698" | "20110185055" | "20120106354" | "20140075510" | "20050141537" | "20080072307" | "20090172800" | "20100132027" | "6226372" | "20060114899" | "20130061294" | "8726379" | "20060048142" | "20060070122" | "6098172" | "7107613" | "20050286522" | "20140281030" | "20150304354" | "7227842" | "7954143" | "20020186683" | "20030154399" | "20040098511" | "20100011434" | "7478429" | "8004994" | "20030097590" | "20030123456" | "20100242098" | "20020165949" | "20040073655" | "20090138938" | "20100268799" | "20140201123" | "6484261" | "7227842" | "7331061" | "8042167" | "8495725" | "9094445" | "20040193943" | "20050229246" | "20080229415" | "20140283030" | "8037517" | "9124552" | "20080163333" | "20090222877" | "20100107240" | "20130117852" | "8117655" | "20030188192" | "20040088542" | "20040151155" | "20080235755" | "20110270956" | "7710885" | "7721084" | "20110055916" | "20040177139" | "20060104202" | "20100011433" | "6662235" | "20020165949" | "20020198981" | "20050125697" | "20060048142" | "20100303240" | "9094445" | "9160713" | "20010039579" | "20040250124" | "20130047020" | "20120240135" | "6611875" | "8856926" | "20130254766" | "20060136987" | "20080279196" | "20030120622" | "20040010712" | "20040088542" | "20050125697" | "20110055923" | "20140115654" | "8037517" | "20030120622" |	AT; EPO			

		"20040073655" | "20070083924" | "20080077705" | "20080301765" | "20100011433" | "20100268799" | "20140215574" | "6662235" | "8042167" | "20030105976" | "20060137009" | "20070211644" | "20100232445" | "20150334125").PN.				
S159	100	(US-6137792-$ or US-6055236-$ or US-5706348-$ or US-5710760-$ or US-5805705-$ or US-5987520-$ or US-5991401-$ or US-6011910-$ or US-6026085-$ or US-6147987-$ or US-6233232-$ or US-4774658-$ or US-4799153-$ or US-4901348-$ or US-4965804-$ or US-5247513-$ or US-5251203-$ or US-5280529-$ or US-5442708-$ or US-5444782-$ or US-5485455-$ or US-5490252-$ or US-5491694-$ or US-5521910-$ or US-5615340-$ or US-5640456-$).did. or (US-5642421-$ or US-5657452-$ or US-5684800-$ or US-5729594-$ or US-5737318-$ or US-5751952-$ or US-5768525-$ or US-5781550-$ or US-5790546-$ or US-5796942-$ or US-5799285-$ or US-5828846-$ or US-5864683-$ or US-5896499-$ or US-5913037-$ or US-5935249-$ or US-5946308-$ or US-5950172-$ or US-5953337-$ or US-6009528-$ or US-6035405-$ or US-6070243-$ or US-6081524-$ or US-6084858-$ or US-6098173-$ or US-6101539-$ or US-6101170-$).did. or (US-6118775-$ or US-6141755-$ or US-6148402-$ or US-6147995-$ or US-6167052-$ or US-6172991-$ or US-6188671-$ or US-6195705-$ or US-6199113-$ or US-6202081-$ or US-6230002-$ or US-6230271-$ or US-6249519-$ or US-4332980-$ or US-4445214-$ or US-4509073-$ or US-4768204-$ or US-4771422-$ or US-4787082-$ or US-4802220-$ or US-4823389-$ or US-4866770-$ or US-4872160-$ or US-4896319-$ or US-4922486-$ or US-4985895-$ or US-5048087-$).did. or (US-5029207-$ or US-5220501-$ or US-5228083-$ or US-5235644-$ or US-5237610-$ or US-5247380-$ or US-5261044-$ or US-5261059-$ or US-5268962-$ or US-5282244-$ or US-5295244-$ or US-5303302-$ or US-5303303-$ or US-5311593-$ or US-5313465-$ or US-5319712-$ or US-5351287-$ or US-5353353-$ or US-5386471-$ or US-5394469-$).did.	USPAT	OR	ON	2016/01/06 13:46
S158	254	(encapsul$9) with (packet) with (header or heading) with (address) with (destination) with (different or new or alternate)	US-PGPUB; USPAT; EPO	OR	ON	2016/01/06 11:55
S157	64	("20030142681" | "20030212900" | "20050117576" | "20070083924" | "20080005795" | "20100082811" | "20110055916" | "20120314617" | "20130059527" | "8806638" | "20110185055" | "20120331543" | "20010039624" | "20070240208" | "6317837" | "20050138204" | "20060212572" | "20100211678" | "20100296441" | "7539186" | "7684400" |	US-PGPUB; USP	OR	ON	2016/01/06 10:02

		"20060146879" | "8306994" | "20060248580" | "20090328219" | "20110088092" | "20120113987" | "8935785" | "20030154297" | "20020049899" | "20030035370" | "9137205" | "20030145225" | "20060048142" | "20060195896" | "20120264443" | "7818794" | "20140366132" | "20050141537" | "20080072307" | "20090172800" | "20100132027" | "6226372" | "20060114899" | "20130061294" | "8726379" | "20100011434" | "7478429" | "8004994" | "20030097590" | "20030123456" | "20100242098" | "20030188192" | "20040088542" | "20040151155" | "20080235755" | "20110270956" | "7710885" | "7721084" | "20120240135" | "6611875" | "8856926" | "20130254766" | "20060136987").PN.	AT; EPO			
S156	1	"20080298373".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/01/05 14:25
S155	1	"20060262798".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/01/05 14:20
S154	98	(vlan or virtual$5 lan) same different$5 with (rout$9) same (destination) with (address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service)	US-PGPUB; USPAT; EPO	ADJ	ON	2016/01/05 14:20
S153	157	(vlan or virtual$5 lan) same different$5 with (rout$9) same (destination) with (address)	US-PGPUB; USPAT; EPO	ADJ	ON	2016/01/05 14:07
S152	456	(vlan or virtual$5 lan) same (rout$9) same (destination) with (address) same different	US-PGPUB; USPAT; EPO	ADJ	ON	2016/01/05 14:07

S151	2204	(vlan or virtual$5 lan) same (rout$9) same (destination) same (address)	US-PGPUB; USPAT; EPO	ADJ	ON	2016/01/05 14:07
S150	1	"20110055916".pn.	US-PGPUB; USPAT; EPO	OR	ON	2016/01/05 10:22
S148	1	"20080043739".pn.	US-PGPUB; USPAT; EPO	OR	ON	2016/01/05 10:20
S147	1	"9137205".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2016/01/04 16:47
S145	1	"9137205".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:59
S144	176	H04L63/20.CPC. and (rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9) and network$9 same (border$5 or boundary or boundaries) and (head or header or heading)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:52
S143	43	H04L63/0263.CPC. and (rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9) and	US-PGPUB; USP	ADJ	ON	2015/12/30 15:52

		network$9 same (border$5 or boundary or boundaries) and (head or header or heading)	AT; EPO			
S142	28	H04L63/0218.CPC. and (rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9) and network$9 same (border$5 or boundary or boundaries) and (head or header or heading)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:52
S141	12	H04L67/02.CPC. and (rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9) and network$9 same (border$5 or boundary or boundaries) and (head or header or heading) and (vlan or virtual$5 local area network or virtual$5 lan)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:52
S140	6	H04L63/0236.CPC. and (rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9) and network$9 same (border$5 or boundary or boundaries) and (head or header or heading) and (vlan or virtual$5 local area network or virtual$5 lan)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:52
S139	4	H04L63/0218.CPC. and (rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9) and network$9 same (border$5 or boundary or boundaries) and (head or header or heading) and (vlan or virtual$5 local area network or virtual$5 lan)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:51
S138	12	H04L63/02.CPC. AND (rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9) and network$9 same (border$5 or boundary or boundaries) and (head or header or heading) and (vlan or virtual$5 local area network or virtual$5 lan)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:51

S137	29	H04L63/20.CPC. AND (rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9) and network$9 same (border$5 or boundary or boundaries) and (head or header or heading) and (vlan or virtual$5 local area network or virtual$5 lan)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:51
S136	314	(rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9) and network$9 same (border$5 or boundary or boundaries) and (head or header or heading) and (vlan or virtual$5 local area network or virtual$5 lan) and (rout$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:51
S135	314	(rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9) and network$9 same (border$5 or boundary or boundaries) and (head or header or heading) and (vlan or virtual$5 local area network or virtual$5 lan)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:51
S134	1264	(rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9) and network$9 same (border$5 or boundary or boundaries) and (head or header or heading)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:49
S133	1418	(rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9) and network$9 same (border$5 or boundary or boundaries)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:48
S132	1418	(rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9) and network$9 same (border or boundary or boundaries)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:48

S131	3288	(rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip address or internet protocol address) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:48
S130	3294	(rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip or internet protocol) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5) and (spoof$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:47
S129	19319	(rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip or internet protocol) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service) and (drop$9 or discard$9 or dump$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:47
S128	31220	(rule or criteria or signature) same (packet or traffic) and (address$10) with (source or destination or network or ip or internet protocol) and (intrusion detect$9 or network protect$9 or ids or dos or denial of service)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:47
S127	9	(centripetal networks).as.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:45
S126	110	(moore adj3 sean).in.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:45
S125	488	(rogers adj3 steven).in.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:45

S124	18904	H04L67/02.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:44
S123	7270	H04L63/20.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:44
S122	1626	H04L63/0236.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:44
S121	1853	H04L63/0263.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:44
S120	720	H04L63/0218.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:44
S119	35	H04L63/02.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing or rout$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/12/30 15:44
S118	123	H04L63/20.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and	US-PGPUB; USP	ADJ	ON	2015/12/30 15:44

		(set or list) and (function or algorithm or filter$9 or processing or rout$9)	AT; EPO			
S117	8	("20020049899" | "20060136987" | "20060146879" | "20070240208" | "20100242098" | "20130061294" | "6317837" | "8306994").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/07/30 16:25
S116	6	("20030154297" | "20060114899" | "20110185055" | "20120331543" | "20130254766" | "8004994").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/07/30 16:25
S115	3	("7478429" | "7818794" | "8935785").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/07/22 10:50
S112	34	H04L63/20.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing or rout$9) and (edge or boundary or boundaries or border$5) with network	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 17:38
S111	51	H04L63/20.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing or rout$9) and (edge or boundary or boundaries or border$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 17:38
S110	96	H04L63/20.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing or rout$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 17:37

S109	8	H04L63/0218.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing or encapsul$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 17:36
S108	12	(US-20060212572-$ or US-20030145225-$ or US-20060048142-$ or US-20010039624-$ or US-20050138204-$ or US-20100296441-$ or US-20080072307-$ or US-20050141537-$ or US-20030142681-$ or US-20100082811-$ or US-20030035370-$ or US-20110088092-$).did.	US-PGPUB	ADJ	ON	2015/03/26 17:35
S107	6	("20030097590" | "20090328219" | "20120240135" | "20120314617" | "6611875" | "8806638").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 14:52
S90	96	H04L63/20.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing or rout$9 or encapsul$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 12:26
S88	8	H04L63/0218.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing or rout$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 12:22
S87	67	H04L63/0263.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing or rout$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 12:22
S86	67	H04L63/0263.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of	US-PGPUB; USP	ADJ	ON	2015/03/26 12:11

		service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing)	AT; EPO			
S85	96	H04L63/20.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 12:11
S84	8	H04L63/0218.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 12:11
S83	1680	H04L63/0263.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 12:04
S82	5918	H04L63/20.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 12:04
S81	655	H04L63/0218.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/26 12:04
S80	6	("20030097590" | "20090328219" | "20120240135" | "20120314617" | "6611875" | "8806638").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/14 21:26
S79	34	(SIP or session initiat$9 protocol) with (URI or uniform resourse) with (header or heading) same (network address$9)	US-PGPUB; USP	ADJ	ON	2015/03/14 21:20

			AT; EPO			
S78	1202	(SIP or session initiat$9 protocol) with (URI or uniform resourse) with (header or heading)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/14 21:20
S77	1806	(SIP or session initiat$9 protocol) same (URI or uniform resourse) same (header or heading)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/03/14 21:19
S76	114	(network with transparent$5 with layer) same address$9 same (link$9) and (secure or security or attack$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 14:01
S75	171	(network with transparent$5 with layer) same address$9 same (link$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 14:00
S74	539	(network with transparent$5 with layer) same address$9	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 14:00
S73	2	("20080005795" | "20090172800").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 13:49
S72	3	("7539186" | "7710885" | "8856926").PN.	US-PGPUB; USP	ADJ	ON	2015/02/24 13:48

			AT; EPO			
S71	66	H04L63/0263.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 11:54
S70	88	H04L63/20.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 11:54
S69	8	H04L63/0218.CPC. AND (gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing)	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 11:54
S68	1654	H04L63/0263.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 11:54
S67	5709	H04L63/20.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 11:54
S66	647	H04L63/0218.CPC.	US-PGPUB; USPAT; EPO	ADJ	ON	2015/02/24 11:53
S65	1	"20140115654".pn.	US-PGPUB; USP	ADJ	ON	2015/02/24 11:53

			AT; EPO			
S64	26	713/1,100,150,151,152,153,154,155,166,167,168.CCLS. AND S61	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 02:26
S63	54	709/201,203,217,218,219,220,223,224,225,226,227,228,229,230,231,238,239,240,242,244,245.CCLS. AND S61	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 02:26
S62	31	726/3,6,11,12,13,14,15,16,17,22,23,24,25.CCLS. AND S61	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 02:26
S61	198	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing) same (ipsec or ip security or internet protocol security)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 02:26
S60	24976	713/1,100,150,151,152,153,154,155,166,167,168.CCLS.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 02:26
S59	125386	709/201,203,217,218,219,220,223,224,225,226,227,228,229,230,231,238,239,240,242,244,245.CCLS.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 02:26

S58	26093	726/3,6,11,12,13,14,15,16,17,22,23,24,25.CCLS.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 02:24
S57	1	"20030035370".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 01:42
S56	1	"20050135375".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 01:39
S55	1	"20110088092".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 00:40
S54	69	(spoof$5) with (address$5) with (network or source) with (policy or policies or rule)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 00:28
S53	209	(spoof$5) with (address$5) with (network or source) same (policy or policies or rule)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 00:28
S52	1	"20100082811".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/20 00:08

S51	1	"20080279200".pn.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 23:51
S50	5	(blacklist$5 or black list$9) with (addresses) with (paid or pay)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 23:46
S49	5	(blacklist$5 or black list$9) with (addresses) with (provider) with (subscription or subscribing or subscriber)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 23:42
S48	55	(blacklist$5 or black list$9) with (addresses) with (provider) with (service)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 23:41
S47	15	(blacklist$5 or black list$9) with (addresses) with (subscription or subscriber or subscribing) with (service)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 23:38
S46	222	(blacklist$5 or black list$9) with (addresses) same (subscription or subscriber or subscribing or customer)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 23:38
S45	2	(blacklist$5 or black list$9) with (addresses) with (discard$9 or block$6 or drop$5) with (packet) same (subscription or subscriber or subscribing or customer)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 23:38

S44	3	(differentiat$10 service code point select$5 or dscp select$5 or Diff-Serv Code Point) same (header or heading) same (traffic or packet) same (policy or policies or rule)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 22:48
S43	26	(differentiat$10 service code point select$5 or dscp select$5 or Diff-Serv Code Point) same (header or heading) same (traffic or packet)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 22:47
S42	10	(differentiat$10 service code point select$5 or dscp select$5) same (header or heading) same (traffic or packet)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 22:47
S41	34	(forward$9) with (packet) same (queue or group or buffer$5) same (priority) same (faster or higher) same (policy or policies or whitelist$5 or white list$8)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 21:56
S40	11	(discard$10 or block$5 or drop$5) and (forward$9 or allow$8) with (packet) with (address$5) same (policy or policies or whitelist$5 or white list$8) same (voip or voice over ip or voice over internet protocol) same (call or session or traffic or connection)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 20:32
S39	12	(discard$10 or block$5 or drop$5) and (forward$9 or allow$8) with (packet) with (address$5) same (policy or policies or whitelist$5 or white list$8) same (voip or voice over ip or voice over internet protocol)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 20:32
S38	223	(discard$10 or block$5 or drop$5) and (forward$9 or allow$8) with (packet) with (address$5) same (policy or policies or whitelist$5 or white list$8) and (voip or voice over ip or voice over internet protocol)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 20:31

S37	21	(discard$10 or block$5 or drop$5) and (forward$9 or allow$8) with (packet) with (address$5) with (whitelist$9 or white list$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 20:07
S36	5	(discard$10 or block$5 or drop$5) and (forward$9 or allow$8) with (packet) with (address$5) with (whitelist$9 or white list$5) with (only)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 20:07
S35	5	(addresses) with (ip or internet protocol or source) with (discard$9 or block$6 or drop$5) with (packet) and (forward$9 or allow$8) with (packet) with (address$5) with (whitelist$9 or white list$5) with (only)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 20:05
S34	15	(addresses) with (ip or internet protocol or source) with (discard$9 or block$6 or drop$5) with (packet) and (forward$9 or allow$8) with (outside or otherwise or address$5) with (packet) with (address$5) with (whitelist$9 or white list$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 20:04
S33	12	(blacklist$5 or black list$9) with (addresses) with (ip or internet protocol or source) with (discard$9 or block$6 or drop$5) with (packet) and (forward$9 or allow$8) with (outside or otherwise or address$5) with (packet) with (address$5) with (blacklist$5 or black list$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 18:28
S32	19	(blacklist$5 or black list$9) with (addresses) with (ip or internet protocol or source) with (discard$9 or block$6 or drop$5) with (packet) and (forward$9 or allow$8) with (outside or otherwise or address$5) with (packet) with (address$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 18:28
S31	1	(blacklist$5 or black list$5) with (address$9) with increas$9 with (policy or policies)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 18:26

S30	546	(set or list$5) with (addresses) with (ip or internet protocol or source) with (discard$9 or block$6 or drop$5) with (packet) and (forward$9 or allow$8) with (outside or otherwise or address$5) with (packet) with (address$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 18:24
S29	705	(set or list$5) with (addresses) with (ip or internet protocol or source) with (discard$9 or block$6 or drop$5) same (packet) and (forward$9 or allow$8) with (outside or otherwise or address$5) same (packet) with (address$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 18:24
S28	1857	(set or list$5) with (addresses) with (ip or internet protocol or source) same (discard$9 or block$6 or drop$5) same (packet) and (forward$9 or allow$8) with (outside or otherwise or address$5) same (packet) same (address$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 18:24
S27	8993	(set or list$5) with (addresses) with (ip or internet protocol or source) same (discard$9 or block$6 or drop$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 18:23
S26	74	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (function or algorithm or filter$9 or processing) same (ipsec or ip security or internet protocol security) and (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) same (policy or policies) and (address$10) with (source or destination or network or ip or internet protocol)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 15:35
S25	9	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (function or algorithm or filter$9 or processing) same (ipsec or ip security or internet protocol security) and (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) same (policy or policies) and (pipelin$5 or parallel$5)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 15:25
S24	28	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (function or algorithm or filter$9 or processing) same (ipsec or ip security or internet protocol	US-PGPUB; USP	ADJ	ON	2014/10/19 15:25

		security) and (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) same (policy or policies)	AT; EPO			
S23	198	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing) same (ipsec or ip security or internet protocol security)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 15:24
S22	253	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing) and (ipsec or ip security or internet protocol security)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 15:23
S21	252	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing) and (ipsec or ip security)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 15:23
S20	534	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list) and (function or algorithm or filter$9 or processing)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:19
S19	534	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9) and (set or list)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:18
S18	551	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service) and (server or manager or managing or supervis$9)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:18

S17	570	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) same (security or secure or protect$9 or ids or intrusion or dos or denial of service)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:18
S16	1430	(gateway) same (policy or policies) same (packet or traffic) and (rule) same (address$10) with (source or destination or network or ip or internet protocol) and (security or secure or protect$9 or ids or intrusion or dos or denial of service)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:17
S15	3295	(gateway) same (policy or policies) same (packet or traffic) and (rule) and (address$10) with (source or destination or network or ip or internet protocol) and (security or secure or protect$9 or ids or intrusion or dos or denial of service)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:16
S14	3686	(gateway) same (policy or policies) same (packet or traffic) and (rule) and (address$10) with (source or destination or network or ip or internet protocol)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:15
S13	4415	(gateway) same (policy or policies) same (packet or traffic) and (rule)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:14
S12	7	("20120113987" | "20060195896" | "7684400" | "20060248580" | "20110055916" | "0000000" | "20110270956" | "20130059527" | "20100011434" | "20120264443" | "6226372" | "20040151155" | "20030212900" | "20050117576" | "20060048142" | "20030188192" | "7721084" | "20030123456" | "20070083924" | "20100211678").PN. and (gateway) and (policy or policies)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:12
S11	17	S7 and (gateway) and (policy or policies)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:05

S10	17	S6 and (gateway) and (policy or policies)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:05
S9	7	S8 and (gateway) and (policy or policies)	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:03
S8	20	("20050071655" | "20040098618" | "20090038008" | "7975059" | "6715084" | "20060143709" | "20010020255" | "20020066034" | "20040148520" | "20060143688" | "20090037682" | "20120167120" | "20020078382" | "20040128543" | "20020162026" | "20040044912" | "8214900" | "20020083175" | "20030145225" | "20030204632").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/19 00:01
S7	54	("20060173992" | "20030084329" | "20030035370" | "20010042200" | "20020133721" | "20030023733" | "20060095965" | "20060230444" | "20020073155" | "20030233328" | "20060212524" | "20070180510" | "7536715" | "20060212572" | "20020198956" | "20040199793" | "20030126468" | "20050050338" | "20040073800" | "20060050719" | "20050262556" | "20040049574" | "20030101260" | "20020198956" | "20030035370" | "20040190522" | "20070157316" | "20050182950" | "20020073337" | "20030145225" | "20040117624" | "20040128538" | "20040148520" | "20070056030" | "20040004941" | "20030061514" | "20030014665" | "20060193470" | "20080176536" | "7409712" | "20020133721" | "20020166063" | "20030204632" | "20060137012" | "7574740" | "20050086502" | "7331060" | "20030023733" | "20050278415" | "20020178378" | "20030101260" | "20070180511" | "20020162026" | "20050037733" | "20050039104" | "7702739" | "20010042200" | "20020073337" | "20030145225" | "20040117624" | "20050180416" | "20020083175" | "20060048142").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/18 23:56
S6	53	("20060173992" | "20030084329" | "20030035370" | "20040128538" | "20010042200" | "20060230444" | "20020073155" | "20030233328" | "20060212524" | "20070180510" | "7536715" | "20060212572" | "20020178378" | "20040199793" | "20030126468" | "20050050338" | "20060095965" | "20060050719" | "20050262556" | "20040049574" | "20030101260" | "20040073800" |	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/18 23:55

		"20020198956" | "20040190522" | "20070157316" | "20050182950" | "20040117624" | "20040148520" | "20070056030" | "20040004941" | "20030061514" | "20030014665" | "20060193470" | "20080176536" | "7409712" | "20020133721" | "20020166063" | "20030204632" | "20060137012" | "7574740" | "20050086502" | "7331060" | "20030023733" | "20070180511" | "20020162026" | "20050037733" | "20050039104" | "7702739" | "20020073337" | "20030145225" | "20050180416" | "20020083175" | "20060048142").PN.				
S5	3	(centripetal networks).as.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/18 14:50
S4	95	(moore adj3 sean).in.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/18 14:49
S3	443	(rogers adj3 steven).in.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/18 14:49
S2	5511	726/1.CCLS.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/18 14:49
S1	19	("20120113987" | "20060195896" | "7684400" | "20060248580" | "20110055916" | "0000000" | "20110270956" | "20130059527" | "20100011434" | "20120264443" | "6226372" | "20040151155" | "20030212900" | "20050117576" | "20060048142" | "20030188192" | "7721084" | "20030123456" | "20070083924" | "20100211678").PN.	US-PGPUB; USPAT; EPO	ADJ	ON	2014/10/18 14:49

4/12/2020 3:04:58 PM
C:\Users\kchang3\Documents\EAST\Workspaces\16728766_CON4.wsp

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

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. 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	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\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
/KC/	1	6098172		2000-08-01	Coss et al.	
	2	6147976	A	2000-11-14	Shand et al.	
	3	6226372	B1	2001-05-01	Beebe et al.	
	4	6279113	B1	2001-08-21	Vaidya	
	5	6317837	B1	2001-11-13	Kenworthy	
	6	6484261	B1	2002-11-19	Wiegel	
	7	6611875		2003-08-26	Chopra et al.	
	8	6662235	B1	2003-12-09	Callis et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

/KC/	9	6826694		2004-11-30	Dutta et al.	
	10	6907042	B1	2005-06-14	Oguchi	
	11	6971028	B1	2005-11-29	Lyle et al.	
	12	7089581	B1	2006-08-08	Nagai et al.	
	13	7095716		2006-08-22	Ke et al.	
	14	7107613	B1	2006-09-12	Chen et al.	
	15	7143438	B1	2006-11-28	Coss et al.	
	16	7152240	B1	2006-12-19	Green et al.	
	17	7185368		2007-02-27	Copeland, III	
	18	7215637	B1	2007-05-08	Ferguson et al.	
	19	7225269	B2	2007-05-29	Watanabe	

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

/KC/	20	7227842	B1	2007-06-05	Ji et al.	
	21	7237267	B2	2007-06-26	Rayes et al.	
	22	7263099	B1	2007-08-28	Woo et al.	
	23	7296288	B1	2007-11-13	Hill et al.	
	24	7299353	B2	2007-11-20	Le Pennec et al.	
	25	7331061	B1	2008-02-12	Ramsey et al.	
	26	7478429	B2	2009-01-13	Lyon	
	27	7499412		2009-03-03	Matityahu et al.	
	28	7539186	B2	2009-05-26	Aerrabotu et al.	
	29	7610621	B2	2009-10-27	Turley et al.	
	30	7684400	B2	2010-03-23	Govindarajan et al.	

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

/KC/	31	7710885	B2	2010-05-04	Ilnicki et al.	
	32	7721084	B2	2010-05-18	Salminen et al.	
	33	7792775	B2	2010-09-07	Matsuda	
	34	7814158	B2	2010-10-12	Malik	
	35	7814546	B1	2010-10-12	Strayer et al.	
	36	7818794	B2	2010-10-19	Wittman	
	37	7849502		2010-12-07	Bloch et al.	
	38	7913303	B1	2011-03-22	Rouland et al.	
	39	7954143	B2	2011-05-31	Aaron	
	40	8004994		2011-08-23	Darisi et al.	
	41	8009566	B2	2011-08-30	Zuk et al.	

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

/KC/	42	8037517	B2	2011-10-11	Fulp et al.	
	43	8042167	B2	2011-10-18	Fulp et al.	
	44	8117655	B2	2012-02-14	Spielman	
	45	8156206	B2	2012-04-10	Kiley et al.	
	46	8176561	B1	2012-05-08	Hurst et al.	
	47	8219675		2012-07-10	Ivershen	
	48	8271645		2012-09-18	Rajan et al.	
	49	8306994	B2	2012-11-06	Kenworthy	
	50	8307029	B2	2012-11-06	Davis et al.	
	51	8331234	B1	2012-12-11	Newton et al.	
	52	8422391		2013-04-16	Zhu	

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

/KC/	53	8495725	B2	2013-07-23	Ahn	
	54	8510821	B1	2013-08-13	Brandwine et al.	
	55	8726379	B1	2014-05-13	Stiansen et al.	
	56	8806638	B1	2014-08-12	Mani	
	57	8832832	B1	2014-09-09	Visbal	
	58	8856926	B2	2014-10-07	Narayanaswamy et al.	
	59	8935785	B2	2015-01-13	Pandrangi	
	60	9094445	B2	2015-07-28	Moore et al.	
	61	9124552	B2	2015-09-01	Moore	
	62	9137205	B2	2015-09-15	Rogers et al.	
	63	9154446	B2	2015-10-06	Gemelli et al.	

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

/KC/	64	9160713	B2	2015-10-13	Moore	
	65	9172627		2015-10-27	Kjendal et al.	
	66	9419942	B1	2016-08-16	Buruganahalli et al.	
	67	9531672	B1	2016-12-27	Li et al.	
	68	9634911		2017-04-25	Meloche	
	69	9686193	B2	2017-06-20	Moore	
	70	8789135	B1	2014-07-22	Pani	
	71	6678827	B1	2004-01-13	Rothermel 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
/KC/	1	20010039579	A1	2001-11-08	TRCKA et al.	

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

/KC/	2	20010039624		2001-11-08	Kellum	
	3	20020016858	A1	2002-02-07	Sawada et al.	
	4	20020038339	A1	2002-03-28	Xu	
	5	20020049899	A1	2002-04-25	Kenworthy	
	6	20020083345	A1	2002-06-27	Halliday et al.	
	7	20020112188	A1	2002-08-15	Syvanne	
	8	20020152209	A1	2002-10-17	Merugu et al.	
	9	20020164962	A1	2002-11-07	Mankins et al.	
	10	20020165949	A1	2002-11-07	Na et al.	
	11	20020186683	A1	2002-12-12	Buck et al.	
	12	20020198981	A1	2002-12-26	Corl et al.	

