



European Patent Office
80298 MUNICH
GERMANY

Questions about this communication?
Contact Customer Services at www.epo.org/contact



Samson & Partner Patentanwälte mbB
Widenmayerstraße 6
80538 München
ALLEMAGNE

Formalities officer
Leinmüller-Fiat, Christine

Date
07.10.2022

Reference I4690018EPI00Lr	OPPO 01	Application No./Patent No. 19170936.9 - 1216 / 3550795
Applicant/Proprietor Centripetal Networks Inc.		

BRIEF COMMUNICATION

Subject: ☐ Your letter of
☐ Our telephone conversation of
☐ Communication of
☐

Enclosure(s): ☒ Letter from the proprietor of the patent of 30.09.2022
☐ Letter from the opponent of
☐ Copy (copies)

Communication:

All annexes to the letter as well as the consolidated list of all opposition citations are available for inspection via the European Patent Register at www.epo.org/register. Should you wish to receive these documents in paper format, they will be supplied to you free of charge if specifically requested on receipt of this communication (OJ EPO 2022, A28).



For the Opposition Division

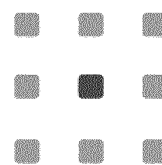


☐ **Registered letter**

EPO Form 2911O 04.22 (04/10/22)

page 1 of 1

MFG Patentanwälte | Amalienstr. 62 | D-80799 München
Europäisches Patentamt (EPA)
80298 München



mfg

PATENTANWÄLTE

European Patent Attorneys

European Trade Mark Attorneys

European Design Attorneys

Per Epoline

Dipl.-Phys., Dr. rer. nat.

Frank Meyer-Wildhagen, LL.M.

Dipl.-Phys., Dr. rer. nat.

Martin Meggle-Freund

Ihr Zeichen / Your Ref.:

Unser Zeichen / Our Ref.

Datum / Date:

210444EPPO/MF/HE

30 September 2022

Dipl.-Ing., Dipl.-Wirtsch.-Ing.

Till Gerhard

Application No.:	19 170 936.9
Patent No.:	3 550 795
Date of mention of grant:	2 June 2021
Title of the patent:	Methods and systems for protecting a secured network
Patentee:	Centripetal Networks Inc. Herndon, Virginia 20171 / US
Opponent:	Ixia Santa Rosa, CA 95403 / US
Intervenor 1:	Cisco Systems GmbH 85748 Garching / DE
Intervenor 2:	Keysight Technologies Deutschland GmbH 71034 Böblingen / DE
Intervenor 3:	Palo Alto Networks, Inc. Santa Clara, CA 95054 / US

To the opposition dated 2 March 2022, intervention 1 dated 23 May 2022, intervention 2 dated 27 May 2022, and intervention 3 dated 15 June 2022, we respond on behalf of the patentee of the above-identified patent (hereinafter: patent opposed) as follows:

A. Requests

We request

MFG Patentanwälte Meyer-Wildhagen Meggle-Freund Gerhard PartG mbB
Amtsgericht München: PR 1065 - USt-IdNr./VAT: DE277240401
Raiffeisenbank München-Süd eG – IBAN: DE43 7016 9466 0000 4988 15 – SWIFT-BIC: GENODEF1M03
Stadtparkasse München – IBAN: DE42 7015 0000 1001 8197 78 – SWIFT-BIC: SSKMDEMM

Amalienstraße 62
D-80799 München
Telefon +49 (0)89 - 41 61 72 99 0
Fax +49 (0)89 - 41 61 72 99 9
mail@mfg-ip.de
www.mfg-ip.de

- that the opposition be rejected and that the patent opposed be maintained as granted.

We further request, as an auxiliary measure,

- oral proceedings pursuant to Article 116 EPC, in case that maintenance of the patent opposed cannot occur in the written proceedings.

B. Preliminary Remarks

- 1 In section C, it is shown that the patent opposed discloses the invention in a manner sufficiently clear and complete to be carried out by a skilled person.
- 2 In section D, it is set forth that the subject-matter of independent claim 1 does not extend beyond the content of the application as filed and the parent application.
- 3 Section E pertains to the novelty of the subject-matter of independent claim 1.
- 4 In Section F, it is shown that the subject-matter of independent claim 1 comprises an inventive step over the teaching in the cited prior art.
- 5 Finally, patentability of the dependent claims is discussed in section G.

C. No insufficiency of disclosure

- 6 Intervenor 2 set forth that an automatic creation or alteration of packet filtering rules as per feature 1.1.3 is not disclosed in a sufficient manner.
- 7 Intervenor 2 grounds this by asserting that automatic generation and alteration of packet filtering rules includes very complex and non-obvious methods of recognising malicious threats in a network (cf. intervention 2, marginal 40)
- 8 However, the alleged recognition of malicious threats is not claimed.
- 9 Feature 1.1.3 reads

“wherein one or more first packet filtering rules, of the first set of packet filtering rules, was automatically created or altered by the security policy management server based on malicious traffic information received from a malicious host tracker service;”
- 10 The above underling wording indicates that the malicious traffic information is already provided by the malicious host tracker service. In other words, the malicious host tracker service recognises the malicious threats.
- 11 Feature 1.1.3 only requires that the security policy management server automatically creates or alters the packet filtering rules based on this already provided malicious traffic information.

- 12 Hence, intervenor 2's objection regarding an insufficiency of disclosure regarding malicious traffic information is moot and the patent opposed complies with the provisions of Art. 83 EPC.

D. No added-matter

- 13 The opponent as well as intervenors 1 and 2 brought forth numerous added-matter objections against claim 1 as granted. However, as will be shown below, these objections do not have any merits, since the subject-matter of claim 1 as granted is unambiguously and directly derivable from the original disclosure. The original disclosure herein refers to the parent application of the patent opposed (D6), which has the same content as the application documents of the patent opposed (D1).
- 14 As will be shown below, the claimed subject-matter does not extend beyond the content of the parent application and, accordingly, beyond the content of the application as filed for the patent opposed.

I. Combination of routing to a monitoring device (feature 1.2.6) and generating and reformatting a record (features 1.2.3 to 1.2.5) is disclosed

- 15 The opponent and intervenors 1 and 2 assert that a packet digest logging function specified by features 1.2.3 to 1.2.5 is not disclosed in combination with the routing function according to feature 1.2.6 (cf. opposition, page 4, section i); intervention 1, p. 22ff, intervention, p. 17, section d)).
- 16 We disagree. The original disclosure provides disclosure bases for these claim features.
- 17 To this end, it is referred to par. [41] of the original disclosure which reads as follows (emphasis added):

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,

Excerpt of par. [41] of D6 (emphasis added)

- 18 Each packet transformation function may be able to perform multiple functions on one (and, therefore, the same) packet.
- 19 Notably, par. [41] is directed to a general packet security gateway **112** of fig. 2, wherein no further application of an explicit scenario is mentioned.
- 20 At a fundamental level, the packet security gateway 112 is generally configured to perform one or more packet transformation functions (see D6, para. [43], emphasis added):

[43] 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.

Par. [43] of D6 (emphasis added)

- 21 An exemplary effect of a packet transformation function is the claimed packet digest logging (cf. D6, e.g., paras. [54] and [84], emphasis added):

that are of interest to an organization that operates the secured network. Such rules may further specify a packet transformation function that, when applied to a packet that matches such a rule, produces a digest version, or log, of the packet. This packet log (or digest) may

Excerpt of par. [54] of D6 (emphasis added)

packet-identification criteria. Referring to FIG. 12, at step 1202, each of a plurality of packet security gateways associated with a security policy management server may receive a dynamic security policy that includes at least one rule specifying packet-identification criteria and a packet transformation function comprising a packet digest logging function to be performed on packets corresponding to the packet-identification criteria from the security policy management server. For example, packet security

Excerpt of par. [84] of D6 (emphasis added)

- 22 Furthermore, routing packets (see D6, e.g., paras. [52] and [68], emphasis added) is also disclosed as an exemplary effect of a packet transformation function:

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

Excerpt of par. [52] of D6 (emphasis added)

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.

Excerpt of par. [68] of D6 (emphasis added)

- 23 The claimed functions of packet transformation, namely routing (see paras [68] to [71]) and packet digest logging (see paras [84] to [86]), are described as exemplary packet transformations in the context of the packet security gateway 112.
- 24 Therefore, par. [41] provides a basis for the aspect that a packet transformation function performed by the packet security gateway 112 may have a plurality of arbitrary effects, and examples thereof include the claimed packet digest logging and the claimed routing of packets.

- 25 In summary, the original disclosure provides, first, that one or more – e.g., two – functions may be applied to the same packet, and second, that such functions may be, for example, the packet digest logging function and the routing function. Thus, the claimed combination of features directed to a creation of a log from a packet and a routing of the same packet is disclosed in the original disclosure as filed.
- 26 Intervenor 1 further seeks to rely on the fact that a logging of packets on the one hand and a storing of packets on the other hand are directed to fundamentally different scenarios. According to intervenor 1, no scenario is disclosed in which there is a technical need both for a record comprising subsets of information and for the complete packet itself (see intervention 1, p. 22f). Therefore, according to intervenor 1, a combination of logging and storing of packets, which are described in separate embodiments, is allegedly not originally disclosed.
- 27 However, such a technical need as identified by intervenor 1 is not relevant to the question of whether subject-matter is derivable from the original disclosure. Logging and routing/storing packets are described as embodiments.
- 28 Moreover, from a technical-functional point of view, the same packet security gateway 112 can be used for logging and forwarding packets (see D6, e.g., para [69] and para [85], emphasis added).

[69] 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

Excerpt of par. [69] of D6 (emphasis added)

[85] At step 1206, the packet security gateway may identify from amongst the packets associated with the network protected by the packet security gateway, and on a packet-by-packet basis, one or more packets corresponding to the packet-identification criteria. For example, packet security gateway 112 may identify from amongst the packets associated with network A 102 one or more packets corresponding to the packet-identification criteria (e.g., by determining that the packet(s) comprise the specified

[...]

destination port within the specified range of destination ports). At step 1208, the packet security gateway may perform, on a packet-by-packet basis, the packet digest logging function on each of the packets corresponding to the packet-identification criteria. For example, packet security gateway 112 may perform the packet digest logging function on each of the identified packets.

Excerpt of par. [85] of D6 (emphasis added)

- 29 Additionally, the opponent argues that par. [53], which mentions “forwarding of packets to a monitoring device”, does not disclose that the monitoring device is provided for subsequent analysis.

It is further asserted that only in par. [67] to [70] of the original disclosure, analysis application is disclosed, but only included or performed by so-called SIP switches.

- 30 However, this is wrong. In fact, par. [0070] of the original disclosure reads as follows (emphasis added):

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

Excerpt of par. [70] of the D6 disclosure (emphasis added)

- 31 Thus, par. [70] the original disclosure provides literal disclosure that the monitoring device is configured to perform subsequent analysis.

II. Routing to monitoring device (feature 1.2.6) being part of the packet digest logging function (feature 1.2.2) is disclosed

- 32 Further, the opponent and intervenor 1 and 2 opine that the original disclosure does not indicate that a packet transformation function corresponds to a packet digest logging function (feature 1.2.2) (cf. opposition, p. 6, section ii); intervention 1, p. 24, section a); intervention 2, p. 16, section b)).

- 33 In particular, intervenor 1 refers to claim 10 and par. [84] of D6, which state the following:

“a packet transformation function comprising a packet digest logging function”

- 34 It is thereby disclosed that the packet digest logging function is to be regarded as part of the packet transformation function and thus a relation between the packet transformation function and the packet digest logging function is given. Therefore, the packet transformation function corresponds to the packet digest logging function.

- 35 Furthermore, intervenor 1 opines that routing a packet to a monitoring device (feature 1.2.6) is not included in the packet digest logging function according to the original disclosure (cf. intervention, p. 24, section b)).

- 36 Contrary to intervenor 1's view, however, the original application provides a broad disclosure regarding a packet transformation function and, in particular, regarding the packet digest logging function:

- 37 As set forth above in present marginal 18 to 24, a packet transformation function is generally configured to perform multiple functions.

- 38 With respect to the packet digest logging function, par. [86] reads as follows (emphasis added):

[86] In some embodiments, performing the packet digest logging function may include identifying a subset of information specified by the packet digest logging function (*e.g.*, a portion of data from the packet, a source address of the packet, a source port of the packet, a destination address of the packet, a destination port of the packet, a transport-protocol type of the packet, a uniform resource identifier (URI) from the packet, an arrival time of the packet, a size of the packet, a flow direction of the packet, an identifier of an interface of the packet security gateway that received the packet, and/or one or more media access control (MAC) addresses associated with the packet) for each of the identified packets, and generating a record comprising the subset of information for each of the identified packets. In some embodiments, packet security gateway 112 may be configured to temporarily store data comprising the subset of information for each of the identified packets, and to utilize the stored data to generate a message comprising the subset of information (or a portion thereof) for each of the identified packets. In such embodiments, packet security gateway 112 may communicate the message to a different computing device (*e.g.*, security policy management server 120). In some embodiments, the subset of information (or a portion thereof) may be reformatted (*e.g.*, by packet security gateway 112 and/or security policy management server 120) in accordance with a logging system standard (*e.g.*, syslog).

Par. [86] of D6 (emphasis added)

- 39 According to par. [86] of D6, the packet digest logging function comprises “*identifying a subset of information*”, “*generating a record comprising the subset of information*” and “*reformatting the subset of information*”.
- 40 In addition, par. [86] describes that the packet digest logging function “*may include* [...]” indicates a non-exhaustive list of steps, which means that there may well be further steps present in the packet digest logging function.
- 41 Since a packet transformation function can perform one or more functions (cf. D6, par. [41]) and a routing of packets is such a function, it is also disclosed in the original disclosure as filed that the packet digest logging function can further perform a routing of a packet.
- 42 Consequently, it is directly and unambiguously derivable from D6, *e.g.* from paragraph [86] in combination with paragraph [41], that routing of packets can be a part of the packet digest logging function.

III. Automatic creation or alteration of rules in combination with packet digest logging function (features 1.1.3, 1.2, and 1.2.2)

- 43 The opponent and intervenors 1 and 2 object that the original disclosure provides no basis for automatically created or altered rules which specify a packet digest logging function (see opposition, p. 7ff, section iii); intervention 1, p. 27ff; intervention 2, p. 20, section iii).
- 44 We disagree with this finding.
- 45 However, D6 discloses an automatic updating of rules specifying a packet digest logging function. Par. [64] of the original disclosure as filed (D6) reads as follows (emphasis added):

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

Fig. 8, D43 (marking added)

- 46 It is thus disclosed in a general way that rules are updated. As disclosed throughout several passages in the description of D6, packet transformation functions are specified by rules (see D6, e.g., paras [41], [44], [45] and [84]). In particular, par. [84] discloses that such rules may specify the very packet transformation function executing a packet digest logging function. Thus, it is apparent for a person skilled in the art from par. [64] in combination with, for example, par. [84] that rules specifying packet digest logging function can be automatically created or modified.
- 47 Furthermore, intervenor 1 tries to argue that par. [64] of D6 does not perform an automatic update for rules in general, but for network addresses in particular. The omission of this specification in claim 1 is allegedly not permissible (cf. intervention 1, p. 28, penultimate par.).
- 48 However, this specification is not necessary, since par [64] provides the literal disclosure to “automatically create or modify one or more such rules”. It is therefore the rules, and not the network addresses, that are updated.
- 49 Finally, intervenor 1 contends that automatic creation or alteration of rules is not disclosed in combination with a packet digest logging function that includes the claimed generation of records and routing (cf. intervention, p. 28, section b)).
- 50 However, as explained above, D6 discloses an association of (automatically updated) rules with a packet digest logging function. The fact that a packet digest logging function can further comprise a routing of packets was explained in marginals 32 to 42.
- 51 The association objected to by intervenor 1 thus follows directly and unambiguously from the original application.
- 52 The opponent further asserts that par. [64] of the original disclosure discloses the automatic creation or alteration of rules only in the context of determination of new network addresses associated with malicious traffic (cf. opposition, p. 7, fourth par.).
- 53 In this regard, par. [64] of the original disclosure states the following (emphasis added):

[64] 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.

Par. [64] of D6 (emphasis added)

54 As can be taken from the above, the security policy management server 120 automatically creates or alters "*as new network addresses associated with malicious traffic are determined*". The network addresses are part of updates received from a malicious host tracker service 508 which aggregates information associated with malicious network traffic (in other words, malicious traffic information). Thus, the rules are updated based on the malicious traffic information received from the malicious host tracker service 508. Insofar, the feature 1.1.3 is disclosed in par. [64] of the original disclosure.

IV. Providing an awareness service by packet digest logging function is disclosed without requiring generated logs to be accessed by an awareness application server

55 According to the opponent and intervenor 2, part of feature 1.2.2 reading "*a packet digest logging function that provides a network communications awareness service*" is allegedly not disclosed in the original disclosure (cf. opposition, p. 8, penultimate par.; intervention 2, p. 18, section ii).

56 However, par. [54] of the original disclosure, which reads as follows (emphasis added), states:

[54] In some embodiments, a dynamic security policy may include one or more rules, the combination of which may effectuate an implementation of an informational service for performing a network communications awareness service, a network security awareness service, and/or a network threat awareness service (e.g., for a particular network environment). For example, a dynamic security policy may include one or more rules that specify criteria such as one or more network addresses, protocol types, method types, and/or directions (e.g., inbound, outbound, or the like) that are indicative of packet communications that are of interest to an organization that operates the secured network. Such rules may further specify a packet transformation function that, when applied to a packet that matches such a rule, produces a digest version, or log, of the packet. This packet log (or digest) may contain selected packet information and/or system information (e.g., associated network addresses, ports, protocol types, URLs, arrival times, packet sizes, directions, interface names, media access control (MAC) addresses, matching rule IDs, metadata associated with matching rules, enforced policy names, or the like). The associated packet security gateway may store and/or forward packet logs using a logging system based on a standard (e.g., syslog, or the like). Awareness application servers may read packet logs and perform various transformations on the logs to produce awareness information, which may be accessed by client applications.

Par. [54] of D6 (emphasis added)

- 57 As per above, in order to provide the network communication awareness service performed by a dynamic security policy, the dynamic security policy includes, e.g., a rule which in turn specifies a packet transformation function for producing logs, i.e., a packet digest logging function. This is different than the opponent's assertion that *"the network communications awareness service [is] required to obtain information from one of the packet logs"* (see opposition, p. 8, last par.).
- 58 The generated logs *"may"* be read by awareness application servers. The formulation *"may"* indicates that the step of reading the logs is optional. But generating the log is the basis for the dynamic security policy to be able to provide the network communication awareness service.
- 59 Therefore, par. [54] of the original disclosure discloses that the packet digest logging function provides the network communication awareness service.

