



BARDEHLE PAGENBERG - Postfach 86 06 20 - 81633 München

European Patent Office

80298 München

Munich, May 23, 2022

- BRIEF CONTAINS COLORED DRAWINGS -

Opposition against: EP 3550795 (19170936.9)
Proprietor: Centripetal Networks Inc.
Opponent: Cisco Systems GmbH
Our ref: C159362EPT1EIN6 KAU/JH/MRJ/HMS/hea

**BARDEHLE
PAGENBERG**

Tobias Kaufmann
tobias.kaufmann@bardehle.de

Prinzregentenplatz 7
81675 München
T +49.(0)89.928 05-0
F +49.(0)89.928 05-444
www.bardehle.com

**URGENT – INFRINGEMENT PROCEEDINGS PENDING –
ACCELERATED PROCESSING REQUESTED**

On behalf of

Cisco Systems GmbH, Parkring 20, 85748 Garching, Germany

(hereinafter: “*the intervenor*”) we herewith file a

NOTICE OF INTERVENTION

in accordance with Articles 99, 105 EPC and Rule 89 EPC into the opposition proceedings against the European patent **EP 3 550 795** (hereinafter the “*opposed patent*”).

BARDEHLE PAGENBERG
Partnerschaft mbB
Patentanwälte Rechtsanwälte
Amtsgericht München
Partnerschaftsregister 1152
ISO 9001 certified

In cooperation with:


YUSARN AUDREY
www.yusarn.com
Singapore

The opposed patent is submitted¹ as

- document D2 -.

The intervenor **requests**

1. **to revoke the opposed patent in its entirety and**
2. **to summon for oral proceedings in accordance with Article 116 EPC in case the first request cannot be granted in the written procedure.**
3. **Accelerated processing of the opposition is requested in line with section E-VIII, 5 of the Guidelines for Examination and OJ EPO 2008, 221, as an infringement action in respect of the opposed patent is pending.**

The opposition fee in the amount of EUR 840,00 is paid via online fee payment from our account 28000212.

The opposed patent is to be revoked on the following **grounds for opposition**:

- The subject matter of the opposed patent extends beyond the content of the parent application as originally filed and the application as originally filed within the meaning of Article 100 c) EPC as shown in detail in **section E** below.
- The subject matter of the opposed patent is not patentable within the meaning of Article 100 a) EPC in conjunction with Article 52 to 57 EPC, in particular as the claimed subject-matter lacks novelty (see **section F**) and at least an inventive step (see **section G**).

¹ The enumeration is continued from document D2 in accordance with the consolidated list of March 2, 2022 available in the EPO register.

- The opposed patent does not disclose the invention in a manner which is sufficiently clear and complete for it to be carried out by a person skilled in the art within the meaning of Article 100 b) EPC as shown in **section H** for the dependent claims below.

In detail:

A. Procedural aspects

An opposition against the opposed patent has been filed by Ixia, Santa Rosa, California on March 2, 2022. The opposition brief was not signed when it was filed, but this curable deficiency was corrected with letter of May 5, 2022 within the time limit set in the Communication dated April 13, 2022. The opposition was therefore validly filed. The intervention into these opposition proceedings is admissible since an infringement complaint was brought by the proprietor of the opposed patent against the intervenor. A copy of the infringement complaint is submitted as

- Document D3 -.

Confidential information that is of no relevance for the instant opposition proceedings has been redacted in D3. The infringement complaint was served on the representatives of the intervenor on March 8, 2022 (c.f. the stamp on the first page). Thus, an intervention is possible as the three-months period starting from the service date has not expired yet (Rule 89 (1) EPC, T 694/01).

The infringement complaint based on the opposed patent was filed as an “*extension*” of a previous complaint under Section 264 item 2 German Civil Procedural Code (§ 294 Nr. 2 ZPO). The infringement proceedings have been separated with court order served on March 15, 2022, submitted as

- Document D4 -.

B. Bibliographic information

The opposed patent (EP 3 550 795 B1) resulted from European application EP 19170936.9. The documents of the application underlying the opposed patent as filed are submitted as

- document D5 -.

The opposed patent is based on a first-generation divisional application of parent application EP15722292.8 (which resulted in EP 3 132 587 B1). The documents as filed with the parent application are submitted as

- document D6 -.

These documents appear to correspond to the publication of the PCT application submitted as document D2 by the opponent (Ixia), which was re-enumerated as document D1 in the consolidated list.