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

/KC/	13	20030005122	A1	2003-01-02	Freimuth et al.	
	14	20030014665	A1	2003-01-16	Anderson et al.	
	15	20030018591	A1	2003-01-23	Komisky	
	16	20030035370	A1	2003-02-20	Brustoloni, Jose	
	17	20030051026	A1	2003-03-13	Carter et al.	
	18	20030088787	A1	2003-05-08	Egevang	
	19	20030097590	A1	2003-05-22	Syvanne	
	20	20030105976	A1	2003-06-05	Copeland	
	21	20030120622	A1	2003-06-26	Nurmela et al.	
	22	20030123456	A1	2003-07-03	Denz et al.	
	23	20030142681	A1	2003-07-31	Chen et al.	

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

/KC/	24	20030145225	A1	2003-07-31	Bruton et al.	
	25	20030154297	A1	2003-08-14	Suzuki et al.	
	26	20030154399	A1	2003-08-14	Zuk et al.	
	27	20030188192	A1	2003-10-02	Tang et al.	
	28	20030212900	A1	2003-11-13	Liu et al.	
	29	20030220940	A1	2003-11-27	Futoransky et al.	
	30	20040010712	A1	2004-01-15	Hui et al.	
	31	20040015719	A1	2004-01-22	Lee et al.	
	32	20040073655	A1	2004-04-15	Kan et al.	
	33	20040088542	A1	2004-05-06	Daude et al.	
	34	20040093513	A1	2004-05-13	Cantrell et al.	

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

/KC/	35	20040098511	A1	2004-05-20	Lin et al.	
	36	20040114518	A1	2004-06-17	MacFaden et al.	
	37	20040123220	A1	2004-06-24	Johnson et al.	
	38	20040131056	A1	2004-07-08	Dark	
	39	20040148520	A1	2004-07-29	Talpade et al.	
	40	20040151155	A1	2004-08-05	Jouppi	
	41	20040172529	A1	2004-09-02	Culbert	
	42	20040172557	A1	2004-09-02	Nakae et al.	
	43	20040177139	A1	2004-09-09	Schuba et al.	
	44	20040193943	A1	2004-09-30	Angelino et al.	
	45	20040199629	A1	2004-10-07	Bomer et al.	

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

/KC/	46	20040205360	A1	2004-10-14	Norton et al.	
	47	20040250124	A1	2004-12-09	Chesla et al.	
	48	20050010765	A1	2005-01-13	Swander et al.	
	49	20050024189	A1	2005-02-03	Weber	
	50	20050071650	A1	2005-03-31	Jo et al.	
	51	20050076227	A1	2005-04-07	Kang et al.	
	52	20050108557	A1	2005-05-19	Kayo et al.	
	53	20050114704	A1	2005-05-26	Swander	
	54	20050117576	A1	2005-06-02	McDysan et al.	
	55	20050125697	A1	2005-06-09	Tahara	
	56	20050138204	A1	2005-06-23	Iyer et al.	

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

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

Application Number	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\US

/KC/	57	20050138353	A1	2005-06-23	Spies et al.	
	58	20050141537	A1	2005-06-30	Kumar et al.	
	59	20050183140	A1	2005-08-18	Goddard	
	60	20050229246	A1	2005-10-13	Rajagopal et al.	
	61	20050249214	A1	2005-11-10	Peng	
	62	20050251570	A1	2005-11-10	Heasman et al.	
	63	20050283823	A1	2005-12-22	Okajo et al.	
	64	20050286522	A1	2005-12-29	Paddon et al.	
	65	20060031928	A1	2006-02-09	Conley et al.	
	66	20060048142	A1	2006-03-02	Roese et al.	
	67	20060053491	A1	2006-03-09	Khuti et al.	

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

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

Application Number	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\US

/KC/	68	20060070122	A1	2006-03-30	Bellovin	
	69	20060080733	A1	2006-04-13	Khosmood et al.	
	70	20060085849	A1	2006-04-20	Culbert	
	71	20060104202	A1	2006-05-18	Reiner	
	72	20060114899	A1	2006-06-01	Toumura et al.	
	73	20060133377	A1	2006-06-22	Jain	
	74	20060136987	A1	2006-06-22	Okuda	
	75	20060137009	A1	2006-06-22	Chesla	
	76	20060146879	A1	2006-07-06	Anthias et al.	
	77	20060159028	A1	2006-07-20	Curran-Gray et al.	
	78	20060195896	A1	2006-08-31	Fulp et al.	

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

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

Application Number	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\US

/KC/	79	20060212572	A1	2006-09-21	Afek et al.	
	80	20060248580	A1	2006-11-02	Fulp et al.	
	81	20060262798	A1	2006-11-23	Joshi et al.	
	82	20070056038	A1	2007-03-08	Lok	
	83	20070083924	A1	2007-04-12	Lu	
	84	20070118894	A1	2007-05-24	Bhatia	
	85	20070211644	A1	2007-09-13	Ottamalika et al.	
	86	20070240208	A1	2007-10-11	Yu et al.	
	87	20070291789	A1	2007-12-20	Kutt et al.	
	88	20080005795	A1	2008-01-03	Acharya et al.	
	89	20080028467	A1	2008-01-31	Kommareddy et al.	

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

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

Application Number	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\US

/KC/	90	20080043739	A1	2008-02-21	SUH et al.	
	91	20080072307	A1	2008-03-20	Maes	
	92	20080077705	A1	2008-03-27	Li et al.	
	93	20080080493	A1	2008-04-03	Weintraub et al.	
	94	20080086435	A1	2008-04-10	Chesla	
	95	20080101234	A1	2008-05-01	Nakil et al.	
	96	20080163333	A1	2008-07-03	Kasralikar	
	97	20080201772	A1	2008-08-21	Mondaeev et al.	
	98	20080229415	A1	2008-09-18	Kapoor et al.	
	99	20080235755	A1	2008-09-25	Blaisdell et al.	
	100	20080279196	A1	2008-11-13	Friskney et al.	

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

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

Application Number	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\US

/KC/	101	20080301765	A1	2008-12-04	Nicol et al.	
	102	20080313738	A1	2008-12-18	Enderby	
	103	20080320116	A1	2008-12-25	Briggs	
	104	20090028160	A1	2009-01-29	ESWARAN et al.	
	105	20090138938	A1	2009-05-28	Harrison et al.	
	106	20090150972	A1	2009-06-11	MOON et al.	
	107	20090172800	A1	2009-07-02	WOOL	
	108	20090222877	A1	2009-09-03	Diehl et al.	
	109	20090240698	A1	2009-09-24	Shukla et al.	
	110	20090262723	A1	2009-10-22	Pelletier et al.	
	111	20090262741	A1	2009-10-22	Jungck et al.	

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

/KC/	112	20090300759	A1	2009-12-03	Wang et al.	
	113	20090328219	A1	2009-12-31	Narayanaswamy	
	114	20100011433	A1	2010-01-14	HARRISON et al.	
	115	20100011434	A1	2010-01-14	Kay	
	116	20100082811	A1	2010-04-01	Van Der Merwe et al.	
	117	20100095367	A1	2010-04-15	Narayanaswamy	
	118	20100107240	A1	2010-04-29	Thaler et al.	
	119	20100115621	A1	2010-05-06	Staniford et al.	
	120	20100132027	A1	2010-05-27	Ou	
	121	20100195503	A1	2010-08-05	Raleigh	
	122	20100199346	A1	2010-08-05	Ling et al.	

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

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

Application Number	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\US

/KC/	123	20100202299	A1	2010-08-12	Strayer et al.	
	124	20100211678	A1	2010-08-19	McDysan et al.	
	125	20100232445	A1	2010-09-16	Bellovin	
	126	20100242098	A1	2010-09-23	Kenworthy	
	127	20100268799	A1	2010-10-21	Maestas	
	128	20100296441	A1	2010-11-25	Barkan	
	129	20100303240	A1	2010-12-02	Beachem et al.	
	130	20110055916	A1	2011-03-03	Ahn	
	131	20110055923	A1	2011-03-03	Thomas	
	132	20110088092	A1	2011-04-14	Nguyen et al.	
	133	20110141900	A1	2011-06-16	Jayawardena et al.	

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

/KC/	134	20110185055	A1	2011-07-28	NAPPIER et al.	
	135	20110214157	A1	2011-09-01	Korsunsky et al.	
	136	20110270956	A1	2011-11-03	McDysan et al.	
	137	20110277034	A1	2011-11-10	Hanson	
	138	20120023576	A1	2012-01-26	Sorensen et al.	
	139	20120084866	A1	2012-04-05	Stolfo	
	140	20120106354	A1	2012-05-03	Pleshek et al.	
	141	20120113987	A1	2012-05-10	Riddoch et al.	
	142	20120240135	A1	2012-09-20	Risbood et al.	
	143	20120240185	A1	2012-09-20	Kapoor et al.	
	144	20120264443	A1	2012-10-18	Ng et al.	

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

/KC/	145	20120314617	A1	2012-12-13	Erichsen et al.	
	146	20120331543	A1	2012-12-27	Bostrom et al.	
	147	20130047020	A1	2013-02-21	Hershko et al.	
	148	20130059527	A1	2013-03-07	HASESAKA et al.	
	149	20130061294	A1	2013-03-07	Kenworthy	
	150	20130104236	A1	2013-04-25	RAY et al.	
	151	20130117852	A1	2013-05-09	Stute	
	152	20130139236	A1	2013-05-30	Rubinstein et al.	
	153	20130254766	A1	2013-09-26	Zuo et al.	
	154	20130291100	A1	2013-10-31	Ganapathy et al.	
	155	20130305311	A1	2013-11-14	Puttaswamy Naga et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

/KC/	156	20140075510	A1	2014-03-13	Sonoda et al.	
	157	20140082204	A1	2014-03-20	Shankar et al.	
	158	20140082730	A1	2014-03-20	VASHIST et al.	
	159	20140115654	A1	2014-04-24	Rogers et al.	
	160	20140150051	A1	2014-05-29	Bharali et al.	
	161	20140201123	A1	2014-07-17	Ahn et al.	
	162	20140215561	A1	2014-07-31	Roberson et al.	
	163	20140215574	A1	2014-07-31	Erb et al.	
	164	20140259170	A1	2014-09-11	Amsler	
	165	20140281030	A1	2014-09-18	Cui et al.	
	166	20140283004	A1	2014-09-18	Moore	

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

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

Application Number	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\US

/KC/	167	20140283030	A1	2014-09-18	Moore et al.	
	168	20140317397	A1	2014-10-23	Martini	
	169	20140337613	A1	2014-11-13	Martini	
	170	20140366132	A1	2014-12-11	Stiansen et al.	
	171	20150033336	A1	2015-01-29	Wang et al.	
	172	20150106930	A1	2015-04-16	HONDA et al.	
	173	20150128274	A1	2015-05-07	Giokas	
	174	20150135325	A1	2015-05-14	Stevens et al.	
	175	20150207809	A1	2015-07-23	MACAULAY	
	176	20150237012	A1	2015-08-20	Moore	
	177	20150244734	A1	2015-08-27	Olson et al.	

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

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

Application Number	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\US

/KC/	178	20150256431	A1	2015-09-10	Buchanan et al.	
	179	20150304354	A1	2015-10-22	Rogers et al.	
	180	20150334125	A1	2015-11-19	BARTOS et al.	
	181	20150341389	A1	2015-11-26	KURAKAMI	
	182	20150350229	A1	2015-12-03	Mitchell	
	183	20150372977	A1	2015-12-24	Yin	
	184	20150373043	A1	2015-12-24	Wang et al.	
	185	20160020968	A1	2016-01-21	Aumann et al.	
	186	20160028751	A1	2016-01-28	Cruz Mota et al.	
	187	20160065611	A1	2016-03-03	Fakeri-Tabrizi et al.	
	188	20160112443	A1	2016-04-21	GROSSMAN et al.	

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

/KC/	189	20160119365	A1	2016-04-28	Barel	
	190	20160191558	A1	2016-06-30	DAVISON	
	191	20160205069	A1	2016-07-14	Blocher et al.	
	192	20160219065	A1	2016-07-28	Dasgupta et al.	
	193	20160285706	A1	2016-09-29	RAO	
	194	20160294870	A1	2016-10-06	Banerjee et al.	
	195	20160366099	A1	2016-12-15	Jordan	
	196	20170223046	A1	2017-08-03	Singh	
	197	20170272469	A1	2017-09-21	Kraemer et al.	
	198	20150347246	A1	2015-12-03	MATSUI et al.	
	199	20120110656	A1	2012-05-03	Santos et al.	

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\US

/KC/	200	20090144819	A1	2009-06-04	BABBAR et al.	
	201	20130007257	A1	2013-01-03	Ramaraj et al.	
	202	20160127417	A1	2016-05-05	Janssen	
	203	20040181690	A1	2004-09-16	Rothermel et al.	
	204	20140317737	A1	2014-10-23	SHIN et al.	
	205	20070147380	A1	2007-06-28	ORMAZABAL et al.	
	206	20140245423	A1	2014-08-28	Lee	
	207	20110154470	A1	2011-06-23	Grimes et al.	
	208	20150052601	A1	2015-02-19	White et al.	
	209	20140365372	A1	2014-12-11	Ross et al.	

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

FOREIGN PATENT DOCUMENTS Remove

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\US

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	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]
/KC/	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		
	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		

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

/KC/	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		
	17	2007109541	WO	A2	2007-09-27	Brubaker, Curtis		

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
/KC/	1	"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>	
/KC/	2	2006 Sept 11 - (WO) Written Opinion of the International Searching Authority - App PCT/US05/47008	

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

/KC/	3	2007 Aug 31 - (EP) Communication Pursuant to Rules 109 and 110 - App 05857614.1
	4	2008 Jul 03 - (WO) Written Opinion of the International Searching Authority - App PCT/US06/11291
	5	2009 Jun 24 - (US) Office Action - App 11/390,976
	6	2009 Sept 14 (US) Office Action - App 11/316,331
	7	2010 Apr 29 - (US) Interview Summary - App 11/390,976
	8	2010 Aug 20 - (AU) Office Action - App 2005328336
	9	2010 Jun 23 - (US) Final Rejection - App 11/316,331
	10	2010 Mar 26 - (US) Final Rejection - App 11/390,976
	11	2010 Sept 10 - (AU) Office Action - App 2006230171
	12	2010 Sept 30 - (US) Office Action - App 11/390,976
	13	2011 Apr 27 - (WO) International Search Report and Written Opinion - App PCT/US2010/054520

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

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

Application Number	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\US

/KC/	14	2011 Aug 25 - (US) Non Final Rejection - App 12/871,806	
	15	2011 Feb 14 - (EP) Search Report - App 06758213.0	
	16	2011 Jun 09 - (US) Notice of Allowance - App 11/390,976	
	17	2011 Mar 03 - (EP) Communication Pursuant to Rules 70(2) and 70a(2) - App 06758213.0	
	18	2011 Mar 04 - (US) Notice of Allowance - App 11/316,331	
	19	2011 Nov 11 - (AU) Second Office Action - App 2006230171	
	20	2011 Oct 18 - (EP) Communication Pursuant to Article 94(3) - App 06 758 213.0	
	21	2012 Aug 07 - (US) Non Final Rejection - App 12/871,806	
	22	2012 Feb 06 - (US) Final Rejection - App 12/871,806	
	23	2012 Jun 09 - (AU) Notice of Acceptance - App 2006230171	
	24	2012 Jun 26 - (EP) Extended Search Report - App 05857614.1	

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

/KC/	25	2012 Nov 20 - (EP) Communication under rule 71(3) - App 06 758 213.0	
	26	2012 Nov 26 - (US) Final Rejection - App 12/871,806	
	27	2013 Apr 04 - (US) Notice of Allowance - App 12/871,806	
	28	2013 Apr 18 - (EP) Decision to Grant a European Patent - App 06758212.0	
	29	2013 Jan 16 - (CA) Office Action - App 2,594,020	
	30	2013 Jan 17 - (CA) Office Action - App 2,600,236	
	31	2013 Nov 7 (WO) International Search Report - App. PCT/US2013/057502	
	32	2014 Jun 24 (WO) International Search Report - App. PCT/US2014/023286	
	33	2014 Jun 26 (WO) International Search Report - App. PCT/US2014/027723	
	34	2014 Mar 24 (WO) International Search Report - App. PCT/US2013/072566	
	35	2014 May 26 - (CA) Office Action - App 2010297968	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

/KC/	36	2015 Apr 28 (WO) International Preliminary Report on Patentability - App. PCT/US2013/057502, dated April 28, 2015.	
	37	2015 Dec 22 - (US) Final Office Action - App 14/714,207	
	38	2015 Jan 14 - (EP) Extended Search Report - App 10819667.6	
	39	2015 Jul 10 - (WO) Communication Relating to the Results of the Partial International Search for International App - PCT/US2015/024691	
	40	2015 Jul 14 - (WO) International Preliminary Report on Patentability - App PCT/US2013/072566	
	41	2015 May 14 - (US) Non Final Rejection - App 13/940,240	
	42	2015 May 25 - (AU) Notice of Acceptance - App 2010297968	
	43	2015 Nov 02 - (AU) Office Action - App 2013372879	
	44	2015 Nov 27 - (US) Final Rejection - App 13/940,240	
	45	2015 Sept 15 (WO) International Preliminary Report on Patentability - App. - PCT/US2014/027723.	
	46	2015 Sept 15 (WO) International Preliminary Report on Patentability - App. PCT/US2014/023286.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\US

/KC/	47	2015 Sept 16 (WO) International Search Report and Written Opinion - App. No. PCT/US2015/024691.
	48	2015 Sept 4 (US) Notice of Allowance - App. 14/702,755 (007742.00036)
	49	2016 Apr 15 - (US) Notice of Allowance - App 14/855,374
	50	2016 Apr 26 - (US) Office Action - App 14/745,207

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

EXAMINER SIGNATURE

Examiner Signature	/KENNETH W CHANG/	Date Considered	04/12/2020

*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.

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

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. 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	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\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]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\US

/KC/	1	D. Eppstein et al., "Internet Packet Filter Management and Rectangle Geometry", Proceedings of the Symposium on Discrete Algorithms, 827-835, 2001	
	2	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	
	3	E. Al-Shaer et al., "Modeling and Management of Firewall Policies", IEEE Transactions on Network and Service Management, 1(1): 2004	
	4	E. Fulp et al., "Network Firewall Policy Tries", Technical Report, Computer Science Department, Wake Forest University, 2004	
	5	E. Fulp, "Optimization of Network Firewall Policies Using Ordered Sets and Directed Acyclical Graphs", Technical Report, Computer Scient Department, Wake Forest University, January 2004	
	6	E. Fulp, "Preventing Denial of Service Attacks on Quality of Service", Proceedings of the 2001 DARPA Information Survivability Conference and Exposition II, 2001	
	7	E.L. Lawler, "Sequencing Jobs to Minimize Total Weighted Completion Time Subject to Precedence Constraints", Annals of Discrete Mathematics, 2: 75-90, 1978	
	8	E.W. Fulp, "Firewall Architectures for High Speed Networks", U.S. Department of Energy Grant Application, Funded September 2003	
	9	Fulp, "Trie-Based Policy Representations for Network Firewalls," Proceedings of the IEEE International Symposium on Computer Communications (2005)	
	10	Fulp, Errin: "CV: Errin Fulp," XP002618346, www.cs.wfu.edu/fulp/ewfPub.html, pgs. 1-5 (Copyright 2010)	
	11	G. Brightwell et al., "Counting Linear Extensions is #P-Complete", Proceedings of the Twenty-Third Annual ACM Symposium on Theory of Computing, 1991	

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

Application Number	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\US

/KC/	12	G.V. Rooij, "Real Stateful TCP Packet Filtering in IP Filter", Proceedings of the 10th USENIX Security Symposium, 2001	
	13	Greenwald, Michael; "Designing an Academic Firewall: Policy, Practice, and Experience with SURF"; IEEE, Proceedings of SNDSS, 1996.	
	14	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	
	15	J.K. Lenstra et al., "Complexity of Scheduling Under Precedence Constraints", Operations Research, 26(1): 22-35,1978	
	16	Kindervag, et al. "Build Security Into Your Network's DNA: The Zero Trust Network Architecture," Forrester Research Inc.; Novermber 5, 2010, pps: 1-26.	
	17	L. Qui et al., "Fast Firewall Implementations for Software and Hardware-Based Routers", Proceedings of ACM Sigmetrics, June 2001	
	18	Lee et al., "Development Framework for Firewall Processors," IEEE, pgs. 352-355 (2002)	
	19	M. Al-Suwaiyel et al., "Algorithms for Trie Compaction", ACM Transactions on Database Systems, 9(2): 243-263, June 1984	
	20	M. Christiansen et al., "Using IDDs for Packet Filtering," Technical Report, BRICS, October 2002	
	21	M. Degermark et al., "Small Forwarding Tables for Fast Routing Lookups", Proceedings of ACM SIGCOMM, 4-13, 1997	
	22	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.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

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

Application Number	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\US

/KC/	23	Moore, S, "SBIR Case Study: Centripetal Networks: How CNI Leveraged DHS S&T SBIR Funding to Launch a Successful Cyber Security Company," 2012 Principal Investigators' Meeting, Cyber Security Division, October 10, 2014.	
	24	O. Paul et al., "A full Bandwidth ATM Firewall", Proceedings of the 6th European Symposium on Research in Computer Security ESORICS'2000, 2000	
	25	P. Warkhede et al., "Fast Packet Classification for Two-Dimensional Conflict-Free Filters", Proceedings of IEEE INFOCOM, 1434-1443, 2001	
	26	Palo Alto Networks; "Designing A Zero Trust Network With Next-Generation Firewalls"; pps. 1-10; last viewed on October 21, 2012.	
	27	R. Funke et al., "Performance Evaluation of Firewalls in Gigabit-Networks", Proceedings of the Symposium on Performance Evaluation of Computer and Telecommunication Systems, 1999	
	28	R. Rivest, "On Self-Organizing Sequential Search Heuristics", Communications of the ACM, 19(2): 1976	
	29	R.L. Graham et al., "Optimization and Approximation in Deterministic Sequencing and Scheduling: A Survey", Annals of Discrete Mathematics, 5: 287-326, 1979	
	30	Reumann, John; "Adaptive Packet Filters"; IEEE, 2001, Department of Electrical Engineering and Computer Science, The University of Michigan, Ann Arbor, MI	
	31	S,M. Bellovin et al., "Network Firewalls", IEEE Communications Magazine, 50-57, 1994	
	32	S. Goddard et al., "An Unavailability Analysis of Firewall Sandwich Configurations", Proceedings of the 6th IEEE Symposium on High Assurance Systems Engineering, 2001	
	33	S. Suri et al., "Packet Filtering in High Speed Networks", Proceedings of the Symposium on Discrete Algorithms, 969-970, 1999	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

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

Application Number	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\US

/KC/	34	Singh, Rajeev et al. "Detecting and Reducing the Denial of Service attacks in WLANs", December 2011, World Congress on Information and Communication TEchnologies, pp. 968-973	
	35	Statement RE: Related Application, dated July 24, 2015	
	36	Tarsa et al., "Balancing Trie-Based Policy representations for Network Firewalls," Department of Computer Science, Wake Forest University, pgs. 1-6 (2006)	
	37	U. Ellermann et al., "Firewalls for ATM Networks", Proceedings of INFOSEC'COM, 1998	
	38	V. Srinivasan et al., "Fast and Scalable Layer Four Switching", Proceedings of ACM SIGCOMM, 191-202, 1998	
	39	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	
	40	W.E. Leland et al., "On the Self-Similar Nature of Ethernet Traffic", IEEE Transactions on Networking, 2(1); 15, 1994	
	41	W.E. Smith, "Various Optimizers for Single-Stage Productions", Naval Research Logistics Quarterly, 3: 59-66, 1956	
	42	X. Gan et al., "LSMAC vs. LSNAT: Scalable Cluster-based Web servers", Journal of Networks, Software Tools, and Applications, 3(3): 175-185, 2000	
	43	2018 Jul 5 (US) Non-Final Office Action - App. 15/413,750 (007742.00084)	
	44	2018 Jul 13 (US) Notice of Allowance - App. 15/414,117 (007742.00065)	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

/KC/	45	2018 Jul 27 (US) Non-Final Office Action - App. 15/382,806 (007742.00082)
	46	Sourcefire 3D System User Guide, Version 4.10, March 16, 2011, 2123 pages.
	47	2018 Jul 11 (US) Declaration of Kevin Jeffay, PhD in Support of Petition for Inter Partes Review of U.S. Patent No. 9,565,213 - IPR2018-01386
	48	Ylonen, et al, "The Secure Shell (SSH) Transport Layer Protocol," SSH Communication Security Corp, Newtork Working Group RFC 4253, January 2006, 32 pages.
	49	2018 Jul 20 (US) Declaration of Dr. Stuart Staniford in Support of Petition for Inter Partes Review of U.S. Patent No. 9,160,713 - IPR2018-01437
	50	2018 Jul 20 (US) Declaration of Dr. Stuart Staniford in Support of Petition for Inter Partes Review of U.S. Patent No. 9,124,552 - IPR2018-01436

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

EXAMINER SIGNATURE

Examiner Signature	/KENNETH W CHANG/	Date Considered	04/12/2020

*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.

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

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. 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	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\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]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\US

/KC/	1	2016 Dec 05 - (US) Notice of Allowance - App 14/714,207
	2	2016 Feb 24 - (AU) Office Action - App 2014228257
	3	2016 Feb 25 - (AU) Office Action - App 2014249055
	4	2016 Feb 26 - (US) Non Final Office Action - App 14/253,992
	5	2016 Jan 11 - (US) Non Final Rejection - App 14/698,560
	6	2016 Jan 28 - (WO) International Search Report and Written Opinion - App PCT/US2015/062691
	7	2016 Jul 11 - (EP) Office Action - App 14720824.3
	8	2016 Jul 20 - (AU) Office Action - App 2013335255
	9	2016 Jul 22 - (US) Office Action - App 14/921,718
	10	2016 Jun 09 - (WO) International Search Report - PCT/US2016/026339
	11	2016 Jun 14 - (US) Office Action - App 14/625,486

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

Application Number	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\US

/KC/	12	2016 Jun 16 - (CA) Office Action - App 2,888,935	
	13	2016 May 06 - (US) Office Action - App 14/714,207	
	14	2016 May 13 - (US) Office Action - App 13/940,240	
	15	2016 Nov 21 - (US) Office Action - App 14/745,207	
	16	2016 Oct 05 - (US) Notice of Allowance - App 14/698,560	
	17	2016 Oct 26 - (US) Office Action - App 13/940,240	
	18	2016 Sept 13 - (CA) Office Action - App 2,902,206	
	19	2016 Sept 14 - (CA) Office Action - App 2,897,737	
	20	2016 Sept 26 - (CA) Office Action - App 2,902,158	
	21	2017 Apr 12 - (US) Office Action - App 14/757,638	
	22	2017 Aug 15 (WO) International Preliminary Report on Patentability - App. PCT/US2015/062691 (007742.00064)	

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

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

Application Number	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\US

/KC/	23	2017 Aug 21 (AU) First Examination Report - App. 2015248067 (007742.00079)	
	24	2017 Feb 10 - (US) Notice of Allowance - App 14/625,486	
	25	2017 Feb 15 - (US) Notice of Allowance - App 14/921,718	
	26	2017 Jul 20 (US) Complaint for Patent Infringement - Case No. 2:17-cv-00383-HCN-LRL, Document 1, 38 pages.	
	27	2017 Jun 07 - (US) Office Action - App 14/745,207	
	28	2017 Jun 07 - (WO) International Search Report and Written Opinion - App PCT/US2016/067111	
	29	2017 Mar 06 - (WO) International Search Report and Written Opinion - App PCT/US2016/068008	
	30	2017 Nov 21 (US) Notice of Allowance - App. 14/690,302 (007742.00042)	
	31	2017 Nov 3 (US) Non-Final Office Action - App. 15/413,834 (007742.00085)	
	32	2017 Oct 17 (WO) International Preliminary Report on Patentability - App. PCT/US2016/026339 (007742.00075)	
	33	2017 Sep 5 (US) Defendant Ixia's Partial Answer to Complaint for Patent Infringement - Case No. 2:17-cv-00383-HCN-LRL, Document 29, 14 pages.	