V. Security policy management server being external from the network is disclosed in isolation

- 60 The opponent refers to Fig. 5 of the original disclosure and asserts that externality of the malicious host tracker service is inextricably linked to the externality of the security policy management server.
- 61 Apart from Fig. 5 of the original disclosure, the security policy management server (SPM) being external to networks is also disclosed in, e.g., Figures 1 and 6 to 8 reproduced below (red arrows added).

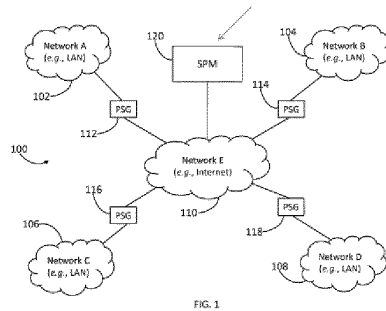


Fig. 1 of D6 (red arrow added)

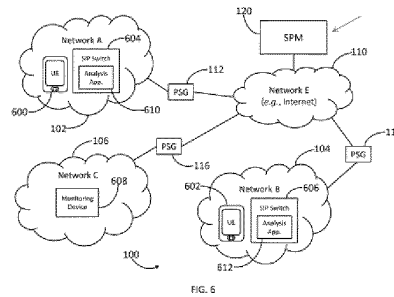


Fig. 6 of D6 (red arrow added)

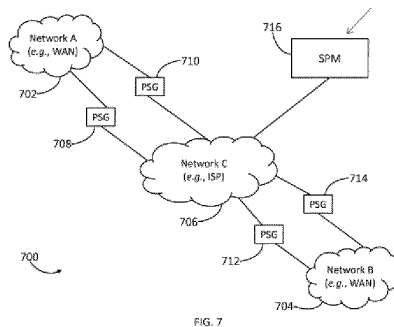


Fig. 7 of D6 (red arrow added)

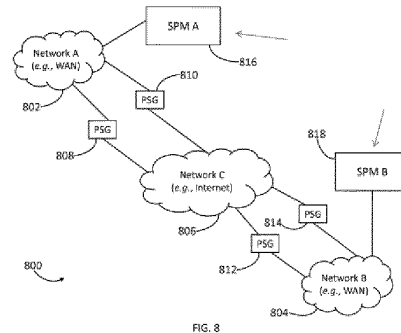


Fig. 8 of D6 (red arrow added)

- 62 As readily apparent from the above figures, the security policy management server SPM is external to various networks even without the presence of a malicious host tracker server.
- 63 Further, par. [64] of the original disclosure, which refers to Fig. 5, does not mentioned the malicious host tracker service 508 to be external of the protected networks. Thus, externality of the security policy management server is not inextricably linked to an externality of the malicious host tracker service.
- 64 Hence, the security policy management server being external to protected networks is disclosed in isolation by at least Fig. 1 and 5 to 8 in view of par. [64] of the original disclosure.

VI. A subset of information being „specified by the packet” (feature 1.2.4) is disclosed

- 65 Feature 1.2.4 of claim 1 as granted requires “generating a record comprising the subset of information specified by the packet”.
- 66 Intervenor 1 considers the underlined wording to be not originally disclosed. According to intervenor 1, in par. [86] and claims 13 to 16 of D6, it is allegedly disclosed only that the subset of information is specified by the packet logging function, and not by the packet itself (see intervention 1, p. 25).
- 67 However, the wording “subset of information specified by the packet” of claim 1 as granted requires only that the packet identifies the values for the information in the packet (e.g., “192.168.1.1” for a source

address identified). In other words, the wording “*subset of information specified by the packet*” indicates that the subset of information is included in the packet.

68 For example, claim 12 of D6 elaborates on what information in a packet is to be read from the packet by the packet digest logging function:

12. The method of claim 11, wherein the subset of information comprises at least one of a portion of data from the packet, a source address of the packet, a source port of the packet, a destination address of the packet, a destination port of the packet, a transport-protocol type of the packet, a uniform resource identifier (URI) from the packet, an arrival time of the packet, a size of the packet, a flow direction of the packet, an identifier of an interface of the packet security gateway that received the packet, or one or more media access control (MAC) addresses associated with the packet.

Claim 12 of D6

69 Exactly the listed information is also comprised in the packet and thereby also specified by the packet. To this end, par. [54] of D6 reads as follows (emphasis added):

such a rule, produces a digest version, or log, of the packet. This packet log (or digest) may contain selected packet information and/or system information (e.g., associated network addresses, ports, protocol types, URIs, arrival times, packet sizes, directions, interface names, media access control (MAC) addresses, matching rule IDs, metadata associated with matching rules, enforced policy names, or the like). The associated packet security gateway

Excerpt of par. [54] of D6 (emphasis added)

70 Thus, feature 1.2.4 is originally disclosed.

VII. “Performing ... packet filtering ... by performing... one ... packet transformation functions” (features 1.2 to 1.2.2) is disclosed

71 Claim 1 requires that packet filtering is performed by performing at least one packet transformation function which is specified by a packet filtering rule and corresponds to a packet digest logging function.

72 Intervenor 1 identifies this as a tautological feature wording (cf. intervention 1, 25ff).

73 We disagree.

74 The claimed aspect that the packet filtering is based on packet filtering rules runs throughout the original disclosure and is disclosed, for example, in par. [0074] (emphasis added):

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

Excerpt of par. [74] of D6 (emphasis added)

- 75 The further claimed aspect that packet filtering based on packet filtering rules also includes the performing at least one packet transformation function also runs throughout the original disclosure. It is referred by way of example to Fig. 3 and the corresponding description, in which packet transformation functions (last column of the table: “Action”) are disclosed as part of the packet filtering rules (there “Rules #1, ..., #5”).
- 76 Intervenor 1’s objections are therefore moot.
- 77 Intervenor 1 also erroneously states that only those packet transformations that perform forwarding or dropping of packets are in the context of packet filtering (cf. intervention 1, p. 26 and 27).
- 78 Particularly, this assertion is inconsistent with the disclosure in par. [40] and [41] of D6 that the packet security gateway 112 examines packets using a packet filter 214 and then transmits them to corresponding packet transformation functions 1-N 216, 218, and 220. In this regard, each of these packet transformation functions 1-N 216, 218, and 220 may perform one or more functions. As stated in marginal 23, the packet digest logging function is one such function. Consequently, packet filtering is not to be seen only in the context of packet transformation functions that perform as an action a forwarding or dropping of packets.
- 79 In summary, the original disclosure as filed, e.g., in par. [43], discloses performing packet filtering together with performing a packet transformation function.

VIII. Routing (feature 1.2.6) is not an undisclosed generalisation

1.2.6 *routing, by the packet security gateway, the packet to a monitoring device configured to store the packet for subsequent analysis;*

- 80 Intervenor 2 tries to limit the disclosure pertaining to the routing of packets to the embodiment shown in fig. 6 of the original disclosure, which is directed to an implementation of a multi-dimensional routing service. Therefrom, intervenor 2 derives that the routing function has to include a multi-dimensional routing and an encapsulation of the packet (cf. intervention 2, p. 14, section f).
- 81 However, by doing so, intervenor 2 neglects the general disclosure of par. [0045], which mentions routing of packets without any indication of multi-dimensional routing and encapsulation of the routed packet:

[45] 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.

Par. [45] of D6 (emphasis added)

82 Thus, the original disclosure does not require that the routing of a packets is multi-dimensional and that the packet is encapsulated.

IX. First and second sets of packet filtering rules comprised in a security policy (features 1.1.1 and 1.3)

83 Features 1.1.1 and 1.3 read as follows:

1.1.1 *a first set of packet filtering rules from the security policy management server,*

1.3 *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,*

84 Intervenor 2 opines that a subdivision of the dynamic security policy into a first and a second set of packet filtering rules is not originally disclosed.

85 However, according to feature 1.3.1, the second set of packet filtering rules comprises “an update to the first set of packet filtering rules”. Therefore, the second set of packet filtering rules also includes the updated rules of the first set. In other words, there is an initial set of rules, which is then updated. The entire set of rules initially present in the dynamic security policy corresponds to the first set of rules and the rules present after the update correspond to the second set of rules.

86 Contrary to intervenor 2’s assertion, there is no subdivision into the first and second set of packet filtering rules after the update.

87 However, the possibility of updating is mentioned throughout the original disclosure, e.g. in par. [87] (emphasis added):

set of network addresses. For example, security policy management server 120 may update one or more rules of dynamic security policy 300 (e.g., a rule specifying a deny packet

Excerpt of par. [87] of D6 (emphasis added)

88 Therefore, the “first set of packet filtering rules” as defined in feature 1.1.1 and the “second set of packet filtering rules” as defined in feature 1.3 is at least unambiguously and directly derivable from the original disclosure.

X. Packet matching criterion specified by more than one filtering rule (feature 1.1.2)

89 Feature 1.1.2 reads as follows:

1.1.2 *wherein each packet filtering rule of the first set of packet filtering rules comprises at least one packet matching criterion specified by one or more packet filtering rules,*

90 According to intervenor 2, a packet matching criterion being specified by more than one packet filtering rule is allegedly not originally disclosed.

- 91 However, the contrary is the case. In fact, the original disclosure mentions that two or more rules may specify overlapping criteria (cf. par. [46], emphasis added):

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

Excerpt of par. [46] of D6 (emphasis added)

- 92 Therefrom can be inferred, that two rules may specify the same (packet matching) criterion. Thus, a packet matching criterion being specified by more than one packet filtering rule is originally disclosed.

XI. Receiving updated filtering rules at the packet security gateway and filtering packets with updated filtering rules (feature group 1.3 and feature 1.4)

- 93 Feature group 1.3 and feature 1.3 read as follows:

1.3 *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,*

1.3.1 *wherein the updated second set of packet filtering rules comprises an update to the first set of packet filtering rules generated by the security policy management server based on updated malicious traffic information received from the malicious host tracker service;*

1.4 *performing, on a packet by packet basis, packet filtering on a second portion of the packets as sociated with the network protected by the packet security gateway based on the updated second set of packet filtering rules*

- 94 Intervenor 2 objects that using the updated set of rules to perform packet filtering is not originally disclosed.

- 95 Par. [40] of the original disclosure reads as follows (emphasis added):

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

Excerpt of par. [40] of D6 (emphasis added)

- 96 In other words, the packet filter 214 performs packet filtering on packets received by the packet security gateway 112.

- 97 The packet filtering is performed on the basis of the rules included in the dynamic security policy (cf. D6, par. [41], emphasis added):

[41] 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

Excerpt of par. [41] of D6 (emphasis added)

98 Now, when the dynamic security policy is updated with the second set of packet filtering rules, it necessarily follows that the packet filtering is performed on the basis of the updated rules within the dynamic security policy.

99 As such, performing packet filtering using the updated packet filtering rules is unambiguously and directly derivable from par. [41] and [42] of the original disclosure.

XII. Rewording of features defined in claim 1 is disclosed

100 On pages 10 and 11 of the opposition, the opponent sets forth that some terms of claim 1 do not appear in the original disclosure.

101 However, a mere rewording of feature does not necessarily result in subject-matter going beyond the content of the original disclosure. Rather, the standard underlying the assessment of amendments is what technical information can the skilled person unambiguously and directly derive from the application as filed (or, in this case, from the original disclosure). The opponent has not given any substantive reasons, why the wording should result in added-matter.

102 In the following, we provide explanations and bases in the patent application to as to why the objected-to terms do not add matter going beyond the content of the original disclosure.

XIII. Added-matter: Conclusion

103 In the above, it has been shown that the opponents' objections are moot and that the subject-matter of claim 1 does not extend beyond the scope of the original disclosure.

E. No lack of novelty

I. Sourcefire manual v5.1.1 (D23)

1. Sourcefire manual v5.1.1 (D23) is not publicly available

104 To substantiate an alleged public accessibility of the Sourcefire Manual v5.1.1 (D23), Defendant relies on an affidavit of Ms. Sarah Ehrig (D24) and another affidavit of Mr. Jacob Baugher III (D21).

105 But from these affidavits alone, the public availability of the Sourcefire manual v5.1.1 (D23) cannot be inferred.

106 The affidavit D24 of Ms Sarah Ehrig fails to state whether sales of Sourcefire appliances actually occurred. In particular, no actual sales numbers of Sourcefire appliances including Sourcefire manuals

- of version 5.1.1 were provided. It is set forth in e.g. items 4.3 and 5 of affidavit D24 only that Sourcefire *“enclosed each of the technical document PDF files (e.g., the SF 3D System user guide) documentation discs (CD-ROM or DVD) [are] included with each Sourcefire 3D System appliance (e.g., 3D Sensor, Defense Center) sold to a customer”*.
- 107 Hence, D24 fails to specify any concrete sales numbers or other details indicating the occurrence of sales. Item 5 of the affidavit D24 states that Ms Sarah Ehrig deduces from the timestamp on page 2 of the Sourcefire manual v5.1.1 and the general practice she describes that the document was made available to customers before the priority of the patent opposed (16 April 2014). Such a conclusion from more general principles is not a positive confirmatory statement that the document was in fact available to any customers, because it remains unclear if there were any number of sales in the relevant time and to whom.
- 108 Further, with respect to login credentials for downloading technical document PDF files, the affidavit D24 indicates merely that *“each of the technical document PDF files were publicly accessible for download by persons who had received a login and password from SF to SF’s customer-facing support website”* (emphasis added). However, no explanations are given on how to obtain said login credentials or if any people who may constitute a relevant representation of the public did in fact receive said login credentials.
- 109 In affidavit D21 of Jacob Baugher III, only the sales number of Sourcefire appliances delivered with Sourcefire manual v4.10 (D19) are presented. In item 6 of the affidavit D21 it is stated that Mr Baugher *“determined that there were 1299 customers that purchased and obtained the Sourcefire 3D System within the above identified time period [starting April 2011 and before 16 April 2014] including Version 4.10”*. The priority date of the opposed patent is 16 April 2014. At no point does the affidavit D24 confirm that Sourcefire manual v5.1.1 (D23) was shipped to any customers before that date.
- 110 Regarding shipment of devices with the Sourcefire manual v5.1.1 (D23), Mr. Baugher III only states very vaguely that he has “personal knowledge” about shipment D23 to some customers. No actual facts are given about an actual sale or shipment of devices with the Sourcefire manual v5.1.1.
- 111 The affidavit E11 only asserts sales numbers for any Sourcefire appliances without any indication of Sourcefire manuals (such as D10) shipped therewith.
- 112 Therefore, there is a link missing in affidavits E11 and E9 which are unfit to unambiguously demonstrate that Sourcefire appliances, to which Sourcefire manuals v5.1.1 were allegedly enclosed, correspond to the actually sold Sourcefire appliances as stated in E9.
- 113 In summary: Affidavit D24 by Ms. Ehrig states only that the Sourcefire manual v5.1.1 was allegedly included with the Sourcefire devices. In the affidavit D21 of Mr. Baugher III only sales numbers for Sourcefire devices are given, to which version 4.10 of the Sourcefire manual D19 was attached. Thus, even linking affidavit D21 to affidavit D24 does not prove that Sourcefire devices allegedly accompanied by Sourcefire manuals v5.1.1 were actually sold prior to the priority date of the patent opposed.

- 114 In light of the foregoing, Affidavits D21 and D24 cannot establish that Sourcefire manual v5.1.1 (D23) was publicly available prior to the priority date of the patent opposed.
- 115 Moreover, none of the affidavits D21 and D24 indicates where Sourcefire appliances were available for purchase by customers. In particular, affidavits D21 and D24 do not indicate where Sourcefire appliances could be purchased, whether it was possible for any person to purchase Sourcefire appliances, and whether the purchase thereof was subject to any conditions such as non-disclosure agreements.
- 116 Even if the Sourcefire Manual v5.1.1 (D23) were considered prior art, it does not anticipate the subject-matter of claim 1 of the patent opposed in a manner detrimental to novelty.
- 117 Contrary to intervenor 1's assertion, the Sourcefire Manual v5.1.1 (D23) does not anticipate the subject-matter of the independent claims. At any rate, features 1.1.3, 1.2.5, 1.2.6, 1.4, and feature group 1.3 of claim 1 of the patent opposed (and corresponding features of claims 14 and 15) are not disclosed in the Sourcefire Manual v5.1.1 (D23), as explained below.

2. Teaching of Sourcefire manual v5.1.1 (D23)

- 118 The Sourcefire manual v5.1.1 discloses a Defense Center that includes policies, such as an access control policy (cf. D23, p. 163).

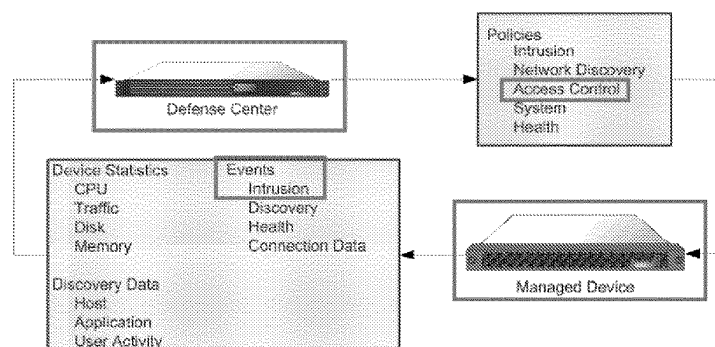


Figure of p. 163, D23 (red emphasis added)

- 119 An access control policy comprises access control rules and specifies a security intelligence (cf. D23, p. 2131).
- 120 Intervenor 1 submits that the Defense Center of the D23 corresponds to a security policy management server according to feature 1.1 and that a managed device of D23 corresponds to a packet security gateway according to feature 1.1. Intervenor 1 considers the access control policy to be a “dynamic security policy” according to feature 1.1.