The opposed patent has the filing date of April 7, 2015, and claims priority of US 14/253,992 filed on April 16, 2014. A copy of the priority document is submitted as

- document D7 -.

A feature analysis (see **section D**) is submitted as

- document D8 -.

C. Evidence

A markup copy of the claim amendments over the parent application (see **section E**) is submitted as

- **document D9** -.

This notice of intervention is based on a number of pertinent prior art documents. Firstly, we submit – and base this intervention on – references considered during the examination proceedings:

US 2004/123220 A1 (document D1 during examination), submitted as

- **document D10** -.

US 2006/136987 A1 (document D2 during examination), submitted as

- **document D11** -.

US 2007/240208 A1 (document D3 during examination), submitted as

- **document D12** -.

US 2006/146879 A1 (document D4 during examination), submitted as

- **document D13** -.

US 8 306 994 B2 (document D5 during examination), submitted as

- **document D14** -.

US 2005/138204 A1 (document D6 during examination), submitted as

- **document D15** -.

US 2006/195896 A1 (document D7 during examination), submitted as



- **document D16** -.

US 2006/248580 A1 (document D8 during examination), submitted as

- **document D17** -.

US 2011/055916 A1 (document D9 during examination), submitted as

- **document D18** -.

Even more, this notice of intervention is further based on the following documents, which were not considered during the examination:

„Sourcefire 3D System User Guide“ (herein also: Sourcefire manual) version 4.10, published in 2011, submitted as

- **document D19** -,

Affidavit of Ms. Sarah Ehrig regarding the publication procedure of the Sourcefire manual in version 4.10, submitted as

- **document D20** -,

Affidavit of Mr. Jacob H. Baugher III regarding sale of Sourcefire products (which included the Sourcefire manual), submitted as

- **document D21** -,

Final decision by the US Court of Appeals of the Federal Circuit confirming the public availability of document D19 before the priority date of the opposed patent, submitted as

- **document D22** -,

„Sourcefire 3D System User Guide“ (herein also: Sourcefire manual) version 5.1.1, published in 2012, submitted as



- document D23 -

Affidavit of Ms. Sarah Ehrig regarding the publication procedure of the Sourcefire manual in version 5.1.1, submitted as

- document D24 -

News article published in Frost & Sullivan “*Frost & Sullivan Recognizes Sourcefire for Next-Generation IPS*”, published on May 14, 2013, submitted as

- document D25 -

News article published in Daily News Egypt, “*For CyberSecurity Professionals, is the Concept of “Control” a Pipe Dream?*”, published on January 16, 2014, submitted as

- document D26 -

Article “*Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™)*”, Sean Barnum, published on February 20, 2014, submitted as

- document D27 -

Excerpt from Wayback machine² with TAXII Website excerpt showing FAQ, dated February 19, 2014, submitted as

- document D28 -

Excerpt from Wayback machine showing the date of archival of the TAXII Website excerpt, dated February 19, 2014, submitted as

² Accessible at <https://web.archive.org/web/20140219012227/http://taxii.mitre.org:80/about/faqs.html>; most recently accessed on May 4, 2022.



- document D29 -,

Article from TOTALTELECOM, “*Infoblox gives global businesses greater network control*”, published January 24, 2013, submitted as

- document D30 -,

US 2011/0072506 A1, published on March 24, 2011, submitted as

- document D31 -,

US 2010/257598 A1, published on October 7, 2010, submitted as

- document D32 -,

„Syslog“, RFC 5424, published in March 2009, available at <https://tools.ietf.org/html/rfc5424> submitted as

- document D33 -,

“Syslog” change history, available at <https://data-tracker.ietf.org/doc/rfc5424/history/> submitted as

- document D34 -,

US 8 204 082 B2, published on June 19, 2012, submitted as

- document D35 -,

US 2011/0314177 A1, published on December 22, 2011, submitted as

- document D36 -,

„An Architecture for Differentiated Services“, RFC 2475, available at <https://tools.ietf.org/html/rfc2475>, published in December 1998, submitted as



- document D37 -,

Publication history of „*An Architecture for Differentiated Services*“, available at <https://datatracker.ietf.org/doc/rfc2475/history/>, submitted as

- document D38 -.

D. Subject-matter of the opposed patent

The opposed patent relates to protecting IP networks from malicious attacks, such as a “*distributed denial of service*” attack (opposed patent, paragraph [0001]).