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

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

Application Number	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\US

/KC/	34	2017 Sep 5 (US) Memorandum in Support of Defendant's Ixia and Keysight Technologies, Inc's Motion to Dismiss for Unpatentability Under 35 U.S.C. § 101 - Case No. 2:17-cv-00383-HCM-LRL, Document 21, 29 pages.	
	35	2017 Sep 5 (US) Request for Judicial Notice in Support of Defendants Ixia and Keysight Technologies, Inc's Motion to Dismiss for Unpatentability under 35 U.S.C. § 101 - Case No. 2:17-cv-00383-HCN-LRL, Document 22, 3 pages.	
	36	2017 Sept 29 (CA) Examination Report - App. 2,772,630	
	37	2018 Apr 17 (US) Non-Final Office Action - App. 15/610,995 (007742.00090)	
	38	2018 Mar 15 (EP) Second Communication pursuant to Article 94(3) EPC - App. 13765547.8 (007742.00044)	
	39	2018 Mar 16 (EP) Communication Pursuant to Rule 164(2)(b) and Article 94(3) EPC - App. 15722292.8	
	40	2018 Mar 21 (AU) First Examination Report - App. 2015382393 (007742.00096)	
	41	2018 Mar 8 (US) Non-Final Office Action - App. 14/745,207	
	42	2018 May 25 (US) Notice of Allowance - App. 15/413,834	
	43	A. Feldmann et al., "Tradeoffs for Packet Classification", Proceedings of the IEEE INFOCOM, 397-413, 2000	
	44	A. Hari et al., "Detecting and Resolving Packet Filter Conflicts", Proceedings of IEEE INFOCOM, 1203-1212, 2000	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

/KC/	45	Acharya et al, "OPTWALL: A Hierarchical Traffic-Aware Firewall," Department of Computer Science, Telecommunications Program, University of Pittsburgh, pgs. 1-11 (2007)
	46	Bellion, "HIgh Performance Packet Classification", http://www.hipac.org (Publication Date Unknown)
	47	C. Benecke, "A Parallel Packet Screen for High Speed Networks", Proceedings of the 15th Annual Computer Security Applications Conference, 1999
	48	Chen, et al, "Research on the Anomaly Discovering Algorithm of the Packet Filtering Rule Sets," September 2010, First International Confererence on Pervasive Computing, Signal Processing and Applications, pp. 362-366.
	49	D. Comer, "Analysis of a Heuristic for Full Trie Minimization", ACM Transactions on Database Systems, 6(3): 513-537, Sept. 1981
	50	D. Decasper et al., "Router Plugins: A Software Architecture for Next-Generation Routers", IEEE/ACM Transactions on Networking, 8(1): February 2000

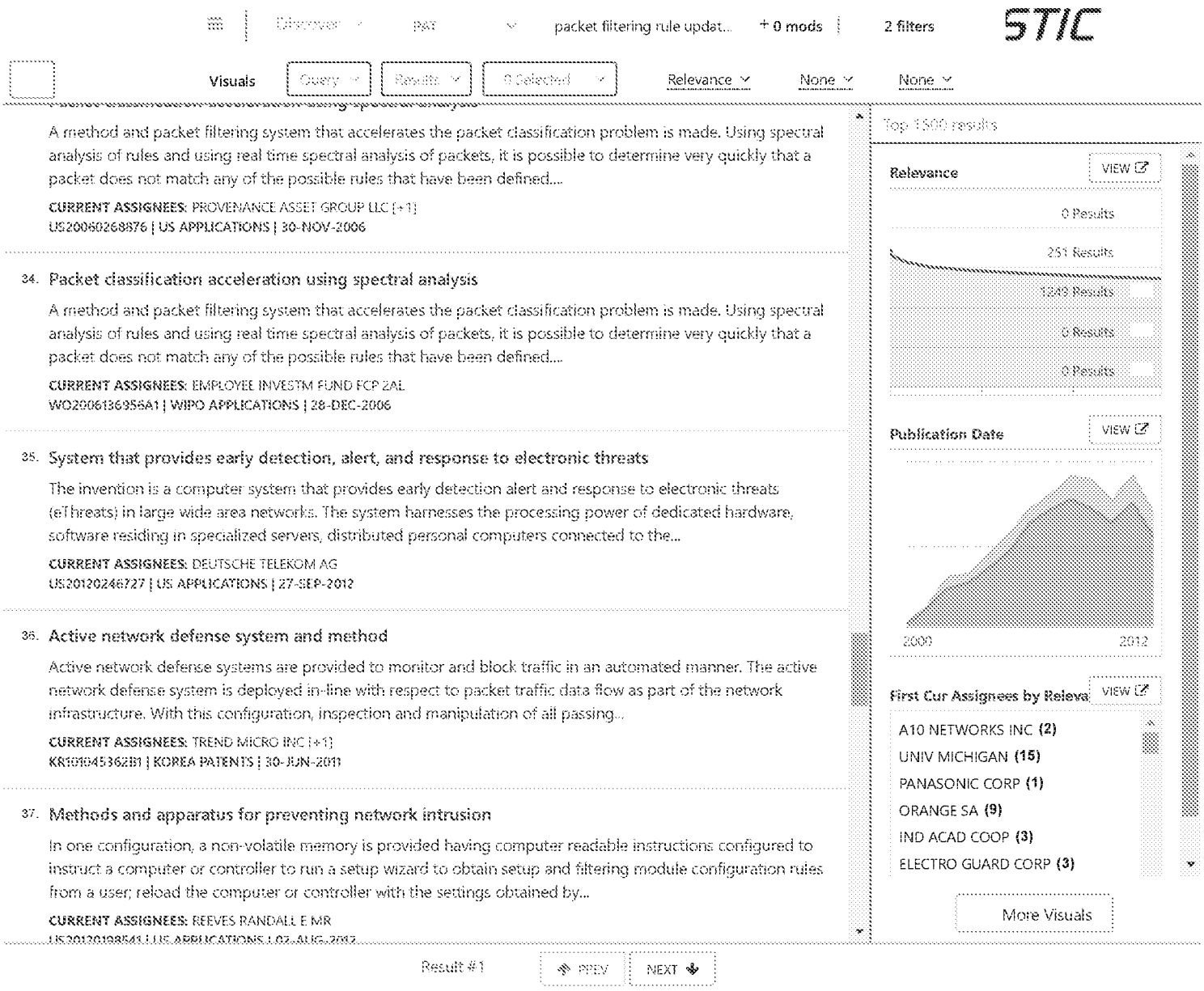
If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/KENNETH W CHANG/	Date Considered	04/12/2020

*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.


Discover
PAT
packet filtering rule updat...
+ 0 mods
2 filters
STIC
Visuals
Query
Results
0 Selected
Relevance
None
None
A method and packet filtering system that accelerates the packet classification problem is made. Using spectral analysis of rules and using real time spectral analysis of packets, it is possible to determine very quickly that a packet does not match any of the possible rules that have been defined....
CURRENT ASSIGNEES: PROVENANCE ASSET GROUP LLC [+1]
US20060268876 | US APPLICATIONS | 30-NOV-2006
34. Packet classification acceleration using spectral analysis
A method and packet filtering system that accelerates the packet classification problem is made. Using spectral analysis of rules and using real time spectral analysis of packets, it is possible to determine very quickly that a packet does not match any of the possible rules that have been defined....
CURRENT ASSIGNEES: EMPLOYEE INVESTM FUND FCP ZAL
WO2006136956A1 | WIPO APPLICATIONS | 28-DEC-2006
35. System that provides early detection, alert, and response to electronic threats
The invention is a computer system that provides early detection alert and response to electronic threats (eThreats) in large wide area networks. The system harnesses the processing power of dedicated hardware, software residing in specialized servers, distributed personal computers connected to the...
CURRENT ASSIGNEES: DEUTSCHE TELEKOM AG
US20120246727 | US APPLICATIONS | 27-SEP-2012
36. Active network defense system and method
Active network defense systems are provided to monitor and block traffic in an automated manner. The active network defense system is deployed in-line with respect to packet traffic data flow as part of the network infrastructure. With this configuration, inspection and manipulation of all passing...
CURRENT ASSIGNEES: TREND MICRO INC [+1]
KR101045362B1 | KOREA PATENTS | 30-JUN-2011
37. Methods and apparatus for preventing network intrusion
In one configuration, a non-volatile memory is provided having computer readable instructions configured to instruct a computer or controller to run a setup wizard to obtain setup and filtering module configuration rules from a user; reload the computer or controller with the settings obtained by...
CURRENT ASSIGNEES: REEVES RANDALL E MR
US20120198543 | US APPLICATIONS | 02-AUG-2012
Top 1500 results
Relevance
VIEW
0 Results
251 Results
1249 Results
0 Results
0 Results
Publication Date
VIEW
2000
2012
First Cur Assignees by Releva
VIEW
A10 NETWORKS INC (2)
UNIV MICHIGAN (15)
PANASONIC CORP (1)
ORANGE SA (9)
IND ACAD COOP (3)
ELECTRO GUARD CORP (3)
More Visuals
Result #1
PREV
NEXT

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

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. 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	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\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]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH /KC/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\US

/KC/	1	2018 Jul 26 (US) Declaration of Kevin Jeffay, PhD in Support of Second Petition for Inter Partes Review of U.S. Patent No. 9,137,205 - IPR2018-01444	
	2	Nichols, et al, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers," Network Working Group RFC 2474, December 1998, 20 pages.	
	3	2018 Jul 26 (US) Declaration of Kevin Jeffay, PhD in Support of First Petition for Inter Partes Review of U.S. Patent No. 9,137,205 - IPR2018-01443	
	4	Perkins, "IP Encapsulation with IP," Network Working Group RFC 2003, October 1996, 14 pages.	
	5	2018 Jul 12 (US) Petition for Inter Partes Review of U.S. Patent No. 9,565,213 - IPR2018-01386	
	6	2018 Jul 20 (US) Petition for Inter Partes Review of U.S. Patent No. 9,160,713 - IPR2018-01437	
	7	2018 Jul 20 (US) Petition for Inter Partes Review of U.S. Patent No. 9,124,552 - IPR2018-01436	
	8	Blake, et al, "An Architecture for Differentiated Services," Network Working Group RFC 2475, December 1998, 36 pages.	
	9	2018 Jul 27 (US) Second Petition for Inter Partes Review of U.S. Patent No. 9,137,205 - IPR2018-01444	
	10	2018 Jul 27 (US) First Petition for Inter Partes Review of U.S. Patent No. 9,137,205 - IPR2018-01443	
	11	Anonymous: "The Distribution of Malicious Domains," The DomainTools Report, 2016 Edition, 9 March 2016 (2016-03-09), pages 1-11, XP055502306, Retrieved from: https://www.domaintools.com/resources/white-papers/the-domaintools-report-the-distribution-of-malicious-domains	

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

Application Number	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\US

/KC/	12	2018 Aug 20 (US) Petition for Inter Partes Review of U.S. Patent No. 9,565,213 - IPR2018-01512	
	13	2018 Aug 15 (US) Declaration of Kevin Jeffay, PhD in Support of Petition for Inter Partes Review of U.S. Patent No. 9,565,213 - IPR2018-01512	
	14	"Cisco ACNS Softward Configuration Guide for Centrally Managed Deployments," Release 5.5. Text Part Number: OL-9136-01, Cisco Systems, Inc., 2006, 944 pages.	
	15	Blake, et al., "An Architecture for Differentiated Services," also known as the Diffserv architecture, as defined in RFC 2475, Network Working Group, Decemer 1998, 36 pages.	
	16	"Examining SSL-encrypted Communications: Netronome SSL InspectorTM Solution Overview," January 1, 2008, XP055036015, retrieved from <http://www.infosecurityproductsguide.com/technology/2008/Netronome_Examining_SSL-encrypted_Communications.pdf>, 8 pages.	
	17	2018 Aug 29 (CA) Office Action - App. 2,888,935 (007742.00046)	
	18	2019 Feb 6 (US) Final Office Action - App. 15/413,750 (007742.00084)	
	19	FRAHIM, et al., "Cisco ASA: All-in-One Firewall, IPS, and VPN Adaptive Security Appliance," Indiana: Cisco Press: 2006, 54 pages.	
	20	2018 Aug 10 (US) Declaration of Kevin Jeffay, PhD in Support of Fourth Petition for Inter Partes Review of U.S. Patent No. 9,137,205 - IPR2018-01506	
	21	2018 Aug 10 (US) Fourth Petition for Inter Partes Review of U.S. Patent No. 9,137,205 - IPR2018-01506	
	22	2018 Aug 03 (US) Third Petition for Inter Partes Review of U.S. Patent No. 9,137,205 - IPR2018-01505	

Keysight Technologies Ex. 1002

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /KC/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

/KC/	23	2018 Aug 03 (US) Declaration of Kevin Jeffay, PhD in Support of Third Petition for Inter Partes Review of U.S. Patent No. 9,137,205 - IPR2018-01505
	24	2018 Aug 03 (US) Declaration of Kevin Jeffay, PhD in Support of Third Petition for Inter Partes Review of U.S. Patent No. 9,560,077 - IPR2018-01513
	25	2019 Apr 2 (US) Decision - Institution of Inter Partes Review of U.S. Patent 9,560,077 - IPR 2018-01513
	26	2018 Aug 10 (US) Petition for Inter Partes Review of Claims 1-20 of U.S. Patent No. 9,560,077 - IPR2018-01513
	27	2019 May 24 (US) Non-Final Office Action - App. 16/111,524 (007742.00123)
	28	2019 Jun 3 (EP) Communication pursuant to Article 94(3) EPC - Third Examination Report - App. 13765547.8 (007742.00044)
	29	2019 Aug 2 (CA) Office Action - App. 2,888,935 (007742.00046)
	30	2019 Aug 2 (US) Non-Final Office Action - App. 16/448,969 (007742.00143)
	31	2019 Aug 16 (EP) Extended Search Report - App. 19170936.9 (007742.00140)

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

EXAMINER SIGNATURE

Examiner Signature	/KENNETH W CHANG/	Date Considered	04/12/2020

*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.

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

BIB DATA SHEET

CONFIRMATION NO. 8018

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
16/728,766	12/27/2019	726	2438	007742.00151\US

APPLICANTS

Centripetal Networks, Inc., Portsmouth, NH;

INVENTORS

Steven Rogers, Leesburg, VA;
Sean Moore, Hollis, NH;

**** CONTINUING DATA ***************************

This application is a CON of 16/111,524 08/24/2018 PAT 10567437
which is a CON of 15/413,834 01/24/2017 PAT 10091246
which is a CON of 14/698,560 04/28/2015 PAT 9560077
which is a CON of 13/657,010 10/22/2012 PAT 9137205

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
01/21/2020

Foreign Priority claimed	❑ Yes ☑ No	❑ Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
35 USC 119(a-d) conditions met	❑ Yes ☑ No		VA	10	27	4
Verified and Acknowledged	/KENNETH W CHANG/ Examiner's Signature	Initials				

ADDRESS

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

TITLE

METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK

FILING FEE RECEIVED		
1365	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	❑ All Fees ❑ 1.16 Fees (Filing) ❑ 1.17 Fees (Processing Ext. of time) ❑ 1.18 Fees (Issue) ❑ Other _____ ❑ Credit

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. 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	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\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	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	1	2020 Feb 11 (US) Final Written Decision Determining All Challenged Claims Unpatentable of U.S. Patent 9,137,205 B2 - IPR 2018-01444
	2	2020 Feb 11 (US) Final Written Decision Determining All Challenged Claims Unpatentable of U.S. Patent 9,137,205 B2 - IPR 2018-01443
	3	2020 Mar 19 (US) Final Written Decision Determining All Challenged Claims Unpatentable of U.S. Patent 9,565,213 B2 - IPR 2018-01512
	4	2020 Jan 23 (US) Final Written Decision Determining All Challenged Claims Unpatentable of U.S. Patent 9,565,213 B2 - IPR 2018-01386
	5	2020 Mar 31 (US) Final Written Decision Determining All Challenged Claims Unpatentable of U.S. Patent 9,560,077 B2 - IPR 2018-01513

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	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\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	/Scott M Kelly/	Date (YYYY-MM-DD)	2020-04-07
Name/Print	Scott M. Kelly	Registration Number	65,121

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:	39088167
Application Number:	16728766
International Application Number:	
Confirmation Number:	8018
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	Scott M Kelly/Niki Rollhauser
Filer Authorized By:	Scott M Kelly
Attorney Docket Number:	007742.00151\US
Receipt Date:	07-APR-2020
Filing Date:	27-DEC-2019
Time Stamp:	16:01:36
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	2020_Feb_11_US_Final_Written_Decision_Determining_All_Challenged_Claims_Unpatent_20429842.PDF	455363 770ce5f6d399e13136e53f5986b0721da2763176	no	63

Warnings:

Information:					
2	Non Patent Literature	2020_Feb_11_US_Final_Written_Decision_Determining_All_Challenged_Claims_Unpatent_20429837.PDF	452608 fd9178236c8b5ba32786e796da073ba93f01675d	no	56
Warnings:					
Information:					
3	Non Patent Literature	2020_Mar_19_US_Final_Written_Decision_Determining_All_Challenged_Claims_Unpatent_20429849.PDF	657483 2d353c172623f0afc2d9c3956f87464e574da9d6	no	85
Warnings:					
Information:					
4	Non Patent Literature	2020_Jan_23_US_Final_Written_Decision_Determining_All_Challenged_Claims_Unpatent_20429846.PDF	601308 d4354c3d234fd9fb6e75885152208e72ff633f29	no	62
Warnings:					
Information:					
5	Non Patent Literature	2020_Mar_31_US_Final_Written_Decision_Determining_All_Challenged_Claims_Unpatent_20429853.PDF	720237 49618ee166ed426422b725e9e399e539d9a76bc0	no	52
Warnings:					
Information:					
6	Information Disclosure Statement (IDS) Form (SB08)	Information_Disclosure_Statement_Fillable_PDF_20431099.pdf	1034353 0c46081a687ba786a9085d88a1046de489096c65	no	4
Warnings:					
Information:					
A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.					
		Total Files Size (in bytes):	3921352		

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/SB/08a (02-18)
Approved for use through 11/30/2020. 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	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\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	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	1	2018 Jul 26 (US) Declaration of Kevin Jeffay, PhD in Support of Second Petition for Inter Partes Review of U.S. Patent No. 9,137,205 - IPR2018-01444	
	2	Nichols, et al, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers," Network Working Group RFC 2474, December 1998, 20 pages.	
	3	2018 Jul 26 (US) Declaration of Kevin Jeffay, PhD in Support of First Petition for Inter Partes Review of U.S. Patent No. 9,137,205 - IPR2018-01443	
	4	Perkins, "IP Encapsulation with IP," Network Working Group RFC 2003, October 1996, 14 pages.	
	5	2018 Jul 12 (US) Petition for Inter Partes Review of U.S. Patent No. 9,565,213 - IPR2018-01386	
	6	2018 Jul 20 (US) Petition for Inter Partes Review of U.S. Patent No. 9,160,713 - IPR2018-01437	
	7	2018 Jul 20 (US) Petition for Inter Partes Review of U.S. Patent No. 9,124,552 - IPR2018-01436	
	8	Blake, et al, "An Architecture for Differentiated Services," Network Working Group RFC 2475, December 1998, 36 pages.	
	9	2018 Jul 27 (US) Second Petition for Inter Partes Review of U.S. Patent No. 9,137,205 - IPR2018-01444	
	10	2018 Jul 27 (US) First Petition for Inter Partes Review of U.S. Patent No. 9,137,205 - IPR2018-01443	
	11	Anonymous: "The Distribution of Malicious Domains," The DomainTools Report, 2016 Edition, 9 March 2016 (2016-03-09), pages 1-11, XP055502306, Retrieved from: https://www.domaintools.com/resources/white-papers/the-domaintools-report-the-distribution-of-malicious-domains	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	12	2018 Aug 20 (US) Petition for Inter Partes Review of U.S. Patent No. 9,565,213 - IPR2018-01512	
	13	2018 Aug 15 (US) Declaration of Kevin Jeffay, PhD in Support of Petition for Inter Partes Review of U.S. Patent No. 9,565,213 - IPR2018-01512	
	14	"Cisco ACNS Softward Configuration Guide for Centrally Managed Deployments," Release 5.5. Text Part Number: OL-9136-01, Cisco Systems, Inc., 2006, 944 pages.	
	15	Blake, et al., "An Architecture for Differentiated Services," also known as the Diffserv architecture, as defined in RFC 2475, Network Working Group, Decemer 1998, 36 pages.	
	16	"Examining SSL-encrypted Communications: Netronome SSL InspectorTM Solution Overview," January 1, 2008, XP055036015, retrieved from <http://www.infosecurityproductsguide.com/technology/2008/Netronome_Examining_SSL-encrypted_Communications.pdf>, 8 pages.	
	17	2018 Aug 29 (CA) Office Action - App. 2,888,935 (007742.00046)	
	18	2019 Feb 6 (US) Final Office Action - App. 15/413,750 (007742.00084)	
	19	FRAHIM, et al., "Cisco ASA: All-in-One Firewall, IPS, and VPN Adaptive Security Appliance," Indiana: Cisco Press: 2006, 54 pages.	
	20	2018 Aug 10 (US) Declaration of Kevin Jeffay, PhD in Support of Fourth Petition for Inter Partes Review of U.S. Patent No. 9,137,205 - IPR2018-01506	
	21	2018 Aug 10 (US) Fourth Petition for Inter Partes Review of U.S. Patent No. 9,137,205 - IPR2018-01506	
	22	2018 Aug 03 (US) Third Petition for Inter Partes Review of U.S. Patent No. 9,137,205 - IPR2018-01505	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	23	2018 Aug 03 (US) Declaration of Kevin Jeffay, PhD in Support of Third Petition for Inter Partes Review of U.S. Patent No. 9,137,205 - IPR2018-01505
	24	2018 Aug 03 (US) Declaration of Kevin Jeffay, PhD in Support of Third Petition for Inter Partes Review of U.S. Patent No. 9,560,077 - IPR2018-01513
	25	2019 Apr 2 (US) Decision - Institution of Inter Partes Review of U.S. Patent 9,560,077 - IPR 2018-01513
	26	2018 Aug 10 (US) Petition for Inter Partes Review of Claims 1-20 of U.S. Patent No. 9,560,077 - IPR2018-01513
	27	2019 May 24 (US) Non-Final Office Action - App. 16/111,524 (007742.00123)
	28	2019 Jun 3 (EP) Communication pursuant to Article 94(3) EPC - Third Examination Report - App. 13765547.8 (007742.00044)
	29	2019 Aug 2 (CA) Office Action - App. 2,888,935 (007742.00046)
	30	2019 Aug 2 (US) Non-Final Office Action - App. 16/448,969 (007742.00143)
	31	2019 Aug 16 (EP) Extended Search Report - App. 19170936.9 (007742.00140)

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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

[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	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\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	/Scott M Kelly/	Date (YYYY-MM-DD)	2020-03-25
Name/Print	Scott M. Kelly	Registration Number	65,121

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.

Docket No.: 007742.00151\US
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Steven Rogers et al.

Application No.: 16/728,766 | Confirmation No.: 8018

Filed: December 27, 2019 | Art Unit: 2438

For: METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK | Examiner: K. W. Chang

INFORMATION DISCLOSURE STATEMENT UNDER §1.97(B)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

Pursuant to 37 C.F.R. § 1.56 and in compliance with 37 C.F.R. § 1.97, Applicant submits herewith form PTO/SB/08, identifying information for consideration by the Examiner.

This application relies, under 35 U.S.C. § 120, on the earliest effective filing date of prior U.S. patent application 16/111,524, filed August 24, 2018, and its parent applications (if any). The NPL documents identified on the attached PTO/SB/08 were submitted to and/or cited by the Office in a prior application that is relied upon for priority and, therefore, copies are not required to be provided in this application.

Applicant does not waive any rights to take appropriate action to establish patentability over the listed documents should they be applied as a reference against the claims of the present application.

Consideration of the cited information and making the same of record in the prosecution of the above noted application are respectfully requested. Should the Patent and Trademark Office determine that a fee is required, please charge our Deposit Account No. 19-0733.

Dated: March 25, 2020

Respectfully submitted,

By: /Scott M Kelly/
Scott M. Kelly
Registration No.: 65,121

BANNER & WITCOFF, LTD.
1100 13th St. NW, STE 1200
Washington, DC 20005
(202) 824-3000

Electronic Acknowledgement Receipt

EFS ID:	38967499
Application Number:	16728766
International Application Number:	
Confirmation Number:	8018
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	Scott M Kelly/Niki Rollhauser
Filer Authorized By:	Scott M Kelly
Attorney Docket Number:	007742.00151\US
Receipt Date:	25-MAR-2020
Filing Date:	27-DEC-2019
Time Stamp:	16:03:17
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	IPR2018-01512_Petition_19398704.pdf	1376455 b852411a163448b27165aa71fef886b2b9c0a5ea	no	93

Warnings:

Information:					
2	Non Patent Literature	IPR2018-01512_Exhibit_1004_19398712.pdf	2394173 489037fb21efbdb8e1a203c3c188b6baf8f72fc8	no	167
Warnings:					
Information:					
3	Non Patent Literature	OTT01-9182132-v1-PAT_82827W-1_Corr_from_PTO_-_Office_Action_dtd_08-29-2018_19429528.PDF	2542659 d370f61c054a597f144507a62a0aaef58de003d2	no	4
Warnings:					
Information:					
4	Other Reference-Patent/App/Search documents	Final_Rejection__892__1449_19586326.pdf	1411297 d08945ba26cc0dc20b442a326ccbe53f34900b98	no	36
Warnings:					
Information:					
5	Non Patent Literature	03_Jun_2019_EP_Third_Examination_Report_13765547_19836161.PDF	447608 7809730cb6ae6efa98ff8fb67faacc60a73077c8	no	11
Warnings:					
Information:					
6	Non Patent Literature	CIPO_OA_dtd_08-02-2019_19926836.PDF	312757 e5a56e2ff1242c6cbaad04f520fb88f12988d590	no	6
Warnings:					
Information:					
7	Other Reference-Patent/App/Search documents	Non-Final_Rejection__892__1449_19912157.pdf	3300675 bd155d20620ab819ff31fb95411f2ae31ffd9dd5	no	114
Warnings:					
Information:					
8	Other Reference-Patent/App/Search documents	2019_Aug_16_EP_Extended_Srch_Rpt__WO_19972746.PDF	494262 737cc617fcd7931a4531c104166b919fd575155f	no	7
Warnings:					
Information:					

9	Information Disclosure Statement (IDS) Form (SB08)	Information_Disclosure_Statement_Fillable_PDF_1_of_4-1_20402849.pdf	1043034 15f68577160bba7d51b78120bd20a01d888ffa59	no	35
Warnings:					
Information:					
10	Information Disclosure Statement (IDS) Form (SB08)	Information_Disclosure_Statement_Fillable_PDF_2_of_4-1_20402850.pdf	1036235 5b9c47ce6b805f1b19ecf1e80d8164540b81954f	no	8
Warnings:					
Information:					
A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.					
11	Information Disclosure Statement (IDS) Form (SB08)	Information_Disclosure_Statement_Fillable_PDF_3_of_4-1_20402851.pdf	1037804 53e8615e905d554ed4713c0891f808377705538b	no	8
Warnings:					
Information:					
A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.					
12	Information Disclosure Statement (IDS) Form (SB08)	Information_Disclosure_Statement_Fillable_PDF_4_of_4-1_20402852.pdf	1035768 2fd0ee7014af161e7f36a89c48c7d2a7ec26f9be	no	7
Warnings:					
Information:					
A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.					
13	Transmittal Letter	Information_Disclosure_Statement_Under_1_20404988.pdf	17741 17175f29f58888a88f9f0286b4b6e2ccce70679b	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	16450468		

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/SB/08a (02-18)
Approved for use through 11/30/2020. 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	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\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	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	1	2016 Dec 05 - (US) Notice of Allowance - App 14/714,207	
	2	2016 Feb 24 - (AU) Office Action - App 2014228257	
	3	2016 Feb 25 - (AU) Office Action - App 2014249055	
	4	2016 Feb 26 - (US) Non Final Office Action - App 14/253,992	
	5	2016 Jan 11 - (US) Non Final Rejection - App 14/698,560	
	6	2016 Jan 28 - (WO) International Search Report and Written Opinion - App PCT/US2015/062691	
	7	2016 Jul 11 - (EP) Office Action - App 14720824.3	
	8	2016 Jul 20 - (AU) Office Action - App 2013335255	
	9	2016 Jul 22 - (US) Office Action - App 14/921,718	
	10	2016 Jun 09 - (WO) International Search Report - PCT/US2016/026339	
	11	2016 Jun 14 - (US) Office Action - App 14/625,486	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	12	2016 Jun 16 - (CA) Office Action - App 2,888,935	
	13	2016 May 06 - (US) Office Action - App 14/714,207	
	14	2016 May 13 - (US) Office Action - App 13/940,240	
	15	2016 Nov 21 - (US) Office Action - App 14/745,207	
	16	2016 Oct 05 - (US) Notice of Allowance - App 14/698,560	
	17	2016 Oct 26 - (US) Office Action - App 13/940,240	
	18	2016 Sept 13 - (CA) Office Action - App 2,902,206	
	19	2016 Sept 14 - (CA) Office Action - App 2,897,737	
	20	2016 Sept 26 - (CA) Office Action - App 2,902,158	
	21	2017 Apr 12 - (US) Office Action - App 14/757,638	
	22	2017 Aug 15 (WO) International Preliminary Report on Patentability - App. PCT/US2015/062691 (007742.00064)	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	23	2017 Aug 21 (AU) First Examination Report - App. 2015248067 (007742.00079)	
	24	2017 Feb 10 - (US) Notice of Allowance - App 14/625,486	
	25	2017 Feb 15 - (US) Notice of Allowance - App 14/921,718	
	26	2017 Jul 20 (US) Complaint for Patent Infringement - Case No. 2:17-cv-00383-HCN-LRL, Document 1, 38 pages.	
	27	2017 Jun 07 - (US) Office Action - App 14/745,207	
	28	2017 Jun 07 - (WO) International Search Report and Written Opinion - App PCT/US2016/067111	
	29	2017 Mar 06 - (WO) International Search Report and Written Opinion - App PCT/US2016/068008	
	30	2017 Nov 21 (US) Notice of Allowance - App. 14/690,302 (007742.00042)	
	31	2017 Nov 3 (US) Non-Final Office Action - App. 15/413,834 (007742.00085)	
	32	2017 Oct 17 (WO) International Preliminary Report on Patentability - App. PCT/US2016/026339 (007742.00075)	
	33	2017 Sep 5 (US) Defendant Ixia's Partial Answer to Complaint for Patent Infringement - Case No. 2:17-cv-00383-HCN-LRL, Document 29, 14 pages.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	34	2017 Sep 5 (US) Memorandum in Support of Defendant's Ixia and Keysight Technologies, Inc's Motion to Dismiss for Unpatentability Under 35 U.S.C. § 101 - Case No. 2:17-cv-00383-HCM-LRL, Document 21, 29 pages.	
	35	2017 Sep 5 (US) Request for Judicial Notice in Support of Defendants Ixia and Keysight Technologies, Inc's Motion to Dismiss for Unpatentability under 35 U.S.C. § 101 - Case No. 2:17-cv-00383-HCN-LRL, Document 22, 3 pages.	
	36	2017 Sept 29 (CA) Examination Report - App. 2,772,630	
	37	2018 Apr 17 (US) Non-Final Office Action - App. 15/610,995 (007742.00090)	
	38	2018 Mar 15 (EP) Second Communication pursuant to Article 94(3) EPC - App. 13765547.8 (007742.00044)	
	39	2018 Mar 16 (EP) Communication Pursuant to Rule 164(2)(b) and Article 94(3) EPC - App. 15722292.8	
	40	2018 Mar 21 (AU) First Examination Report - App. 2015382393 (007742.00096)	
	41	2018 Mar 8 (US) Non-Final Office Action - App. 14/745,207	
	42	2018 May 25 (US) Notice of Allowance - App. 15/413,834	
	43	A. Feldmann et al., "Tradeoffs for Packet Classification", Proceedings of the IEEE INFOCOM, 397-413, 2000	
	44	A. Hari et al., "Detecting and Resolving Packet Filter Conflicts", Proceedings of IEEE INFOCOM, 1203-1212, 2000	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	45	Acharya et al, "OPTWALL: A Hierarchical Traffic-Aware Firewall," Department of Computer Science, Telecommunications Program, University of Pittsburgh, pgs. 1-11 (2007)	
	46	Bellion, "HIgh Performance Packet Classification", http://www.hipac.org (Publication Date Unknown)	
	47	C. Benecke, "A Parallel Packet Screen for High Speed Networks", Proceedings of the 15th Annual Computer Security Applications Conference, 1999	
	48	Chen, et al, "Research on the Anomaly Discovering Algorithm of the Packet Filtering Rule Sets," September 2010, First International Confererence on Pervasive Computing, Signal Processing and Applications, pp. 362-366.	
	49	D. Comer, "Analysis of a Heuristic for Full Trie Minimization", ACM Transactions on Database Systems, 6(3): 513-537, Sept. 1981	
	50	D. Decasper et al., "Router Plugins: A Software Architecture for Next-Generation Routers", IEEE/ACM Transactions on Networking, 8(1): February 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	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\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	/Scott M Kelly/	Date (YYYY-MM-DD)	2020-03-25
Name/Print	Scott M. Kelly	Registration Number	65,121

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.