3. No disclosure of feature 1.1.3 and feature group 1.3

1.1.3 wherein one or more first packet filtering rules, of the first set of packet filtering rules, was automatically created or altered by the security policy management server based on malicious traffic information received from a malicious host tracker service;

- 121 According to feature 1.1.3, the packet filtering rules of the first set of packet filtering rules are automatically updated by the security policy management server. Here, the first set of packet filtering rules is part of a dynamic security policy received by the packet security gateway from the security policy management server (features 1.1 and 1.1.1).
- 122 Intervenor 1 asserts that the “Security Intelligence” with the “Security Intelligence Feed” of D23 corresponds to the “first set of packet filtering rules” according to feature 1.1.1 (see intervention 38, section (iii)).
- 123 However, this is not correct:
- 124 The Security Intelligence is not a packet filtering rule in the sense of feature 1.1.3. The access control policy according to D23 contains, in addition to the access control rules (i.e., the alleged packet filtering rules), the Security Intelligence as a component distinct from the access control rules (cf. D23, p. 311, figure reproduced below, red marked added for the two distinct components):

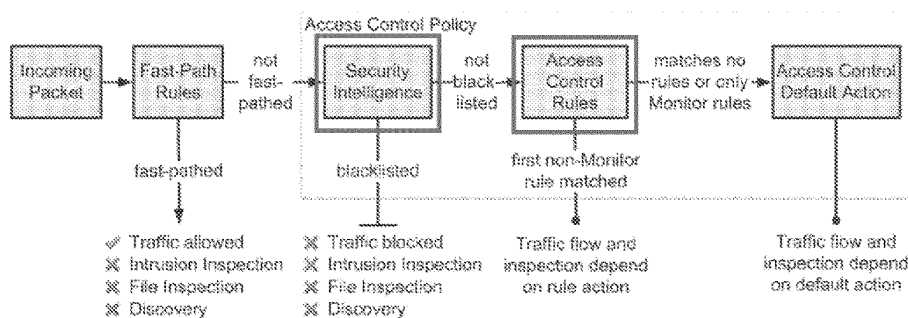


Figure of p. 311, D23 (red marked added)

- 125 In the above figure, the Security Intelligence is not shown as part of the access control rules (the alleged packet filter rules).
- 126 The Security Intelligence is used to control network traffic, in particular by blacklisting predetermined IP addresses. Blacklisting denies traffic to and from the predetermined IP addresses before the network traffic is subjected to the access control rules (cf. D23, p. 2151). Again, this shows that the Sourcefire manual v5.1.1 makes a distinction between the Security Intelligence and access control rules:

Security Intelligence A feature that allows you to specify the traffic that can traverse your network, per access control policy, based on the source or destination IP address. This is especially useful if you want to blacklist — deny traffic to and from — specific IP addresses, before the traffic is subjected to analysis by access control rules. Optionally, you can use a monitor setting for Security Intelligence filtering, which allows the system to analyze connections that would have been blacklisted, but also logs the match to the blacklist.

Excerpt of p. 2151, D23 (emphasis added)

- 127 The Security Intelligence with the Security Intelligence feed, to which intervenor 1 refers, is thus not a packet filtering rule within the meaning of feature 1.1.3. For this reason alone, feature 1.1.3 is not realized by the Security Intelligence with the Security Intelligence feed of the Sourcefire Manual v5.1.1, contrary to intervenor 1's arguments.
- 128 However, the access control rules of the Sourcefire manual v5.1.1, to which intervenor 1 also refers, do not realize feature 1.1.3 either. This is because these access control rules are not associated with any malicious traffic information.
- 129 Furthermore with regard to the Security Intelligence, it is not stated in the Sourcefire manual v5.1.1 that the Security Intelligence is transferred from the Defense Center to a managed device.
- 130 Intervenor 1 asserts that the received access control policy also includes the Security Intelligence and refers to the definition of access control policy on p. 2131 of D23:

access control policy A policy that you apply to managed devices to perform access control on the network traffic monitored by those devices. An access control policy may include multiple access control rules; it also specifies a default action, which determines the handling and logging of traffic that does not meet the criteria of any of those rules. An access control policy can also specify HTTP response page, Security Intelligence, and other advanced settings.

Excerpt of p. 2131, D23 (emphasis added)

- 131 However, the above definition indicates only that the access control policy specifies the Security Intelligence. A transfer of the Security Intelligence from the Defense Center to the managed device is not described.
- 132 In fact, there is no disclosure in D23 that the Security Intelligence feed is transmitted from the Defense Center to the managed device. At most, it is disclosed that the Security Intelligence feed can be provided to help an administrator manually build blacklists directly on the device (cf. D23, p. 142). In any case, the Security Intelligence itself, which uses the Security Intelligence feed, is not transmitted from the Defense Center to the managed device, as explained above.
- 133 Updating the Security Intelligence of the access control policy is also done without transmitting the access control policy from the Defense Center to the managed device. The Sourcefire manual v5.1.1 on p. 142 states that the access control policies do not need to be reapplied after a feed has been created or modified or after a scheduled feed update:

Comparing Feeds and Lists

A Security Intelligence *feed* is a dynamic collection of IP addresses that the Defense Center downloads from an HTTP or HTTPS server at the interval you configure. Because feeds are regularly updated, the system can use up-to-date information to filter your network traffic. To help you build blacklists, Sourcefire provides the *Sourcefire Intelligence Feed*, which represents IP addresses determined by the Sourcefire VRT to have a poor reputation.

When the Defense Center downloads updated feed information, it automatically updates its managed devices. Although it may take a few minutes for a feed update to take effect throughout your deployment, you do not have to reapply access control policies after you create or modify a feed, or after a scheduled feed update.

Excerpt of p. 142, D23 (emphasis added)

- 134 In other words, an update of Security Intelligence and thus a blacklist is performed on the managed device itself and not on the Defense Center.
- 135 However, this update process of the Sourcefire Handbook v5.1.1 (D23) is different from the automatic creation or alteration of packet filtering rules according to feature 1.1.3. According thereto, the packet filtering rules (of the first set of packet filtering rules) are updated by the security policy management server and then sent to the packet security gateway as part of the dynamic security policy.
- 136 Also for this reason, the Sourcefire manual v5.1.1 does not disclose feature 1.1.3.
- 137 Consequently, feature group 1.3 is not disclosed which reads as follows:

1.3 *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,*

1.3.1 *wherein the updated second set of packet filtering rules comprises an update to the first set of packet filtering rules generated by the security policy management server based on updated malicious traffic information received from the malicious host tracker service;*

- 138 In this regard, intervenor refers also to p. 142 of the Sourcefire Manual v5.1.1 (D23), according to which the Defense Center downloads the updated feed information of the Security Intelligence feed. However, this downloading of the Security Intelligence feed does not constitute automatic rule creation by the Defense Center, as explained above.

4. No disclosure of feature 1.2.5

1.2.5 *reformatting the subset of information specified by the packet in accordance with a logging system standard; and*

- 139 Feature 1.2.5 (in conjunction with feature 1.2.2) requires reformatting of the subset of information as part of a packet digest logging function.
- 140 For the disclosure of this feature, intervenor 1 refers to the syslog format on p. 470 of the Sourcefire manual v5.1.1 (D23) (cf. intervention 1, p. 46).
- 141 However, the syslog format is mentioned in the Sourcefire manual v5.1.1 (D23) only in the context of an automatic alerting in general. Syslog alert responses can be generated for events such as intrusion events (cf. D23, p. 905):

There is another type of alerting you can perform in the Sourcefire 3D System, outside of your intrusion policies. You can configure email, SNMP, and syslog alert responses for other types of events, including intrusion events with specific impact flags, or connection events logged by specific access control rules. For more information, see Configuring External Alerting on page 403

Excerpt of p. 905, D23 (emphasis added)

- 142 According to the above excerpt of p. 905, the alerting by means of a syslog notification is done “outside of your intrusion policies”, i.e. not as part of packet filtering rules. However, the syslog alert responses

about intrusion events of the Sourcefire manual v5.1.1 (D23) are thus not an aspect of a packet digest logging function in the sense of the patent opposed. When creating an intrusion event, the information of a packet is not reformatted according to the syslog format, but at most messages about intrusion events are transmitted according to the syslog standard, which, however, is not part of an intrusion policy and consequently has nothing to do with the packet filtering rules, packet transformation functions or the packet digest logging function according to the patent opposed.

5. No disclosure of feature 1.2.6

1.2.6 *routing, by the packet security gateway, the packet to a monitoring device configured to store the packet for subsequent analysis;*

- 143 The packet specified in feature 1.2.6 is the same packet specified in feature 1.2.3, namely the packet that matches the packet matching criterion of a packet filtering rule that specifies the packet digest logging function. In other words, the packet from which a log is created is also routed to the monitoring device.
- 144 Intervenor 1, however, focuses on copies of events being recorded, reformatted and transmitted to the Defense Center (cf. intervention 1, p. 46, first and last paras.).
- 145 But p. 469 of the Sourcefire manual v5.1.1 as cited by intervenor 1 does not disclose that copies of events are transmitted:

The Sourcefire 3D System can help you monitor your network for traffic that could affect the availability, integrity, and confidentiality of a host and its data. By placing managed devices on key network segments, you can examine the packets that traverse your network for malicious activity. The system has several mechanisms it uses to look for the broad range of exploits that attackers have developed.

When the system identifies a possible intrusion, it generates an *intrusion event*, which is a record of the date, time, the type of exploit, and contextual information about the source of the attack and its target. For packet-based events, a copy of the packet or packets that triggered the event is also recorded. Managed devices transmit their events to the Defense Center where you can view the aggregated data and gain a greater understanding of the attacks against your network assets.

Excerpt of p. 469, D23 (emphasis added)

- 146 Further, intervenor 1 equates the Defense Center already with the security policy management server of feature 1.1. In contrast, feature 1.2.6 requires routing to “*a monitoring device*” and thus to a device other than the security policy management server.

6. Interim conclusion

- 147 Thus, the subject-matter of claim 1 as granted (and therefore claims 14 and 15) is not anticipated by the Sourcefire manual v5.1.1 (D23) in a manner that is prejudicial to novelty.

II. Sourcefire manual v4.10 (D19)

148 Also, contrary to intervenor 1's assertion, the Sourcefire manual v4.10 (D19) does not anticipate the subject-matter of the claim 1 as granted. At least features 1.1, 1.1.3, 1.2.5, 1.2.6, 1.3.1 as well as 1.4 are not disclosed in the Sourcefire manual v4.10 (D19), as we explain below in section E.II.2.

149 It is further noted that intervenor 2 also relies on the Sourcefire manual v4.10 (D19) for asserting a lack of novelty of claim 1 (cf. section E.II.3) and provides an alternative attack in particular with respect to feature 1.1.3 (cf. section E.II.3.a).

150 However, as will set forth below, the subject-matter of claim 1 is novel over the Sourcefire manual v4.10.

1. Teaching of Sourcefire manual v4.10 (D19)

151 The Sourcefire manual v4.10 (D19) is an earlier version of the Sourcefire manual v5.1.1 (D23) discussed above. It comprises less information than the later version v5.1.1 and therefore falls even further short in its disclosure content with respect to the features of the patent opposed.

152 The Sourcefire Manual v4.10 (D19), like the Sourcefire Manual v5.1.1 (D23), discloses a Defense Center that has policies, such as an intrusion policy (see D19, p. 107).

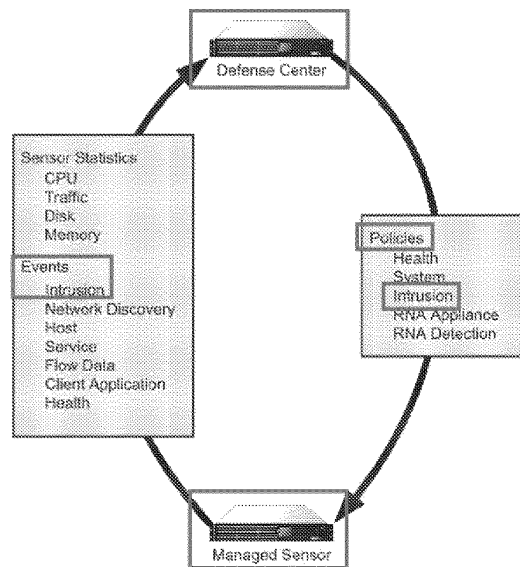


Figure of p. 107, D19 (emphasis added)

153 An intrusion policy comprises in turn a plurality of intrusion rules (cf. D19, p. 2084, emphasis added):.

intrusion policy

A variety of components that you can configure to inspect your network traffic for intrusions and policy violations. These components include intrusion rules that inspect the protocol header values, payload content, and certain packet size characteristics; variables commonly used in intrusion rules; RNA recommended rules configuration; advanced settings such as preprocessors and other detection and performance features; and preprocessor rules that allow you to generate events for associated preprocessor options.

intrusion rule

A set of keywords and arguments that, when applied to captured network traffic, identify potential intrusions, policy violations, and security breaches. IPS compares packets against the conditions specified in each rule and, if the packet data matches all the conditions specified in the rule, the rule triggers and generates an intrusion event. Intrusion rules include alert rules, drop rules, and pass rules.

Ausschnitt von S. 2084, D19 (Hervorhebungen hinzugefügt)

154 There are two types of intrusion rules, i.e., shared object rules and standard text rules (cf. D19, p. 761):

Note the following:

- For a *drop* rule in an inline deployment, IPS drops the packet and generates an event. For more information on drop rules, see Setting Rule States on page 435.
- Sourcefire provides two types of intrusion rules: shared object rules and standard text rules. The Sourcefire Vulnerability Research Team can use shared object rules to detect attacks against vulnerabilities in ways that traditional standard text rules cannot. You cannot create shared object rules. When you write your own intrusion rule, you are creating a standard text rule.

Excerpt of p. 761, D19 (emphasis added)**2. Re intervention 1****a. No disclosure of feature 1.1**

1.1 *receiving, by a packet security gateway (112) configured for protection of a network and associated with a security policy management server (120) external from the network, a dynamic security policy comprising*

155 Intervenor 1 asserts that the managed sensor described in the Sourcefire Manual v4.10 (D19) receives a “dynamic security policy” within the meaning of feature 1.1 from a central Defense Center that allegedly serves as an security policy management server.

156 However, the text cited by intervenor 1 to this end does not speak of the transmission of a dynamic security policy - as required by feature 1.1 - but only of a “policy” (cf. D19, p. 34):

“You can also push policies created on the Defense Center and software updates to managed sensors.”

157 These “policies” of the managed sensor are not dynamic security policies in the sense of feature 1.1, because according to the IPS section on page 34 of the Sourcefire manual v4.10 (D19), no aspect of such a policy is generated automatically, but the entire policy manually by a team of employees, the so-called “Sourcefire Vulnerability Research Team” (VRT):

„3D Sensors that are licensed to use IPS include a set of intrusion rules developed by the Sourcefire Vulnerability Research Team (VRT).”

158 Consequentially, p. 37 of the Sourcefire manual v4.10 (D19) also states that the policies cannot be managed from the Defense Center (emphasis added):

„Although you cannot manage policies or rules for an Intrusion Agent from the Defense Center, you can do analysis and reporting on those events. If the network map on the Defense Center has entries for the target host in a given event, the Defense Center assigns impact flags to the events. You can continue to manually tune Snort rules and preprocessors with the Intrusion Agent in place.”

159 Thus, Sourcefire manual v4.10 (D19) with the policies mentioned there does not disclose a dynamic security policy according to feature 1.1.

b. No disclosure of feature 1.1.3

1.1.3 *wherein one or more first packet filtering rules, of the first set of packet filtering rules, was automatically created or altered by the security policy management server based on malicious traffic information received from a malicious host tracker service;*

160 With regard to the automatic creation of rules, intervenor 1 relies on the automatic import of “Security Enhancement Updates” (hereinafter “SEU”) by the Defense Center (cf. intervention 1, p. 62f).

161 These SEUs include new and updated standard text rules and shared object rules and are published by the Sourcefire VRT (see D19, p. 1716).

As new vulnerabilities are identified, the Sourcefire Vulnerability Research Team (VRT) releases Security Enhancement Updates (SEUs). An SEU contains new and updated standard text rules and shared object rules and may contain updated versions of Snort® and features such as preprocessors and decoders. You can automatically download and install SEUs.

Excerpt of p. 1716, D19 (emphasis added)

162 The SEUs, and thus the rules they contain, are therefore not created or modified by the Defense Center, but rather by the VRT. The Defense Center merely downloads the SEUs at regular intervals.

163 Thus, the Sourcefire Manual v4.10 (D19) does not disclose any automatic creation of rules by an security policy management server as defined in feature 1.1.3.

164 Further, intervenor 1 attempts to show that a “malicious host tracker service” as per feature 1.1.3 is equivalent to the Sourcefire VRT mentioned in the Sourcefire manual v4.10 (D19).

165 However, the Sourcefire VRT does not identify (or, literally, “track”) malicious hosts (e.g., network addresses of hosts that are the source of malicious traffic). Rather, the Sourcefire VRT identifies “vulnerabilities” (cf. D19, p. 1716) contained in a packet payload. This is also evident from the definition of intrusion rules (see marginal 153), which states that an intrusion rule is a “*set of keywords and arguments that, when applied to captured network traffic, identify potential intrusions, policy violations, and security breaches*”.

166 Keywords and arguments are included in a rule option of a standard text rule (which is a form of an intrusion rule, see marginal 154). The rule option is one of two logical sections of the standard text rule. The other logical section is a rule header that defines a rule action and IP header values of a packet such as source and destination IP address (cf. D19, p. 762).

All standard text rules contain two logical sections: the rule header and the rule options. The rule header contains:

- the rule's action or type
- the protocol
- the source and destination IP addresses and netmasks
- direction indicators showing the flow of traffic from source to destination
- the source and destination ports

The rule options section contains:

- event messages
- keywords and their parameters and arguments
- patterns that a packet's payload must match to trigger the rule
- specifications of which parts of the packet the rules engine should inspect

Excerpt of p. 762, D19 (emphasis added)

167 As per p. 764 of the Sourcefire manual v4.10 (D19), the rule header specifies which packets are to be checked. A match of received packets with the values specified in the rule header (e.g. source IP addresses) therefore does not trigger the effect of the intrusion rule. That is, an intrusion rule is not aimed at detecting malicious traffic based on network addresses (e.g. source IP addresses) and a subsequent dropping of such packets.

168 But this is precisely what is contemplated in the patent opposed. For example, par. [0051] of the patent opposed reads that the security policy management server creates or alters the dynamic security policy rules to block network traffic associated with certain network addresses.

“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.”

169 That an intrusion rule of the Sourcefire manual v4.10 (D19) is not directed at examining a host address can also be inferred from the fact that the Sourcefire manual v4.10 (D19) describes the role of its preprocessors in the context of applying intrusion rules, wherein the preprocessors normalize traffic (see D19, p. 34) and reformat traffic to ensure that the rules engine reads traffic in the same format in which it is received from the host (see D19, p. 484).

3D Sensors that are licensed to use IPS include a set of *intrusion rules* developed by the Sourcefire Vulnerability Research Team (VRT). You can choose to enable rules that would detect the attacks you think most likely to occur on your network. You can also create custom intrusion rules tuned to your environment. In addition, 3D Sensors with IPS run *preprocessors* against detected network traffic to normalize traffic and detect malicious packets.

Excerpt of p. 34, D19 (emphasis added)

3D Sensors with IPS use preprocessors to reformat traffic to make sure the rules engine reads the traffic in the same format it will be received by the host. Without preprocessing, the IPS component cannot appropriately evaluate traffic because protocol differences make pattern matching impossible. Sourcefire preprocessors normalize traffic and help identify network layer and transport layer protocol anomalies by identifying inappropriate header options, defragmenting IP datagrams, providing TCP stateful inspection and stream reassembly, providing UDP stream preprocessing, resolving application command syntax, and validating checksums.