Proactive and reactive solutions were already known prior art to protect against such attacks on an IP network. The opposed patent discloses that the reactive solutions are disadvantageous, as the attack has already taken place and thus cannot be prevented anymore (opposed patent, paragraph [0002]). However, proactive solutions are considered unsuitable for large networks because it is not possible to filter high data volumes with high throughput (opposed patent, paragraph [0003]).

1. The problem underlying the opposed patent and the alleged solution

In view of the above, the (subjective) problem of the opposed patent is to enable improved, proactive protection of IP networks from harmful attacks (opposed patent, paragraphs [0003] and [0006]).

2. Solution

Independent method claim 1 may be structured as follows (also submitted as document D8):

- 1** *A method, comprising:*
 - 1.1** *receiving, by a packet security gateway (112) configured for protection of a network and associated with a security policy management server external from the network, a dynamic security policy comprising*
 - 1.1.1** *a first set of packet filtering rules from the security policy management server,*
 - 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, and*
 - 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;*
 - 1.2** *performing, by the packet security gateway and on a packet-by-packet basis, packet filtering on a first portion of packets associated with the network protected by the packet security gateway based on the first set of packet filtering rules by performing*
 - 1.2.1** *at least one of multiple packet transformation functions specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets,*
 - 1.2.2** *wherein at least one of the multiple packet transformation functions specified by the at least one packet filtering rule of the first set of packet filtering rules corresponds to a packet digest logging function that provides a network communications awareness service and comprises:*
 - 1.2.3** *identifying a subset of information specified by a packet matching the packet matching criterion of a packet filtering rule that specified the packet digest logging function;*

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;*

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 up-dated malicious traffic information received from the malicious host tracker service; and*

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

Independent system claim 14 may be structured as follows:

14.0 *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.*

3. Claim analysis

Below, we will explain the features of method claim 1 according to the understanding of the person skilled in the art. It should be noted that method claim 1, system claim 14, and computer program claim 15, which merely

reference claim 1, are written from the perspective of the packet security gateway.

The relevant person skilled in the art is a graduate engineer of electrical engineering or computer science with experience in the design and implementation of network security systems. He is familiar with firewalls, routers, switches, and protocols that exchange data over IP networks.

a. Feature 1

1 *A method comprising*

Claim 1 concerns a method comprising several steps (feature groups 1.1, 1.2, 1.3 and 1.4), all of which are carried out by a packet security gateway, i.e.:

- receiving a dynamic security policy (feature 1.1)
- performing packet filtering (feature group 1.2)
- receiving an updated second set of packet filtering rules for the dynamic security policy (feature group 1.3)
- performing packet filtering based on the updated second set of packet filtering rules (feature group 1.4)

Accordingly, claim 1 describes the method from the perspective of the packet security gateway.

b. 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 external from the network, a dynamic security policy comprising*

Feature 1.1 defines the role of the packet security gateway in more detail, which is configured, i.e., suitable, to protect a network and associated with a security policy management server located outside of the protected

network. The packet security gateway receives a dynamic security policy from the security policy management server.

The dynamic security policy is specified in more detail by the following features 1.1.1 through 1.1.3 and feature group 1.3.

c. Features 1.1.1 and 1.1.2

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

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, and*

According to feature 1.1.1, the dynamic security policy comprises a first set of packet filtering rules that the packet security gateway receives from the security policy management server. A set includes several individual rules.

Each packet filtering rule of the first set specifies at least one packet matching criterion (feature 1.1.2).

A packet matching criterion may be, for example, a network address that is associated with malicious network traffic (see dependent claim 2). The opposed patent also mentions as possible packet matching criteria the destination and source address, the protocol used as well as the source and destination ports. These are referred to as a so-called five-tuple (dependent claim 8 as well as Fig. 3 of the opposed patent and pars. [0071], [0013]).

d. 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;*

According to feature 1.1.3, one or more first packet filtering rules of the first set of packet filtering rules were created or modified (note the passive form) automatically by the security policy management server. This creation or modification was based on malicious traffic information received from a malicious host tracker service.

e. Features 1.2 to 1.2.2

1.2 *performing, by the packet security gateway and on a packet-by-packet basis, packet filtering on a first portion of packets associated with the network protected by the packet security gateway based on the first set of packet filtering rules by performing*

1.2.1 *at least one of multiple packet transformation functions specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets,*

1.2.2 *wherein at least one of the multiple packet transformation functions specified by the at least one packet filtering rule of the first set of packet filtering rules corresponds to a packet digest logging function that provides a network communications awareness service and comprises:*

According to feature 1.2, the packet security gateway carries out filtering on a first portion of packets associated with the network protected by the packet security gateway. Packets are associated with the network when they are intended for or are coming from a host located in the network. This means that packets sent to a host in a protected network, or packets leaving a protected network, are filtered (opposed patent, paragraph [0012]).