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. 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	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\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	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	1	D. Eppstein et al., "Internet Packet Filter Management and Rectangle Geometry", Proceedings of the Symposium on Discrete Algorithms, 827-835, 2001	
	2	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	
	3	E. Al-Shaer et al., "Modeling and Management of Firewall Policies", IEEE Transactions on Network and Service Management, 1(1): 2004	
	4	E. Fulp et al., "Network Firewall Policy Tries", Technical Report, Computer Science Department, Wake Forest University, 2004	
	5	E. Fulp, "Optimization of Network Firewall Policies Using Ordered Sets and Directed Acyclical Graphs", Technical Report, Computer Scient Department, Wake Forest University, January 2004	
	6	E. Fulp, "Preventing Denial of Service Attacks on Quality of Service", Proceedings of the 2001 DARPA Information Survivability Conference and Exposition II, 2001	
	7	E.L. Lawler, "Sequencing Jobs to Minimize Total Weighted Completion Time Subject to Precedence Constraints", Annals of Discrete Mathematics, 2: 75-90, 1978	
	8	E.W. Fulp, "Firewall Architectures for High Speed Networks", U.S. Department of Energy Grant Application, Funded September 2003	
	9	Fulp, "Trie-Based Policy Representations for Network Firewalls," Proceedings of the IEEE International Symposium on Computer Communications (2005)	
	10	Fulp, Errin: "CV: Errin Fulp," XP002618346, www.cs.wfu.edu/fulp/ewfPub.html, pgs. 1-5 (Copyright 2010)	
	11	G. Brightwell et al., "Counting Linear Extensions is #P-Complete", Proceedings of the Twenty-Third Annual ACM Symposium on Theory of Computing, 1991	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	12	G.V. Rooij, "Real Stateful TCP Packet Filtering in IP Filter", Proceedings of the 10th USENIX Security Symposium, 2001	
	13	Greenwald, Michael; "Designing an Academic Firewall: Policy, Practice, and Experience with SURF"; IEEE, Proceedings of SNDSS, 1996.	
	14	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	
	15	J.K. Lenstra et al., "Complexity of Scheduling Under Precedence Constraints", Operations Research, 26(1): 22-35,1978	
	16	Kindervag, et al. "Build Security Into Your Network's DNA: The Zero Trust Network Architecture," Forrester Research Inc.; Novermber 5, 2010, pps: 1-26.	
	17	L. Qui et al., "Fast Firewall Implementations for Software and Hardware-Based Routers", Proceedings of ACM Sigmetrics, June 2001	
	18	Lee et al., "Development Framework for Firewall Processors," IEEE, pgs. 352-355 (2002)	
	19	M. Al-Suwaiyel et al., "Algorithms for Trie Compaction", ACM Transactions on Database Systems, 9(2): 243-263, June 1984	
	20	M. Christiansen et al., "Using IDDs for Packet Filtering," Technical Report, BRICS, October 2002	
	21	M. Degermark et al., "Small Forwarding Tables for Fast Routing Lookups", Proceedings of ACM SIGCOMM, 4-13, 1997	
	22	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.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	23	Moore, S, "SBIR Case Study: Centripetal Networks: How CNI Leveraged DHS S&T SBIR Funding to Launch a Successful Cyber Security Company," 2012 Principal Investigators' Meeting, Cyber Security Division, October 10, 2014.	
	24	O. Paul et al., "A full Bandwidth ATM Firewall", Proceedings of the 6th European Symposium on Research in Computer Security ESORICS'2000, 2000	
	25	P. Warkhede et al., "Fast Packet Classification for Two-Dimensional Conflict-Free Filters", Proceedings of IEEE INFOCOM, 1434-1443, 2001	
	26	Palo Alto Networks; "Designing A Zero Trust Network With Next-Generation Firewalls"; pps. 1-10; last viewed on October 21, 2012.	
	27	R. Funke et al., "Performance Evaluation of Firewalls in Gigabit-Networks", Proceedings of the Symposium on Performance Evaluation of Computer and Telecommunication Systems, 1999	
	28	R. Rivest, "On Self-Organizing Sequential Search Heuristics", Communications of the ACM, 19(2): 1976	
	29	R.L. Graham et al., "Optimization and Approximation in Deterministic Sequencing and Scheduling: A Survey", Annals of Discrete Mathematics, 5: 287-326, 1979	
	30	Reumann, John; "Adaptive Packet Filters"; IEEE, 2001, Department of Electrical Engineering and Computer Science, The University of Michigan, Ann Arbor, MI	
	31	S,M. Bellovin et al., "Network Firewalls", IEEE Communications Magazine, 50-57, 1994	
	32	S. Goddard et al., "An Unavailability Analysis of Firewall Sandwich Configurations", Proceedings of the 6th IEEE Symposium on High Assurance Systems Engineering, 2001	
	33	S. Suri et al., "Packet Filtering in High Speed Networks", Proceedings of the Symposium on Discrete Algorithms, 969-970, 1999	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	34	Singh, Rajeev et al. "Detecting and Reducing the Denial of Service attacks in WLANs", December 2011, World Congress on Information and Communication TEchnologies, pp. 968-973	
	35	Statement RE: Related Application, dated July 24, 2015	
	36	Tarsa et al., "Balancing Trie-Based Policy representations for Network Firewalls," Department of Computer Science, Wake Forest University, pgs. 1-6 (2006)	
	37	U. Ellermann et al., "Firewalls for ATM Networks", Proceedings of INFOSEC'COM, 1998	
	38	V. Srinivasan et al., "Fast and Scalable Layer Four Switching", Proceedings of ACM SIGCOMM, 191-202, 1998	
	39	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	
	40	W.E. Leland et al., "On the Self-Similar Nature of Ethernet Traffic", IEEE Transactions on Networking, 2(1); 15, 1994	
	41	W.E. Smith, "Various Optimizers for Single-Stage Productions", Naval Research Logistics Quarterly, 3: 59-66, 1956	
	42	X. Gan et al., "LSMAC vs. LSNAT: Scalable Cluster-based Web servers", Journal of Networks, Software Tools, and Applications, 3(3): 175-185, 2000	
	43	2018 Jul 5 (US) Non-Final Office Action - App. 15/413,750 (007742.00084)	
	44	2018 Jul 13 (US) Notice of Allowance - App. 15/414,117 (007742.00065)	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	45	2018 Jul 27 (US) Non-Final Office Action - App. 15/382,806 (007742.00082)	
	46	Sourcefire 3D System User Guide, Version 4.10, March 16, 2011, 2123 pages.	
	47	2018 Jul 11 (US) Declaration of Kevin Jeffay, PhD in Support of Petition for Inter Partes Review of U.S. Patent No. 9,565,213 - IPR2018-01386	
	48	Ylonen, et al, "The Secure Shell (SSH) Transport Layer Protocol," SSH Communication Security Corp, Newtork Working Group RFC 4253, January 2006, 32 pages.	
	49	2018 Jul 20 (US) Declaration of Dr. Stuart Staniford in Support of Petition for Inter Partes Review of U.S. Patent No. 9,160,713 - IPR2018-01437	
	50	2018 Jul 20 (US) Declaration of Dr. Stuart Staniford in Support of Petition for Inter Partes Review of U.S. Patent No. 9,124,552 - IPR2018-01436	

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	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\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	/Scott M Kelly/	Date (YYYY-MM-DD)	2020-03-25
Name/Print	Scott M. Kelly	Registration Number	65,121

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.

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. 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	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\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	6098172		2000-08-01	Coss et al.	
	2	6147976	A	2000-11-14	Shand et al.	
	3	6226372	B1	2001-05-01	Beebe et al.	
	4	6279113	B1	2001-08-21	Vaidya	
	5	6317837	B1	2001-11-13	Kenworthy	
	6	6484261	B1	2002-11-19	Wiegel	
	7	6611875		2003-08-26	Chopra et al.	
	8	6662235	B1	2003-12-09	Callis et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	9	6826694		2004-11-30	Dutta et al.	
	10	6907042	B1	2005-06-14	Oguchi	
	11	6971028	B1	2005-11-29	Lyle et al.	
	12	7089581	B1	2006-08-08	Nagai et al.	
	13	7095716		2006-08-22	Ke et al.	
	14	7107613	B1	2006-09-12	Chen et al.	
	15	7143438	B1	2006-11-28	Coss et al.	
	16	7152240	B1	2006-12-19	Green et al.	
	17	7185368		2007-02-27	Copeland, III	
	18	7215637	B1	2007-05-08	Ferguson et al.	
	19	7225269	B2	2007-05-29	Watanabe	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	20	7227842	B1	2007-06-05	Ji et al.	
	21	7237267	B2	2007-06-26	Rayes et al.	
	22	7263099	B1	2007-08-28	Woo et al.	
	23	7296288	B1	2007-11-13	Hill et al.	
	24	7299353	B2	2007-11-20	Le Pennec et al.	
	25	7331061	B1	2008-02-12	Ramsey et al.	
	26	7478429	B2	2009-01-13	Lyon	
	27	7499412		2009-03-03	Matityahu et al.	
	28	7539186	B2	2009-05-26	Aerrabotu et al.	
	29	7610621	B2	2009-10-27	Turley et al.	
	30	7684400	B2	2010-03-23	Govindarajan et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	31	7710885	B2	2010-05-04	Ilnicki et al.	
	32	7721084	B2	2010-05-18	Salminen et al.	
	33	7792775	B2	2010-09-07	Matsuda	
	34	7814158	B2	2010-10-12	Malik	
	35	7814546	B1	2010-10-12	Strayer et al.	
	36	7818794	B2	2010-10-19	Wittman	
	37	7849502		2010-12-07	Bloch et al.	
	38	7913303	B1	2011-03-22	Rouland et al.	
	39	7954143	B2	2011-05-31	Aaron	
	40	8004994		2011-08-23	Darisi et al.	
	41	8009566	B2	2011-08-30	Zuk et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	42	8037517	B2	2011-10-11	Fulp et al.	
	43	8042167	B2	2011-10-18	Fulp et al.	
	44	8117655	B2	2012-02-14	Spielman	
	45	8156206	B2	2012-04-10	Kiley et al.	
	46	8176561	B1	2012-05-08	Hurst et al.	
	47	8219675		2012-07-10	Ivershen	
	48	8271645		2012-09-18	Rajan et al.	
	49	8306994	B2	2012-11-06	Kenworthy	
	50	8307029	B2	2012-11-06	Davis et al.	
	51	8331234	B1	2012-12-11	Newton et al.	
	52	8422391		2013-04-16	Zhu	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	53	8495725	B2	2013-07-23	Ahn	
	54	8510821	B1	2013-08-13	Brandwine et al.	
	55	8726379	B1	2014-05-13	Stiansen et al.	
	56	8806638	B1	2014-08-12	Mani	
	57	8832832	B1	2014-09-09	Visbal	
	58	8856926	B2	2014-10-07	Narayanaswamy et al.	
	59	8935785	B2	2015-01-13	Pandrangi	
	60	9094445	B2	2015-07-28	Moore et al.	
	61	9124552	B2	2015-09-01	Moore	
	62	9137205	B2	2015-09-15	Rogers et al.	
	63	9154446	B2	2015-10-06	Gemelli et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	64	9160713	B2	2015-10-13	Moore	
	65	9172627		2015-10-27	Kjendal et al.	
	66	9419942	B1	2016-08-16	Buruganahalli et al.	
	67	9531672	B1	2016-12-27	Li et al.	
	68	9634911		2017-04-25	Meloche	
	69	9686193	B2	2017-06-20	Moore	
	70	8789135	B1	2014-07-22	Pani	
	71	6678827	B1	2004-01-13	Rothermel 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	20010039579	A1	2001-11-08	TRCKA et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	2	20010039624		2001-11-08	Kellum	
	3	20020016858	A1	2002-02-07	Sawada et al.	
	4	20020038339	A1	2002-03-28	Xu	
	5	20020049899	A1	2002-04-25	Kenworthy	
	6	20020083345	A1	2002-06-27	Halliday et al.	
	7	20020112188	A1	2002-08-15	Syvanne	
	8	20020152209	A1	2002-10-17	Merugu et al.	
	9	20020164962	A1	2002-11-07	Mankins et al.	
	10	20020165949	A1	2002-11-07	Na et al.	
	11	20020186683	A1	2002-12-12	Buck et al.	
	12	20020198981	A1	2002-12-26	Corl et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	13	20030005122	A1	2003-01-02	Freimuth et al.	
	14	20030014665	A1	2003-01-16	Anderson et al.	
	15	20030018591	A1	2003-01-23	Komisky	
	16	20030035370	A1	2003-02-20	Brustoloni, Jose	
	17	20030051026	A1	2003-03-13	Carter et al.	
	18	20030088787	A1	2003-05-08	Egevang	
	19	20030097590	A1	2003-05-22	Syvanne	
	20	20030105976	A1	2003-06-05	Copeland	
	21	20030120622	A1	2003-06-26	Nurmela et al.	
	22	20030123456	A1	2003-07-03	Denz et al.	
	23	20030142681	A1	2003-07-31	Chen et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	24	20030145225	A1	2003-07-31	Bruton et al.	
	25	20030154297	A1	2003-08-14	Suzuki et al.	
	26	20030154399	A1	2003-08-14	Zuk et al.	
	27	20030188192	A1	2003-10-02	Tang et al.	
	28	20030212900	A1	2003-11-13	Liu et al.	
	29	20030220940	A1	2003-11-27	Futoransky et al.	
	30	20040010712	A1	2004-01-15	Hui et al.	
	31	20040015719	A1	2004-01-22	Lee et al.	
	32	20040073655	A1	2004-04-15	Kan et al.	
	33	20040088542	A1	2004-05-06	Daude et al.	
	34	20040093513	A1	2004-05-13	Cantrell et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	35	20040098511	A1	2004-05-20	Lin et al.	
	36	20040114518	A1	2004-06-17	MacFaden et al.	
	37	20040123220	A1	2004-06-24	Johnson et al.	
	38	20040131056	A1	2004-07-08	Dark	
	39	20040148520	A1	2004-07-29	Talpade et al.	
	40	20040151155	A1	2004-08-05	Jouppi	
	41	20040172529	A1	2004-09-02	Culbert	
	42	20040172557	A1	2004-09-02	Nakae et al.	
	43	20040177139	A1	2004-09-09	Schuba et al.	
	44	20040193943	A1	2004-09-30	Angelino et al.	
	45	20040199629	A1	2004-10-07	Bomer et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	46	20040205360	A1	2004-10-14	Norton et al.	
	47	20040250124	A1	2004-12-09	Chesla et al.	
	48	20050010765	A1	2005-01-13	Swander et al.	
	49	20050024189	A1	2005-02-03	Weber	
	50	20050071650	A1	2005-03-31	Jo et al.	
	51	20050076227	A1	2005-04-07	Kang et al.	
	52	20050108557	A1	2005-05-19	Kayo et al.	
	53	20050114704	A1	2005-05-26	Swander	
	54	20050117576	A1	2005-06-02	McDysan et al.	
	55	20050125697	A1	2005-06-09	Tahara	
	56	20050138204	A1	2005-06-23	Iyer et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	57	20050138353	A1	2005-06-23	Spies et al.	
	58	20050141537	A1	2005-06-30	Kumar et al.	
	59	20050183140	A1	2005-08-18	Goddard	
	60	20050229246	A1	2005-10-13	Rajagopal et al.	
	61	20050249214	A1	2005-11-10	Peng	
	62	20050251570	A1	2005-11-10	Heasman et al.	
	63	20050283823	A1	2005-12-22	Okajo et al.	
	64	20050286522	A1	2005-12-29	Paddon et al.	
	65	20060031928	A1	2006-02-09	Conley et al.	
	66	20060048142	A1	2006-03-02	Roese et al.	
	67	20060053491	A1	2006-03-09	Khuti et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	68	20060070122	A1	2006-03-30	Bellovin	
	69	20060080733	A1	2006-04-13	Khosmood et al.	
	70	20060085849	A1	2006-04-20	Culbert	
	71	20060104202	A1	2006-05-18	Reiner	
	72	20060114899	A1	2006-06-01	Toumura et al.	
	73	20060133377	A1	2006-06-22	Jain	
	74	20060136987	A1	2006-06-22	Okuda	
	75	20060137009	A1	2006-06-22	Chesla	
	76	20060146879	A1	2006-07-06	Anthias et al.	
	77	20060159028	A1	2006-07-20	Curran-Gray et al.	
	78	20060195896	A1	2006-08-31	Fulp et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	79	20060212572	A1	2006-09-21	Afek et al.	
	80	20060248580	A1	2006-11-02	Fulp et al.	
	81	20060262798	A1	2006-11-23	Joshi et al.	
	82	20070056038	A1	2007-03-08	Lok	
	83	20070083924	A1	2007-04-12	Lu	
	84	20070118894	A1	2007-05-24	Bhatia	
	85	20070211644	A1	2007-09-13	Ottamalika et al.	
	86	20070240208	A1	2007-10-11	Yu et al.	
	87	20070291789	A1	2007-12-20	Kutt et al.	
	88	20080005795	A1	2008-01-03	Acharya et al.	
	89	20080028467	A1	2008-01-31	Kommareddy et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	90	20080043739	A1	2008-02-21	SUH et al.	
	91	20080072307	A1	2008-03-20	Maes	
	92	20080077705	A1	2008-03-27	Li et al.	
	93	20080080493	A1	2008-04-03	Weintraub et al.	
	94	20080086435	A1	2008-04-10	Chesla	
	95	20080101234	A1	2008-05-01	Nakil et al.	
	96	20080163333	A1	2008-07-03	Kasralikar	
	97	20080201772	A1	2008-08-21	Mondaeev et al.	
	98	20080229415	A1	2008-09-18	Kapoor et al.	
	99	20080235755	A1	2008-09-25	Blaisdell et al.	
	100	20080279196	A1	2008-11-13	Friskney et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	101	20080301765	A1	2008-12-04	Nicol et al.	
	102	20080313738	A1	2008-12-18	Enderby	
	103	20080320116	A1	2008-12-25	Briggs	
	104	20090028160	A1	2009-01-29	ESWARAN et al.	
	105	20090138938	A1	2009-05-28	Harrison et al.	
	106	20090150972	A1	2009-06-11	MOON et al.	
	107	20090172800	A1	2009-07-02	WOOL	
	108	20090222877	A1	2009-09-03	Diehl et al.	
	109	20090240698	A1	2009-09-24	Shukla et al.	
	110	20090262723	A1	2009-10-22	Pelletier et al.	
	111	20090262741	A1	2009-10-22	Jungck et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	112	20090300759	A1	2009-12-03	Wang et al.	
	113	20090328219	A1	2009-12-31	Narayanaswamy	
	114	20100011433	A1	2010-01-14	HARRISON et al.	
	115	20100011434	A1	2010-01-14	Kay	
	116	20100082811	A1	2010-04-01	Van Der Merwe et al.	
	117	20100095367	A1	2010-04-15	Narayanaswamy	
	118	20100107240	A1	2010-04-29	Thaler et al.	
	119	20100115621	A1	2010-05-06	Staniford et al.	
	120	20100132027	A1	2010-05-27	Ou	
	121	20100195503	A1	2010-08-05	Raleigh	
	122	20100199346	A1	2010-08-05	Ling et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	123	20100202299	A1	2010-08-12	Strayer et al.	
	124	20100211678	A1	2010-08-19	McDysan et al.	
	125	20100232445	A1	2010-09-16	Bellovin	
	126	20100242098	A1	2010-09-23	Kenworthy	
	127	20100268799	A1	2010-10-21	Maestas	
	128	20100296441	A1	2010-11-25	Barkan	
	129	20100303240	A1	2010-12-02	Beachem et al.	
	130	20110055916	A1	2011-03-03	Ahn	
	131	20110055923	A1	2011-03-03	Thomas	
	132	20110088092	A1	2011-04-14	Nguyen et al.	
	133	20110141900	A1	2011-06-16	Jayawardena et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	134	20110185055	A1	2011-07-28	NAPPIER et al.	
	135	20110214157	A1	2011-09-01	Korsunsky et al.	
	136	20110270956	A1	2011-11-03	McDysan et al.	
	137	20110277034	A1	2011-11-10	Hanson	
	138	20120023576	A1	2012-01-26	Sorensen et al.	
	139	20120084866	A1	2012-04-05	Stolfo	
	140	20120106354	A1	2012-05-03	Pleshek et al.	
	141	20120113987	A1	2012-05-10	Riddoch et al.	
	142	20120240135	A1	2012-09-20	Risbood et al.	
	143	20120240185	A1	2012-09-20	Kapoor et al.	
	144	20120264443	A1	2012-10-18	Ng et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	145	20120314617	A1	2012-12-13	Erichsen et al.	
	146	20120331543	A1	2012-12-27	Bostrom et al.	
	147	20130047020	A1	2013-02-21	Hershko et al.	
	148	20130059527	A1	2013-03-07	HASESAKA et al.	
	149	20130061294	A1	2013-03-07	Kenworthy	
	150	20130104236	A1	2013-04-25	RAY et al.	
	151	20130117852	A1	2013-05-09	Stute	
	152	20130139236	A1	2013-05-30	Rubinstein et al.	
	153	20130254766	A1	2013-09-26	Zuo et al.	
	154	20130291100	A1	2013-10-31	Ganapathy et al.	
	155	20130305311	A1	2013-11-14	Puttaswamy Naga et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	156	20140075510	A1	2014-03-13	Sonoda et al.	
	157	20140082204	A1	2014-03-20	Shankar et al.	
	158	20140082730	A1	2014-03-20	VASHIST et al.	
	159	20140115654	A1	2014-04-24	Rogers et al.	
	160	20140150051	A1	2014-05-29	Bharali et al.	
	161	20140201123	A1	2014-07-17	Ahn et al.	
	162	20140215561	A1	2014-07-31	Roberson et al.	
	163	20140215574	A1	2014-07-31	Erb et al.	
	164	20140259170	A1	2014-09-11	Amsler	
	165	20140281030	A1	2014-09-18	Cui et al.	
	166	20140283004	A1	2014-09-18	Moore	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	167	20140283030	A1	2014-09-18	Moore et al.	
	168	20140317397	A1	2014-10-23	Martini	
	169	20140337613	A1	2014-11-13	Martini	
	170	20140366132	A1	2014-12-11	Stiansen et al.	
	171	20150033336	A1	2015-01-29	Wang et al.	
	172	20150106930	A1	2015-04-16	HONDA et al.	
	173	20150128274	A1	2015-05-07	Giokas	
	174	20150135325	A1	2015-05-14	Stevens et al.	
	175	20150207809	A1	2015-07-23	MACAULAY	
	176	20150237012	A1	2015-08-20	Moore	
	177	20150244734	A1	2015-08-27	Olson et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	178	20150256431	A1	2015-09-10	Buchanan et al.	
	179	20150304354	A1	2015-10-22	Rogers et al.	
	180	20150334125	A1	2015-11-19	BARTOS et al.	
	181	20150341389	A1	2015-11-26	KURAKAMI	
	182	20150350229	A1	2015-12-03	Mitchell	
	183	20150372977	A1	2015-12-24	Yin	
	184	20150373043	A1	2015-12-24	Wang et al.	
	185	20160020968	A1	2016-01-21	Aumann et al.	
	186	20160028751	A1	2016-01-28	Cruz Mota et al.	
	187	20160065611	A1	2016-03-03	Fakeri-Tabrizi et al.	
	188	20160112443	A1	2016-04-21	GROSSMAN et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	189	20160119365	A1	2016-04-28	Barel	
	190	20160191558	A1	2016-06-30	DAVISON	
	191	20160205069	A1	2016-07-14	Blocher et al.	
	192	20160219065	A1	2016-07-28	Dasgupta et al.	
	193	20160285706	A1	2016-09-29	RAO	
	194	20160294870	A1	2016-10-06	Banerjee et al.	
	195	20160366099	A1	2016-12-15	Jordan	
	196	20170223046	A1	2017-08-03	Singh	
	197	20170272469	A1	2017-09-21	Kraemer et al.	
	198	20150347246	A1	2015-12-03	MATSUI et al.	
	199	20120110656	A1	2012-05-03	Santos et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	200	20090144819	A1	2009-06-04	BABBAR et al.	
	201	20130007257	A1	2013-01-03	Ramaraj et al.	
	202	20160127417	A1	2016-05-05	Janssen	
	203	20040181690	A1	2004-09-16	Rothermel et al.	
	204	20140317737	A1	2014-10-23	SHIN et al.	
	205	20070147380	A1	2007-06-28	ORMAZABAL et al.	
	206	20140245423	A1	2014-08-28	Lee	
	207	20110154470	A1	2011-06-23	Grimes et al.	
	208	20150052601	A1	2015-02-19	White et al.	
	209	20140365372	A1	2014-12-11	Ross et al.	