Excerpt of p. 484, D19 (emphasis added)

- 170 The Sourcefire manual v4.10 (D19) teaches that without preprocessing, the IPS component cannot adequately evaluate traffic because protocol differences make pattern matching impossible. If the intrusion rules of Sourcefire manual v4.10 were concerned with where packets originated (e.g., the network addresses of the hosts sending the traffic), there would be no need for preprocessors to normalize traffic to detect patterns indicative of malicious activity. Because the intrusion rules of the Sourcefire Manual v4.10 deal with the content of a packet and not the host from which it originates, intervenor 1 has not demonstrated that the Sourcefire VRT can be equated to the malicious host tracker service of feature 1.1.3. In other words, intervenor 1 has not shown that the Sourcefire VRT identifies a malicious host.
- 171 Consequently, Sourcefire manual v4.10 (D19) does not disclose a malicious host tracker service as per feature 1.1.3.

c. No disclosure of feature 1.2.5

1.2.5 *reformatting the subset of information specified by the packet in accordance with a logging system standard;*
and

- 172 According to intervenor 1, reformatting is disclosed by generating an intrusion event.
- 173 However, the Sourcefire manual v4.10 (D19) does not describe reformatting according to a logging system standard when generating intrusion events.
- 174 The pages 293ff of the Sourcefire manual v4.10 (D19) cited by intervenor in this regard describe only a "Packet View" for viewing packet information. In packet view, packet information is presented in tabular manner. But reformatting information according to a logging system standard is not apparent from it.
- 175 Furthermore, intervenor refers to pages 752ff of the Sourcefire manual v4.10 (D19) with reference to feature group 2 and states that reformatting is based on a syslog standard.
- 176 Pages 752ff of the Sourcefire manual v4.10 concern so-called syslog responses. It describes that so-called syslog alerts, which are intrusion event notifications, can be sent to a syslog on a device. The syslog is a standard logging mechanism that indicates, among other things, from which device the syslog alert was generated.

The system log, or syslog, is the standard logging mechanism for network event logging. You can send syslog alerts, which are intrusion event notifications, to the syslog on an appliance. The syslog allows you to categorize information in the syslog by priority and facility. The priority reflects the severity of the alert and the facility indicates the subsystem that generated the alert. Facilities and priorities are not displayed in the actual message that appears in syslog, but are instead used to tell the system that receives the syslog message how to categorize it.

Excerpt of p. 752, D19 (emphasis added)

- 177 It therefrom follows that reformatting based on a syslog standard is not done when intrusion events are created, but in a syslog. This is also apparent from p. 261 and 262 of the Sourcefire manual v4.10 (D19), according to which alarm mechanisms such as feedback can be provided in addition to intrusion events. In particular, alarms can be set up for the syslog.

In addition to generating intrusion events based on attacks, you can use an extensive list of alerting mechanisms to make sure that specific attacks are brought to your attention immediately. Conversely, you can suppress events that are less likely to affect critical systems or set a threshold that the number of events must reach before you are alerted.

For more information about automated alerting, see Configuring External Responses to Intrusion Events on page 734.

You can use the following tools to set up automatic responses to intrusion events:

- * automated alerting that you can configure for SNMP, email, and syslog
For more information, see Configuring External Responses to Intrusion Events on page 734.

Excerpt of p. 261 and 262, D19 (emphasis added)

- 178 Thus, D19 does not disclose reformatting of information according to feature 1.2.5.

d. No disclosure of feature 1.2.6

1.2.6 *routing, by the packet security gateway, the packet to a monitoring device configured to store the packet for subsequent analysis;*

- 179 Intervenor 1 sees the feature disclosed, in the Sourcefire manual v4.10 (D19), by sending an intrusion event to the Defense Center. In particular, an intrusion event is also the identified packet itself which matches the packet match criterion (see intervention 1, p. 65).
- 180 The intrusion event being the identified packet is incorrect. An intrusion event corresponds to a record that includes the date, time, type of attack, and contextual information about a source of the attack and its target. In cases of “packet-based” events, a copy of the packet that triggered the packet is recorded (cf. D19, p. 35). However, recording the packet copy does not correspond to routing the identified packet to another device.

When a 3D Sensor identifies a possible intrusion, it generates an *intrusion event*, which is a record of the date, time, the type of exploit, and contextual information about the source of the attack and its target. For packet-based events, a copy of the packet or packets that triggered the event is also recorded.

Excerpt of p. 35, D19

- 181 Thus, the Sourcefire manual v4.10 (D19) does not disclose routing of the (logged) packet.

- 182 Furthermore, the Sourcefire manual v4.10 also does not disclose routing of the packet to a monitoring device. In the Sourcefire manual v4.10, the intrusion event (and thus the alleged packet) is allegedly sent to the Defense Center. However, intervenor 1 equates the Defense Center with the security policy management server according to feature 1.1. By contrast, feature 1.2.6 requires routing to “a monitoring device” and thus to a device other than the security policy management server.
- 183 Accordingly, Sourcefire manual v4.10 does not disclose routing a packet to a monitoring device as per feature 1.2.6.

e. No disclosure of feature 1.3.1

1.3.1 *wherein the updated second set of packet filtering rules comprises an update to the first set of packet filtering rules generated by the security policy management server based on updated malicious traffic information received from the malicious host tracker service;*

- 184 The updated second set of packet filtering rules is provided for the dynamic security policy (cf. feature 1.3) and is consequently a part thereof. According to feature 1.3.1, the second set of packet filtering rules comprises an update of the first set of packet filtering rules and is also based on malicious traffic information received from the malicious host tracker service. Thus, for example, the security policy management server may automatically receive updated traffic information from the malicious host tracker service as part of a subscription and then create or alter (cf. patent opposed, par. [0051]) or combine (cf. patent opposed, par. [0052]) rules of a dynamic security policy using this information. That is, the security policy management server creates the updated rules.
- 185 Regarding feature 1.3, intervenor 1 refers to the Security Enhancement Updates, SEU, manually created by the Sourcefire VRT (cf. intervention 1, p67f). The SEUs are imported by the Defense Center and then applied to the managed sensor.
- 186 However, the updating, i.e., creating or altering, of the rules is not performed by the Defense Center, but by the Sourcefire VRT. But this process is different from feature 1.3.1, which requires the security policy management server to create or alter the rules.
- 187 Finally, the Sourcefire VRT cannot be considered a malicious host tracker service either, since the Sourcefire VRT does not identify malicious hosts, but rather vulnerabilities (exploits) in the package itself. Accordingly, the Sourcefire VRT focuses on what is in the package rather than where it came from (as explained in marginals 165ff).
- 188 Consequently, updating rules by the security policy management server according to feature 1.3.1 is not disclosed in Sourcefire manual v4.10.

f. No disclosure of feature 1.4

1.4 *performing, on a packet by packet basis, packet filtering on a second portion of the packets as sociated with the network protected by the packet security gateway based on the updated second set of packet filtering rules*

189 Feature 1.4 is directed to packet filtering based on the updated second set of packet filtering rules. Since this second set of packet filtering rules is not disclosed in the Sourcefire manual v4.10 (D19), no packet filtering based on it can be performed. Thus, feature 1.4 is also not disclosed in the Sourcefire manual v4.10 (D19).

3. Re intervention 2

190 Intervenor 2 also cites – like intervenor 1 - Sourcefire manual v4.10 (D19) for an alleged lack of novelty of the independent claims. With respect to feature 1.1.3 pertaining to the automatic creation or alteration of packet filtering rules by a security policy management server, intervenor 2 also refers – like intervenor 1 – to the security enhancement updates allegedly provided by the Sourcefire VRT. As an additional alternative attack, intervenor 2 refers to an automated recommended rule state generation described in D19 as alleged disclosure of feature 1.1.3 (cf. intervention 2, marginals 135 to 137). In the following, only the difference between the intervention 1 and intervention 2 are discussed.

191 Nonetheless, it will be shown below that also intervenor 2's alternative novelty attack is to no avail.

a. No disclosure of feature 1.1.3

1.1.3 *wherein one or more first packet filtering rules, of the first set of packet filtering rules, was automatically created or altered by the security policy management server based on malicious traffic information received from a malicious host tracker service;*

192 Intervenor 2 cites p. 1725 of D19 which describes to automatically generate recommendation for rule state (of an intrusion rule):

Automating Recommended Rule State Generation

Platform: DC

Component: IPS + RNA

You can automatically generate rule state recommendations based on RNA data for your network using the most recently saved configuration settings in your custom intrusion policy.

IMPORTANT! If the system automatically generates scheduled recommendations for an intrusion policy with unsaved changes, you must discard your changes in that policy and commit the policy if you want the policy to reflect the automatically generated recommendations. See Committing Intrusion Policy Changes on page 345 for more information.

When the task runs, the system automatically generates recommended rule states. Optionally, depending on the configuration of your policy, it also modifies the states of intrusion rules based on the criteria described in Managing RNA Rule State Recommendations on page 468. Modified rule states take effect the next time you apply your intrusion policy. See Using RNA Recommendations on page 472 for more information.

Excerpt of p. 1725, D19 (emphasis added)

193 The above cited page also refers to p. 468 pertaining to managing RNA rules state recommendation which describes the “RNA Recommended Rules” feature. In particular, this feature enables the recommendation of rule states and, optionally, the setting of the rule state according to the recommendation:

When you configure the RNA Recommended Rules feature, the system identifies hosts and services on your network, searches your base policy for rules that protect against vulnerabilities associated with the identified hosts and services, and identifies the current state of rules in your base policy. The system then recommends rule states and, optionally, sets the rules to the recommended states using the following criteria:

Excerpts of p. 468 and 469, D19 (emphasis added)

- 194 In the Sourcefire manual v4.10, a “rule state” indicates whether an intrusion rule in an intrusion policy is enabled or disabled (cf. D19, p. 2090 and 2091, emphasis added):

rule state	Whether an intrusion rule is enabled (set to Generate Events or Drop and Generate Events), <u>or disabled (set to Disable)</u> within an intrusion policy. If you enable a rule, it is used to evaluate your network traffic; if you disable a rule, it is not used. A drop rule can drop packets that trigger the rule in an inline deployment.
-------------------	--

Excerpt of p. 2090 and 2091, D19 (emphasis added)

- 195 Accordingly, the recommended states by the “RNA Recommended Rules” feature can be either “enabled” or “disabled” (D19, p. 2091, emphasis added):

RNA recommended rules	<u>A feature that recommends which rules should be enabled or disabled in your intrusion policy, based on information from your RNA network map. You can choose to allow the system to modify rule states based on recommendations, in which case the system adds a read-only RNA Recommendations layer.</u>
------------------------------	--

Excerpt of p. 2091, D19 (emphasis added)

- 196 Thus, recommending rule states as described in Sourcefire manual v4.10 relates to recommendations for deactivating or activating an already existing rule of an intrusion policy.
- 197 However, with respect to a rule, disabling or enabling does not correspond to a creating or altering. First, creating a rule means to generate a new rule – this is clearly not envisaged by changing a state of an already existing rule. Second, altering a rule in the sense of claim 1 means modifying the rule. The packet filtering rule defined in claim 1 includes a packet matching criterion (feature 1.1.2). These are components of a rules which can be modified, i.e., “altered”. The alteration of a rule being an alteration of its components is described in the patent opposed, e.g., in last sentence of par. [0036] which reads as follows (emphasis added):

ated 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).

Excerpt of par. [0036] of patent opposed (emphasis added)

Here, the security policy management server may alter a rule by modifying a packet matching criterion of the rule (or in the wording of par. [0036], “criteria”). Another example of altering a rule is described with respect to figure 13 of the patent opposed, according to which a rule is updated (or altered) by

including new network addresses (which are -as set forth in par. [0031] –criteria for matching packets) (cf. par. [0075] of patent opposed).

198 Such an alteration of a rule as envisaged by the patent opposed does not, however, correspond to disabling or enabling a rule.

199 Therefore, D19 does not disclose feature 1.1.3.

b. No disclosure of features 1.2.5 and 1.2.6

1.2.5 *reformatting the subset of information specified by the packet in accordance with a logging system standard; and*

1.2.6 *routing, by the packet security gateway, the packet to a monitoring device configured to store the packet for subsequent analysis;*

200 Regarding the above features, intervenor 2 refers to intrusion events and syslog responses (cf. intervention 2, marginals 150 to 152).

201 The arguments set forth by intervenor 2 do not go beyond the arguments of intervenor 1. Thus, it is referred to the arguments presented in present marginals 172 to 183 indicating lack of disclosure of features 1.2.5 and 1.2.6 within D19.

c. No disclosure of feature group 1.3 and feature 1.4

1.3 *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,*

1.3.1 *wherein the updated second set of packet filtering rules comprises an update to the first set of packet filtering rules generated by the security policy management server based on updated malicious traffic information received from the malicious host tracker service;*

1.4 *performing, on a packet by packet basis, packet filtering on a second portion of the packets as sociated with the network protected by the packet security gateway based on the updated second set of packet filtering rules*

202 Intervenor 2 merely brought forth the unsubstantiated assertion that the rules of the intrusion policy can be updated by the Defense Center without any reference to D19.

203 However, as shown above in present marginals 194 to 199, setting a state of an intrusion rule according to a recommend state cannot be equated to updating (i.e. altering) rules. As such, D19 does not disclose that the Defense center updates the rules of an intrusion policy.

204 Insofar, D19 fails to disclose feature group 1.3 and feature 1.4.

4. Interim conclusion

205 Thus, the subject-matter of claim 1 and, correspondingly, claims 14 and 15 is novel over the Sourcefire manual v4.10 (D19).

III. Juniper (D41)

- 206 In order to ground lack of novelty, intervenor 2 cites a reference guide for configuring and managing a Juniper Networks security device through Screen OS (cf. D41, p. 4). In the following, the reference guide is hereinafter referred to as “Juniper reference guide”.

1. Teaching of Juniper reference guide (D41)

- 207 The Juniper reference guide (D41) discloses Juniper Network security devices (hereinafter “security devices”) which secure a network by inspecting and then allowing or blocking connection attempts across security zones. Policies are used to determine the flow of traffic between zones (cf. D41, p. 20):

Policies

Juniper Networks security devices secure a network by inspecting, and then allowing or denying, all connection attempts that require passage from one security zone to another.

By default, a security device denies all traffic in all directions. Through the creation of policies, you can control the traffic flow from zone to zone by defining the kinds of traffic permitted to pass from specified sources to specified destinations at scheduled times. At the broadest level, you can allow all kinds of traffic from any source in one zone to any destination in all other zones without any scheduling restrictions. At the narrowest level, you can create a policy that allows only one kind of traffic between a specified host in one zone and another specified host in another zone during a scheduled period, see Figure 5 on page 21.

Excerpt of p. 20, D41

- 208 Security policies include rules that can be installed on managed devices (cf. D41, p. 588):

Configuring Security Policies

A security policy defines how your managed devices handle network traffic. You can configure multiple security policies in NSM, but a device can only have one active security policy at a time. You can install the same security policy on multiple devices, or you can install a unique security policy on each device in your network.

About Security Policies

Each instruction in a security policy is called a rule. Security policies can contain multiple rules. You create rules in *rulebases*, sets of rules that combine to define a security policy. Each security policy contains the Zone and Global firewall rulebases, which cannot be deleted. You can add or delete any other rulebase—Multicast, IDP, Exempt, and Backdoor—in a security policy; however, a single policy can only contain one instance of any type of rulebase. Each security policy (all rulebases combined) can contain a maximum of 40,000 rules.

Excerpt of p. 588, D41 (emphasis added)

- 209 A Network and Security Manger (NSM) is a software application for configuring and monitoring the security devices (cf. D41, p. 312):

Management with the Network and Security Manager

Network and Security Manager (NSM) is Juniper Networks' enterprise-level management software application that configures and monitors multiple Juniper Networks security devices over a local area network (LAN) or a wide area network (WAN) environment.

Excerpt of p. 312, D41

2. No disclosure of feature 1.1

1.1 *receiving, by a packet security gateway (112) configured for protection of a network and associated with a security policy management server (120) external from the network, a dynamic security policy comprising*

210 Intervenor 2 equates a security device of D41 with a “packet security gateway” and security policy of D41 with a “dynamic security policy”. Further, the NMS of D41 is equated with the “security policy management server”.

211 However, in D41, there is no disclosure that the security device receives from the NMS the security policy.

212 In fact, even p. 580 of D41 cited by intervenor 2 (with respect to the above feature) merely describes that multiple security policies may be configured in the NSM, but fails to indicate how a security policy is ultimately applied to the security device.

213 Even more, D41 describes vaguely that a security policy is assigned, validated and then installed on managed devices (cf. D41, p. 589, emphasis added):

Installing Security Policies

After you create a security policy by building rules in one or more rulebases, you can assign, validate, and install that policy on specific managed devices. For detailed information about installing security policies, see the Network and Security Manager documentation at <http://www.juniper.net/techpubs/software/management/security-manager>.

Excerpt of p. 589, D41 (emphasis added)

214 Thus, D41 fails to disclose feature 1.1

3. No disclosure of feature 1.1.3

1.1.3 *wherein one or more first packet filtering rules, of the first set of packet filtering rules, was automatically created or altered by the security policy management server based on malicious traffic information received from a malicious host tracker service;*

215 With respect to the above feature, intervenor 2 refers to regularly provided updates for “attack databases” (cf. intervention 2, marginal 113).

216 The attack database updates are provided by Juniper Networks and include, inter alia, intrusion prevention and detection (IDP) attack objects (cf. D41, p. 647, emphasis added):

About Attack Database Updates

Juniper Networks periodically provides attack database updates, in the form of a download file, on the Juniper Web site. Attack database updates can include the following:

- New or modified predefined IDP attack objects and groups
- New or modified signatures used by the Deep Inspection (DI) feature
- Updates to the IDP engine, which runs in the security device

Excerpt of p. 647, D41 (emphasis added)

- 217 An “attack objects” is used by a IDP rule to identify malicious activity in monitored traffic (cf. D41, p. 593 and 594, emphasis added):

Configuring IDP Rules

The IDP rulebase protects your network from attacks by using attack objects to identify malicious activity and then by taking action to thwart the attacks. Avoid creating too large number of IDP rules. It is important to balance the complexity and number of IDP rules you configure against their potential to cause issues with performance. For more information about performance issues, see the Network and Security Manager documentation

at <http://www.juniper.net/techpubs/software/management/security-manager>.

When you create an IDP rule, you must specify the following:

Excerpt of p. 593, D41 (emphasis added)

- The attack(s) you want IDP to match in the monitored network traffic. Each attack is defined as an attack object, which represents a known pattern of attack. Whenever this known pattern of attack is encountered in the monitored network traffic, the attack object is matched. You can add attack objects individually or by category, operating system, or severity.
- The action you want IDP to take when the monitored traffic matches the rule's attack objects. You can specify the following:
 - **Action:** The action you want IDP to perform against the current connection.
 - **IP Actions:** The action you want IDP to perform against future connections that use the same IP address.
 - **Notification:** Choose **none**; or enable logging, then select the appropriate logging options for your network.
 - **Severity:** Use the default severity settings of the selected attack objects, or choose a specific severity for your rule.