This filtering is performed by performing at least one of several packet transformation functions specified by at least one packet filtering rule of the first set of packet filtering rules (feature 1.2.1). Exemplary packet transformation functions are shown in the right column (“Action”) of Fig. 3 depicted below, which shows an exemplary dynamic security policy.

five-tuple

300

Rule #	Protocol	Source Address	Source Port	Destination Address	Destination Port	Action
1 (302)	TCP	140.*	*	130.*	20	Accept
2 (304)	TCP	140.*	*	*	80	Accept
3 (306)	TCP	150.*	*	120.*	90	Accept & Route to Monitoring Device
4 (308)	UDP	150.*	*	*	3030	Accept
5 (310)	*	*	*	*	*	Deny

FIG. 3

Fig 1: Fig. 3 of the opposed patent.

According to feature 1.2.2, at least one of the plurality of packet transformation functions corresponds to a “*packet digest logging function*”. The packet digest logging function provides a network communications awareness service.

A network communications awareness service could be a service that collects information about communication based on IP packets. This information may be of interest to an organization maintaining the network (opposed patent, paragraph [0041]). The network communications awareness service is at least provided if the method steps in accordance with features 1.2.3 through 1.2.6 are carried out.

f. Features 1.2.3 through 1.2.5

1.2.3 *identifying a subset of information specified by a packet matching the packet matching criterion of a packet filtering rule that specified the packet digest logging function;*

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*

According to feature 1.2.3, a subset of information specified by a packet matching the packet matching criterion of a packet filtering rule that specified the packet digest logging function is identified.

According to feature 1.2.4, the packet digest logging function further comprises generating a record comprising the subset of information specified by the packet. For example, if a destination address is specified as the subset, the generated record includes this destination address.

According to feature 1.2.5, the packet digest logging function further comprises reformatting the subset of information specified by the packet in accordance with a logging system standard. As an example of a logging standard, the opposed patent discloses the syslog standard (opposed patent, paragraph [0073]).

g. 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;*

According to feature 1.2.6, the packet digest logging function comprises routing the packet to a monitoring device configured to store the packet for subsequent analysis.

h. Features 1.3 and 1.3.1

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 up-dated malicious traffic information received from the malicious host tracker service; and*

According to feature 1.3 the packet security gateway receives an updated second set of packet filtering rules for the dynamic security policy from the security policy management server.

The second set of packet filtering rules is further specified by feature 1.3.1. It includes an update to the first set of packet filtering rules.

i. Feature 1.4

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

According to feature 1.4, the packet security gateway carries out packet filtering on a second portion of the packets, on a packet-by-packet basis, associated with the network protected by the packet security gateway. Thus, packet filtering is based on the (updated) second set of packet filtering rules.

E. Added-matter (Articles 100 c), 123(2), and 76(1) EPC)

The opposition filed by Ixia correctly identifies numerous added-matter issues of the claims as granted. Furthermore, the intervenor submits the following:

In order to conveniently assess the added-matter objections raised, intervenor submits the following markup-up version of claim 1 as granted for the opposed patent and claim 1 as filed with the parent application (document D6). As is evident from the comparison below, claim 1 was drafted essentially completely from scratch with the filing of the divisional application underlying the opposed patent. Since system claim 14 and computer program claim 15 refer back to claim 1, these claims also comprise added-matter for at least the reasons discussed with regard to claim 1.