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

FOREIGN PATENT DOCUMENTS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	16728766
Filing Date	2019-12-27
First Named Inventor	Steven Rogers
Art Unit	2438
Examiner Name	K. W. Chang
Attorney Docket Number	007742.00151\US

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		
	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		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	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		
	17	2007109541	WO	A2	2007-09-27	Brubaker, Curtis		

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	"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>	
	2	2006 Sept 11 - (WO) Written Opinion of the International Searching Authority - App PCT/US05/47008	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	3	2007 Aug 31 - (EP) Communication Pursuant to Rules 109 and 110 - App 05857614.1	
	4	2008 Jul 03 - (WO) Written Opinion of the International Searching Authority - App PCT/US06/11291	
	5	2009 Jun 24 - (US) Office Action - App 11/390,976	
	6	2009 Sept 14 (US) Office Action - App 11/316,331	
	7	2010 Apr 29 - (US) Interview Summary - App 11/390,976	
	8	2010 Aug 20 - (AU) Office Action - App 2005328336	
	9	2010 Jun 23 - (US) Final Rejection - App 11/316,331	
	10	2010 Mar 26 - (US) Final Rejection - App 11/390,976	
	11	2010 Sept 10 - (AU) Office Action - App 2006230171	
	12	2010 Sept 30 - (US) Office Action - App 11/390,976	
	13	2011 Apr 27 - (WO) International Search Report and Written Opinion - App PCT/US2010/054520	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	14	2011 Aug 25 - (US) Non Final Rejection - App 12/871,806	
	15	2011 Feb 14 - (EP) Search Report - App 06758213.0	
	16	2011 Jun 09 - (US) Notice of Allowance - App 11/390,976	
	17	2011 Mar 03 - (EP) Communication Pursuant to Rules 70(2) and 70a(2) - App 06758213.0	
	18	2011 Mar 04 - (US) Notice of Allowance - App 11/316,331	
	19	2011 Nov 11 - (AU) Second Office Action - App 2006230171	
	20	2011 Oct 18 - (EP) Communication Pursuant to Article 94(3) - App 06 758 213.0	
	21	2012 Aug 07 - (US) Non Final Rejection - App 12/871,806	
	22	2012 Feb 06 - (US) Final Rejection - App 12/871,806	
	23	2012 Jun 09 - (AU) Notice of Acceptance - App 2006230171	
	24	2012 Jun 26 - (EP) Extended Search Report - App 05857614.1	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	25	2012 Nov 20 - (EP) Communication under rule 71(3) - App 06 758 213.0	
	26	2012 Nov 26 - (US) Final Rejection - App 12/871,806	
	27	2013 Apr 04 - (US) Notice of Allowance - App 12/871,806	
	28	2013 Apr 18 - (EP) Decision to Grant a European Patent - App 06758212.0	
	29	2013 Jan 16 - (CA) Office Action - App 2,594,020	
	30	2013 Jan 17 - (CA) Office Action - App 2,600,236	
	31	2013 Nov 7 (WO) International Search Report - App. PCT/US2013/057502	
	32	2014 Jun 24 (WO) International Search Report - App. PCT/US2014/023286	
	33	2014 Jun 26 (WO) International Search Report - App. PCT/US2014/027723	
	34	2014 Mar 24 (WO) International Search Report - App. PCT/US2013/072566	
	35	2014 May 26 - (CA) Office Action - App 2010297968	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	36	2015 Apr 28 (WO) International Preliminary Report on Patentability - App. PCT/US2013/057502, dated April 28, 2015.	
	37	2015 Dec 22 - (US) Final Office Action - App 14/714,207	
	38	2015 Jan 14 - (EP) Extended Search Report - App 10819667.6	
	39	2015 Jul 10 - (WO) Communication Relating to the Results of the Partial International Search for International App - PCT/US2015/024691	
	40	2015 Jul 14 - (WO) International Preliminary Report on Patentability - App PCT/US2013/072566	
	41	2015 May 14 - (US) Non Final Rejection - App 13/940,240	
	42	2015 May 25 - (AU) Notice of Acceptance - App 2010297968	
	43	2015 Nov 02 - (AU) Office Action - App 2013372879	
	44	2015 Nov 27 - (US) Final Rejection - App 13/940,240	
	45	2015 Sept 15 (WO) International Preliminary Report on Patentability - App. - PCT/US2014/027723.	
	46	2015 Sept 15 (WO) International Preliminary Report on Patentability - App. PCT/US2014/023286.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\US

	47	2015 Sept 16 (WO) International Search Report and Written Opinion - App. No. PCT/US2015/024691.	
	48	2015 Sept 4 (US) Notice of Allowance - App. 14/702,755 (007742.00036)	
	49	2016 Apr 15 - (US) Notice of Allowance - App 14/855,374	
	50	2016 Apr 26 - (US) Office Action - App 14/745,207	

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	16728766
	Filing Date	2019-12-27
	First Named Inventor	Steven Rogers
	Art Unit	2438
	Examiner Name	K. W. Chang
	Attorney Docket Number	007742.00151\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	/Scott M Kelly/	Date (YYYY-MM-DD)	2020-03-25
Name/Print	Scott M. Kelly	Registration Number	65,121

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.

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 NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/728,766	12/27/2019	Steven Rogers	007742.00151\US	8018

22907 7590 01/27/2020

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

EXAMINER	

ART UNIT	PAPER NUMBER
2438	

NOTIFICATION DATE	DELIVERY MODE
01/27/2020	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

GPD@bannerwitcoff.com
eofficeaction@bannerwitcoff.com

Decision Granting Request for Prioritized Examination (Track I)	**Application No.** 16/728,766	**Applicant(s)** Rogers et al.	
	Examiner CHERYL P GIBSON BAYLOR	**Art Unit** OPET	**AIA (FITF) Status** No

1. THE REQUEST FILED 27 December 2019 IS **GRANTED** .

   The above-identified application has met the requirements for prioritized examination
   - A. ☑ for an original nonprovisional application (Track I).
   - B. ☐ for an application undergoing continued examination (RCE).

2. **The above-identified application will undergo prioritized examination**. The application will be accorded special status throughout its entire course of prosecution until one of the following occurs:
   - A. filing a **petition for extension of time** to extend the time period for filing a reply;
   - B. filing an **amendment to amend the application to contain more than four independent claims, more than thirty total claims** , or a multiple dependent claim;
   - C. filing a **request for continued examination** ;
   - D. filing a notice of appeal;
   - E. filing a request for suspension of action;
   - F. mailing of a notice of allowance;
   - G. mailing of a final Office action;
   - H. completion of examination as defined in 37 CFR 41.102; or
   - I. abandonment of the application.

Telephone inquiries with regard to this decision should be directed to CHERYL GIBSON BAYLOR at (571)272-3213. In his/her absence, calls may be directed to Petition Help Desk at (571) 272-3282.

/CHERYL GIBSON BAYLOR/ Paralegal Specialist, OPET	

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
16/728,766	12/27/2019		1365	007742.00151\US	27	4

CONFIRMATION NO. 8018

FILING RECEIPT

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

OC000000114081170

Date Mailed: 01/23/2020

Receipt is acknowledged of this non-provisional utility 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 FIRST INVENTOR, 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 corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction 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 provided that the request is grantable.

Inventor(s)

Steven Rogers, Leesburg, VA;
Sean Moore, Hollis, NH;

Applicant(s)

Centripetal Networks, Inc., Portsmouth, NH;

Power of Attorney: The patent practitioners associated with Customer Number 22907

Domestic Priority data as claimed by applicant

This application is a CON of 16/111,524 08/24/2018
which is a CON of 15/413,834 01/24/2017 PAT 10091246
which is a CON of 14/698,560 04/28/2015 PAT 9560077
which is a CON of 13/657,010 10/22/2012 PAT 9137205

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: 01/21/2020

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 16/728,766**

Projected Publication Date: 04/30/2020

Non-Publication Request: No

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

METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK

Preliminary Class

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.

Keysight Technologies Ex. 1002
Page 392 of 460

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 16/728,766

APPLICATION AS FILED - PART I

	(Column 1)		(Column 2)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED		NUMBER EXTRA	RATE($)	FEE($)		RATE($)	FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A		N/A	N/A	75		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A		N/A	N/A	330		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A		N/A	N/A	380		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	27	minus 20 =	* 7	x 50 =	350	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	4	minus 3 =	* 1	x 230 =	230			
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	1365		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
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)		(Column 2)	(Column 3)					
		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		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.

Doc Code: TRACK1.REQ
Document Description: TrackOne Request

PTO/AIA/424 (04-14)

CERTIFICATION AND REQUEST FOR PRIORITIZED EXAMINATION UNDER 37 CFR 1.102(e) (Page 1 of 1)

First Named Inventor:	Steven Rogers	Nonprovisional Application Number (if known):	Not Yet Assigned
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK		

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS PRIORITIZED EXAMINATION FOR THE ABOVE-IDENTIFIED APPLICATION.

1. The processing fee set forth in 37 CFR 1.17(i)(1) and the prioritized examination fee set forth in 37 CFR 1.17(c) have been filed with the request. The publication fee requirement is met because that fee, set forth in 37 CFR 1.18(d), is currently $0. The basic filing fee, search fee, and examination fee are filed with the request or have been already been paid. I understand that any required excess claims fees or application size fee must be paid for the application.
2. I understand that the application may not contain, or be amended to contain, more than four independent claims, more than thirty total claims, or any multiple dependent claims, and that any request for an extension of time will cause an outstanding Track I request to be dismissed.
3. The applicable box is checked below:

I. [x] **Original Application (Track One) - Prioritized Examination under § 1.102(e)(1)**

i. (a) The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a). This certification and request is being filed with the utility application via EFS-Web.

---OR---

(b) The application is an original nonprovisional plant application filed under 35 U.S.C. 111(a). This certification and request is being filed with the plant application in paper.

ii. An executed inventor's oath or declaration under 37 CFR 1.63 or 37 CFR 1.64 for each inventor, **or** the application data sheet meeting the conditions specified in 37 CFR 1.53(f)(3)(i) is filed with the application.

II. [ ] **Request for Continued Examination - Prioritized Examination under § 1.102(e)(2)**

i. A request for continued examination has been filed with, or prior to, this form.
ii. If the application is a utility application, this certification and request is being filed via EFS-Web.
iii. The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a), or is a national stage entry under 35 U.S.C. 371.
iv. This certification and request is being filed prior to the mailing of a first Office action responsive to the request for continued examination.
v. No prior request for continued examination has been granted prioritized examination status under 37 CFR 1.102(e)(2).

Signature	/Scott M Kelly/	Date	December 27, 2019
Name (Print/Typed)	Scott M. Kelly	Practitioner Registration Number	65,121

Note: *This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required.**

[x] *Total of 1 forms are submitted.

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Filer:	Scott M Kelly/Tanika LaFortune
Attorney Docket Number:	007742.00151\US

Filed as Small Entity

Filing Fees for Track I Prioritized Examination - Nonprovisional Application under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
UTILITY FILING FEE (ELECTRONIC FILING)	4011	1	75	75
UTILITY SEARCH FEE	2111	1	330	330
UTILITY EXAMINATION FEE	2311	1	380	380
REQUEST FOR PRIORITIZED EXAMINATION	2817	1	2000	2000
Pages:				
Claims:				
CLAIMS IN EXCESS OF 20	2202	7	50	350
INDEPENDENT CLAIMS IN EXCESS OF 3	2201	1	230	230

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous-Filing:				
PUBL. FEE- EARLY, VOLUNTARY, OR NORMAL	1504	1	0	0
PROCESSING FEE, EXCEPT PROV. APPLS.	2830	1	70	70
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**3435**

Electronic Acknowledgement Receipt

EFS ID:	38152576
Application Number:	16728766
International Application Number:	
Confirmation Number:	8018
Title of Invention:	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
First Named Inventor/Applicant Name:	Steven Rogers
Customer Number:	22907
Filer:	Scott M Kelly/Tanika LaFortune
Filer Authorized By:	Scott M Kelly
Attorney Docket Number:	007742.00151\US
Receipt Date:	27-DEC-2019
Filing Date:	
Time Stamp:	16:12:06
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$3435
RAM confirmation Number	E2019BQG14056336
Deposit Account	190733
Authorized User	Tanika LaFortune

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

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	Application Data Sheet	Application_Data_Sheet_Fillable_PDF_20207027.pdf	1255818 9029100dcbf1ea7f8593dff90f6f5ca354bc6e33	no	9
Warnings:					
Information:					
2	Power of Attorney	POA_or_Authorization_of_Agent_20207481.pdf	496770 a18c859ba7220c2ebdd2df685579f93c5a037bf8	no	2
Warnings:					
Information:					
3	Drawings-only black and white line drawings	00774200151_Drawings_-_Continuation_of_00123_20208763.PDF	809331 8f2e3c09c1394aa8464d5c22d79f9efd706342a7	no	10
Warnings:					
Information:					
4		7742-151_Continuation_Specification_20209379.pdf	150419 b93c5954f3232c1ce227c9954a57ef1d5370df8d	yes	38

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	29
Claims	30	37
Abstract	38	38

Warnings:					
Information:					
5	Oath or Declaration filed	7742-151_Declarations_from_Parent_20207617.PDF	637339 c5fed7f702d851e3dea30f77e4f78d648a49e2b6	no	2

Warnings:					
Information:					
6	TrackOne Request	Certification_and_Request_for_Prioritized_Examination_20209559.pdf	34182 34a069892418d07d50924e359c7e501b7b7203fa	no	1
Warnings:					
Information:					
7	Fee Worksheet (SB06)	fee-info.pdf	43080 54c770e7ad669587ec54de7054144203d6a37997	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	3426939		

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/14 (02-18)
Approved for use through 11/30/2020. 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	007742.00151\US
	Application Number	
Title of Invention	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK	

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
	Steven		Rogers	

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

City	State/Province	Country of Residence
Leesburg	VA	US

Mailing Address of Inventor:

Address 1	c/o Centripetal Networks, Inc.
Address 2	99 Bow Street, Suite 300W

City	State/Province	Postal Code	Country
Portsmouth	NH	03801	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	State/Province	Country of Residence
Hollis	NH	US

Mailing Address of Inventor:

Address 1	c/o Centripetal Networks, Inc.
Address 2	99 Bow Street, Suite 300W

City	State/Province	Postal Code	Country
Portsmouth	NH	03801	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).

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. 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	007742.00151\US
	Application Number	
Title of Invention	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK	

☐ **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	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK		
Attorney Docket Number	007742.00151\US	**Small Entity Status Claimed**	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)		**Suggested Figure for Publication (if any)**	

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.

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		

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. 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	007742.00151\US
	Application Number	
Title of Invention	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK	

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	Pending			Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)	
	Continuation of	16/111524	2018-08-24	

Prior Application Status	Patented			Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
16/111524	Continuation of	15/413834	2017-01-24	10091246	2018-10-02

Prior Application Status	Patented			Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
15/413834	Continuation of	14/698560	2015-04-28	9560077	2017-01-31

Prior Application Status	Patented			Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14/698560	Continuation of	13/657010	2012-10-22	9137205	2015-09-15

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

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. Add

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. 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	007742.00151\US
	Application Number	
Title of Invention	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK	

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 (02-18)
Approved for use through 11/30/2020. 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	007742.00151\US
	Application Number	
Title of Invention	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK	

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 (02-18)
Approved for use through 11/30/2020. 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	007742.00151\US
	Application Number	
Title of Invention	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK	

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 — Remove

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	c/o Centripetal Networks, Inc.		
Address 2	99 Bow Street, Suite 300W		
City	Portsmouth	**State/Province**	NH
Country	US	Postal Code	03801
Phone Number		Fax Number	
Email Address			

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

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 (02-18)
Approved for use through 11/30/2020. 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	007742.00151\US
	Application Number	
Title of Invention	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK	

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.

Remove

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. Add

Signature:

Remove

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	/Scott M Kelly/			Date (YYYY-MM-DD)	2019-12-27
First Name	Scott	Last Name	Kelly	Registration Number	65,121

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

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. 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	007742.00151\US
	Application Number	
Title of Invention	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK	

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.**

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 records.

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 CooperationTreaty.

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.

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

PTO/AIA/82A (07-13)
Approved for use through 03/31/2021. 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.

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	Not Yet Assigned
Filing Date	Concurrently Herewith
First Named Inventor	Steven Rogers
Title	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	007742.00151\US

SIGNATURE of Applicant or Patent Practitioner

Signature	/Scott M Kelly/	Date (Optional)	December 27, 2019
Name	Scott M. Kelly	Registration Number	65,121
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.

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.

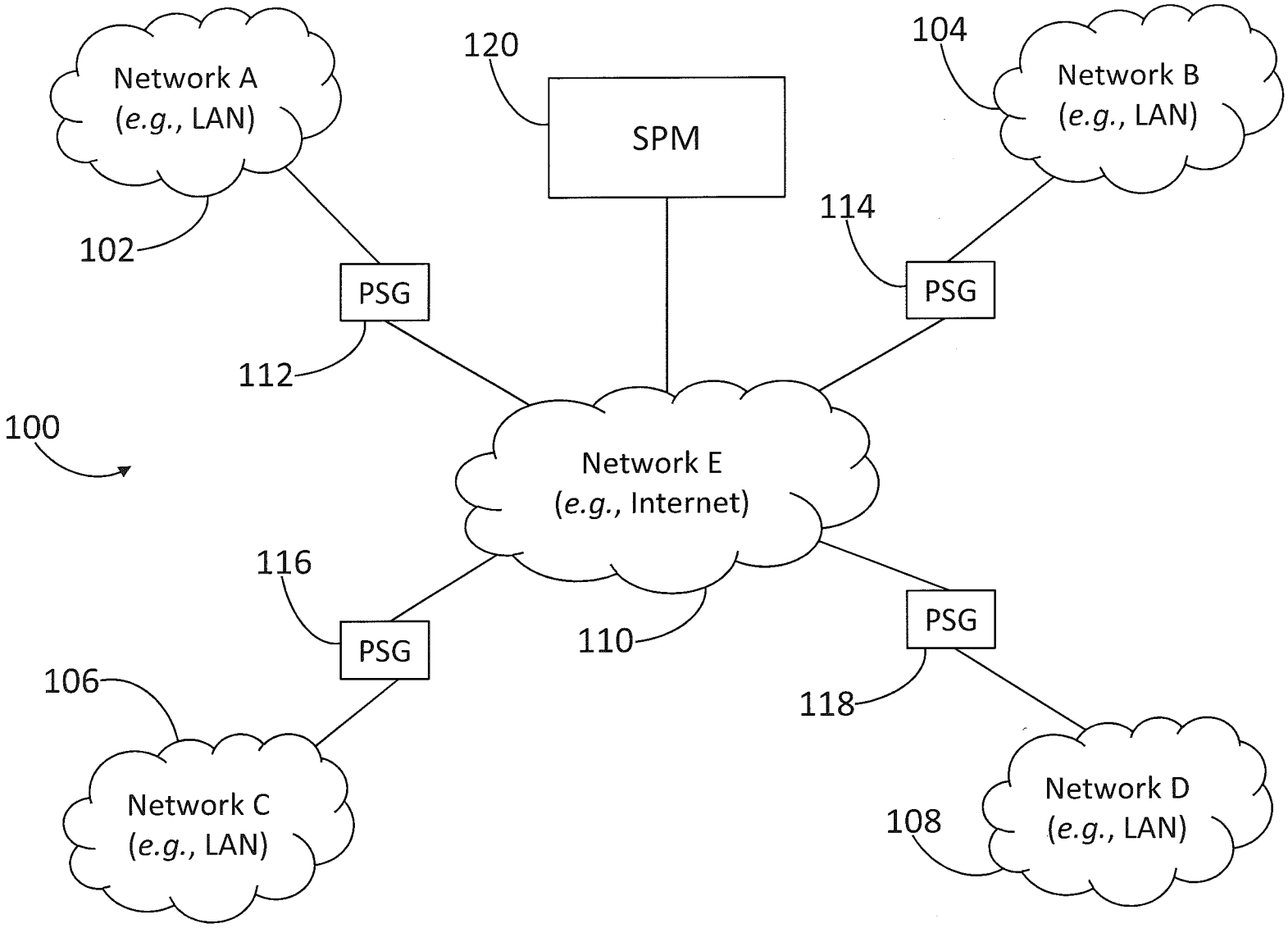

Network A
(e.g., LAN)
102
120
SPM
104
Network B
(e.g., LAN)
114
PSG
PSG
112
100
Network E
(e.g., Internet)
116
PSG
110
PSG
106
118
Network C
(e.g., LAN)
Network D
(e.g., LAN)
108

FIG. 1

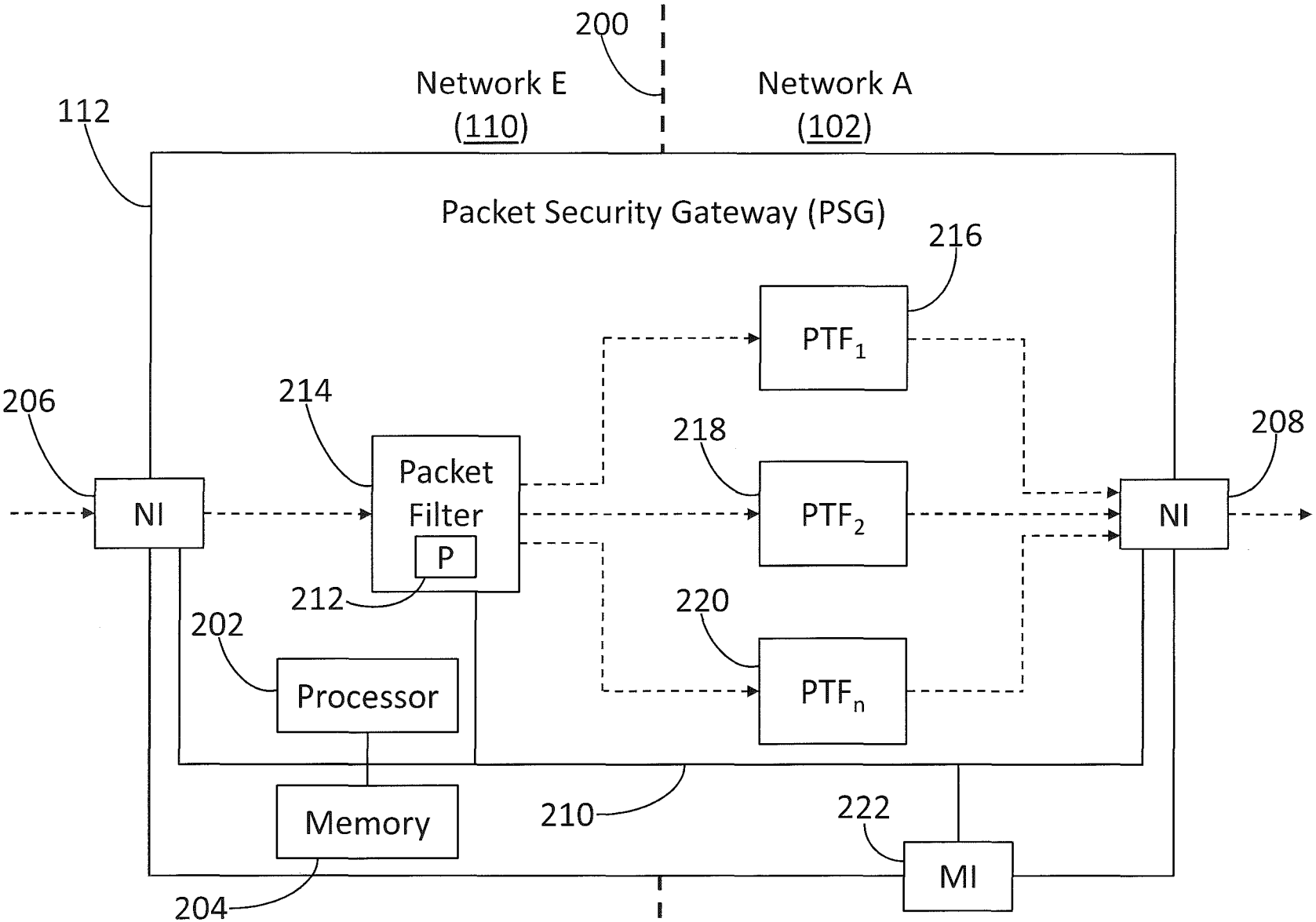
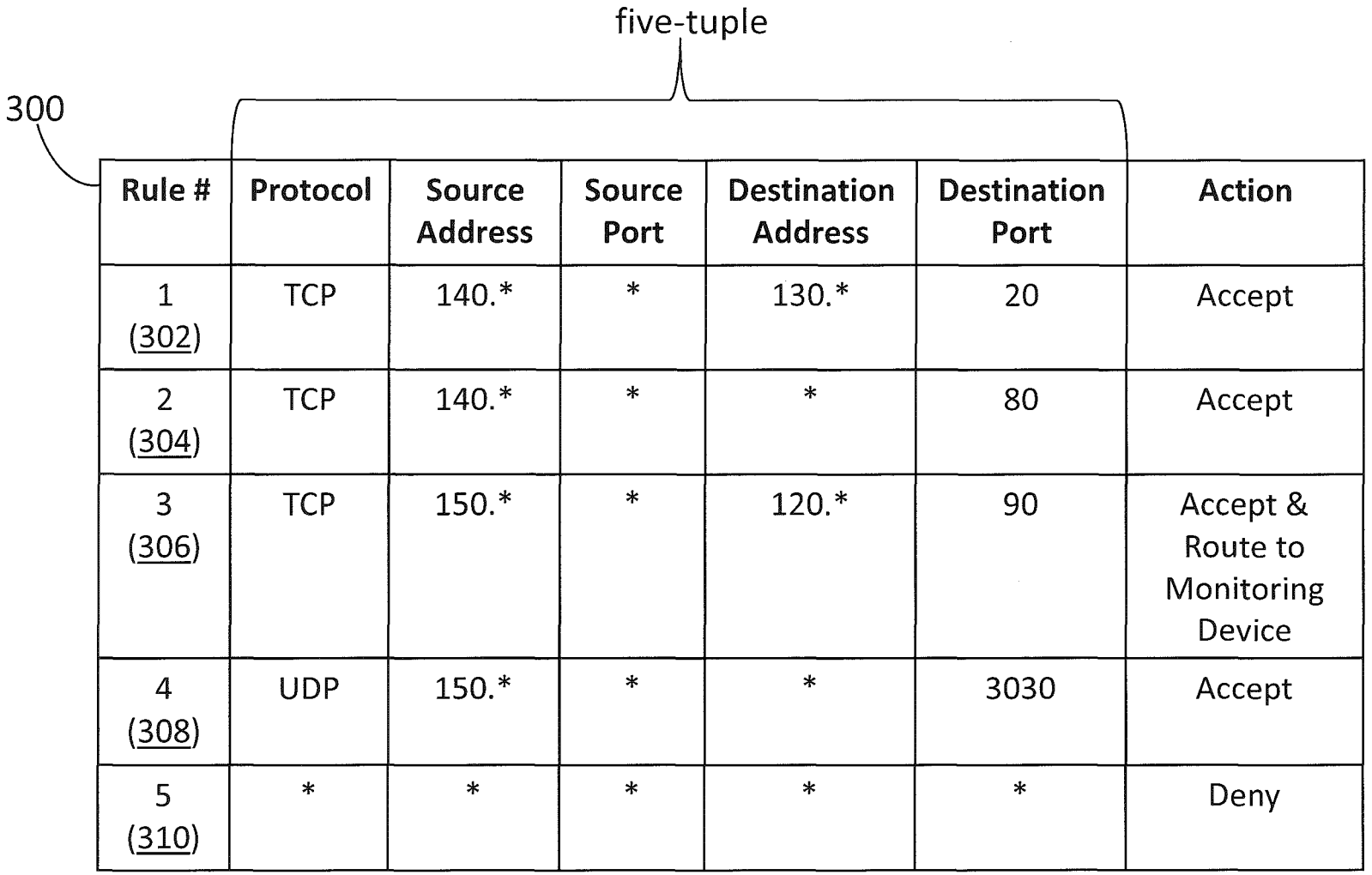


FIG. 2

Inventor(s): Steven Rogers, et al.
Title: METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
Attorney Docket No. 007742.00151
Sheet 2 of 10



Rule #	Protocol	Source Address	Source Port	Destination Address	Destination Port	Action
1 (302)	TCP	140.*	*	130.*	20	Accept
2 (304)	TCP	140.*	*	*	80	Accept
3 (306)	TCP	150.*	*	120.*	90	Accept & Route to Monitoring Device
4 (308)	UDP	150.*	*	*	3030	Accept
5 (310)	*	*	*	*	*	Deny

FIG. 3

Inventor(s): Steven Rogers, et al.
Title: METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK
Attorney Docket No. 007742.00151
Sheet 3 of 10