Excerpt of p. 593, D41 (emphasis added)

- 218 Intervenor 2 opines that the automatic updates of attack databases lead to an automatic update of rules (cf. intervention 2, marginal 113), but fails to substantiate this. Intervenor 2 merely cites p. 647 of D41, which describes that the attack data base updates are periodically provided by Juniper Networks and are downloaded by the NSM GUI server. Further, it is indicated that “predefined IDP attack objects or groups” cannot be created, edited, or deleted, but updated.

- 219 P. 647 of D41 does not disclose any updates of the IDP rules. Instead, the cited page even describes that only the attack objects – and not any rules – are pushed from the GUI server to the managed device:

When you download updated IDP attack objects and groups to the GUI server, any new attack objects in the update are available for selection in an IDP rulebase in a security policy. When you install a security policy on your managed device, only the attack objects that are used in IDP rules for the device are pushed from the GUI server to the device.

Excerpt of p. 647, D41 (emphasis added)

- 220 At another place in the intervention 2, it is referred to attack database updates for deep inspection (DI) signature packs with respect to automatic generation of rules (cf. intervention 2, marginal 98). However, the cited p. 532 of D41 used therefor does not disclose any automatic generation of rules by the NSM.
- 221 According to cited p. 532, Juniper Networks updates signature packs with newly discovered attack patterns. However, this update does not correspond to the automatic updates of features 1.1.3 in at least two ways. First, the security device (and not the NSM) downloads the attack object database from an attack object database server (cf. D41, p. 533, fig. 144). Second, the security device replaces its attack object database with the newer (=updated) version (cf. D41, p. 532, emphasis added):

Automatic Update

The **Automatic Update** option, downloads the signature pack at user-scheduled times if the database on the server is a newer version than that previously loaded on the device. Juniper Networks regularly updates the signature pack with newly discovered attack patterns. Therefore, because of its changing nature, you must also update the signature pack on your security device regularly. For this operation to work, you must first configure the attack object database server settings.

In this example (see Figure 144 on page 533), you set a schedule to update the database on the security device every Monday at 04:00 AM. At that scheduled time, the device compares the version of the database on the server with that on the device. If the version on the server is more recent, the security device automatically replaces its database with the newer version.

For example, select Server to update the server signature pack. See Table 57 on page 530 for a list of predefined signatures packs and the corresponding URLs.

Excerpt of p. 532, D41 (emphasis added)

Figure 144: Updating DI Signatures Automatically

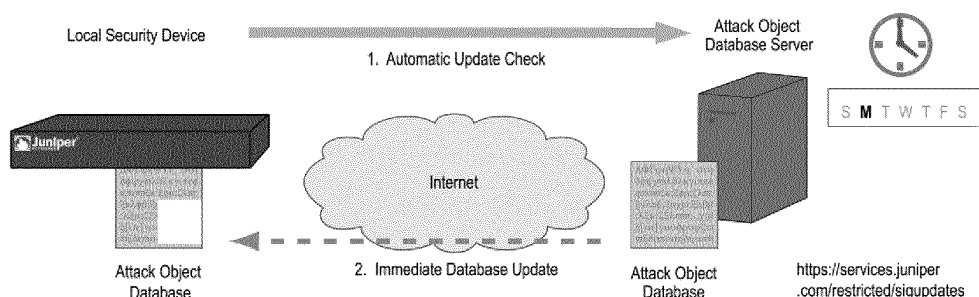


Fig. 144 on p. 533, D41 (emphasis added)

222 Thus, D41 is silent about feature 1.1.3.

4. No disclosure of feature 1.2.6

1.2.6 *routing, by the packet security gateway, the packet to a monitoring device configured to store the packet for subsequent analysis;*

223 Intervenor 2 equates logged traffic data (included in a syslog reports) with a packet (cf. intervention 2, marginal 104).

224 This is however an unjustified and unsubstantiated assertion.

225 In particular, a log in the sense of claim 1 of the patent opposed is, as per feature 1.2.3, “a record of a subset of information of a packet”. Therefore, the term “log” refers to only a part of information of the packet. This difference is thus apparent from claim 1 which refers to the record of a subset of information of packet, i.e. a log, (feature 1.2.3) and the packet (feature 1.2.6). Applying this rationale to logged traffic data (in other words, logs pertaining to traffic data), it necessarily follows that the logged traffic data of D41 is not the traffic data itself.

226 As indicated in the citation used by intervenor 2, D41 merely discloses to send syslog reports (cf. p. 1148), but not packets:

Setting Static Routes

In Figure 319 on page 1150, a security device operating with its Trust zone interface in Network Address Translation (NAT) mode protects a multilevel network. There is both local and remote management (via Network and Security Manager). The security device sends SNMP traps and syslog reports to the local administrator (located on a network in the Trust zone) and it sends Network and Security Manager (NSM) reports to the remote administrator (located on a network in the Untrust zone). The device uses a SecurID server in the Demilitarized Zone (DMZ) to authenticate users and a Websense server in the Trust zone to perform Web filtering.

Excerpt of p. 1148, D41 (emphasis added)

227 Therefore, D41 fails to disclose feature 1.2.6.

5. No disclosure of feature group 1.3 and feature 1.4

1.3 *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,*

1.3.1 *wherein the updated second set of packet filtering rules comprises an update to the first set of packet filtering rules generated by the security policy management server based on updated malicious traffic information received from the malicious host tracker service;*

1.4 *performing, on a packet by packet basis, packet filtering on a second portion of the packets as sociated with the network protected by the packet security gateway based on the updated second set of packet filtering rules*

- 228 Feature group 1.3 pertains to the automatic update of packet filtering rules and feature 1.4 to a packet filtering using the updated packet filtering rules.
- 229 With respect thereto, intervenor 2 refers to their arguments provided with respect to feature 1.1.3. But as shown above in present marginals 215ff, an automatic creation or alteration of rules by the NSM as per feature 1.1.3 is not disclosed in D41.
- 230 Consequently, feature group 1.3 and feature 1.4 is not disclosed in D41.

6. Interim conclusion

- 231 As shown above, the Juniper reference guide (D41) fails to disclose at least the features 1.1, 1.1.3, 1.2.6 1.4 and feature group 1.3. Therefore, D41 does not anticipate the subject-matter of claim 1 as granted and, correspondingly, claims 14 and 15 in a novelty destroying manner.

IV. US 2013/0263247 A1 (D43)

- 232 Further, US patent application US 2013/0263247 A1 (D43) is cited by intervenor 2 as novelty destroying prior art. However, this not the case.

1. Teaching of D43

- 233 D43 discloses a packet interceptor/processing apparatus for enhancing an infrastructure of a network such as the Internet. The apparatus applies one or more rules to the intercepted packets. The apparatus is capable of analyzing the header and payload of a packet (cf. D43, abstract). The packet interceptor can be an edge adapter/packet interceptor system 700 (cf. fig. 7) which includes a router 702 and a packet interceptor adapter 720 coupled to the router, wherein the router 702 is located within an internet service provider located in an edge 124 of a network 100 (cf. D43, paras. [0057] and [0058], fig. 1 and fig. 7).

FIG. 1

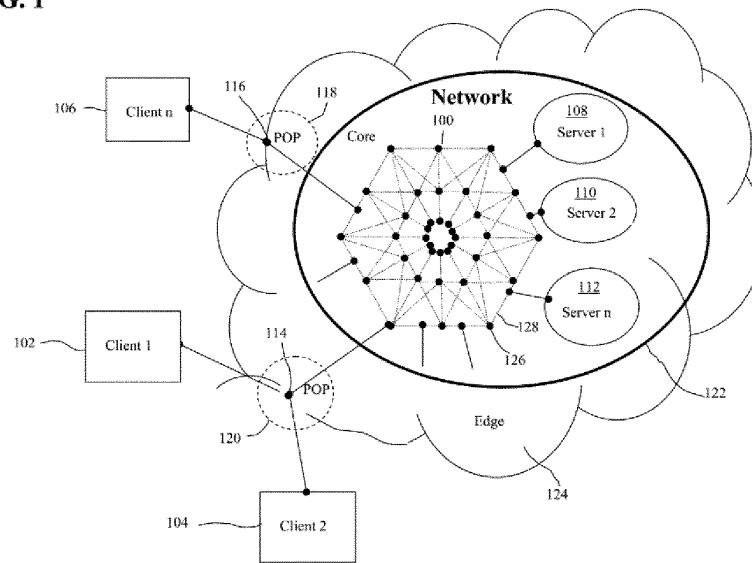


Fig. 1 of D43

2. No disclosure of feature 1.1.3

1.1.3 wherein one or more first packet filtering rules, of the first set of packet filtering rules, was automatically created or altered by the security policy management server based on malicious traffic information received from a malicious host tracker service;

- 234 Intervenor 2 equates the packet interceptor adapter 720 of D43 with a “packet security gateway”. Further, with respect to the automatic creation and alteration of rules, intervenor 2 refers to implementing rule 732 which consider historical packet activity, and asserts that historical packet activity corresponds to “malicious packet information from all protected networks” (cf. intervention 2, marginal 170).
- 235 However, intervenor 2 fails to indicate where such rules 732 are created/altered and that they are automatically created.
- 236 In order to implement such rules taking into account historical packet activity, information about past packet activity has to be stored. To this end, D43 indicates that data about a packet 704 has to be stored in a memory (cf. D43, par. [0085]):

[0085] In addition, data about the packet 704 may be stored in a memory for use by other rules, for processing the current or future packets 704. This allows stateful processing, i.e. state based rules, of packets 704 as they flow through the packet analyzer 720. By storing information about past packet 704 activity that the packet analyzer 720 has processed, rules 732 may be implemented which take into account historical packet activity. An additional basic opera-

Excerpt of par. [0085], D43 (emphasis added)

- 237 The packet interceptor adapter 720 comprises a bulk data storage (e.g., SDRAM) 806 (cf. D43, par. [0090] and fig. 8), in which packets or packet data is stored (cf. D43, par. [0099]):

a state memory. For example, a rule 732 may defined to watch for multiple malformed packets 704. Where a single malformed packet 704 is received, the rule 732 will take no action as this may be due to a random network error. However, data regarding that malformed packet, or the entire packet itself, will be stored. If another malformed packet 704, similar to the first malformed packet 704, is subsequently received, the rule 732 may determine that some malicious activity is underway and delete the second packet 704. Other state information

Excerpt of par. [0085], D43 (emphasis added)

241 Such a triggering of rules does, however, not correspond to creation or alteration of a rule, let alone in an automatic manner.

242 Hence, D41 fails to disclose feature 1.1.3.

3. No disclosure of features 1.2.4, 1.2.5 and 1.2.6

1.2.4 *generating a record comprising the subset of information specified by the packet;*

1.2.5 *reformatting the subset of information specified by the packet in accordance with a logging system standard; and*

1.2.6 *routing, by the packet security gateway, the packet to a monitoring device configured to store the packet for subsequent analysis;*

243 The packet defined features 1.2.4 to 1.2.6 refer to a packet which matches a packet matching criterion (cf. feature 1.2.3) and is further processed as per the above features.

244 Intervenor 2 cites to the abstract D43.

245 But intervenor 2 does not provide any further reasons going beyond a mere alleged implicit disclosure that the skilled person derives from the cited passage of the abstract of D43.

246 In fact, intervenor 2 does not indicate at which point in D43 the generation of a specific subset of information is disclosed (feature 1.2.4).

247 Further, D43 is silent about packets matching a criterion (cf. feature 1.2.3) being logged/stored or forwarded as per features 1.2.5 and 1.2.6.

248 Furthermore, D43 does not specify that the external device is a monitoring device as per feature 1.2.6.

249 With respect to a logging system standard of feature 1.2.5, intervenor 2 merely refers to the syslog method mentioned in par. [0183] of D43. However, the syslog method is mentioned with an arbitrary enterprise firewall without any reference to the packet interceptor adapter 720 (cf. D43, par. [0182]). Therefore, the syslog standard is not disclosed with respect to any rule and its action used by the packet interceptor adapter 720.

250 In view of the above, D43 fails to disclose the features 1.2.4 to 1.2.6.

4. No disclosure of feature group 1.3 and feature 1.4

1.3 *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,*

1.3.1 *wherein the updated second set of packet filtering rules comprises an update to the first set of packet filtering rules generated by the security policy management server based on updated malicious traffic information received from the malicious host tracker service;*

1.4 *performing, on a packet by packet basis, packet filtering on a second portion of the packets as sociated with the network protected by the packet security gateway based on the updated second set of packet filtering rules*

251 Intervenor 2 merely opines that the above features are disclosed in D43 by virtue of dynamically re-defining of rules without referring to any passage in the document.

252 Yet as shown above in present marginals 234 to 242, automatic creation or alteration (i.e. updating) of rules is not disclosed in D43. Thus, D43 fails to disclose feature group 1.3 and feature 1.4.

5. Interim conclusion

253 The subject-matter of claim 1 and, correspondingly, claims 14 and 15 is, hence, novel over D43.

V. US 7,966,659 B1 (D44)

254 Intervenor brought forth US 7,966,659 B1 (D43) as allegedly novelty destroying prior art.

1. Teaching of D44

255 D44 pertain to techniques for system wide analysis of industrial protocol traffic for security devices (cf. D44, abstract). A security device may be a firewall, intrusion detection device, etc. (cf. D44, e.g., col 5, lines 7 and 8). A central management tool 202 is configured to acquire information from distributed sources 204, 206 and “*apply, configure, modify, delete, etc. rules and/or policies of a security enabled device*” (cf. D44, col. 7, ll. 39 to 42 and ll. 59 to 65).)

2. No disclosure of feature 1.1.3

1.1.3 *wherein one or more first packet filtering rules, of the first set of packet filtering rules, was automatically created or altered by the security policy management server based on malicious traffic information received from a malicious host tracker service;*

256 Intervenor 2 asserts that malicious traffic information received from a malicious host tracker service is used as a basis for a central management server 202 of D44 to automatically create or alter rules (cf. intervention 2, marginals 191). Specially, with respect to the automatic creation/alteration of rules, intervenor 2 refers, on the one hand, to a rule builder module 322 explained in marginal 184 of the intervention 2, and on the other hand, to col. 7, ll. 39 to 42 of D44, which pertains to a central management tool 202.

257 However, the rule builder module 322 is part of a central management tool 302, which is different to central management tool 202. In fact, the central management tool 202 and the central management tool 302 are different embodiments within the disclosure of D44.

FIG. 2 illustrates another system 200 for automatically determining placement and/or configuration of security device(s) based on information obtained from distributed system sources. System 200 includes a central management tool

Col 6, ll.52 to 55, D44 (emphasis added)

FIG. 3 illustrates a system 300 for utilizing communication traffic to determine a proper location of, or rules for, a security device. Included in system 300 is a central management tool

Col 9, ll. 16 to 18, D44 (emphasis added)

258 Therefore, referring to both embodiments as done in marginal 191 of the intervention 2 for discussing feature 1.1.3 is not appropriate.

259 Nevertheless, none of the central management tools 202, 302 (which intervenor 2 equate with a “security policy management server”) uses (i) malicious traffic information (ii) received from a malicious host tracker service.

260 In particular, central management tool 202 acquires “industrial protocol communication information” from distributed sources 204, 206, which in turn collect and report information regarding communication they receive and/or send (i.e., traffic information). This aggregated information (i.e., the industrial protocol information acquired from the sources 204, 206) may be used to create rules, etc. (cf. D44, col. 7, ll. 31 to 43):

Central management tool 202 can be configured to acquire industrial protocol communication information from distributed sources 204 and 206 that can be configured to collect and report information regarding communications they may receive and/or send (e.g., traffic information). It should be understood that distributed sources, (e.g., software packages, security device, design data stores, . . .) through or to which any communications occur can be involved with reporting traffic. The information reported by distributed sources 204 and 206 can be aggregated by central management tool 202 to create firewall rules, security rules, and/or security authority rules, or information for other analysis purposes that might be utilized online or offline.

col. 7, ll. 31 to 43, D44 (emphasis added)

261 However, “industrial protocol communication information” does not correspond to “malicious traffic information” as defined in feature 1.1.3.

262 Similarly, the central management tool 303 collects communication information from distributed devices 304, 306, and/or 308 from within a system 300 and correlate communication behaviors in system 300. The correlated information is used to create rules for a security device (cf. D44, col. 9, ll. 33 to 45):

system-wide analysis of industrial protocol traffic. For example, central management tool 302 can collect communication information from distributed points in system 300 (e.g., distributed devices 304, 306, and/or 308) when a security rule is not enforced (e.g., traffic is only monitored) or when security rules are partially or fully enforced (e.g., unsecured state, partially secured state, fully secured state) and correlate communication behaviors in system 300. The correlated information can be utilized to determine an optimal location for a security device (e.g., firewall, intrusion detection/prevention, or other security device) and/or to create rules for such devices enabling the devices to be automatically configured.

col. 9, ll. 33 to 45, D44 (emphasis added)

- 263 Here, the correlated information pertains to the communication within the system 300 and, therefore, does not correspond to “malicious traffic information”.
- 264 Further, intervenor 2 equates the distributed source 206 and distributed device 304 with “malicious host tracker service” and the distributed source 204 and distributed device 306 with “packet security gateways” (cf. intervention 2, marginals 187 and 188). However, D44 fails to disclose that the distributed source 206 and distributed device 304 may identify malicious traffic. As such, they do not constitute malicious host tracker services. Thus, the central management tools rather collect information only from “packet security gateways”.
- 265 Thus, feature 1.1.3 is not disclosed in D44.

3. No disclosure of features 1.2.4, 1.2.5 and 1.2.6

- 1.2.4** *generating a record comprising the subset of information specified by the packet;*
- 1.2.5** *reformatting the subset of information specified by the packet in accordance with a logging system standard;*
and
- 1.2.6** *routing, by the packet security gateway, the packet to a monitoring device configured to store the packet for subsequent analysis;*

- 266 With respect to the above features, intervenor 2 refers to arbitrary passages which merely mention some sort of logging and which are scattered all over the disclosure of D44, i.e. col. 1, ll. 34 to 39, col. 7, ll. 3 to 14, col. 8, ll. 58 to 61, col. 12, ll. 18 to 22 (cf. intervention 2, marginals 197 to 200). The cited passages merely mention (re-)routing and logging without indicating any relationship to each other.
- 267 However, as per features 1.2.4 and 1.2.6, logging and routing is performed with respect to the packet matching the packet matching criterion.
- 268 This is not disclosed in D41.
- 269 Further, it is disclosed that an intrusion detection system can log invalid and/or unauthorized accesses (cf. D44, col. 7, ll. 10 to 14). It is further described that an intrusion/prevention device includes an intrusion log that tracks or records observed traffic (cf. D44, col. 8, lines 58 to 61). But in any of the

cited passages, D41 fails to disclose that a subset of information of packet is logged. Thus, D41 fails to disclose feature 1.2.4.