Claim amendments over parent application (insertions underlined, deletions ~~crossed-out~~):

- 1** *A method, comprising:*
 - 1.1** *receiving, by ~~each of a plurality of a~~ packet security gateways (112) configured for protection of a network and associated with a security policy management server external from the network, a dynamic security policy comprising that includes*
 - ~~at least one rule specifying application-layer packet-header information and a packet transformation function to be performed on packets comprising the application-layer packet-header information;~~*
 - 1.1.1** *a first set of packet filtering rules from the security policy management server,*
 - 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, and*

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;

~~receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;~~

1.2 performing, by the packet security gateway and on a packet-by-packet basis, packet filtering on a first portion of packets associated with the network protected by the packet security gateway based on the first set of packet filtering rules by performing

~~performing, by the packet security gateway and on a packet-by-packet basis, the packet transformation function on each of the one or more packets comprising the application layer packet header information³~~

1.2.1 at least one of multiple packet transformation functions specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets,

1.2.2 wherein at least one of the multiple packet transformation functions specified by the at least one packet filtering rule of the first set of packet filtering rules corresponds to a packet digest logging function that provides a network communications awareness service and comprises:

1.2.3 identifying by the packet security gateway, from amongst the packets associated with the network protected by the packet security gateway, and on a packet-by-packet basis, one or more packets comprising the application layer packet header information; and a subset of information specified by a packet matching the packet matching

³ Feature moved up for ease of comparison.

criterion of a packet filtering rule that specified the packet digest logging function;

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;

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 up-dated malicious traffic information received from the malicious host tracker service; and

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

The subject-matter extends beyond the content of the parent application at least for the following reasons:

1. 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 not disclosed

Claim 1 as granted requires that for “a packet matching the packet matching criterion of a packet filtering rule”:

- a record comprising a subset of information is generated and reformatted according to a logging system standard (features 1.2.3 and 1.2.5) and
- the packet is routed to a monitoring device (feature 1.2.6).

The application documents of the parent application as filed (document D6) do not disclose a single embodiment that concerns these two features, let alone that discloses the combination of these features for the same packet.

The generation and reformatting of a record are disclosed in claims 15 and 16 and par. [86] of D6. These embodiments do not relate to routing a packet to a monitoring device at all. A routing to a monitoring device is only disclosed in different embodiments, for example in pars. [45], [53], [68] to [71].

The disclosure of the parent application as filed distinguishes strictly between embodiments concerning a record comprising a subset of information and the routing of the complete packet to a monitoring device. This also makes technical sense. The skilled person understands that these are two different scenarios:

- One scenario in which only a subset of information is required. Hence a record comprising this subset of information is generated (and reformatted).

- A different scenario applies to the case where the whole packet needs to be stored, for example for law enforcement purposes (D6, pars. [53], [66], [70]). This scenario has the disadvantage – according to the proprietor – of reduced memory efficiency.

No scenario is disclosed wherein a technical need exists for both a record of a subset of information specified by the packet and the complete packet itself. Therefore, there is no direct and unambiguous disclosure of the combination of these two distinct embodiments.

The proprietor has not provided any arguments at all why such a combination would (allegedly) be disclosed:

Basis

Basis for claim 1 can be found in at least paragraphs [17], [37]-[38], [44]-[46], [54], [64]-[65], [80], [84] and [87] of the parent application as filed.

(Brief of proprietor, dated April 24, 2019).

The same applies to the proprietor's brief dated April 3, 2020, which does not contain any explanations either.

Thus, different embodiments have been combined to artificially create a new embodiment in violation of Article 76(1) EPC (Case Law of the Boards of Appeal, II-E, 1.6.1).

2. No disclosure that routing (feature 1.2.6) to a monitoring device is part of the “*packet digest logging function*” (feature 1.2.2)

Claim 1 as granted requires that

1.2.2 *wherein at least one of the multiple packet transformation functions specified by the at least one packet filtering rule of the first set of packet filtering rules corresponds to a **packet digest logging function** that provides a network communications awareness service and **comprises**:*

1.2.3 *identifying a subset of information [...]*

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

1.2.5 *reformatting the subset of information [...]*

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

- a. First of all, the documents as filed with the parent application (document D6) do not disclose anywhere that at least one of the plurality of packet transformation functions corresponds to a “*packet digest logging function*” (feature 1.2.2). Claim 10 as filed with the parent application (document D6) instead relates to a “*packet transformation function comprising a packet digest logging function*” (the same applies to D6, par. [84]).
- b. Even more, the parent application does also not disclose that routing of the packet to a monitoring device is comprised in the packet digest logging function as required by claim 1 as granted. On the contrary, the packet digest logging function – already by virtue of its name – generates a “*digest*” of the packet, i.e., a record comprising a subset of information, suitable for “*logging*”. The description of the parent application distinguishes strictly between the generation of a “*digest*” (see claims 15 and 16, and pars. [54] and [86] of D6) and the routing of the entire packet to a monitoring device (see pars. [45], [53], [68] to [71]).
- c. Therefore, the subject-matter of claims 1, 14, and 15 violates Article 76(1) EPC.