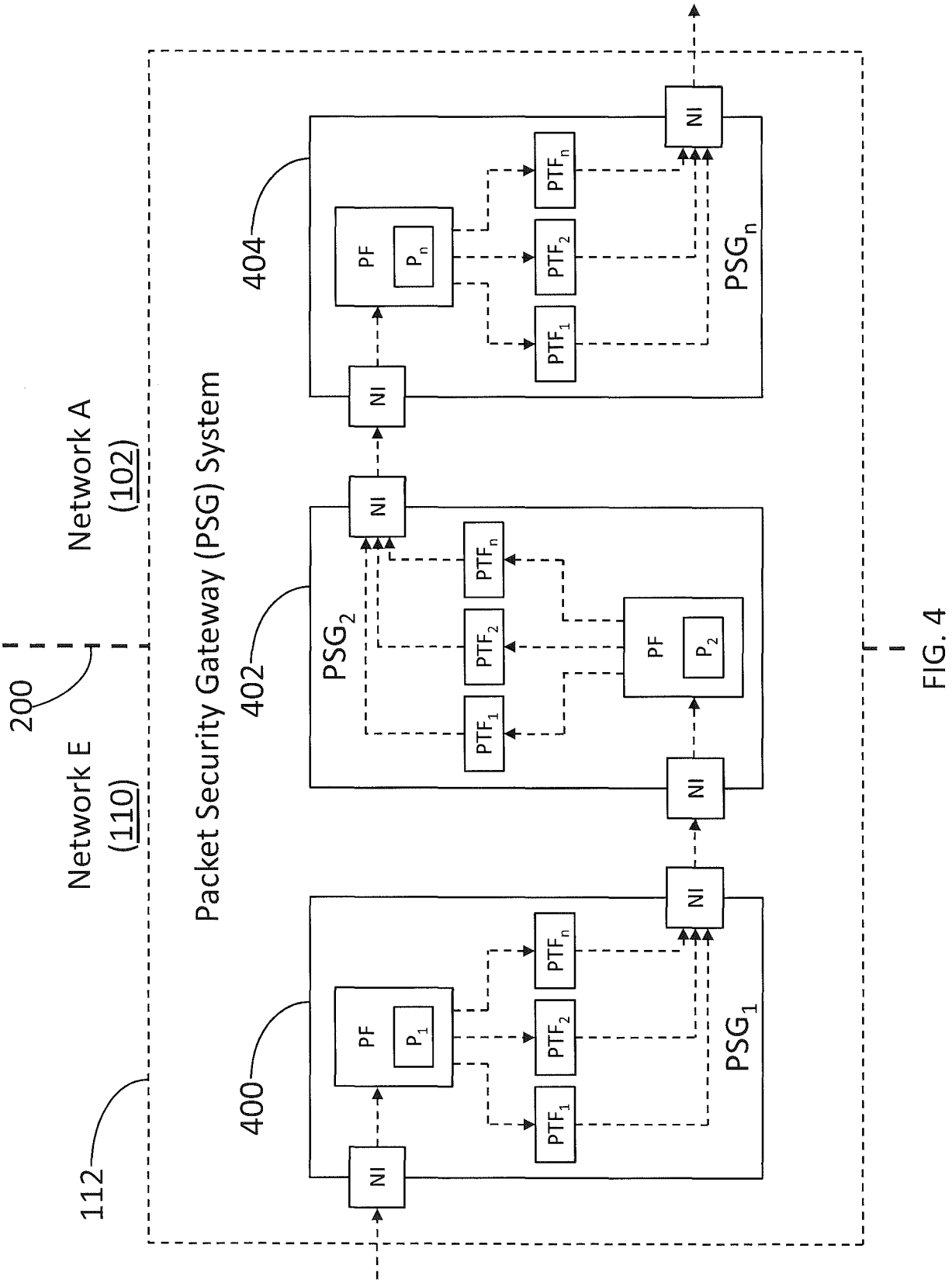

200
Network E
(110)
Network A
(102)
Packet Security Gateway (PSG) System
112
400
402
404
PSG1
PSG2
PSGn
NI
PF
P1
P2
Pn
PTF1
PTF2
PTFn

FIG. 4

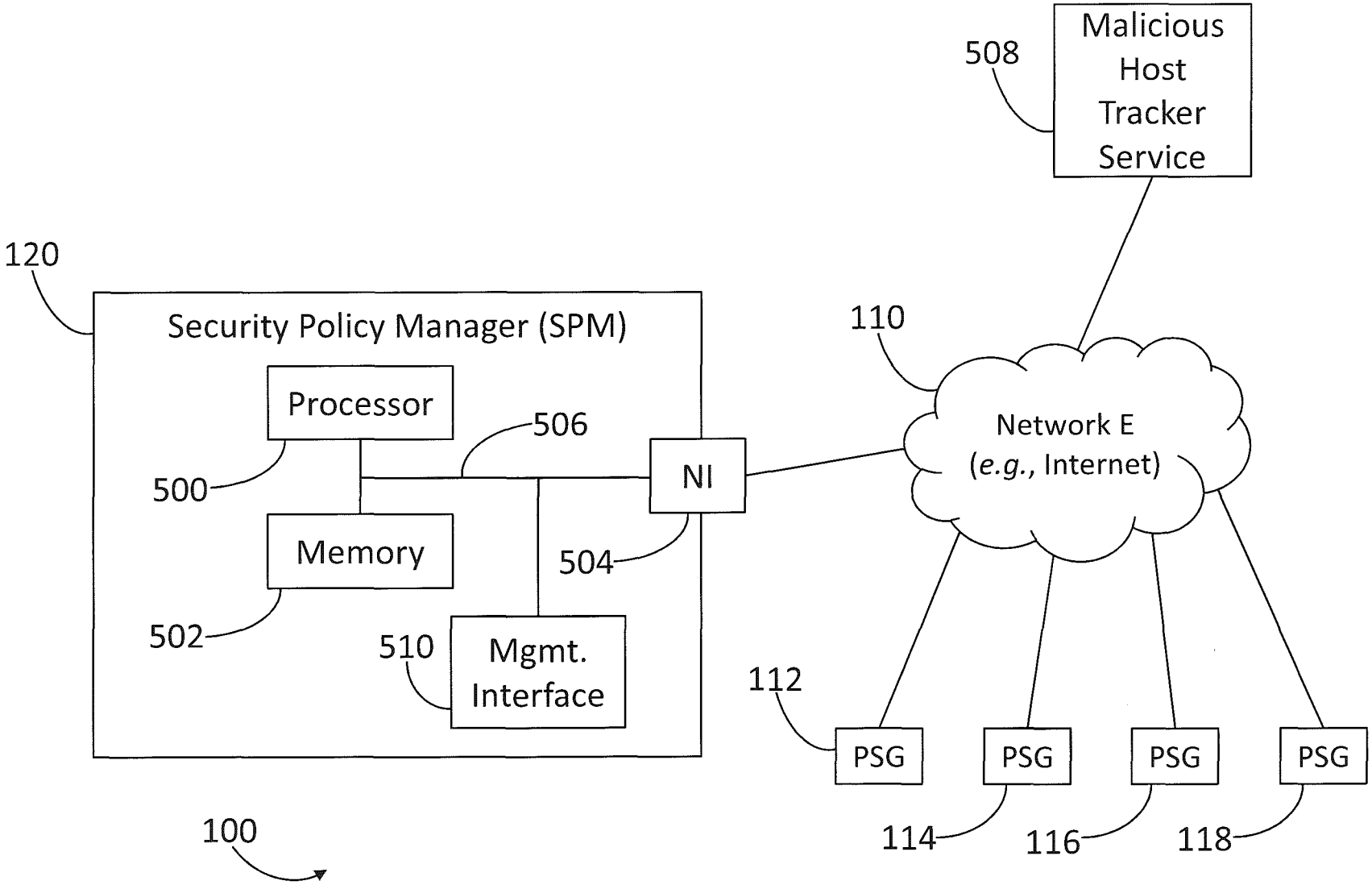

Malicious Host Tracker Service
508
120
Security Policy Manager (SPM)
Processor
506
500
NI
110
Network E (e.g., Internet)
Memory
504
502
510
Mgmt. Interface
112
PSG
PSG
PSG
PSG
114
116
118
100

FIG. 5

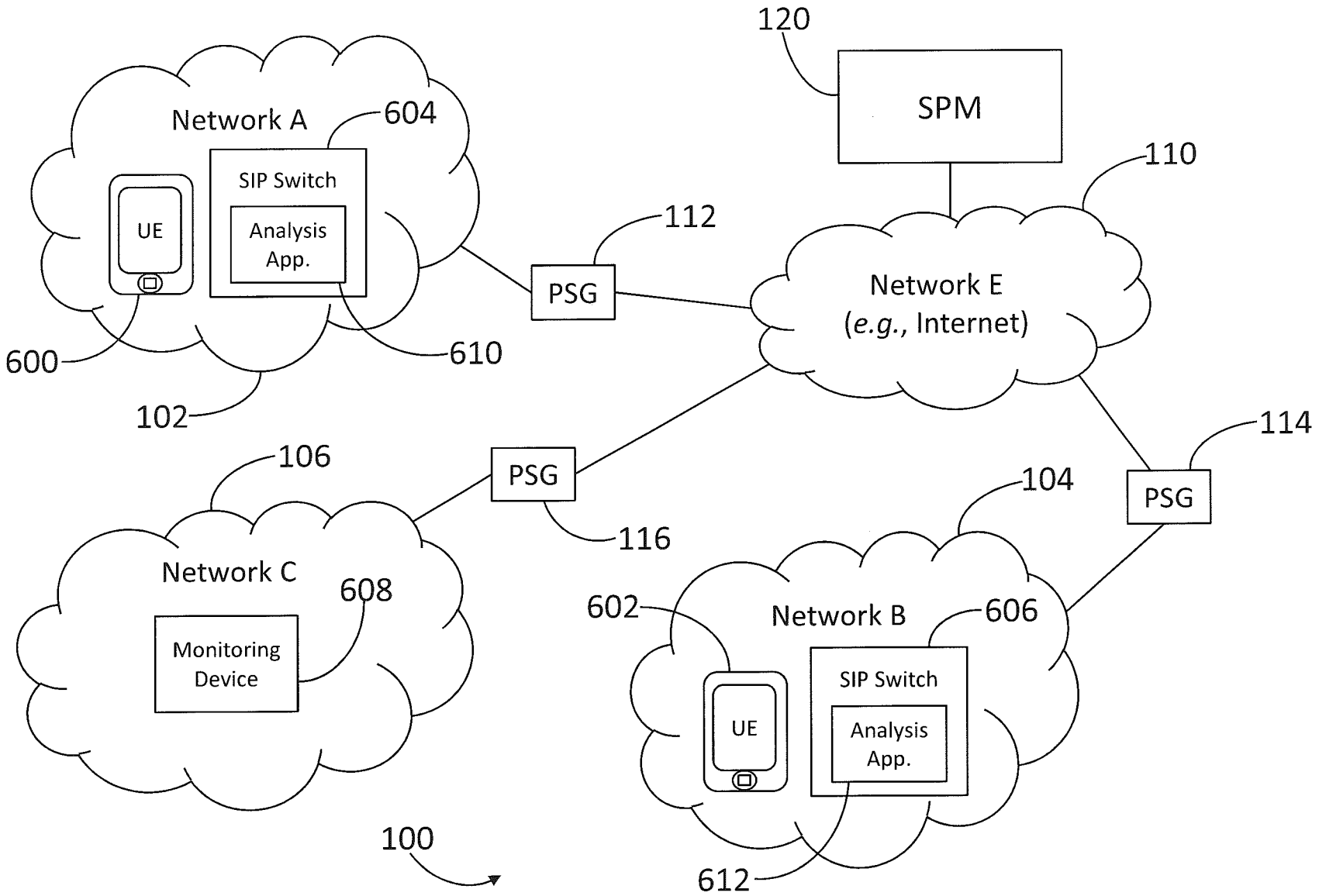

120
SPM
Network A
604
SIP Switch
UE
Analysis App.
110
112
PSG
Network E
(e.g., Internet)
600
610
102
114
106
PSG
PSG
104
116
Network C
608
Monitoring Device
602
Network B
606
SIP Switch
UE
Analysis App.
100
612

FIG. 6

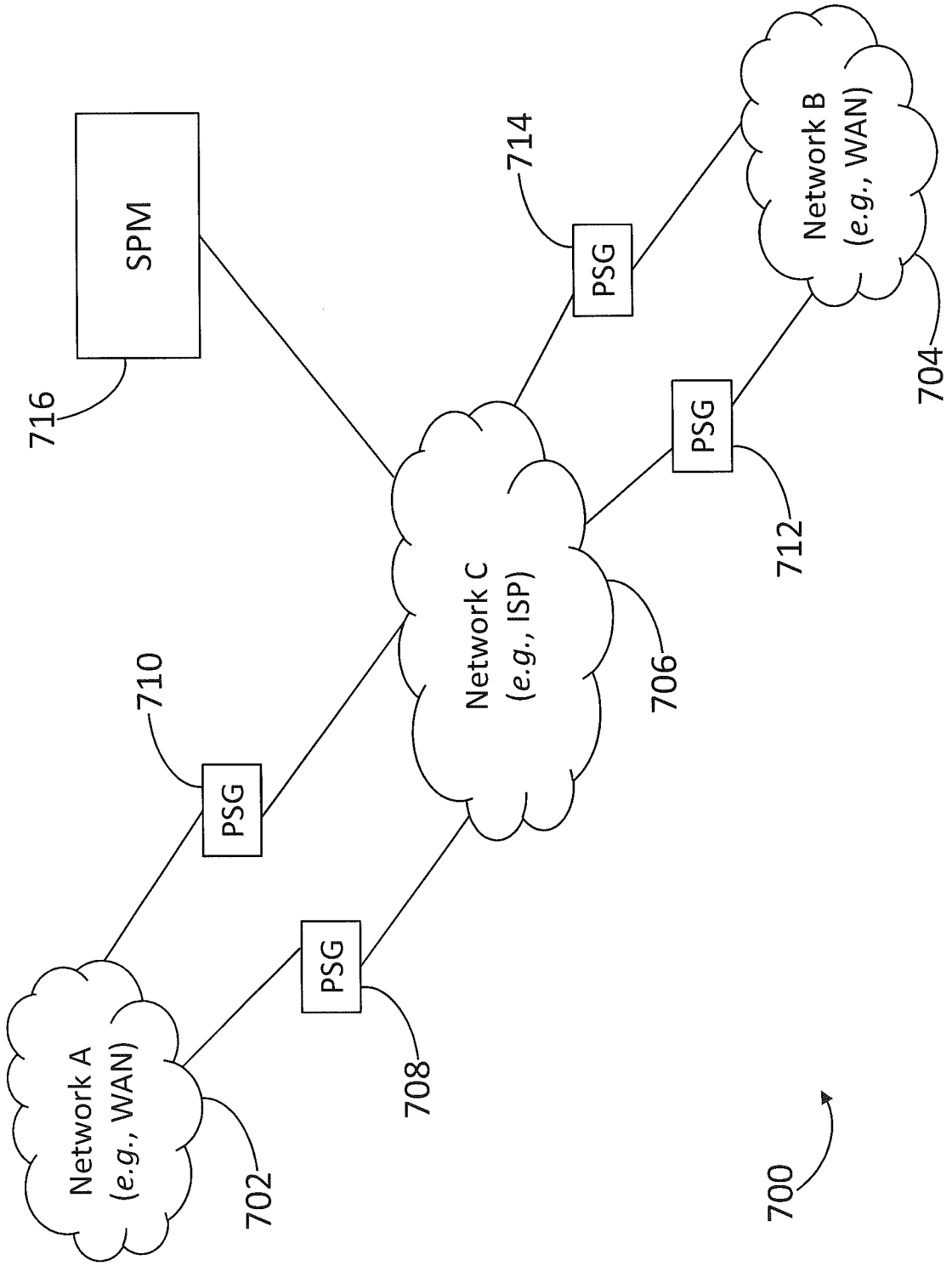

SPM
716
714
PSG
Network B
(e.g., WAN)
704
PSG
712
Network C
(e.g., ISP)
706
710
PSG
PSG
708
Network A
(e.g., WAN)
702
700

FIG. 7

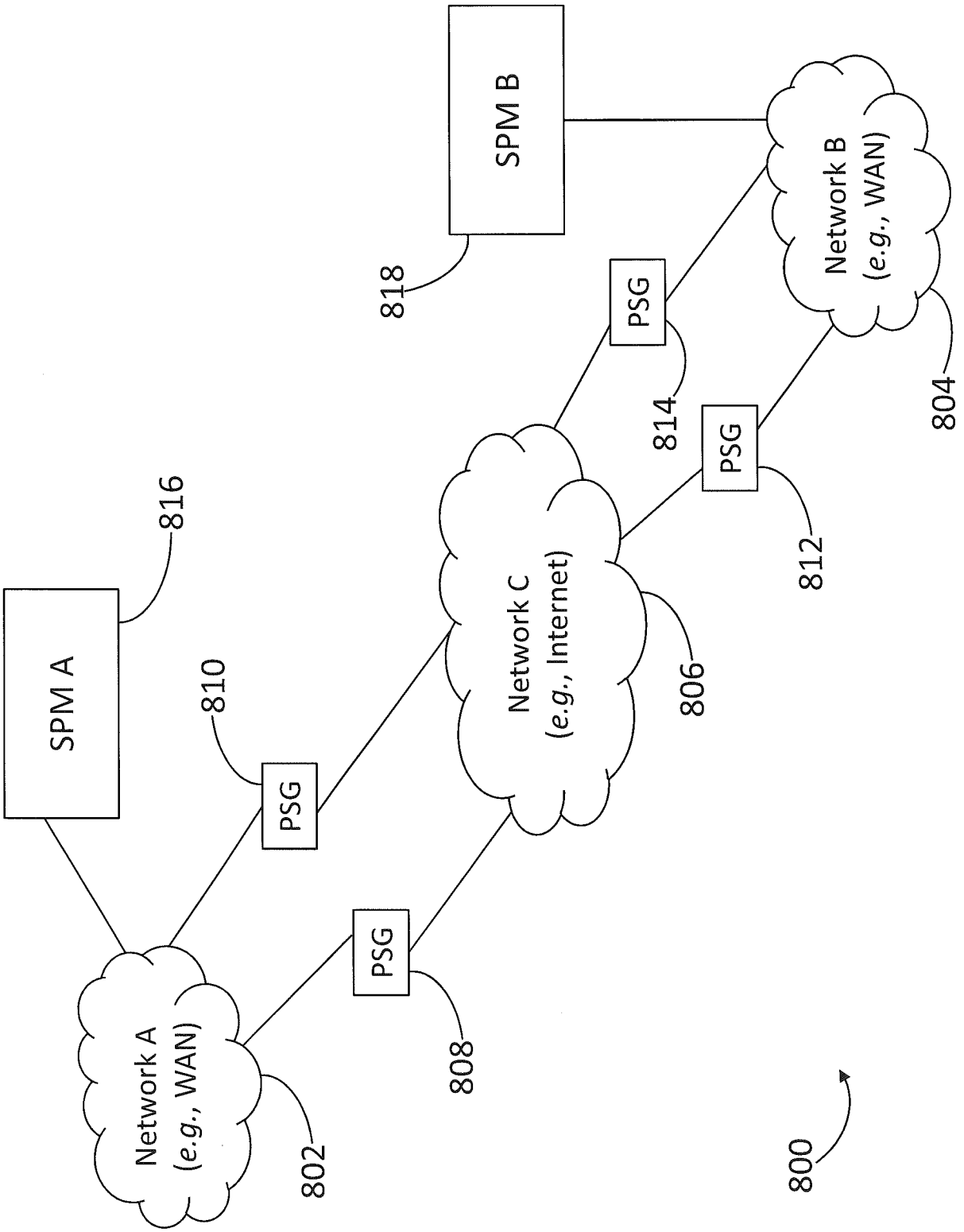

SPM B
818
Network B
(e.g., WAN)
804
PSG
814
PSG
812
816
SPM A
810
PSG
Network C
(e.g., Internet)
806
PSG
808
Network A
(e.g., WAN)
802
800

FIG. 8

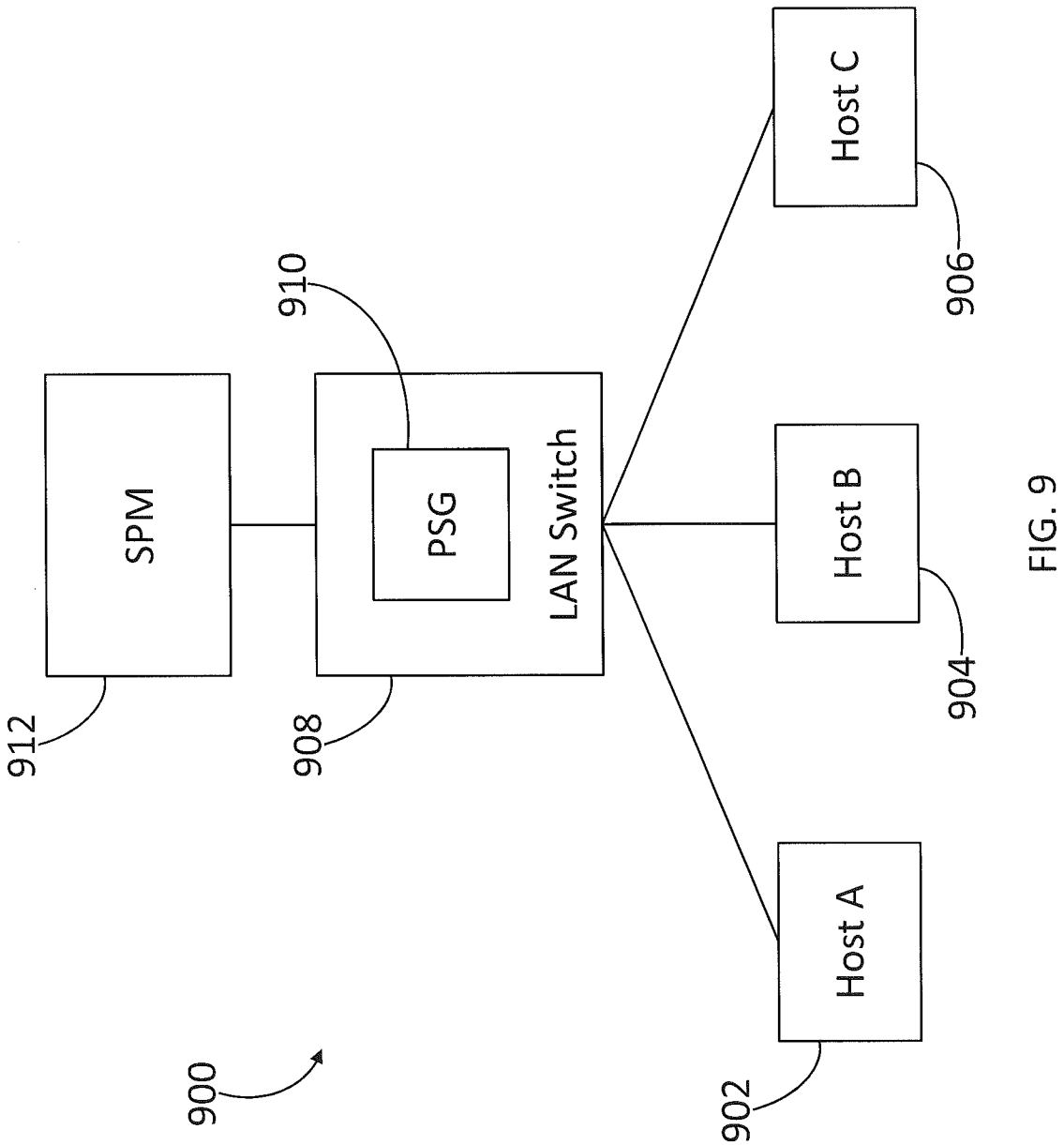

Host C
906
910
SPM
PSG
LAN Switch
Host B
904
912
908
Host A
902
900

FIG. 9

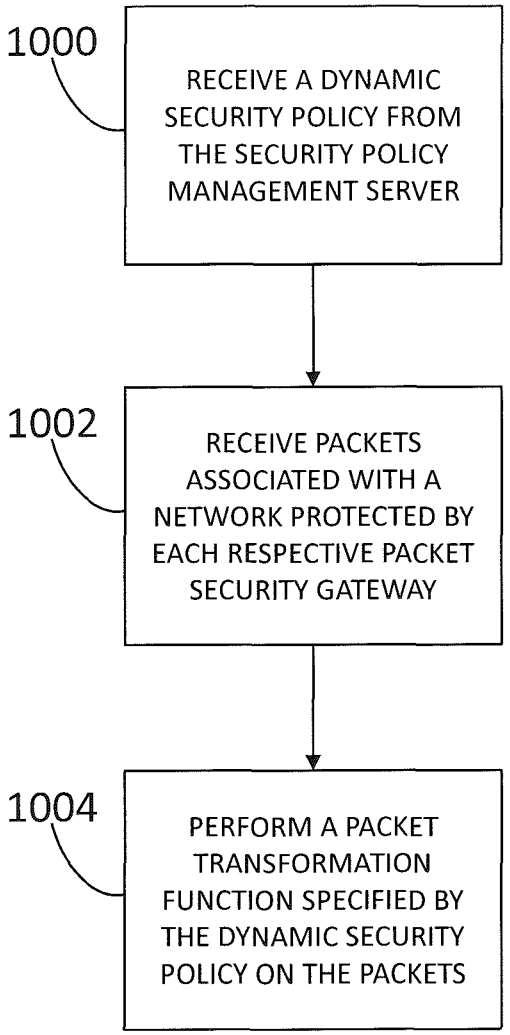

1000
RECEIVE A DYNAMIC SECURITY POLICY FROM THE SECURITY POLICY MANAGEMENT SERVER
1002
RECEIVE PACKETS ASSOCIATED WITH A NETWORK PROTECTED BY EACH RESPECTIVE PACKET SECURITY GATEWAY
1004
PERFORM A PACKET TRANSFORMATION FUNCTION SPECIFIED BY THE DYNAMIC SECURITY POLICY ON THE PACKETS

FIG. 10

METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application is a continuation of co-pending U.S. Patent Application Serial No. 16/111,524, filed November 25, 2019, entitled "METHOD AND SYSTEMS FOR PROTCTING A SECURED NETWORK", which is a continuation of U.S. Patent Application Serial No. 15/413,834, filed January 24, 2017 (now U.S. Patent No. 10,091,246), entitled "METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK," which is a continuation of U.S. Patent Application Serial No. 14/698,560 (now U.S. Patent No. 9,560,077), filed April 28, 2015, entitled "METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK," which is a continuation of U.S. Patent Application Serial No. 13/657,010 (now U.S. Patent No. 9,137,205), filed October 22, 2012, entitled "METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK." The disclosures of each of these applications are incorporated by reference herein in their entirety and made part hereof.

BACKGROUND

[0002] The TCP/IP network protocols (*e.g.*, the Transmission Control Protocol (TCP) and the Internet Protocol (IP)) were designed to build large, resilient, reliable, and robust networks. Such protocols, however, were not originally designed with security in mind. Subsequent developments have extended such protocols to provide for secure communication between peers (*e.g.*, Internet Protocol Security (IPsec)), but the networks themselves remain vulnerable to attack (*e.g.*, Distributed Denial of Service (DDoS) attacks).

[0003] Most existing approaches to protecting such networks are reactive rather than proactive. While reactive approaches may identify the source of an attack and assist in subsequent mitigation efforts, in most instances, the attack will have already been successfully launched.

[0004] Proactive solutions, however, have often been deemed untenable due to an inability to scale to larger networks. A significant challenge associated with building a scalable proactive solution is the need to filter substantially all network traffic at a high resolution. In a large network,

where traffic volumes may be enormous, the time required to provide high resolution filtering has traditionally been thought to render a proactive solution infeasible.

SUMMARY

[0005] The following presents a simplified summary in order to provide a basic understanding of some aspects of the disclosure. It is neither intended to identify key or critical elements of the disclosure nor to delineate the scope of the disclosure. The following summary merely presents some concepts in a simplified form as a prelude to the description below.

[0006] Aspects of this disclosure relate to protecting a secured network. In some embodiments, one or more packet security gateways are associated with a security policy management server. At each of the packet security gateways, a dynamic security policy may be received from the security policy management server, packets associated with a network protected by the packet security gateway may be received, and at least one of multiple packet transformation functions specified by the dynamic security policy may be performed on the packets. Performing the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets may include performing at least one packet transformation function other than forwarding or dropping the packets.

[0007] In some embodiments, two or more of the packet security gateways may be configured in series such that packets forwarded from a first of the packet security gateways are received by a second of the packet security gateways. In some embodiments, the dynamic security policy may include two rules requiring sequential execution. A first of the packet security gateways may perform a packet transformation function specified by one of the rules on the packets and a second of the packet security gateways may subsequently perform a packet transformation function specified by the other of the rules on packets received from the first packet security gateway.

[0008] In some embodiments, the dynamic security policy may include a rule specifying a set of network addresses for which associated packets should be dropped and a rule specifying that all packets associated with network addresses outside the set should be forwarded. Additionally or alternatively, the dynamic security policy may include a rule specifying a set of network addresses for which associated packets should be forwarded and a rule specifying that all packets associated with network addresses outside the set should be dropped. In some embodiments, the security

policy management server may receive information associated with one or more Voice over Internet Protocol (VoIP) sessions and the set of network addresses for which associated packets should be forwarded may be created or altered utilizing the information associated with the one or more VoIP sessions.