270 Also, intervenor 2 tries to establish implicit disclosure of reformatting the subset of information by asserting that transmitting logs to the central management tool necessitates a logging standard. However, it might be very well the reformatting is performed at the central management tool, instead within an intrusion detection device. Therefore, implicit disclosure cannot be derived from the fact that a log is sent to a central management tool.

271 In D41, it is disclosed that firewalls may be used to reroute data communications or route packets (cf. D44, col. 1, ll. 34 to 39, and col. 7, ll. 7 to 14). However, no connection between an intrusion log of a packet and routing the packet is mentioned in D41.

272 Therefore, D41 fails to disclose features 1.2.4 to 1.2.6

4. Interim conclusion

273 As set forth above, the subject-matter of claim 1 and, correspondingly, claims 14 and 15 is novel over D44.

VI. Novelty: Conclusion

274 The opponents objections regarding lack of novelty of the independent claims are moot. To the contrary, it has been demonstrated above that the claimed subject-matter is novel over the prior art brought forth by the opponents.

F. No lack of an inventive step

I. Inventive step when starting from Sourcefire manual v4.10 (D19)

275 Intervenor 1 also objects lack of inventive step starting from Sourcefire manual v4.10 (D19) (cf. intervention 1, p. 68ff). To this end, intervenor 1 assumes that only features 1.1.3 and 1.3.1 are not disclosed.

1.1.3 *wherein one or more first packet filtering rules, of the first set of packet filtering rules, was automatically created or altered by the security policy management server based on malicious traffic information received from a malicious host tracker service;*

1.3.1 *wherein the updated second set of packet filtering rules comprises an update to the first set of packet filtering rules generated by the security policy management server based on updated malicious traffic information received from the malicious host tracker service;*

1. Incorrect formulation of the objective technical problem

276 Intervenor 1 formulates the objective technical problem as “how to provide an alternative method of providing automatic updates for a dynamic security” when starting from Sourcefire manual v4.10 (D19) as closest prior art.

277 However, this is an incorrect formulation of the problem, since the above problem as stated by intervenor 1 already contains hints to the solution, i.e. providing the automatic updates. The Guidelines under G-VII, 5.2 read as follows:

“... the objective technical problem must be so formulated as not to contain pointers to the technical solution, since including part of a technical solution offered by an invention in the statement of the problem must, when the state of the art is assessed in terms of that problem, necessarily result in an ex post facto view being taken of inventive activity (see T229/85)”

278 Notwithstanding the above incorrect formulation, the claimed solution is still inventive in view of the prior art brought forth by intervenor 1.

2. Non-Obviousness

279 Intervenor 1 tries to establish an automatic update function in the Sourcefire manual v4.10 (D19) by citing D25 and D26.

280 But none of D25 and D26 may be able to do so. First, D25 is an article concerning “FirePOWER” which can be used to “power NGIPS [next generation intrusion prevention system]” (cf. D25, p. 1, emphasis added):

Sourcefire NGIPS is powered by FirePOWER(TM), the company's network-based platform. Sourcefire's NGIPS allow customers to support increasing throughput needs by swapping out network modules and reconfiguring devices as their networks grow. Additionally, Sourcefire NGIPS enables automatic updates and intelligent policy tuning that simplifies the security process for customers, creating better network protection while freeing up network administrators for other projects.

Excerpt of p. 1, D25 (emphasis added)

281 However, FirePOWER, to which D25 refers, is not related to the 3D sensors described in the Sourcefire manual v4.10 (D19). Nowhere does the Sourcefire manual v4.10 (D19) mention the term FirePOWER. Thus, there is no connection between D19 and D25.

282 Further, the article D26 by Mr. Antony Perridge, EMEA Channel Director at Sourcefire, mentions automation of security policies and rules without referring to Sourcefire manual v4.10 (D19). In fact, the entire article D26 does not refer to the 3D sensor technology described in the Sourcefire manual v4.10 (D19). Thus, there is also no connection between D19 and D26.

283 Accordingly, D25 and D26 do not prove any automatic update functionality within Sourcefire manual v4.10.

a. Non-Obviousness over Sourcefire manual v4.10 (D19) in combination with D27

- 284 In order to close the gap between the claimed solution and the Sourcefire manual v4.10 (D19), i.e., features 1.1.3 and 1.3.1, intervenor 1 cites article D27 (“Trusted Automated eXchange of Indicator Information (TAXII)”).
- 285 However, D27 does not render feature 1.1.3 obvious.
- 286 In fact, D27 fails to teach or suggest “*one or more first packet filtering rules, of the first set of packet filtering rules, was automatically created or altered by the security policy management server*”
- 287 The article D27 is directed to the standardization of cyber threat intelligence information using a so-called “STIX” format which was developed to provide a unifying architecture for tying together cyber threat information such as cyber observables and indicators (cf. D27, p. 8).
- 288 Here, intervenor 1 tries to equate the “observables” of D27 to the claimed element.
- 289 The observables of D27 without more are not the claimed element which requires packet filtering rules that were automatically created or altered by the security policy management server. (s. D27, p. 14):

9.1 Observables

Observables are the “base” construct within the STIX architecture. Observables are stateful properties or measurable events pertinent to the operation of computers and networks. Information about a file (name, hash, size, etc.), a registry key value, a service being started, or an HTTP request being sent are all simple examples of observables. STIX leverages CybOX for its representation of Observables.

Excerpt of p. 14, D27

- 290 Further, intervenor 1 mentions TAXII (as mentioned in D30) as an effort for standardizing trust, automated exchange of cyber threat information (cf. intervention 1, p. 72, last two par.) as reference to automated security updates.
- 291 Still, TAXII does not result in the automated security updates being configured in the claimed manner. To wit, the TAXII system does not, standing alone, remedy the issues with Sourcefire or teach a system in which packet filtering rules are “*automatically created or altered by the security policy management server*” as required by feature 1.1.3.
- 292 Further, intervenor 1 asserts that the skilled person would provide an interface for TAXII feeds in Sourcefire systems according to the Sourcefire manual v4.10 (D19) (cf. intervention 1, p. 73, second par.).
- 293 However, intervenor 1 fails to indicate how such an interface for using feeds to update packet filtering rules would be envisaged by the Sourcefire manual v4.10. Sourcefire manual v4.10 does not mention any feeds or any interface thereto with respect to automated security updates at all. The Sourcefire

manual v4.10 thus does not provide any reasons to the skilled person for consulting the TAXII disclosure.

294 Thus, the claimed subject-matter is not rendered obvious by a combination of the Sourcefire manual v4.10 (D19) with D27 and D28.

b. Non-Obviousness over Sourcefire manual v4.10 (D19) in combination with D30

295 Intervenor 1 also refers to the “Infoblox” service as described in article D30 as an alleged example of a malicious host tracker service of feature 1.1.3.

296 The article D30 discloses an Infoblox DNS Firewall to prevent DNS exploits (cf. D30, p. 1, emphasis added):

on mobile and tablet devices. Once inside the firewall, malware can go undetected by legacy security approaches, exploiting Domain Name Systems (DNS) as a pathway to connect to a malicious destination or botnet controller. The new Infoblox DNS Firewall, an add-on option to the Infoblox DDI (DNS, DHCP, and IPAM) solution, is designed to prevent this from happening with up-to-date malware detection and automated flags for corporate IT teams. Using a real-

Excerpt of p.1, D30 (emphasis added)

297 Hence, D30 teaches a firewall, and not a malicious host tracker service.

298 Therefore, the claimed subject-matter is not rendered obvious by a combination of the Sourcefire manual v4.10 (D19) and D30.

II. Inventive step when starting from US 2011/0072506 A1 (D31)

299 Intervenor 1 refers to US 2011/0072506 A1 (D31) as alternative closest prior art for presenting arguments for an alleged lack of an inventive step of the subject-matter of claim 1 as granted.

300 D31 pertains to Unified Threat Management System (“UTMS”). UTMS secures a process control system 100 (cf. D1, e.g., Fig. 1A). The process control system includes UTMS-configured network devices (e.g., firewalls) 146a, 146b which include rulesets for inspecting and dropping packets (cf. D1, par. [0051 and [0052]]. The rulesets can be updated to remain effective against network threats. To this end, a third party, cyber security risk management firm 305 collects threat data 310 from a plurality of various sources 315 (cf. D31, par. [0088].

301 The above underlined aspects are highlighted with red markings in the below reproduced fig. 3 of D31:

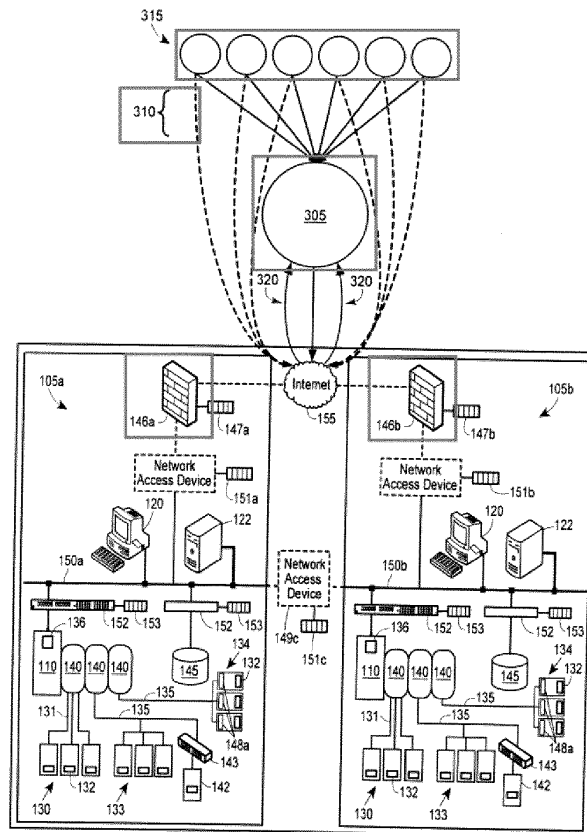


Fig. 3 of D31 (markings added)

Intervenor 1 equates an alleged server of the third party cyber security risk management firm 305 to the “security policy management server”, the firewalls 146a, b to “packet security gateways”, the threat data 310 to “malicious traffic information” and the sources 315 of threat data 310 to “malicious host tracker services” (cf. intervention 1, p. 76).

As conceded by intervenor 1, D31 fails to disclose the features 1.2.4 to 1.2.6 of claim 1 as granted.

1. Distinguishing features over D31

In addition to features 1.2.4 to 1.2.6 identified by intervenor 1, D31 further fails to disclose at least features 1.1, 1.1.3, feature group 1.3 and feature 1.4 as set out below.

a. Feature 1.1

1.1 *receiving, by a packet security gateway (112) configured for protection of a network and associated with a security policy management server (120) external from the network, a dynamic security policy comprising*

Intervenor 1 opines that the third-party cyber security management firm 305 of D31 provides the rulesets to the firewalls 146 by means of a server (cf. intervention 1, p. 79).

However, D31 does not disclose a “server”. The alleged “server” is nowhere mentioned in D31. Providing the rulesets to the firewalls 146 does not necessarily mean that the third-party cyber security management firm 305 implements a server.

307 Thus, D31 fails to disclose an security policy management server in the sense of feature 1.1

b. Feature 1.1.3

1.1.3 *wherein one or more first packet filtering rules, of the first set of packet filtering rules, was automatically created or altered by the security policy management server based on malicious traffic information received from a malicious host tracker service;*

308 With respect to feature 1.1.3, intervenor 1 refers to the triggering of automated updates in D31, when certain network conditions are met (cf. D31, par. [0083], emphasis added):

ured object, etc. Detection of certain network conditions may also trigger an automatic update of the rulesets 147, 148, 151, 153 or an alarm to prompt a user to perform a manual update of the rulesets or another action to fully secure the system 100.

Excerpt of par. [0083], D, 31 (emphasis added)

309 However, the cited paragraph of D31 merely pertains to a general update of rulesets, and fails to disclose that the ruleset is automatically updated. D31 does not provide any information on how the updated rulesets are generated.

310 Par. [0088] of D31 indicates that the third party cyber security risk management firm 305 collects the threat data 310 from various sources 315 to construct the rulesets (emphasis added):

FIG. 3, a third party, cyber security risk management firm 305 such as Wurldtech Security, Inc. of Vancouver, BC Canada, or other entity, may collect threat data 310 from a plurality of various sources 315 to construct the various rulesets 147, 148, 151, 153, validate the rulesets, verify, and distribute the

Excerpt of par. [0088], D, 31 (emphasis added)

311 Herein, it is merely disclosed that the third party cyber security risk management firm 305 itself constructs the rulesets. The disclosure of D31 provides no indications whatsoever which could lead to the conclusion that the third party cyber security risk management firm 305 is a server which is configured to automatically create or alter rules of the rulesets.

312 Thus, D31 does not disclose an automatic creation or alteration of packet filtering rules by a security policy management server as defined in feature 1.1.3.

313 Further, intervenor 1 equates the sources 315 of D31 to “malicious host tracker service” of feature 1.1.3.

314 However, intervenor 1 fails to show that the sources 315 track or identify malicious hosts or provide data about malicious hosts. Instead, D31 explains in a general manner that the sources 315 “*may create the threat data 310 by monitoring, defining, and analyzing potential and known threats to the security of the process control network(s) 150*” (cf. D31, par. [0092]). But there is no suggestion that the threat data 310 includes information about malicious hosts.

315 Rather, the threat data 310 of D31 refers to known and yet-to-be-discovered vulnerabilities (e.g., bugs, code defects, flaws, errors, exploits, etc.) associated with the devices that reside within protected

network of D31; in this regard, D31 describes “*devices that are capable of defending against both known and ‘zero day’ vulnerabilities and threats to control systems for both embedded, proprietary devices, and standard, commonly-used devices*” (cf. D31, par. [0022]). More specifically, threat data according to D31 refers to vulnerabilities at the application layer level, which is indicated by “*‘zero day’ application layer attacks*” (cf. D31, par. [0014]) and the circumstance that “*each time a new device or code application is introduced to the system 100, any exposure to bugs or other vulnerabilities may be reduced or eliminated*” (cf. D31, par. [0089]). As such, D31 is not concerned with identifying malicious traffic based on where it originates but rather based on its payload.

316 In short, the sources 315 of D31 do not include information about malicious hosts; therefore sources 315 cannot be equated with the malicious host tracker service of feature 1.1.3.

c. Feature group 1.3 and feature 1.4

1.3 *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,*

1.3.1 *wherein the updated second set of packet filtering rules comprises an update to the first set of packet filtering rules generated by the security policy management server based on updated malicious traffic information received from the malicious host tracker service;*

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

317 Intervenor 1 refers to the par. [0088] of D31, which he also cited with respect to feature 1.1.3.

318 However, as set forth above, par. [0088] of D31 fails to disclose an automatic creation or alteration of rules of the rulesets by a server. As such, the cited passage fails to disclose feature group 1.3. Consequently, due to the lack of updating the rules as per feature group 1.3, feature 1.4 is also not disclosed by D31.

d. Interim conclusion

319 D31 fails to disclose features 1.2.4 to 1.2.6 (as already conceded by intervenor 1) and, in addition thereto, also fails to disclose features 1.1.3, feature group 1.3 and feature 1.4.

320 Features 1.2.4. and 1.2.5 pertain to the generation logs containing a reformatted subset of information of identified packets.

321 Feature 1.2.6 pertains to storing the identified packets at a monitoring device.

322 Features 1.1., 1.1.3, feature group 1.3 and feature 1.4 are directed to the automatic creation/alteration of packet filtering rules by the security policy management server and providing these rules to the packet security gateway.

2. The combination of US 2011/0072506 A1 (D31) with US 2010/0257598 A1 (D32) does not render the subject-matter of claim 1 obvious

323 US 2010/0257598 A1 (D32) is cited by intervenor 1 as allegedly showing all the distinguishing features of claim 1.

324 D32 discloses an integrated monitoring system 130 (denoted as “integrated security system 130” in fig. 1 of D32) which monitors data traffic on internal network 110 and/or received from an external network 122 (cf. D32, par. [0062] and fig. 1).

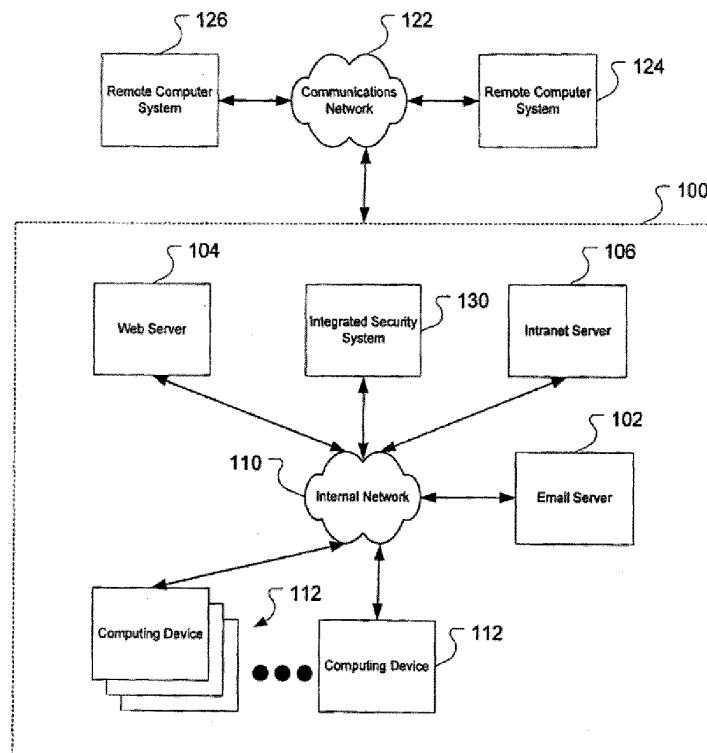


Fig. 1 of D32

325 **Features 1.1., 1.1.3, feature group 1.3 and feature 1.4** pertaining to the automatic creation/alteration of rules are not disclosed in or suggested by D32:

326 Par. [0044] of D32 cited by intervenor with respect thereto teaches to automatically generate rules on the basis of event data stored in an event data base:

[0044] In accordance with other aspects, the present invention relates to a method of automatically generating rules for use by a monitoring module. The method includes analyzing a data packet received from a communication network by the monitoring module using a predetermined set of rules. The data packet includes information identifying the packet's source (e.g., a source IP address) and the packet's destination. In response to the packet failing the analyzing operation, the method searches an event database for events associated with the source of the packet. If the event database contains an event record associated with the source of the packet, a new rule is generated to block subsequent packets from the source of the packet for a predetermined period of time. The new rule is then added to the set of rules used by the monitoring module.