[0009] In some embodiments, the packet security gateways may receive three or more dynamic security policies from the security policy management server. A first of the dynamic security policies may specify a first set of network addresses for which packets should be forwarded. A second of the dynamic security policies may be received after the first and may specify a second set of network addresses, which includes more network addresses than the first set, for which packets should be forwarded. A third of the dynamic security policies may be received after the second and may specify a third set of network addresses, which includes more network addresses than the second set, for which packets should be forwarded.

[0010] In some embodiments, the dynamic security policy may include two rules that each specify a set of network addresses. The dynamic security policy may specify that packets associated with the first set of network addresses should be placed in a first forwarding queue and packets associated with the second set of network addresses should be placed in a second forwarding queue. The first forwarding queue may have a different queueing policy, for example, a higher forwarding rate, than the second forwarding queue.

[0011] In some embodiments, the dynamic security policy may include a rule specifying a set of network addresses and an additional parameter. The packet transformation function specified by the dynamic security policy may include routing packets that fall within the specified set and match the additional parameter to a network address different from a destination network address specified by the packets. In some embodiments, the additional parameter may be a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI). The network address different from the destination network address may correspond to a device configured to copy information contained within the packets and forward the packets to the destination network address specified by the packets.

[0012] In some embodiments, the packet transformation function may forward the packets into the network protected by the packet security gateway. In some embodiments, the packet

transformation function may forward the packets out of the network protected by the packet security gateway. In some embodiments, the packet transformation function may forward the one or more packets to an IPsec stack having an IPsec security association corresponding to the packets. In some embodiments, the packet transformation function may drop the packets.

[0013] In some embodiments, the dynamic security policy may include multiple rules. One of the rules may specify the packet transformation function. In some embodiments, one of the rules may specify a five-tuple of values selected from packet header information. The five-tuple may specify one or more protocol types, one or more IP source addresses, one or more source ports, one or more IP destination addresses, and one or more destination ports. In some embodiments, one of the rules may specify a Differentiated Service Code Point (DSCP) that maps to a DSCP field in an IP header of one of the packets.

[0014] In some embodiments, one of the packet security gateways may operate in a network layer transparent manner. For example, the packet security gateway may send and receive traffic at a link layer using an interface that is not addressed at the network layer and simultaneously perform the packet transformation function at the network layer. Additionally or alternatively, the packet security gateway may include a management interface having a network layer address. Access to the management interface may be secured at the application level.

[0015] In some embodiments, the dynamic security policy may include a rule generated based, at least in part, on a list of known network addresses associated with malicious network traffic. In some embodiments, the list of known network addresses associated with malicious network traffic may be received from a subscription service that aggregates information associated with malicious network traffic.

[0016] In some embodiments, the packets associated with the network protected by the packet security gateway may originate within the network protected by the packet security gateway and may be destined for a network distinct from the network protected by the packet security gateway. Additionally or alternatively, the packets associated with the network protected by the packet security gateway may originate within a network distinct from the network protected by the packet security gateway and may be destined for a host within the network protected by the packet security gateway.

[0017] In some embodiments, one of the packet security gateways may be located at each boundary between a protected network associated with the security policy management server and an unprotected network.

[0018] Other details and features will be described in the sections that follow.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019] 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.

[0020] 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.

[0021] FIG. 1 illustrates an exemplary network environment in which one or more aspects of the disclosure may be implemented.

[0022] FIG. 2 illustrates an exemplary packet security gateway.

[0023] FIG. 3 illustrates an exemplary dynamic security policy.

[0024] FIG. 4 illustrates an exemplary configuration of multiple packet security gateways in series.

[0025] FIG. 5 illustrates an exemplary security policy management server.

[0026] FIG. 6 illustrates an exemplary network environment for implementing a monitoring service.

[0027] FIG. 7 illustrates an exemplary network environment that includes a secured network having multiple boundaries with unsecured networks.

[0028] FIG. 8 illustrates an exemplary network environment that includes multiple distinct secured networks.

[0029] FIG. 9 illustrates an exemplary secure LAN environment.

[0030] FIG. 10 illustrates an exemplary method for protecting a secured network.

Keysight Technologies Ex. 1002
Page 425 of 460

DETAILED DESCRIPTION

[0031] 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 present disclosure.

[0032] 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.

[0033] FIG. 1 illustrates an exemplary network environment in which one or more aspects of the disclosure may be implemented. Referring to FIG. 1, network environment **100** may include networks A – E **102**, **104**, **106**, **108**, and **110**. One or more networks within network environment **100** may be a Local Area Network (LAN) or a Wide Area Network (WAN). Such a LAN or WAN may be associated, for example, with an organization (*e.g.*, a company, university, enterprise, or government agency). For example, networks A – D **102**, **104**, **106**, and **108** may be LANs, any combination of which may be associated with one or more organizations. One or more networks within network environment **100** may interface with one or more other networks within network environment **100**. For example, network environment **100** may include a WAN that interfaces one or more LANs within network environment **100** or network environment **100** may include one or more Internet Service Providers (ISPs) that interface one or more LANs or WANs within network environment **100** via the Internet. For example, network E **110** may comprise the Internet and may interface networks A – D **102**, **104**, **106**, and **108**.

[0034] As used herein, a packet security gateway includes any computing device configured to receive packets and perform a packet transformation function on the packets. Optionally, a packet security gateway may further be configured to perform one or more additional functions as described herein. As used herein, a security policy management server includes any computing device configured to communicate a dynamic security policy to a packet security gateway. Optionally, a security policy management server may further be configured to perform one or more additional functions as described herein. As used herein, a dynamic security policy includes any

rule, message, instruction, file, data structure, or the like that specifies criteria corresponding to one or more packets and identifies a packet transformation function to be performed on packets corresponding to the specified criteria. Optionally, a dynamic security policy may further specify one or more additional parameters as described herein.

[0035] Network environment **100** may include one or more packet security gateways and one or more security policy management servers. For example, network environment **100** may include packet security gateways **112**, **114**, **116**, and **118**, and security policy management server **120**. One or more security policy management servers may be associated with a protected network. For example, networks A – D **102**, **104**, **106**, and **108** may each be distinct LANs associated with a common organization and may each form part of a protected network associated with security policy management server **120**. Many network protocols route packets dynamically, and thus the path a given packet may take cannot be readily predicted. Accordingly it may be advantageous to locate a packet security gateway at each boundary between a protected network and an unprotected network. For example, packet security gateway **112** may be located at the boundary between network A **102** and network E **110**. Similarly, packet security gateway **114** may be located at the boundary between network B **104** and network E **110**; packet security gateway **116** may be located at the boundary between network C **106** and network E **110**; and packet security gateway **118** may be located at the boundary between network D **108** and network E **110**. As will be described in greater detail below, each of one or more packet security gateways associated with a security policy management server may be configured to receive a dynamic security policy from the security policy management server, receive packets associated with a network protected by the packet security gateway, and perform a packet transformation function specified by the dynamic security policy on the packets. For example, each of packet security gateways **112**, **114**, **116**, and **118** may be configured to receive a dynamic security policy from security policy management server **120**. Each of packet security gateways **112**, **114**, **116**, and **118** may also be configured to receive packets respectively associated with networks A – D **102**, **104**, **106**, and **108**. Each of packet security gateways **112**, **114**, **116**, and **118** may further be configured to perform a packet transformation function specified by the dynamic security policy received from security policy management server **120** on the packets respectively associated with networks A – D **102**, **104**, **106**, and **108**.

[0036] FIG. 2 illustrates an exemplary packet security gateway according to one or more aspects of the disclosure. Referring to FIG. 2, as indicated above, packet security gateway **112** may be located at network boundary **200** between network A **102** and network E **110**. Packet security gateway **112** may include processor **202**, memory **204**, network interfaces **206** and **208**, packet filter **214**, and management interface **222**. Processor **202**, memory **204**, network interfaces **206** and **208**, packet filter **214**, and management interface **222** may be interconnected via data bus **210**. Network interface **206** may connect packet security gateway **112** to network E **110**. Similarly, network interface **208** may connect packet security gateway **112** to network A **102**. Memory **204** may include one or more program modules that when executed by processor **202**, configure packet security gateway **112** to perform various functions as described herein.

[0037] Packet security gateway **112** may be configured to receive a dynamic security policy from security policy management server **120**. For example, packet security gateway **112** may receive dynamic security policy **212** from security policy management server **120** via management interface **222** (*i.e.*, out-of-band signaling) or network interface **206** (*i.e.*, in-band signaling). Packet security gateway **112** may include one or more packet filters or packet discriminators, or logic for implementing one or more packet filters or packet discriminators. For example, packet security gateway **112** may include packet filter **214**, which may be configured to examine information associated with packets received by packet security gateway **112** and forward the packets to one or more packet transformation functions based on the examined information. For example, packet filter **214** may examine information associated with packets received by packet security gateway **112** (*e.g.*, packets received from network E **110** via management interface **222** or network interface **206**) and forward the packets to one or more of packet transformation functions 1 – N **216**, **218**, and **220** based on the examined information.

[0038] As will be described in greater detail below, dynamic security policy **212** may include one or more rules and the configuration of packet filter **214** may be based on one or more of the rules included in dynamic security policy **212**. For example, dynamic security policy **212** may include one or more rules specifying that packets having specified information should be forwarded to packet transformation function **216**, while all other packets should be forwarded to packet transformation function **218**. Packet transformation functions 1 – N **216**, **218**, and **220** may be configured to perform one or more functions on packets they receive from packet filter **214**.

For example, packet transformation functions 1 – N **216**, **218**, and **220** may be configured to forward packets received from packet filter **214** into network A **102**, forward packets received from packet filter **214** to an IPsec stack having an IPsec security association corresponding to the packets, or drop packets received from packet filter **214**. In some embodiments, one or more of packet transformation functions 1 – N **216**, **218**, and **220** may be configured to drop packets by sending the packets to a local "infinite sink" (*e.g.*, the /dev/null device file in a UNIX/LINUX system).

[0039] In some embodiments, packet security gateway **112** may be configured in a network layer transparent manner. For example, packet security gateway **112** may be configured to utilize one or more of network interfaces **206** and **208** to send and receive traffic at the link layer. One or more of network interfaces **206** and **208**, however, may not be addressed at the network layer. Because packet filter **214** and packet transformation functions 1 – N **216**, **218**, and **220** operate at the network layer, PSG **112** may still perform packet transformation functions at the network layer. By operating in a network layer transparent manner, packet security gateway **112** may insulate itself from network attacks (*e.g.*, DDoS attacks) launched at the network layer because attack packets cannot be routed to the network interfaces **206** and **208**. In some embodiments, packet security gateway **112** may include management interface **222**. Management interface **222** may be addressed at the network level in order to provide packet security gateway **112** with network level addressability. Access to management interface **222** may be secured, for example, at the application level by using a service such as SSH, or secured at the transport level using, *e.g.*, TLS, or secured at the network level by attaching it to a network with a separate address space and routing policy from network A **102** and network E **110**, or secured at the link level, *e.g.*, using the IEEE 802.1X framework, etc.

[0040] The flows illustrated by Figure 2 are merely exemplary and show packets that originate within a network distinct from network A **102** and are destined for a host within network A **102** in order to simplify the illustration. Packet security gateway **112** may be configured to receive and filter packets that originate within a network other than network A **102** (*e.g.*, networks B – E **104**, **106**, **108**, or **110**) and are destined for a host within network A **102**, as well as packets that originate within network A **102** destined for a network distinct from network A **102** (*e.g.*, network B – D **104**, **106**, **108**, or **110**). That is, packet security gateway **112** may be configured to filter and

perform one or more packet transformation functions on packets flowing in either direction and may thus be utilized, for example, to both protect network A **102** from malicious network traffic and to prevent malicious network traffic from leaving network A **102**.

[0041] FIG. 3 illustrates an exemplary dynamic security policy in accordance with one or more embodiments. Referring to FIG. 3, dynamic security policy **300** may include rules 1 – 5 **302**, **304**, **306**, **308**, and **310**. Each rule may specify criteria and one or more packet transformation functions that should be performed for packets associated with the specified criteria. The specified criteria may take the form of a five-tuple of values selected from packet header information, specifying a protocol type of the data section of the IP packet (*e.g.*, TCP, UDP, ICMP, or any other protocol), one or more source IP addresses, one or more source port values, one or more destination IP addresses, and one or more destination ports. For example, rule 1 **302** may specify that IP packets containing TCP packets, originating from a source IP address that begins with 140, having any source port, destined for an IP address that begins with 130, and destined for port 20 should have an accept packet transformation function (*e.g.*, the identity function) performed on them. Similarly, rule 2 **304** may specify that IP packets containing TCP packets, originating from a source IP address that begins with 140, having any source port, destined for any IP address, and destined for port 80 should have an accept packet transformation function performed on them; rule 3 **306** may specify that IP packets containing TCP packets, originating from a source IP address that begins with 150, having any source port, destined for any IP address that begins with 120, and destined for port 90 should have an accept packet transformation function performed on them; rule 4 **308** may specify that IP packets containing UDP packets, originating from a source IP address that begins with 150, having any source port, destined for any IP address, and destined for port 3030 should have an accept packet transformation function performed on them; and rule 5 **310** may specify that IP packets containing any data, originating from any source IP address, having any source port, destined for any IP address, and destined for any port should have a deny packet transformation function performed on them. One or more rules included in dynamic security policy **300** may be specified in IP version 4 or IP version 6.

[0042] As will be described in greater detail below, dynamic security policy **300** may include one or more rules that specify a packet transformation function other than forwarding (accepting or allowing) or dropping (denying) a packet. For example, rule 3 **306** may specify that IP packets

containing TCP packets, originating from a source IP address that begins with 150, having any source port, destined for any IP address that begins with 120, and destined for port 90 should not only have an accept packet transformation function performed on them, but should also be routed to a monitoring device.

[0043] One or more rules within dynamic security policy **300** may be required to execute in a specific order. For example, it may be required that rule 5 **310** be executed last. Because rule 5 **310** specifies that any packet should have a deny packet transformation function performed on it, if it were executed before a rule specifying an accept packet transformation function (*e.g.*, one or more of rules 1 – 4 **302**, **304**, **306**, or **308**), no packets matching the criteria specified by the rule specifying the accept packet transformation function would pass through a packet security gateway implementing dynamic security policy **300**. Similarly, two or more rules within dynamic security policy **300** may specify overlapping criteria and different packet transformation functions. In such cases, the order-of-application of the rules may determine which rule is applied to a packet that would match the two or more rules. Such rules may be merged together or otherwise transformed into a different set of rules without overlapping criteria, which may produce the same result as the original set of rules, when applied to any packet.

[0044] A dynamic security policy may utilize the combination of one or more rules to create policies for governing packets within a network environment or effectuating one or more services within a network environment. For example, a dynamic security policy may include one or more rules, the combination of which may effectuate a blocklist service within a network environment. A dynamic security policy that effectuates a blocklist service within a network environment may include one or more rules specifying criteria (*e.g.*, a set of network addresses) for which associated packets should be blocked, dropped, or denied, and at least one rule specifying that all packets outside the specified block sets should be forwarded, accepted, or allowed. Such a dynamic security policy may be constructed by including one or more rules specifying criteria (*e.g.*, a set of network addresses) for which associated packets should be dropped, and a wildcard rule, designated to be executed last, and specifying that all packets should be allowed. One or more dynamic security policies that effectuate a blocklist service may be utilized to implement one or more Virtual Private Networks (VPNs).

[0045] A dynamic security policy may also include one or more rules, the combination of which may effectuate an allowlist service within a network environment. A dynamic security policy that effectuates an allowlist service within a network environment may include one or more rules specifying criteria (*e.g.*, a set of network addresses) for which associated packets should be forwarded, allowed, or accepted, and at least one rule specifying that all packets outside the specified allow sets should be blocked, denied, or dropped. Such a dynamic security policy may be constructed by including one or more rules specifying criteria (*e.g.*, a set of network addresses) for which associated packets should be forwarded, and a wildcard rule, designated to be executed last, and specifying that all packets should be blocked. For example, dynamic security policy **300** includes rules 1 – 4 **302**, **304**, **306**, and **308**, each of which specifies a set of network addresses for which packets should be allowed, and rule 5 **310** which specifies that all packets should be dropped. Thus, if rules 1 – 5 **302**, **304**, **306**, **308**, and **310** are executed in order, dynamic security policy **300** will effectuate an allowlist service.

[0046] A dynamic security policy may also include one or more rules, the combination of which may effectuate a VoIP firewall service within a network environment. As will be discussed in greater detail below, a security policy management server may receive information associated with VoIP sessions. For example, a security policy management server may receive information associated with VoIP sessions from one or more softswitches (*e.g.*, H.323 softswitches, SIP IP Multimedia Subsystem (IMS) softswitches) or session border controllers when a VoIP session is initialized or set up. In order to allow packets associated with such a VoIP session within a network protected by one or more packet security gateways associated with the security policy management server, the security policy management server may utilize the received information associated with the VoIP sessions to construct one or more rules for allowing the packets associated with the VoIP session. When the VoIP session is terminated or torn down, the softswitch or session border controller may notify the security policy management server, which may create or alter one or more rules to reflect the termination of the VoIP session (*e.g.*, to deny future packets which may match criteria previously associated with the VoIP session).

[0047] A dynamic security policy may also include one or more rules or rule sets, the combination of which may effectuate a phased restoration service within a network environment. Such a phased restoration service may be used in the event of a network attack (*e.g.*, a DDoS

attack). When an attack occurs a network may be overwhelmed with network traffic and be unable to route all or any of the traffic. In the event of such an attack, it may be beneficial to utilize a dynamic security policy which effectuates a phased restoration service. Such a dynamic security policy may include one or more rules or rule sets configured for execution in time-shifted phases. Each of the rules or rule sets may specify progressively larger sets of network addresses. For example, a dynamic security policy may include three rules or rule sets which may be configured for execution in time-shifted phases. A first of the rules or rule sets may specify a relatively small set of network addresses for which packets should be forwarded (*e.g.*, network addresses corresponding to mission critical network devices). A second of the rules or rule sets may specify a relatively larger set of network addresses for which packets should be forwarded (*e.g.*, network addresses corresponding to trusted network devices). A third of the rules or rule sets may specify an even larger set of network addresses for which packets should be forwarded (*e.g.*, network addresses corresponding to all network devices that would be allowed under ordinary circumstances). The dynamic security policy may specify that the rules or rule sets should be implemented in time-shifted phases. That is, the dynamic security policy may specify that the first rule or rule set should be executed first, and that the second rule or rule set should be executed at a time after the time at which the first rule or rule set is executed, and the third rule or rule set should be executed at a time after the time at which the second rule or rule set is executed. Such a dynamic security policy may assist a network in recovering from an attack, by allowing the network to isolate itself from the attack or recover in a controlled manner.

[0048] A dynamic security policy may also include one or more rules, the combination of which may effectuate an enqueueing service within a network environment. A dynamic security policy that effectuates an enqueueing service may include one or more rules that specify sets of network addresses and packet transformation functions that queue packets in one or more queues corresponding to the sets. These queues may then be serviced at varying rates. For example, a dynamic security policy may include two rules, each of which specify a set of network addresses. A first of the rules may specify that packets corresponding to its specified set should be queued in a first forwarding queue. A second of the rules may specify that packets corresponding to its specified set should be queued in a second forwarding queue. The first forwarding queue may be serviced at a higher forwarding rate than the second forwarding queue. Such an enqueueing service

may be utilized during or following a network attack, or generally to provide prioritized service to critical network devices (*e.g.*, when network resources are strained). In some embodiments, one or more rules contained within a dynamic security policy may include an arbitrary selector which may correspond to one or more parameters or fields associated with a packet. For example, a dynamic security policy rule may include a Differentiated Service Code Point (DSCP) selector that corresponds to a DSCP field in an IP header. Thus, two packets having different values within the specified DSCP field may correspond to two distinct rules within a dynamic security policy and have different packet transformation functions performed on them. For example, two otherwise identical packets having different values within the specified DSCP field may be queued in two different forwarding queues that have different forwarding rates, and may thus receive differentiated service.

[0049] A dynamic security policy may also include one or more rules, the combination of which may effectuate a multi-dimensional routing service or a multi-dimensional switching service within a network environment. For example, in some embodiments, a dynamic security policy may include one or more rules that specify a set of network addresses and an additional parameter. Such rules may further specify a packet transformation function configured to route packets within the specified set of network addresses that match the additional parameter to a network address distinct from the packets' respective destination network addresses. For example, the packet transformation function may be configured to encapsulate such packets (*e.g.*, as described by Internet Engineering Task Force (IETF) Request For Comment (RFC) 2003) with an IP header specifying a network address different from their respective destination addresses. The packets may then be routed to the network address specified by the encapsulating IP header, which may correspond to a network device configured to utilize such packets or data contained within them, strip the IP header from the packets, and forward the packets to their respective destination addresses. In some embodiments, the packet transformation function may be configured to alter or modify the destination address of the packets, which may then be routed to the altered or modified destination address. Additionally or alternatively, the packet transformation function may be configured to assign such packets to a particular Layer-2 VLAN (*e.g.*, as described by IEEE 802.1Q). The packets may then be switched to another device on the same VLAN, which

may or may not be on the IP-layer path that the packet would have taken if it were routed according to the packet's destination IP address instead of being switched through the VLAN.

[0050] As will be described in greater detail below, in some embodiments a dynamic security policy may include one or more rules, the combination of which may effectuate an implementation of a multi-dimensional routing service for performing a monitoring service within a network environment. For example, a dynamic security policy may include one or more rules that specify a set of network addresses (*e.g.*, a set of network addresses from which a call that is to be monitored is expected to originate within) and an additional parameter (*e.g.*, a SIP URI corresponding to a caller to be monitored). As indicated above, such rules may further specify a packet transformation function configured to route or switch packets within the specified set of network addresses that match the additional parameter (*e.g.*, the SIP URI) to a network address corresponding to a monitoring device. The network address corresponding to the monitoring device may be different from the packets' destination network address (*e.g.*, an address corresponding to the called party or a softswitch associated with the called party). For example, the packet transformation function may be configured to encapsulate the packets with an IP header specifying the network address corresponding to the monitoring device. The packets may then be routed (or rerouted) to the monitoring device, which may be configured to copy the packets or data contained within them (*e.g.*, for subsequent review by a law enforcement or national security authority), strip the IP header from them, and then forward the packets to their destination address (*e.g.*, the address corresponding to the called party or softswitch associated with the called party).

[0051] As indicated above, a significant challenge associated with building a scalable proactive solution for protecting a secured network, is the need to filter substantially all network traffic at a high resolution. Filtering traffic at a high resolution often requires the use of many rules. In a large network, where traffic volumes may be enormous, the time required to provide high resolution filtering (*e.g.*, the time required to apply a large number of rules to a large volume of traffic) has traditionally been thought to render proactive network protection solutions infeasible. This concern may be particularly acute in network environments that utilize low-latency applications (*e.g.*, VoIP).

[0052] Recent advances in packet filtering technology have reduced the time required to apply large rule sets to network traffic. For example, U.S. Patent Application Publication Nos.

2006/0195896 and 2006/0248580 to Fulp et al., and U.S. Patent Application Publication No. 2011/0055916 to Ahn, describe advanced packet filtering technologies, and are each incorporated by reference herein in their entireties.

[0053] One approach to providing high resolution filtering, while reducing the number of rules applied to network traffic, may be utilized when a dynamic security policy is combinatorially complete. For example, a dynamic security policy may be configured to allow bi-directional communication between a set of N internal hosts $\{I_1, I_2, \ldots, I_N\}$ within a protected network and a set of M external hosts $\{E_1, E_2, \ldots, E_M\}$ outside the protected network. To enable communications between the internal hosts and the external hosts, the dynamic security policy may be constructed to include a set of rules containing each possible combination of internal hosts and external hosts (*e.g.*,$\{\{I_1, E_1\}, \{I_1, E_2\}, \ldots \{I_1, E_M\}, \{I_2, E_1\}, \{I_2, E_2\}, \ldots \{I_2, E_M\}, \ldots, \{I_N, E_1\}, \{I_N, E_2\}, \ldots \{I_N, E_M\}\}$), each of the rules being associated with an allow packet transformation function. Such a dynamic security policy would have N*M rules for allowing communication between the internal hosts and the external hosts that originate from one of the internal hosts and are destined for one of the external hosts, and an additional N*M rules for allowing communications between the internal hosts and the external hosts that originate from one of the external hosts and are destined for one of the internal hosts. An equivalent result may be achieved, however, by constructing two smaller dynamic security policies: a first dynamic security policy that includes rules specifying the N internal hosts (*e.g.*, $\{\{I_1\}, \{I_2\}, \ldots, \{I_N\}\}$), each rule being associated with an accept packet transformation function; and a second dynamic security policy that includes rules specifying the M external hosts (*e.g.*, $\{\{E_1\}, \{E_2\}, \ldots, \{E_M\}\}$), each rule being associated with an accept packet transformation function. Such a construct of dynamic security policies may be implemented using a system of packet security gateways configured in series.

[0054] FIG. 4 illustrates an exemplary configuration of multiple packet security gateways connected in series. Referring to FIG. 4, packet security gateway **112** may include one or more packet security gateways configured in series. For example, packet security gateway **112** may include packet security gateways 1 – N **400**, **402**, and **404**. Packet security gateways 1 – N **400**, **402**, and **404** may be configured so that packets forwarded by packet security gateway 1 **400** are received by packet security gateway 2 **402**, and packets forwarded by packet security gateway 2 **402** are received by the next packet security gateway in the series, all the way through packet

security gateway N **404**. Each of packet security gateways 1 – N **400**, **402**, and **404** may include a packet filter, similar to packet filter **214** described above with respect to FIG. 2, and one or more packet transformation functions, similar to packet transformation functions 1 – N **216**, **218**, and **220** described above with respect to FIG. 2. Packet security gateways 1 – N **400**, **402**, and **404** may be utilized to implement a construct of dynamic security policies similar to that described above.

[0055] For example, packet security gateway 1 **400** may be configured to implement P_1, which may include rules specifying M external hosts (*e.g.*, $\{\{E_1\}, \{E_2\}, \ldots, \{E_M\}\}$), each rule being associated with an accept packet transformation function. Packet security gateway 2 **402** may be configured to implement P_2, which may include rules specifying N internal hosts (*e.g.*, $\{\{I_1\}, \{I_2\}, \ldots, \{I_N\}\}$), each rule being associated with an accept packet transformation function. A packet received by packet security gateway **112** may be initially received via packet security gateway 1 **400**'s network interface. Packet security gateway 1 **400** may apply one or more of the rules in P_1 to the received packet until the packet matches criteria specified by a rule in P_1, at which point packet security gateway 1 **400** may perform a packet transformation function specified by the rule on the packet. For example, a packet may be received by packet security gateway **112** that originates from external host E_5 (*e.g.*, a host within network E **110**) and is destined for internal host I_7 (*e.g.*, a host within network A **102**). Packet security gateway 1 **400** may apply one or more of the rules in P_1 (*e.g.*, $\{\{E_1\}, \{E_2\}, \ldots, \{E_M\}\}$) to the received packet and the received packet may match the criteria specified by one of the rules in P_1 (*e.g.*, $\{\{E_5\}$). The rule may specify that an accept packet transformation function should be performed, and packet security gateway 1 **400** may utilize one or more of its packet transformation functions to perform the accept packet transformation function on the packet and forward the packet to packet security gateway 2 **402**. Packet security gateway 2 **402** may apply one or more of the rules in P_2 (*e.g.*, $\{\{I_1\}, \{I_2\}, \ldots, \{I_N\}\}$) to the packet and the packet may match the criteria specified by one of the rules in P_2 (*e.g.*, $\{\{I_7\}$). The rule may specify that an accept packet transformation function should be performed, and packet security gateway 2 **402** may utilize one or more of its packet transformation functions to perform the accept packet transformation function on the packet and forward the packet to network A **102**.

[0056] It will be appreciated that utilizing multiple packet security gateways in series to implement dynamic security policy constructs may increase performance and decrease memory resource requirements. For example, in the described scenario packet security gateway 1 **400** may have only been required to compare the packet to five rules and packet security gateway 2 **402** may have only been required to compare the packet to seven rules. In a worst case scenario, packet security gateway 1 **400** may have only been required to compare the packet to M rules and packet security gateway 2 **402** may have only been required to compare the packet to N rules. Moreover, the series configuration may enable packet security gateway 1 **400** to begin implementing P_1 with respect to a subsequently received packet, while packet security gateway 2 **402** simultaneously implements P_2 with respect to the packet forwarded by packet security gateway 1 **400**. Furthermore, the memory requirements for this scenario with packet security gateways in series may be comparable to M+N, whereas originally the combinatorially complete set of rules contained in a single packet security gateway may have required memory comparable to N*M.