Par. [0044], D32 (emphasis added)

327 The event database is part of an integrated monitoring system (cf. D32, paras. [0064] and [0074], emphasis added):

[0064] FIG. 2 illustrates the functional components of an embodiment of an integrated monitoring system 200 for a computing system. The integrated monitoring system 200 includes multiple monitor modules 202, 204, 206, 208, 210, and a security system integrator (SSI) 212. The SSI receives

Excerpt of par. [0044], D32 (emphasis added)

[0072] In the embodiment, the monitor modules 202, 204, 206, 208, 210 report event data to a monitor module integrator (SSI) 212. The event data is received by the SSI 212 and stored in an event database 214. In one embodiment, the SSI

Excerpt of par. [0044], D32 (emphasis added)

328 Further, in D32, the integrated monitoring system itself (which analyzes the packets) creates the new rule criteria (cf. D32, par. [0100]):

[0100] The integrated monitoring system also analyzes the event data in an event data analysis operation 412. The event data analysis operation 412 automatically generates new or revised criteria for use by one or more of the packet analysis operations based on the event data received and an event data rule set. The event data analysis operation 412 is discussed in greater detail with reference to FIG. 10.

Par. [0100], D32 (emphasis added)

329 Therefore, D32 fails to disclose or suggest that packet filtering rules are automatically created or altered by the security policy management server based on malicious traffic information received from a malicious host tracker service as defined in feature 1.1.3 (and consequently features 1.1., feature group 1.3 and feature 1.4).

330 Further, **feature 1.2.6** directed to routing an identified packet to a monitoring device is not disclosed in or suggested by D32. In D32, a packet which "fails" a rule (i.e., which matches a rule preventing the packet from entering a protected network, cf. D32, par. [0106]) is deleted (cf. D32, par. [0111]):

[0111] Failure of a packet by the IDS rule analysis operation 504 also results in a delete packet operation 512. This operation 512 deletes the packet from the computer system 300, thereby preventing the packet from reaching its destination and freeing up resources for analysis of later received packets. In an embodiment, deleting the packet may include saving a copy of the packet to a deleted packet database for further analysis. One skilled in the art will recognize that the

Excerpt of par. [0111], D32 (emphasis added)

331 Since D32 teaches to delete the packet, it fails to disclose feature 1.2.6.

332 As D32 does not teach or suggest features 1.1., 1.1.3, feature group 1.3, feature 1.4, and feature 1.2.6, a combination of D31 with D32 cannot lead the skilled person to the subject-matter of claim 1 as granted. Therefore, the subject-matter of claim 1 as granted is inventive over said combination of D31 with D32.

3. The combination of US 2011/0072506 A1 (D31) with common knowledge and D36 does not render the subject-matter of claim 1 obvious

333 Starting from D31, intervenor 1 also asserts that the claimed solution is obvious in view of common knowledge (regarding the alleged “first” partial problem solved by features 1.2.4. and 1.2.5) and US 2011/0314177 A1 (D36) (regarding the alleged “second” partial problem solved by feature 1.2.6.

a. Common knowledge does not teach features 1.2.4 and 1.2.5

334 Intervenor 1 sets forth that it was common general knowledge to use the standardized syslog protocol (set out in D33 and D34) in firewalls. According to intervenor 1, this common general knowledge is allegedly evidenced by US 8 204 082 B2 (D35).

335 D35 mentions syslog in a general manner (cf. D35, col. 39, ll. 34 and 36):

For example, an enterprise firewall may implement a single provisioned rule set and report alerts and logs to a central station via methods such as syslog or SNMP. In a virtual

Col. 39, ll. 34 to 36, D35

336 However, this is only a general mentioning of using syslog in combination with an enterprise firewall. The enterprise firewall mentioned in the cited paragraph does not have any relation to the devices described in D35.

337 The general teaching of D35 with respect to an arbitrary enterprise firewall cannot provide any hints to the skilled person to envisage, when starting from D31 as closest prior art, a rule provided in a dynamic security policy which specifies a packet digest logging function, wherein the packet digest logging function generates a record of a subset of information and reforming the subset of information according with a logging system standard. In short, D35 alone does not teach or suggest the features 1.2.4 and 1.2.5.

b. D36 does not teach feature 1.2.6

338 Intervenor 1 cites D36 as allegedly rendering feature 1.2.6 obvious, which reads as follows:

1.2.6 *routing, by the packet security gateway, the packet to a monitoring device configured to store the packet for subsequent analysis;*

339 This particular step defined in feature 1.2.6 is part of a packet digest logging function specified by a packet filtering rule (cf. feature 1.2.2).

340 D36 does not disclose this feature.

341 D36 addresses the aspect of how internet service providers (ISPs) direct data packets via their routers (cf. D36, paras. [0002] and [0020]). In D36, a network router 104 receives a packet and compares a source or destination address of the packet to a range of lawful intercept IP addresses 262. If so, the network router 104 redirects the packets to a lawful intercept capture system 108 (cf. D36, par. [0061] and [0062] and fig. 4).

342 Intervenor 1 equates the network router 104 of D36 with a “packet security gateway”. This, however, cannot be the case since the network router 104 does not perform any security related functions (like e.g. a firewall) but merely pertains to routing of packets. As such, the network router 104 of D36 is not a packet security gateway as claimed. Consequently, D36 does not disclose that the routing is performed by packet security gateway as required by feature 1.2.6

343 Further, the routing according to feature 1.2.6 is performed as part of the packet digest logging function. Such a function is not disclosed in D36. Accordingly, in D36, the routing is not performed as part of a packet digest logging function.

344 Due to the lack of feature 1.2.6 in D36, the claimed subject-matter cannot be rendered obvious by a combination of D31 with D36.

III. Inventive step over D44 in view of common general knowledge

345 Intervenor 2 asserts that logging packets and routing said packets as defined in features 1.2.4 to 1.2.6 are common knowledge (cf. intervention 2, marginals 206).

346 Intervenor 2 further asserts that this common general knowledge is evidenced by Sourcefire manual v4.10 (D19) and Juniper (D41) (cf. intervention 2, marginals 207).

347 Further, intervenor 2 argues that claim 1 as granted distinguishes over the common general knowledge (i.e., closest prior art) by virtue of feature 1.1.3 alone. Consequently, intervenor 2 finds features 1.2.4 to 1.2.6 to be known from Sourcefire manual v4.10 (D19) and Juniper (D41). Thus, intervenor 2 alleges that a combination of common general knowledge (i.e., D19 and D41) with D44 would result in the claimed subject-matter.

348 However, this is not correct.

349 As explained above in present marginals 223 to 227, Juniper (D41) does not disclose a routing of packets (feature 1.2.6), but merely generating syslog reports. As set forth in marginals 256 to 265

above, D44 fails to disclose feature 1.1.3. Therefore, a combination of D44 with Juniper (D41) or Sourcefire manual v4.10 (D19) cannot lead to the claimed subject-matter.

350 This applies correspondingly to a combination of D44 with D19, due to the lack of disclosure of feature 1.1.3 in D44 (see above marginals 259 to 265).

351 Therefore, the subject-matter of claim 1 and, correspondingly, claims 14 and 15 is not rendered obvious by D44 in view of common general knowledge.

IV. Inventive step over WO 2012/164336 (D45) in view of common general knowledge or, alternatively, in view of the Sourcefire manual v4.10 (D19), or, alternatively, Juniper (D41)

352 Intervenor 2 further refers to WO 2012/164336 (D45) as starting point for an inventive step attack on the subject-matter of claim 1 (cf. intervention 2, marginal 209). In particular, intervenor 2 asserts that the claimed subject-matter is rendered obvious by a combination of D45 with common knowledge (allegedly evidenced by Sourcefire manual v4.10 (D19) and Juniper (D41)), or, alternatively, by a direct combination of D45 with one of these two documents D19 or D41 (cf. intervention 2, marginal 223).

353 D45 discloses an intelligence headquarters (IHQ) 24 which provides a customized threat report 610 to gateway 22 (cf. D45, p. 26, ll. 9 to 13, p. 27, ll. 1 to 5, Fig. 5 and Fig. 7).

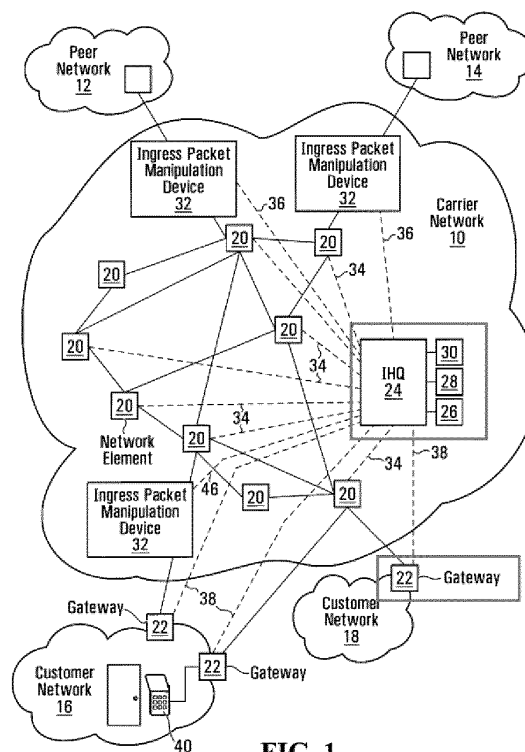


FIG. 1

Fig. 1 of D44 (markings added)

354 In marginal 221 of the intervention 2, intervenor 2 concedes that D45 fails to disclose features 1.2.4, 1.2.5 and 1.2.6 of claim 1:

1.2.4 *generating a record comprising the subset of information specified by the packet;*

1.2.5 *reformatting the subset of information specified by the packet in accordance with a logging system standard;*
and

1.2.6 *routing, by the packet security gateway, the packet to a monitoring device configured to store the packet for subsequent analysis;*

355 According to marginal 222 of the intervention 2, the above features are allegedly known from Sourcefire manual v4.10 (D19) and Juniper (D41).

356 We disagree with this finding.

357 A combination of D45 with Sourcefire manual v4.10 (D19) or Juniper (D41) does not render the claimed subject-matter obvious.

358 First, when starting from D45, the skilled person does not have any motivation to consider Sourcefire manual v4.10 (D19) and Juniper (D41). D45 is focused – as stated by intervenor 2 at marginal 221 of intervention 2 – on the IHQ-side, i.e. to a management server, and not a gateway. Therefore, when improving the teaching of D45, the skilled person would rather focus on aspects of the IHQ than the gateway. The skilled person does not, however, have any motivation to consult gateway-oriented aspects of D19 and D41.

359 Still further, Sourcefire manual v4.10 (D19) merely describes tools to set up responses to intrusion events such as alerting for syslog (cf. D19, p. 262 and our respective statements in marginals 173 to 178 above) and therefore cannot disclose or suggest at least feature 1.2.5.

360 In Juniper (D41), syslog reports are generated (cf. D41, p. 1148, and our respective statements in marginals 225 to 227 above). Consequently, D41 fails to disclose or suggest at least feature 1.2.6.

361 Hence, the gap between D45 and the claimed subject-matter cannot be closed by the teachings of Sourcefire manual v4.10 (D19) and Juniper (D41).

362 We further observe that – contrary to the finding of intervenor 2 – D45 does also not disclose feature 1.1.3.

1.1.3 *wherein one or more first packet filtering rules, of the first set of packet filtering rules, was automatically created or altered by the security policy management server based on malicious traffic information received from a malicious host tracker service;*

363 With respect to this feature 1.1.3, intervenor 2 refers to the automatic creation of the customized threat report 610 by the IHQ 24 (cf. intervention 2, marginal 218).

364 However, the IHQ 24 of D45 does not automatically create or alter packet filtering rules.

365 Thus, D45 fails to disclose the feature 1.1.3. This feature is also not disclosed in or suggested by Sourcefire manual v4.10 (D19) or Juniper (D41) (cf. above sections E.II.2.b, and E.III.3). Correspondingly, a combination of D45 with Sourcefire manual v4.10 (D19) or Juniper (D41) does not render the claimed subject-matter obvious.

366 With respect to feature group 1.3 and feature 1.4., intervenor 2 refers again to the automatic updates of the customized threat reports 610 with respect to providing updates to rules (cf. intervention, marginal 220).

1.3 *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,*

1.3.1 *wherein the updated second set of packet filtering rules comprises an update to the first set of packet filtering rules generated by the security policy management server based on updated malicious traffic information received from the malicious host tracker service;*

1.4 *performing, on a packet by packet basis, packet filtering on a second portion of the packets as sociated with the network protected by the packet security gateway based on the updated second set of packet filtering rules*

367 Since D45 fails to disclose feature 1.1.3, it accordingly fails to disclose feature group 1.3 and, consequently, feature 1.4. Further, Sourcefire manual v4.10 (D19) or Juniper (D41) do also not disclose or suggest features 1.3.1 and 1.4 (cf. above sections E.II.2.e and f, and E.III.4). Thereby, combining D45 with one of Sourcefire manual v4.10 (D19) and Juniper (D41) does not render the claimed subject-matter obvious.

368 Therefore, the subject-matter of claim 1 and, correspondingly, claims 14 and 15 is inventive over D45 in combination with any one of general common knowledge, D19, and D41.

V. Inventive step: Conclusion

369 In summary, the opponents' assertions regarding lack of inventive step in the subject-matter of the independent claims are to no avail.

G. Dependent claims

370 Dependent claims 2 to 15 all depend on independent claim 1 and thus are novel and inventive over the cited prior art due to the reasons given in sections E and F above.

371 Concerning the additional features of dependent claims 2 to 15 we comment as follows:

I. Dependent claim 2

- 372 Dependent claim 2 defines that “*the at least one packet matching criterion comprises at least one network address associated with an indication of malicious network traffic*” (emphasis added).
- 373 The underlined wording was objected against by the opponent as being not disclosed in the original disclosure.
- 374 We disagree. The skilled person learns from the underlined part of the feature that the at least one network address is indicative of or associated of malicious network traffic.
- 375 This teaching that network addresses are associated with malicious network traffic is disclosed in the original disclosure, e.g. par. [15].
- 376 Further, Sourcefire manual v5.1.1 (D23) does not disclose or suggest the additional features of dependent claim 2. Here, intervenor 1 refers to the Security Intelligence Feed being a dynamic collection of IP addresses with a poor reputation (cf. intervention 1, p. 97, section a.)
- 377 However, according to feature 1.1.2, the packet filtering rule comprises the packet matching criterion. But as set forth above in marginals 124ff, the Security Intelligence is not a packet filtering rule. Therefore, the IP addresses of the Security Intelligence feed do not correspond to a packet matching criterion comprised by a packet filtering rule. Since Sourcefire manual v5.1.1 does not disclose that the IP addresses of the Security Intelligence feed are part of an access control rule (of the access control policy), the access control rule of D23 does not comprise a packet matching criterion with at least one network address associated with an indication of malicious network traffic.
- 378 Further, intervenor 1 opines that a standard text rule or “standard objection rule” of Sourcefire manual v4.10 (D19) comprises source and destination IP addresses and that these rules are automatically created by the Sourcefire VRT.
- 379 These rules are, first, not created automatically but rather manually by the Sourcefire VRT as set forth in above marginals 161 to 163. Second, intervenor 1 fails to show that the source and destination IP addresses of these rules are “associated with an indication of malicious network traffic” as defined in dependent claim 2. Third, as set forth in above marginals 164 to 171, the Sourcefire VRT does not identify malicious hosts. Thus, Sourcefire manual v4.10 (D19) does not disclose that a packet matching criterion comprises network addresses, as defined in dependent claim 2.
- 380 In this regard, intervenor 2 refers in a superficial manner to the disclosure of p. 403 of Juniper (D41). The cited page mentions only options offering “protection against IP addresses”. A rule specifying an IP address “*associated with an indication of malicious network traffic*” as defined in dependent claim 2 is not disclosed on the cited page.
- 381 Intervenor 3 refers to US 8,572,717 B2 (D48) and asserts that col. 7, lines 14 to 37 disclose that packets are analyzed to identify an indication of malicious network traffic. The cited passage further indicates that network attacks, viruses and other malicious software carried by a packet flow are

detected by reassembling application-layer communications from payloads. Thus, the malicious activity is indicated by criteria specified in the application-layer and not, as required by dependent claim 2, by a network address which is part of the network layer.

- 382 Therefore, the additional features of dependent claim 2 are not disclosed or suggested by the Sourcefire manuals (D19 and D23), Juniper (D41), or D48.

II. Dependent claim 3

- 383 Dependent claim 3 further specifies that “*at least one packet transformation function comprises a network protective action*” (emphasis added). The opponent and intervenor 1 argue that the underlined wording is a non-disclosed generalisation.
- 384 We disagree. Par. [43] of the original disclosure reads: “*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*” (emphasis added).
- 385 Both protecting a network from malicious network traffic and preventing malicious network traffic from leaving a network correspond to “*network protective actions*”.

III. Dependent claim 4

4. The method of any one of claims 1-3, wherein the dynamic security policy specifies that a first set of the packets should be placed in a first forwarding queue and a second set of the packets should be placed in a second forwarding queue, the first forwarding queue having a higher forwarding rate than the second forwarding queue, the method comprising:

sending, by the packet security gateway, the first set of the packets in the first forwarding queue; and

sending, by the packet security gateway, the second set of the packets in the second forwarding queue.

- 386 Dependent claim 4 is directed to placing packets in corresponding forwarding queues. The opponent asserts that the claimed subject-matter is a non-disclosed generalisation, since claim 4 allegedly lacks that the packets are placed in different queues based on network addresses.
- 387 Here, the opponent overlooked that par. [51] of the original disclosure reads as follows (emphasis added):

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.

Excerpt of par. [51] of original disclosure (emphasis added)

- 388 Thus, the original disclosure states that a predetermined “*arbitrary selector*”, which corresponds to a parameter or field of a packet, may serve as basis for putting packets in different queues. In other words, packets are placed in different queues based on the arbitrary selector included in a rule (of a dynamic security policy).
- 389 Intervenor 1’s alleged added-matter objection asserts that the enqueueing service defined in dependent claim 4 does not relate to packet digest logging function or a routing function.
- 390 Here, intervenor 1 reads into the claim that the packet filtering rule specifying the logging and routing function does also effectuate the enqueueing service. This is, however, not the case. Dependent claim 4 requires merely that the packet security gateway specifies that packets are placed into a first or second forwarding queue (and then sent accordingly) – a connection to the logging and routing function is not required. The packet security gateway specifying the placements of the packets in different queues is disclosed in par. [10] of the original disclosure.
- 391 The subject-matter of dependent claim 4 is hence supported by the original disclosure.
- 392 With respect to the additional features of dependent claim 4, intervenor 1 refers to the inspection of a packet’s type of service (ToS) described in Sourcefire manual v4.10 (D19) as allegedly novelty destroying. However, the “tos keyword” of D19 is merely a criterion against which packets are compared (cf. D19, p. 815: “*The tos keyword allows you to test the packet’s IP header ToS value against the value you specify as the keyword’s argument*”), but does not place the packets in different queues, as required by claim 4.
- 393 The above argument also applies to Sourcefire manual v5.1.1 (D23), since p. 975 of D23 cited by intervenor 1 does to go beyond the disclosure of p. 815 of the older Sourcefire manual v4.10 (D19).
- 394 Further, the cited documents D37 and D38 merely describe the usage of packet classifiers to “steer” packets. But steering packets does not correspond to a queuing of packets as defined in dependent claim 4.
- 395 Intervenor 2 refers to p. 445 to 447 of Juniper (D41), in which the concept of “SYN flood protection” is explained. In Juniper (D41), this flood protection is mentioned in association with network DoS attacks. The cited pages merely pertain to one single queue, i.e., the proxied connection queue. Thus,

the cited pages do not disclose placing packets in different queues with different forwarding rates as defined in dependent claim 4.

396 Intervenor 3 states that, allegedly, D49 would motivate the skilled person to implement forwarding queues as required by claim 4 for improving throughput. Intervenor 3, however, fails to provide any arguments, why the skilled person, starting from any one of the prior art documents on file, should indeed be motivated to consider the teaching of D49.

IV. Dependent claim 5

5. The method of any one of claims 1-4, 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 of the multiple packet transformation functions at the network layer.

397 The opponent asserts that the subject-matter of claim 5 corresponds to a non-disclosed generalisation, since the packet transformation function is not specified to be performed simultaneously. To this end, the opponent refers to par. [14] of the original disclosure.

398 Par. [42] of the original disclosure is directed to embodiments related to the operation in a network layer transparent manner. Yet, par. [42] does not mentioned that the packet transformation function is performed simultaneously, let alone the term “*simultaneously*”.

399 Intervenor 1 asserts that operation of the packet security gateway “*in a network transparent manner*” is not disclosed in combination with the packet digest logging function and routing of the packet. In particular, par. [42] of the original disclosure discloses that, by operating in a network layer transparent manner, attack packets cannot be routed to network interfaces.

400 Here, intervenor 1 overlooks the teaching of par. [14] of the original disclosure, according to which the packet security gateway (when operated in a network layer transparent manner) can send (i.e., route) traffic at a link layer using an interface that is not addressed at the network layer.

401 Therefore, the subject-matter of dependent claim 5 is disclosed in the original disclosure.

402 Further, intervenor 1 asserts that the patent opposed fails to disclose how packets can be received in network layer transparent manner using an interface that is not addressed at the network layer and performing the at least one of the multiple packet transformation functions at the network layer – therefore, subject-matter of dependent claim 5 would be insufficiently disclosed (Art. 83 EPC).

403 This assertion is moot, since par. [0014] of the patent opposed teaches to send and receive traffic by using a link layer and perform packet transformation functions.

404 Therefore, dependent claim 5 is in line with Art. 83 EPC.

- 405 Intervenor 1 refers with respect to dependent claim 5 to a “transparent inline mode” of sensors as described in both Sourcefire manuals v4.10 and v5.1.1 (D19 and D23). According to the manuals, this mode allows the sensor to act as a “bump in the wire” such that the sensor “forwards all network traffic regardless of its source and destination” (cf. D19, p. 266, and D23, p. 233). In other words, the sensor does not process or inspect any packets. Contrary thereto, the additional features of dependent claim 5 require performing at least one packet transformation function at the network layer. Thus, none of D19 and D23 discloses the features of dependent claim 5.
- 406 Juniper (D41) cited by intervenor 2 describes a transparent mode in which a security device filters packets “*without modifying any of the source or destination information in the IP packet header*” (cf. D41, p. 91, last par.). Accordingly, in D41, when in the transparent mode, the security device does not perform any modifications at the network layer (which pertains to IP addresses). But dependent claim 5 requires performing packet transformation functions at this layer. Thus, Juniper (D41) fails to disclose the additional features of dependent claim 5.

V. Dependent claim 6

- 6. The method of any one of claims 1-5, wherein the network communications awareness service comprises a network security awareness service or a network threat awareness service.*
- 407 Dependent claim 6 specifies that “*the network communications awareness service comprises a network security awareness service or a network threat awareness service*”.
- 408 The opponent contends that par. [54] of the original disclosure discloses that the network communications awareness service is juxtaposed, on the same logical level, with the network security awareness service or the network threat awareness service.
- 409 However, par. [54] reads “*informational service for performing a network communications awareness service, a network security awareness service, and/or a network threat awareness service*” (emphasis added). The wording “*and/or*” implies various combinations of the three services and also their hierarchical relation to each other. In particular, the variation in which the network communication awareness service comprising the network security awareness service and the network threat awareness service is encompassed by this wording.

VI. Dependent claim 7

- 410 Dependent claim 7 “*the network communications awareness service is provided based on one or more criteria that are indicative of packet communications that are of interest to an organization that operates the network*” (emphasis added).
- 411 The opponent objects to the underlined features as being a non-disclosed generalisation since par. [54] of the original disclosure allegedly discloses only that an organisation operates “*the secured network*” (emphasis added).

- 412 However, the opponent overlooks the dependency of claim 7. Specifically, claim 7 is dependent on claim 1 which already defines that the network is protected by the packet security gateway. Accordingly, in view of claim 1, the network as defined in claim 7 is also protected/secured.

VII. Dependent claims 8, 9

8. The method of any one of claims 1-7, wherein the at least one packet matching criterion comprises a five-tuple specifying one or more transport-layer protocols, a range of source addresses, a range of source ports, a range of destination addresses, and a range of destination ports.

9. The method of any one of claims 1-8, wherein the at least one packet matching criterion comprises application-layer packet-header information.

- 413 Here, the opponent objects to the feature “packet matching criterion” as being not disclosed the original disclosure.
- 414 We disagree. Original claim 17 of the parent application defines that “*the packet-identification criteria comprises a five-tuple specifying one or more transport-layer protocols, a range of source addresses, a range of source ports, a range of destination addresses, and a range of destination ports*” (*emphasis added*). The formulation “comprises” (=singular) explicitly indicates that the criteria is to be understood as a criterion (=singular). Therefore, the parent application discloses that a rule may also specify one criterion.

VIII. Dependent claim 10

10. The method of any one of claims 1-9, wherein the application-layer packet-header information identifies one or more fully qualified domain names (FQDN) or uniform resource identifiers (URI).

- 415 The opponent objects that feature “*one or more fully qualified domain names (FQDN)*” is not disclosed in the original disclosure.
- 416 Dependent claims 10 defines that “*the application-layer packet-header information identifies one or more fully qualified domain names (FQDN) or uniform resource identifiers (URI)*”.
- 417 Generally, an FQDN is a portion of a URL (Uniform Resource Locator), which in turn is a type of URI that specifies not only a resource, but how to reach it on the internet – like “*http://*”, “*ftp://*” or “*mailto://*”.

- A Uniform Resource Identifier (URI) is a string of characters that uniquely identify a name or a resource on the internet. A URI identifies a resource by name, location, or both. URIs have two specializations known as Uniform Resource Locator (URL), and Uniform Resource Name (URN).
- A Uniform Resource Locator (URL) is a type of URI that specifies not only a resource, but how to reach it on the internet—like *http://*, *ftp://*, or *mailto://*.
- A Uniform Resource Name (URN) is a type of URI that uses the specific naming scheme of urn: —like *urn:isbn:0-486-27557-4* or *urn:isbn:0-395-36341-1*.
- So a URI or URN is like your name, and a URL is a specific subtype of URI that's like your name combined with your address.

<https://danielmiessler.com/study/difference-between-uri-url/>

418 Par. [44] of the original disclosure reads that “[i]n some embodiments, the specified criteria may comprise values selected from application-layer packet-header information. For example, application-layer hypertext transfer protocol (HTTP) packets, which transfer information between instances of web client applications (e.g., web browsers) and web server applications (e.g., named web sites such as *www.examplewebsite.com*), may contain headers that specify methods and/or one or more uniform resource identifiers (URIs) for transferring resources (e.g., files) between client and servers. [...]”.

419 Here, “*www.examplewebsite.com*” is an example of an FQDN.

420 In other words, par. [44] discloses an example of an URI, i.e., the exemplary FQDN (“*www.examplewebsite.com*”). Thus, the original disclosure provides a basis for the feature “FQDN”.

421 Intervenor 1 refers to the “urilen keyword” described in both Sourcefire manuals v4.10 and v5.1.1 (D19 and D23), at p. 830f and p. 990, respectively. However, with the “urilen keyword”, only a length of a uniform resource identifier (URI) is inspected but not the URI itself.

422 Intervenor 2 cites p. 519 of Juniper (D41) which mentions fully qualified domain names (FQDN) to identify a server, with which the security device may communicate (cf. D41, p. 518: “*Configure the security device to communicate with one of the following servers: [...]*”). In particular, the security device may communicate with a “*Websense server*” or “*SurfControl server*”. The setting “Server name” is the IP address or Fully Qualified Domain Name (FQDN) of the computer running the Websense or SurfControl server. However, Juniper (D41) fails to disclose to use the FQDN for inspecting packets, and therefore fails to disclose the additional features of dependent claim 10.

IX. Dependent claim 11

11. The method of any one of claims 1-10, further comprising:
 receiving second malicious traffic information from a second service; and
 correlating the malicious traffic information received from the malicious host tracker service with the second malicious traffic information.

- 423 Dependent claim 11 defines the further method steps of “*receiving second malicious traffic information from a second service; and correlating the malicious traffic information received from the malicious host tracker service with the second malicious traffic information*”. Correlating the malicious traffic information with the second malicious traffic information comprises identifying duplicates or overlap in network addresses ([0052] of the patent opposed).
- 424 The opponent and intervenor 1 object that the original disclosure does not disclose second malicious traffic information.
- 425 However, par. [65] of the original disclosure reads “*security policy management server 120 may receive updates (e.g., as part of a subscription) from malicious host tracker service 508 and/or one or more other services. The updates from the two or more services may be correlated (e.g., by security policy management server 120)*” (emphasis added). The malicious host tracker service 508 (and also other services) aggregate information associated with malicious network traffic (cf. original disclosure, par. [64]). Accordingly, malicious traffic information and second malicious traffic information are received from respective services. Therefore, the wording “*second*” is derivable from at least par. [64] and [65] of the original disclosure.
- 426 Hence, the subject-matter of dependent claim 11 is compliant with Art. 123(2) and 76(1) EPC.
- 427 With respect to novelty, intervenor 1 refers to p. 143 and 146 of Sourcefire manual v5.1.1 (D23) to assert an alleged correlation of malicious traffic information as defined by the additional features of dependent claim 11. However, the cited passages only disclose that a Security Intelligence feed (such as the ZeuS Blacklist) may be configured to “*augment*” the Sourcefire Intelligence feed (cf. D23, p. 143 and 147)
- 428 The additional features of claim 11 are, however, not disclosed in Sourcefire manual v5.1.1 (D23) by “*augmenting*” the Sourcefire Intelligence feed. In fact, D23 fails to indicate any details what augmenting may encompass. The presence of multiple feeds alone does not necessarily result in a correlation of information.
- 429 This also applies correspondingly to the arguments brought forth by intervenor 1 with respect to Sourcefire manual v4.10 (D19), where it is argued that allowing “multiple subscription to malicious host tracker services” implies a correlation of the of the malicious traffic information from the multiple services (cf. intervention 1, p. 115, penultimate par.). Here again, intervenor 1 fails to indicate any correlation of information of the multiple sources.
- 430 Intervenor 2 similarly argues that “the use of multiple services and correlating between them is a well-established practice and common general knowledge” (cf. intervention 2, p. 81). However, the cited p. 530 of Juniper (D41) merely mentions “four predefined signature packs” without any indication of a correlation of their information. Also, the passage of D45 (p. 18, lines 11 to 23) cited by intervenor 2 merely mentions that external seed information can be obtained from multiple sources. But it fails to disclose any correlation of the seed information.

X. Dependent claim 12

12. The method of any one of claims 1-11, wherein performing packet filtering on the second portion of the packets comprises dropping, based on the updated second set of packet filtering rules, one or more of the second portion of packets.

431 Dependent claim 12 is directed to “*dropping, based on the updated second set of packet filtering rules, one or more of the second portion of packets*”.

432 The opponent asserts that there is no disclosure in the original disclosure which relates to specifically dropping packets of a second set of filtering rules.

433 Par. [87] to [89] of the original disclosure describe updating a rule which specifies a “*deny packet transformation function*”, which drops packets (cf. original disclosure, par. [83], last sentence). Hence, the second set of filtering rules (which are the updated rules) are provided for blocking packets.

434 Intervenor 1 asserts that the combination of creating a “record comprising the subset of information” (features 1.2.3 to 1.2.5) and routing the packet to the monitoring device (feature 1.2.6) in combination with the dropping of a packet constitute added-matter.

435 However, dependent claim 12 does not define a packet digest logging function and routing of packets to be combined with dropping packets. In fact, dependent claim 12 merely requires to drop packets based on the second set of packet filtering rules. Hence, intervenor 1’s added-matter objections are moot.

436 Therefore, the subject-matter dependent claim 12 is in line with the provisions of Art. 123(2) and 76(1) EPC.

437 With regard to an alleged non-novelty of the subject-matter of dependent claim 12, intervenor 1 refers to passages of both Sourcefire manuals v4.10 and v5.1.1 (p. 358f and p. 563, respectively) which both disclose the same, namely so-called “drop rules” which cause a packet to be dropped and generate an event. However, the cited passages fail to mention any updates of rules and, correspondingly, that an updated rule drops packets.

438 Similarly, p. 605 of Juniper (D41) (as cited by intervenor 2) merely mentions different actions for IDP rules such as a drop rule. The aspect that a drop rule is an updated rule is not disclosed in the cited passage.

439 Therefore, the subject-matter of dependent claim 12 is novel over both Sourcefire manuals v4.10 and v5.1.1 (D19 and D23) and Juniper (D41).

XI. Dependent claim 13

13. The method of any one of claims 1-12, wherein the update to the first set of packet filtering rules comprises indications of a plurality of network addresses that have been determined to be associated with malicious network traffic, wherein the first set of packet filtering rules do not comprise the indications of the plurality of network addresses.

- 440 Dependent claim 13 defines that “*the first set of packet filtering rules do not comprise the indications of the plurality of network addresses*” (emphasis added). The opponent asserts that the underlined wording is not disclosed in the original disclosure. A similar objection was raised by intervenor 1.
- 441 However, step 1314 of fig. 13 of the original disclosure discloses that the rules are updated “*to include other network address(es) included in the different set of network addresses*”. This means that previously to the update, the other network addresses were not included in the rule(s). This procedure is also explained in par. [88] of the original disclosure.
- 442 Thus, it is unambiguously and directly derivable from the original disclosure that the first set of packet filtering rules does not comprise an indication of the plurality of network addresses.
- 443 Intervenor 1 further asserts that par. [87] of the parent application discloses only that the “different set of network addresses” is received from a different computing device, whereas (according to claim 1) the update is received from the malicious host tracker service.
- 444 Here, intervenor 1 misses the additional teaching of par. [87], according to which the different computing device may be associated with the malicious host tracker service:

For example, security policy management server **120** may receive a security update comprising a different set of network addresses (e.g., {network address B, network address C, network address D, and network address E}) from a different computing device (e.g., a different computing device associated with malicious host tracker service **508** or a computing device associated with a malicious host tracker service different from malicious host tracker service **508**).

Excerpt of par. [87] of original disclosure (emphasis added)

- 445 Insofar, the update is received (at least indirectly) from the malicious host tracker service.
- 446 The subject-matter of dependent claim 13 is hence compliant with Art. 123(2) and 76(1) EPC.
- 447 With respect to alleged non-novelty of dependent claim 13, intervenor 1 refers to the automated SEU imports of Sourcefire manual v4.10 (D19) described on p. 1716. An SEU (security enhancement updated) contains new and updated standard text rules. There is no disclosure in the cited passage that the updated rules of an SEU comprise new network addresses, let alone addresses associated with malicious network traffic. In fact, p. 1716 of D19 fails to mention network addresses or updates thereof at all.
- 448 Further, intervenor 1 points to the Security Intelligence feed of Sourcefire manual v5.1.1 (D23) as being a “*dynamic collection of IP addresses*” (D23, p. 142). However, as set forth above in marginals 124ff, the Security Intelligence feed does not correspond to a packet filtering rule as claimed. But dependent claim 13 requires the packet filtering rule to comprise the network addresses.
- 449 Intervenor 2 cites p. 647 of Juniper (D41) which concerns the updates of attack databases. These updates may include new or modified predefined IDP attack objects and groups, new or modified signatures used by a Deep Inspection feature, and updates to the IDP engine. Nonetheless, the cited passage of D41 does not even mention IP or network addresses.

450 Intervenor 2 further refers to p. 29, lines 20 to 30 of D47. This passage merely describes disposing packets which match traffic attributes contained in a customized threat report. Updating rules with new network addresses as required by dependent claim 12 is not disclosed therein.

XII. Dependent claim 14

14. A system comprising at least one processor of a packet security gateway (112) and a memory storing instructions that, when executed by the at least one processor, cause the system to perform one or more of the methods of claims 1-13.

451 Intervenor 1 asserts that the original disclosure does not disclose that “*at least one processor of a packet security gateway*” may “*cause the system to perform*” an alteration or creation of a packet filtering rule.

452 Firstly, it is noted that intervenor 1 misunderstands claim 14 insofar that the claimed system creates or alters rules. This is however not the case. Claim 14 is merely directed to a system performing the steps of the methods claims 1 to 13. In fact, the methods are performed by the packet security gateway. The alteration or creation of packet filtering rules is, however, not done by the packet security gateway, but by the security policy management server.

453 Regarding the disclosure of the subject-matter of claim 14, par. [39] of the original disclosure indicates that the packet security gateway includes a processor and a memory. The memory includes one or more program modules that when executed by processor, configure packet security gateway to perform various functions as described herein.

454 Hence, the original disclosure provides basis for a system performing the methods of claims 1 to 13.

455 Further, due to the dependency to independent claim 1, the subject-matter of claim 14 is also novel and inventive.

XIII. Dependent claim 15

15. A computer program comprising computer-executable instructions that, when executed by one or more processors of a packet security gateway (112), cause the one or more processors to perform one or more of the methods of claims 1-13.

456 The subject-matter of claim 15 is novel and inventive since it is dependent on claim 1 which is – as set forth above – also novel and inventive.

H. Conclusion

457 The subject-matter of the independent claim 1 does not extend beyond the content of the parent application and the application as originally filed.

458 Further, the cited prior art neither anticipates nor renders obvious the subject-matter of independent claim 1 as granted.

459 The patent opposed discloses the invention in a manner sufficiently clear and complete for it to be carried out by a person skilled in the art.

460 Thus, the request to dismiss the opposition and the interventions and to uphold the patent opposed as granted is justified.

Dr. Martin Meggle-Freund

European Patent Attorney