[0057] FIG. 5 illustrates an exemplary security policy management server. Referring to FIG. 5, security policy management server **120** may include processor **500**, memory **502**, and network interface **504**. One or more of processor **500**, memory **502**, and network interface **504** may be interconnected via data bus **506**. Network interface **504** may interface security policy management server **120** with network E **110**. Memory **502** may include one or more program modules that when executed by processor **500**, configure security policy management server **120** to perform functions described herein. It will be appreciated that as used herein the term "server" designates one or more computing devices configured to perform one or more functions described herein. The term "server" should not be construed to imply that a client/server relationship (*e.g.*, a relationship in which a request is received from a client and then serviced by a server) necessarily exists.

[0058] Security policy management server **120** may be configured to communicate one or more dynamic security policies to one or more packet security gateways within network environment **100**. For example, security policy management server **120** may communicate one or more dynamic security policies stored in memory **502** to one or more of packet security gateways **112**, **114**, **116**, and **118**. For example, security policy management server **120** may be configured to communicate one or more dynamic security policies to one or more of packet security gateways

112, **114**, **116**, and **118** on a periodic basis, under specified network conditions, whenever security policy management server **120** receives a new dynamic security policy, whenever a dynamic security policy stored on security policy management server **120** is changed or altered, or in response to a request from one or more of packet security gateways **112**, **114**, **116**, and **118**.

[0059] Security policy management server **120** may also be configured to provide one or more administrators associated with security policy management server **120** with management interface **510**. For example, security policy management server **120** may be configured to provide one or more administrators with a Graphical User Interface (GUI) or Command Line Interface (CLI). An administrator of security policy management server **120** may utilize security policy management server **120**'s management interface **510** to configure security policy management server **120**. For example, an administrator may configure security policy management server **120** in order to associate security policy management server **120** with one or more of packet security gateways **112**, **114**, **116**, and **118**. An administrator of security policy management server **120** may also utilize security policy management server **120**'s management interface **510** to construct one or more dynamic security policies or to load one or more dynamic security policies into security policy management server **120**'s memory **502**. For example, an administrator associated with security policy management server **120** may manually construct one or more dynamic security policies offline and then utilize security policy management server **120**'s management interface **510** to load such dynamic security policies into security policy management server **120**'s memory **502**.

[0060] In some embodiments, security policy management server **120** may be configured to add, remove, or alter one or more dynamic security policies stored in memory **502** based on information received from one or more devices within network environment **100**. For example, security policy management server **120**'s memory **502** may include a dynamic security policy having one or more rules that specify a list of network addresses known to be associated with malicious network traffic. Security policy management server **120** may be configured to automatically create or alter one or more of such rules as new network addresses associated with malicious network traffic are determined. For example, security policy management server **120** may receive updates (*e.g.* as part of a subscription) from malicious host tracker service **508**. Malicious host tracker service **508** may aggregate information associated with malicious network

traffic and updates received from malicious host tracker service **508** may include one or more network addresses that have been determined to be associated with malicious network traffic. Security policy management server **120** may be configured to create or alter one or more rules included within a dynamic security policy associated with malicious host tracker service **508** to block traffic associated with the network addresses received from malicious host tracker service **508**. Additionally or alternatively, as indicated above, security policy management server **120** may be configured to create or alter one or more dynamic security policies, or one or more rules included in one or more dynamic security policies, to account for VoIP sessions being initiated or terminated by a network device within network environment **100**.

[0061] As indicated above, a dynamic security policy may include one or more rules, the combination of which may effectuate an implementation of a multi-dimensional routing service for performing a monitoring service within a network environment. FIG. 6 illustrates an exemplary network environment for implementing a monitoring service in accordance with one or more embodiments. Referring to FIG. 6, a user of network environment **100** (*e.g.*, a law enforcement or national security authority) may desire to obtain a copy of packets associated with one or more VoIP sessions (*e.g.*, sessions associated with SIP URI exampleuser@exampledomain.com) within network environment **100**. Because many SIP-signaled services are designed to address sessions dynamically, it may not be possible to determine, prior to a session being set up, a particular network address and port from which packets should be copied. Moreover, due to privacy concerns, regulators may require that only packets associated with the specified VoIP sessions (*e.g.*, sessions associated with SIP URI exampleuser@exampledomain.com) be copied.

[0062] For example, a user associated with SIP URI exampleuser@exampledomain.com may utilize User Equipment (UE) **600** within network A **102** to place a VoIP call to a user utilizing UE **602** within network B **104**. SIP switch **604** may be utilized by an operator of network A **102** for switching SIP signals within network A **102**. Similarly, SIP switch **606** may be utilized by an operator of network B **104** for switching SIP signals within network B **104**. One or more of SIP switches **604** and **606** may include an analysis application configured to monitor SIP signals and publish SIP messages associated with specified users to one or more subscribers. For example, the operator of network A **102** may have installed analysis application **610** on SIP switch **604** (*e.g.*,

accessed via a SIP IMS Service Control (ISC) interface associated with SIP switch **604**) and configured analysis application **610** to search for and publish SIP messages associated with SIP URI exampleuser@exampledomain.com to security policy management server **120**. Similarly, the operator of network B **104** may have installed analysis application **612** on SIP switch **606** and configured analysis application **612** to publish SIP messages associated with SIP URI exampleuser@exampledomain.com to security policy management server **120**.

[0063] When the user associated with SIP URI exampleuser@exampledomain.com utilizes UE **600** to place a VoIP call to the user utilizing UE **602**, analysis application **610** may detect one or more SIP signaling messages associated with the call (*e.g.*, SIP signaling messages for setting up the call) and publish the messages to security policy management server **120**. Security policy management server **120** may extract one or more network addresses and port numbers from the SIP signaling messages (*e.g.*, a network address and port number utilized by UE **600** for placing the VoIP call to UE **602**). Security policy management server **120** may utilize the extracted network addresses and port numbers to create a new dynamic security policy or alter one or more rules within an existing dynamic security policy. For example, security policy management server **120** may construct a new dynamic security policy that includes a rule specifying one of the extracted network addresses and port numbers, as well as a packet transformation function configured to route associated packets to monitoring device **608**. Security policy management server **120** may communicate the new or modified dynamic security policy to packet security gateway **112**.

[0064] When packets associated with the VoIP call between UE **600** and UE **602** are received by packet security gateway **112**, packet filter **214** may identify the packets as matching the criteria specified by the dynamic security policy received from security policy management server **120** (*e.g.*, packets addressed to or from the extracted address and port number) and may perform the packet transformation function configured to route the packets to monitoring device **608**. For example, the packet transformation function configured to route the packets to monitoring device **608** may be packet transformation function 2 **218**. When packet transformation function 2 **218** receives the packets from packet filter **214**, it may encapsulate them with an IP header having an address corresponding to monitoring device **608** and may then forward them to network E **110**. Once forwarded, the packets may be routed based on the address specified by the encapsulating

header, and may thus be communicated to monitoring device **608**. When the packets are received by monitoring device **608**, monitoring device **608** may copy the packets or data contained within them, and strip the encapsulating header from them. Monitoring device **608** may then forward the packets, without the encapsulating header, to network E **110**. Network E **110** may receive the packets forwarded by monitoring device **608** and may route them based on their destination address (*e.g.*, to UE **602**).

[0065] In some embodiments, packet security gateway **112** may be configured to perform multiple packet transformation functions on the packets associated with the VoIP call between UEs **600** and **602**. For example, packet filter **214** may identify the packets as matching the criteria specified by the dynamic security policy received from security policy management server **120** and may forward the packets to packet transformation functions 1 **216** and 2 **218**. Packet transformation function 1 **216** may be configured to forward the packets to their destination address (*e.g.*, to UE **602**) and packet transformation function 2 **218** may be configured to encapsulate the packets (or a copy of the packets) with an IP header having an address corresponding to monitoring device **608** and then forward the encapsulated packets to network E **110**. Once forwarded, the encapsulated packets may be routed based on the address specified by the encapsulating header, and may thus be communicated to monitoring device **608**, which may store the packets or data contained within them for subsequent review or analysis (*e.g.*, by a law enforcement or national security authority). In such embodiments, it may not be necessary for monitoring device **608** to strip the encapsulating header from the packets or route them based on their destination address (*e.g.*, to UE **602**) because packet transformation function 1 **216** may have already forwarded the packets to their destination address (*e.g.*, to UE **602**).

[0066] It will be appreciated that SIP switch **604**'s analysis application **610** may similarly detect SIP signaling associated with the termination of the VoIP call between UE **600** and UE **602** and may publish the SIP messages to security policy management server **120**. Security policy management server **120** may utilize one or more network addresses and port numbers within the messages to construct a new dynamic security policy or modify one or more rules within an existing dynamic security policy and communicate the new or modified dynamic security policy to packet security gateway **112** in order to ensure that future packets associated with the network address and port number but not associated with SIP URI exampleuser@exampledomain.com are

not routed to monitoring device **608**. Security policy management server **120** may communicate any dynamic security policy constructed or modified based on SIP messages to any of multiple packet security gateways (*e.g.*, packet security gateways **114** and **116**) within network environment **100** in order to ensure that all packets associated with the VoIP call between UE **600** and UE **602** are forwarded to monitoring device **608**.

[0067] FIG. 7 illustrates an exemplary network environment that includes a secured network having multiple boundaries with unsecured networks in which one or more embodiments may be implemented. Network environment **700** may include networks A – C **702**, **704**, and **706**. Networks A **702** and B **704** may be a LAN or WAN associated with an organization (*e.g.*, a company, university, enterprise, or government agency). One or more networks within network environment **700** may interface with one or more other networks within network environment **700**. For example, the organizations associated with networks A **702** and B **704** may subscribe to an ISP to provide interconnectivity between their respective networks or allow public access to their respective networks (*e.g.*, via the Internet). Each of networks A **702** and B **704** may be connected to network C **706**, which may be the ISP's network. The ISP may desire to offer an interconnection service between networks A **702** and B **704**, but may also want to enforce one or more dynamic security policies with respect to traffic traversing network C **706**.Accordingly, one or more packet security gateways may be located at each boundary between network A **702** and network C **706**, and each boundary between network B **704** and network C **706**. For example, packet security gateway **708** and packet security gateway **710** may be respectively located at first and second boundaries between networks A **702** and C **706**. Similarly, packet security gateways **712** and **714** may be respectively located at first and second boundaries between networks B **704** and C **706**. Each of packet security gateways **708**, **710**, **712**, and **714** may be associated with security policy management server **716**.

[0068] Security policy management server **716** may maintain one or more dynamic security policies configured for protecting network C **706**, and may be managed by the ISP associated with network C **706**. Security policy management server **716** may ensure that each of packet security gateways **708**, **710**, **712**, and **714** protect each of their respective boundaries with network C **706** in a uniform manner. For example, security policy management server **716** may be configured to communicate one or more dynamic security policies it maintains to each of packet security

gateways **708**, **710**, **712**, and **714** on a periodic basis, in response to being directed to by a network operator associated with network environment **700**, in response to detected network conditions (*e.g.*, an attack or high resource utilization), or in response to a request from one or more of packet security gateways **708**, **710**, **712**, or **714**.

[0069] In some embodiments, security policy management server **716** may be configured to communicate different dynamic security policies to one or more of packet security gateways **708**, **710**, **712**, and **714** based on, for example, their respective locations within network environment **700**. For example, security policy management server **716** may be configured to implement one or more anti-spoofing techniques (*e.g.*, ingress filtering or Best Current Practice (BCP) 38, as described by Internet Engineering Task Force (IETF) Request For Comment (RFC) 2827) with respect to network environment **700**. Effective implementation of such techniques may require that a dynamic security policy be based on the location at which it is being implemented. For example, a dynamic security policy that implements ingress filtering may comprise one or more rules that filter based on a packet's source address, identifying packets having source addresses that could not possibly have originated from a network downstream of the ingress filtering point (*e.g.*, packets having spoofed source addresses). Such rules may vary depending on the boundary point for which they are implemented (*e.g.*, a packet for one boundary may be properly identified as spoofed, yet a packet having the same source address may be legitimate traffic at a different boundary point). Accordingly, security policy management server **716** may be configured to communicate different dynamic security policies to one or more of packet security gateways **708**, **710**, **712**, and **714** based on their respective locations within network environment **700**. For example, security policy management server **716** may communicate a dynamic security policy to packet security gateways **708** and **710** that includes one or more rules for performing ingress filtering for network A **702** (*e.g.*, for identifying packets having source addresses that could not have originated within network A **702**) and a different dynamic security policy to packet security gateways **712** and **714** that includes one or more rules for performing ingress filtering for network B **704** (*e.g.*, for identifying packets having source addresses that could not have originated within network B **704**).

[0070] It will be appreciated that by maintaining uniform dynamic security policies at each boundary between networks A **702** and C **706**, as well as at each boundary between networks B

Keysight Technologies Ex. 1002
Page 444 of 460

704 and C **706**, security policy management server **716** and packet security gateways **708**, **710**, **712**, and **714** may aid the ISP associated with network C **706** in protecting network C **706** from network attacks.

[0071] FIG. 8 illustrates an exemplary network environment that includes multiple distinct secured networks in which one or more embodiments may be implemented. Referring to FIG. 8, network environment **800** may include networks A **802**, B **804**, and C **806**. Each of networks A **802** and B **804** may interface with network C **806** at multiple boundaries within network environment **800**. Packet security gateways **808** and **810** may be respectively located at first and second boundaries between networks A **802** and C **806**. Similarly, packet security gateways **812** and **814** may be respectively located at first and second boundaries between networks B **804** and C **806**.

[0072] Network A **802** and B **804** may both be associated with a common organization (*e.g.*, a company, university, enterprise, or government agency), or may each be associated with a distinct organization. In the former case, the common organization may desire to utilize one or more dynamic security policies with respect to network A **802** and one or more different dynamic security policies with respect to network B **804**. In the latter case, an organization associated with network A **802** may desire to utilize one or more dynamic security policies with respect to network A **802** and a different organization associated with network B **804** may desire to utilize one or more different dynamic security policies with respect to network B **804**. Network environment **800** may include security policy management servers A **816** and B **818**. Security policy management server A **816** may be associated with network A **802** and may maintain one or more dynamic security policies configured for protecting network A **802**. Similarly, security policy management server B **818** may be associated with network B **804** and may maintain one or more dynamic security policies configured for protecting network B **804**.

[0073] Packet security gateways **808** and **810** may be associated with security policy management server A **816**. Similarly, packet security gateways **812** and **814** may be associated with security policy management server B **818**. Security policy management server A **816** may ensure that packet security gateways **808** and **810** protect each of their respective boundaries with network C **806** in a uniform manner. For example, security policy management server A **816** may be configured to communicate one or more dynamic security policies it maintains to packet

Keysight Technologies Ex. 1002
Page 445 of 460

security gateways **808** and **810** on a periodic basis, in response to being directed to by a network operator associated with network A **802**, in response to detected network conditions (*e.g.*, an attack or high resource utilization), or in response to a request from packet security gateway **808** or **810**. Similarly, security policy management server B **818** may ensure that packet security gateways **812** and **814** protect each of their respective boundaries with network C **806** in a uniform manner. For example, security policy management server B **818** may be configured to communicate one or more dynamic security policies it maintains to packet security gateways **812** and **814** on a periodic basis, in response to being directed to by a network operator associated with network B **804**, in response to detected network conditions (*e.g.*, an attack or high resource utilization), or in response to a request from packet security gateway **812** or **814**. By utilizing distinct security policy management servers (*e.g.*, security policy management servers A **816** and B **818**), one or more operators associated with distinct networks (*e.g.*, networks A **802** and B **804**) may maintain uniform dynamic security policies at each boundary of their respective networks, while simultaneously enabling different dynamic security policies to be maintained for each network. Similarly, by utilizing distinct security policy management servers (*e.g.*, security policy management servers A **816** and B **818**), one or more operators associated with a single organization that desires to maintain distinct networks (*e.g.*, networks A **802** and B **804**) may maintain uniform dynamic security policies at each boundary of their distinct networks, while simultaneously enabling different dynamic security policies to be maintained for each network.

[0074] FIG. 9 illustrates an exemplary secure LAN environment protected in accordance with one or more aspects of the disclosure. Referring to FIG. 9, network environment **900** may be a LAN, including hosts A **902**, B **904**, and C **906**. It may also include LAN switch **908**. LAN switch **908** may be configured to switch network traffic (*e.g.*, packets) between one or more of hosts A **902**, B **904**, and C **906**. For example, LAN switch **908** may include a switching matrix configured to switch packets received from one or more of hosts A **902**, B **904**, and C **906** to one or more of hosts A **902**, B **904**, and C **906**. LAN switch **908** may be associated with packet security gateway **910**, and network environment **900** may include security policy management server **912**.

[0075] In some embodiments, packet security gateway **910** may be embedded within LAN switch **908**. Alternatively, packet security gateway **910** may be a device distinct from LAN switch **908**, and LAN switch **908** may be configured to route network traffic through packet security

Keysight Technologies Ex. 1002
Page 446 of 460

gateway **910** (*e.g.*, by modifying LAN switch **908**'s switching matrix). Packet security gateway **910** may be configured to receive one or more dynamic security policies from security policy management server **912**. The dynamic security policies received from security policy management server **912** may include one or more rules specifying criteria associated with one or more of hosts A **902**, B **904**, and C **906**, and may further specify one or more packet transformation functions to be performed on packets matching the specified criteria. Packet security gateway **910** may identify packets matching one or more of the criteria specified by the rules and may perform the associated packet transformation functions on the identified packets. By utilizing packet security gateway **910** within network environment **900**, an operator of network environment **900** may be able to protect network environment **900** from network attacks, as well as implement one or more services (*e.g.*, blocklist service, allowlist service, VoIP firewall service, phased restoration service, enqueueing service, multi-dimensional routing service, or monitoring service) within network environment **900**. Network environment **900** may include multiple LAN switches with embedded or associated packet security gateways, each of the packet security gateways configured to receive one or more dynamic security policies from security policy management server **912**.

[0076] FIG. 10 illustrates an exemplary method for protecting a secured network in accordance with one or more embodiments. The steps may be performed at each of one or more packet security gateways associated with a security policy management server. For example, each of packet security gateways **112**, **114**, **116**, and **118** may be associated with security policy management server **120**, and the steps may be performed at each of packet security gateways **112**, **114**, **116**, and **118**. At step **1000**, a dynamic security policy is received from the security policy management server. For example, packet security gateway **112** may receive dynamic security policy **300** from security policy management server **120**. At step **1002**, packets associated with a network protected by each respective packet security gateway are received. For example, packet security gateway **112** may receive UDP packets from a device within network E **110** having an address that begins with 150 and that are destined for port 3030 of a device within network A **102**. At step **1004**, a packet transformation function specified by the dynamic security policy is performed on the packets. For example, rule **308** of dynamic security policy **300** may specify that packets using the UDP protocol, coming from a source address that begins with 150, having any source port, destined for any address, and destined for port 3030 should have an accept packet transformation function

performed on them, packet filter **214** may identify the UDP packets received from the device within network E **110** as matching the criteria specified by rule **308**, packet transformation function 1 **216** may be configured to forward packets, and packet security gateway **112** may utilize packet transformation function 1 **216** to perform the accept packet transformation function specified by rule **308** on the UDP packets received from the device within network E **110**.

[0077] 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 various embodiments. 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.

[0078] Although not required, one of ordinary skill in the art will appreciate that various aspects described herein may be embodied as a method, an apparatus, or as one or more computer-readable media storing computer-executable instructions. Accordingly, those 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.

[0079] As described herein, the various methods and acts may be operative across one or more computing servers and one or more networks. The functionality may be distributed in any manner, or may be located in a single computing device (*e.g.*, a server, a client computer, etc.).

[0080] 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 steps illustrated may be optional.

Keysight Technologies Ex. 1002
Page 449 of 460

CLAIMS

What is claimed is:

1. A method of filtering packets at a packet security gateway, of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway and one or more networks other than the network protected by the packet security gateway, the method comprising:

receiving, by the packet security gateway and from a security policy management server external from the network protected by the packet security gateway, a dynamic security policy comprising a first set of packet filtering rules to be applied to all network traffic traversing the boundary, wherein:

each packet filtering rule of the first set of packet filtering rules comprises at least one packet matching criterion and a corresponding packet transformation function, and

one or more first packet filtering rules of the first set of packet filtering rules were automatically created or altered by the security policy management server based on malicious traffic information received from a malicious host tracker service;

performing, on a packet by packet basis, packet filtering on a first portion of packets corresponding to network traffic traversing the boundary via the packet security gateway based on the first set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets;

receiving, by the packet security gateway and after performing packet filtering on the first portion of the packets, an updated second set of packet filtering rules for the dynamic security policy from the security policy management server, wherein the updated second set of packet filtering rules comprises an update to the one or more first packet filtering rules created or altered by the security policy management server based on updated malicious traffic information received from the malicious host tracker service; and

performing, on a packet by packet basis, packet filtering on a second portion of the packets corresponding to network traffic traversing the boundary via the packet security gateway based on the updated second set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the second set of packet filtering rules on the second portion of packets.

2. The method of claim 1, wherein the at least one packet matching criterion corresponding to the one or more first packet filtering rules automatically created or altered by the security policy management server comprises at least one network address indicated by the malicious traffic information.

3. The method of claim 1, wherein the malicious host tracker service comprises a subscription service that aggregates information associated with malicious network traffic.

4. The method of claim 1, wherein the malicious traffic information comprises a list of network addresses known to be associated with malicious network traffic.

5. The method of claim 1, wherein at least one packet transformation function comprises a network protective action.

6. The method of claim 1, further comprising:

receiving, by the packet security gateway, packets in a network layer transparent manner using an interface that is not addressed at the network layer; and

performing the at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets at the network layer.

7. The method of claim 1, wherein one or more packet filtering rules of the first set of packet filtering rules specify a packet transformation function other than forwarding or dropping the corresponding packets.

8. A packet security gateway, of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway and one or more networks other than the network protected by the packet security gateway, comprising:

one or more processors; and

memory storing instructions that, when executed by the one or more processors, cause the packet security gateway to:

receive, from a security policy management server external from the network protected by the packet security gateway, a dynamic security policy comprising a first set of packet filtering rules to be applied to all network traffic traversing the boundary, wherein:

each packet filtering rule of the first set of packet filtering rules comprises at least one packet matching criterion and a corresponding packet transformation function, and

one or more first packet filtering rules of the first set of packet filtering rules were automatically created or altered by the security policy management server based on malicious traffic information received from a malicious host tracker service;

perform, on a packet by packet basis, packet filtering on a first portion of packets corresponding to network traffic traversing the boundary via the packet security gateway based on the first set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets;

receive, after performing packet filtering on the first portion of the packets, an updated second set of packet filtering rules for the dynamic security policy from the security policy management server, wherein the updated second set of packet filtering rules comprises an update to the one or more first packet filtering rules created or altered by the security policy management server based on updated malicious traffic information received from the malicious host tracker service; and

perform, on a packet by packet basis, packet filtering on a second portion of the packets corresponding to network traffic traversing the boundary via the packet security

gateway based on the updated second set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the second set of packet filtering rules on the second portion of packets.

9. The packet security gateway of claim 8, wherein the at least one packet matching criterion corresponding to the one or more first packet filtering rules automatically created or altered by the security policy management server comprises at least one network address indicated by the malicious traffic information.

10. The packet security gateway of claim 8, wherein the malicious host tracker service comprises a subscription service that aggregates information associated with malicious network traffic.

11. The packet security gateway of claim 8, wherein the malicious traffic information comprises a list of network addresses known to be associated with malicious network traffic.

12. The packet security gateway of claim 8, wherein at least one packet transformation function comprises a network protective action.

13. The packet security gateway of claim 8, wherein the instructions further cause the packet security gateway to:

receive packets in a network layer transparent manner using an interface that is not addressed at the network layer; and

perform the at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets at the network layer.

14. The packet security gateway of claim 8, wherein one or more packet filtering rules of the first set of packet filtering rules specify a packet transformation function other than forwarding or dropping the corresponding packets.

15. One or more non-transitory computer readable media storing instructions that, when executed by at least one processor, cause a packet security gateway, of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway and one or more networks other than the network protected by the packet security gateway, to perform steps comprising:

receiving, from a security policy management server external from the network protected by the packet security gateway, a dynamic security policy comprising a first set of packet filtering rules to be applied to all network traffic traversing the boundary, wherein:

each packet filtering rule of the first set of packet filtering rules comprises at least one packet matching criterion and a corresponding packet transformation function, and

one or more first packet filtering rules of the first set of packet filtering rules were automatically created or altered by the security policy management server based on malicious traffic information received from a malicious host tracker service;

performing, on a packet by packet basis, packet filtering on a first portion of packets corresponding to network traffic traversing the boundary via the packet security gateway based on the first set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets;

receiving, after performing packet filtering on the first portion of the packets, an updated second set of packet filtering rules for the dynamic security policy from the security policy management server, wherein the updated second set of packet filtering rules comprises an update to the one or more first packet filtering rules created or altered by the security policy management server based on updated malicious traffic information received from the malicious host tracker service; and

performing, on a packet by packet basis, packet filtering on a second portion of the packets corresponding to network traffic traversing the boundary via the packet security gateway based on the updated second set of packet filtering rules by performing

at least one packet transformation function specified by at least one packet filtering rule of the second set of packet filtering rules on the second portion of packets.

16. The computer readable media of claim 15, wherein the at least one packet matching criterion corresponding to the one or more first packet filtering rules automatically created or altered by the security policy management server comprises at least one network address indicated by the malicious traffic information.

17. The computer readable media of claim 15, wherein the malicious host tracker service comprises a subscription service that aggregates information associated with malicious network traffic, and wherein the malicious traffic information comprises a list of network addresses known to be associated with malicious network traffic.

18. The computer readable media of claim 15, wherein at least one packet transformation function comprises a network protective action.

19. The computer readable media of claim 15, further comprising:

receiving, by the packet security gateway, packets in a network layer transparent manner using an interface that is not addressed at the network layer; and

performing the at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets at the network layer.

20. The computer readable media of claim 15, wherein one or more packet filtering rules of the first set of packet filtering rules specify a packet transformation function other than forwarding or dropping the corresponding packets.

21. A method of filtering packets at a packet security gateway configured for protection of a network and associated with a security policy management server external from the network, the method comprising:

receiving, by the packet security gateway, a dynamic security policy comprising a first set of packet filtering rules from the security policy management server, wherein each packet filtering rule of the first set of packet filtering rules comprises at least one packet matching criterion and a corresponding packet transformation function, and wherein one or more first packet filtering rules of the first set of packet filtering rules were automatically created or altered by the security policy management server based on malicious traffic information received from a malicious host tracker service;

performing, on a packet by packet basis, packet filtering on a first portion of packets associated with the network protected by the packet security gateway based on the first set of packet filtering rules by performing at least one of multiple packet transformation functions specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets;

receiving, by the packet security gateway and after performing packet filtering on the first portion of the packets, an updated second set of packet filtering rules for the dynamic security policy from the security policy management server, wherein the updated second set of packet filtering rules comprises an update to the one or more first packet filtering rules created or altered by the security policy management server based on updated malicious traffic information received from the malicious host tracker service; and

performing, on a packet by packet basis, packet filtering on a second portion of the packets associated with the network protected by the packet security gateway based on the updated second set of packet filtering rules.

22. The method of claim 21, wherein the at least one packet matching criterion corresponding to the one or more first packet filtering rules automatically created or altered by the security policy management server comprises at least one network address indicated by the malicious traffic information.

23. The method of claim 21, wherein the malicious host tracker service comprises a subscription service that aggregates information associated with malicious network traffic.

24. The method of claim 21, wherein the malicious traffic information comprises a list of network addresses known to be associated with malicious network traffic.

25. The method of claim 21, wherein at least one packet transformation function comprises a network protective action.

26. The method of claim 21, further comprising:

receiving, by the packet security gateway, packets in a network layer transparent manner using an interface that is not addressed at the network layer; and

performing the at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets at the network layer.

27. The method of claim 21, wherein one or more packet filtering rules of the first set of packet filtering rules specify a packet transformation function other than forwarding or dropping the corresponding packets.

Keysight Technologies Ex. 1002
Page 457 of 460

Abstract

Methods and systems for protecting a secured network are presented. For example, one or more packet security gateways may be associated with a security policy management server. At each packet security gateway, a dynamic security policy may be received from the security policy management server, packets associated with a network protected by the packet security gateway may be received, and at least one of multiple packet transformation functions specified by the dynamic security policy may be performed on the packets. Performing the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets may include performing at least one packet transformation function other than forwarding or dropping the packets.

Keysight Technologies Ex. 1002
Page 458 of 460

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	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK

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 _____

  filed on _____.

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: Steven Rogers Date (Optional): _____

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.

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	METHODS AND SYSTEMS FOR PROTECTING A SECURED NETWORK

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [x] The attached application, or
- [ ] United States application or PCT international application number _____ filed on _____.

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): 08-Oct-2012

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.

Privacy Act Statement: In accordance with the Privacy Act of 1974, Pub. L. 93-579, 5 U.S.C. 552a, and the Paperwork