3. **No disclosure of a subset of information “*specified by the packet*” (feature 1.2.4)**

Feature 1.2.4 of claim 1 as granted requires generating a record comprising the subset of information “*specified by the packet*”.

This is not originally disclosed since the parent application as filed discloses throughout that the subset of information is specified by the packet digest logging function and not by the packet itself, see for example:

“identifying a subset of information specified by the packet digest logging function for each of the one or more packets corresponding to the packet-identification criteria; and generating, for each of the one or more packets corresponding to the packet identification criteria, a record comprising the subset of information specified by the packet digest logging function.” (D6, claim 11 as filed, emphasis added)

The same applies, for example, to claims 13 to 16 and par. [0086] of the description of the parent application (document D6).

There is no disclosure in the parent application that the subset is specified by the packet rather than the packet digest logging function.

Thus, claims 1, 14, and 15 extend beyond the parent application as filed in violation of Article 76(1) EPC.

4. **No disclosure of “*performing ... packet filtering ... by performing... one ... packet transformation functions*” (features 1.2 to 1.2.2)**

The claim comprises the awkward, and apparently tautological, amendment “*performing ... by performing*”, in features 1.2 to 1.2.2:

*“**performing**, by the packet security gateway and on a packet-by-packet basis, packet filtering on a first portion of packets associated with the network protected by the packet security gateway based*

on the first set of packet filtering rules **by performing**

at least one of multiple packet transformation functions [...]

wherein at least one of the multiple packet transformation functions specified by the at least one packet filtering rule of the first set of packet filtering rules corresponds to a packet digest logging function [...] that comprises

Thus, the claim requires that packet filtering is performed at least partly by performing a packet digest logging function. This is not disclosed anywhere in the application documents of the parent application.

The term “packet filtering” is disclosed only in the context of a packet transformation function that performs operations such as forwarding or dropping of packets, see for example par. [41] of document D6:

“For example, packet transformation functions 1 – N 216, 218, and 220 may be configured to forward packets received from packet filter 214 into network A 102, forward packets received from packet filter 214 to an IPsec stack having an IPsec security association corresponding to the packets, or drop packets received from packet filter 214. In some embodiments, one or more of packet transformation functions 1 – N 216, 218, and 220 may be configured to drop packets by sending the packets to a local “infinite sink” (e.g., the /dev/null device file in a UNIX/LINUX system).”

This also makes technical sense since a mere logging of packets by the packet digest logging function does not effect any filtering to protect a network from malicious network traffic and to prevent malicious network traffic from leaving network (c.f. D6, par. [43], see also spoofing protection in par. [74]).

The performance of a “packet digest logging function” is not disclosed at all in the context of a packet filtering. For instance, claims 10, 11, and 13 to 16 of D6, which concern a packet digest logging function, do not relate to packet filtering. The same applies to Fig. 12 and the corresponding paragraphs [84] to [86] as well as paragraph [54]. No other passage of the

parent application as filed (document D6) discloses a “*packet digest logging function*”.

It is settled case law that the content of an application must not be considered to be a reservoir from which features pertaining to separate embodiments of the application could be combined in order to artificially create a particular embodiment (Case Law of the Boards of Appeal, II-E, 1.6.1).

The performance of packet filtering by performing a packet digest logging function is not directly and unambiguously disclosed in the parent application as filed.

Thus, the claims as granted violate Article 76(1) EPC.

5. **Automatic creation or alteration of rules is not disclosed in combination with packet digest logging function (features 1.1.3, 1.2, and 1.2.2)**

Feature 1.1.3 requires

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;*

According to granted claim 1, rules are used by the packet digest logging function for generating the record and routing the packet to a monitoring device:

1.2.2 *wherein at least one of the multiple packet transformation functions specified by **the at least one packet filtering rule** of the first set of packet filtering rules **corresponds to a packet digest logging function** [...]*

There is no teaching in the parent application that automatically created or altered rules are used for generating the record and routing the packet:

- a. The sole disclosure of an **automatic** creation or alteration of rules is found in par. [64] of D6. This paragraph does not relate at all to a packet digest logging function. Instead, par. [64] discloses that “rules” are automatically created or altered “*as new network addresses associated with malicious network traffic are determined*”, to block this malicious 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. [...] 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.**”*

Therefore, the automatic creation or alteration of rules as now claimed violates Article 76(1) EPC in at least two regards:

Firstly, there was no disclosure that any automatically created or altered rule is used for generating the record (D6, claims 15 and 16 and par. [86]), let alone for routing (D6, pars. [45], [53], [68] to [71]) the packet to a monitoring device. This combination, however, is now claimed. Thus, the proprietor has, once more, impermissibly used the original application as a reservoir to artificially define a particular, undisclosed embodiment (Case Law of the Boards of Appeal, II-E, 1.6.1).

Secondly, par. [64] does not relate to a general update of the rules but instead to a specific update of network addresses. This feature was in par. [64] disclosed as related to the automatic creation or alteration, and its omission is not permitted either (Guidelines for Examination, H-V 3.2.1).

- b. Moreover, even the broadest disclosure on creation and alteration of rules, i.e., including any non-automatic creation and alteration, does not provide

for any link to the packet digest logging function comprising the claimed generation of the record and routing.

The passages dealing with creation or alteration of rules are found in pars. [49], [64], [65], and [87]. None of these paragraphs relates to generating the record (which is referred to in D6 in claims 15 and 16 and par. [86]) or routing the packet to a monitoring device (which is referred to in D6 in pars. [45], [53], [68] to [71]). In particular par. [86] concerns the embodiment of Fig. 12 (concerning a packet digest logging function) while par. [87] concerns the embodiment of Fig. 13 (concerning security updates), without any disclosure how to link the respective teachings.

- c. In summary, the parent application as filed does not disclose the combination of an any creation or alteration, let alone an automatic creation or alteration, of rules (feature 1.1.3), the generation of a record (features 1.2.4 and 1.2.5) and the routing (feature 1.2.6) of the packet to a monitoring device.

Thus, claims 1, 14, and 15 as granted violated Article 76(1) EPC.

F. Lack of novelty (Articles 100 a), 54 EPC)

The subject-matter of the independent claim of the opposed patent is anticipated by each of two manuals, Sourcefire manual version 5.1.1 (document D23, section 1. below), as well as Sourcefire manual version 4.10 (document D19, section 2. below):

1. Lack of novelty over the Sourcefire manual version 5.1.1 (document D23)

D23 discloses a network security system comprising packet filtering based on an access control policy. Part of the access control policy are packet filtering rules that are updated automatically based on “*Security Intelligence Feeds*” (D23, pages 141 ff.). In particular, D23 discloses that a Sourcefire Intelligence Feed may be used to provide an updated list of malicious IP addresses:

Working with the Sourcefire Intelligence Feed

LICENSE: Any

To help you build blacklists, Sourcefire provides the Sourcefire Intelligence Feed, which is comprised of several regularly updated lists of IP addresses determined by the VRT to have a poor reputation. Each list in the feed represents a specific category: open relays, known attackers, bogus IP addresses (bogon), and so on. In an access control policy, you can blacklist any or all of the categories.

Because the intelligence feed is regularly updated, the system can use up-to-date information to filter your network traffic. Malicious IP addresses that represent security threats such as malware, spam, botnets, and phishing may appear and disappear faster than you can update and apply new policies.

Although you cannot delete the Sourcefire Intelligence Feed, editing it allows you to change the frequency of its updates. By default, the feed updates every two hours.

(D23, page 146, emphasis added).

D23 also discloses that it is possible to use third-party Security Intelligence Feeds:

Working with Custom Security Intelligence Feeds

LICENSE: Any

Custom or third-party Security Intelligence feeds allow you to augment the Sourcefire Intelligence Feed with other regularly-updated reputable whitelists and blacklists on the internet. You can also set up an internal feed, which is useful if you want to update multiple Defense Centers in your deployment using one source list.

(D23, page 147, emphasis added).

Document D23, which was publicly made available prior to the opposed patent's priority date (section **a.** below), discloses all features of the independent claims (section **b.** below):

a. Public availability of document D23

- aa.** The Sourcefire manual in version 5.1.1 (document D23) bears the timestamp "2012-Oct-30 15:41" (D23, page 2, bottom left), i.e., about 18 months before the priority date of the opposed patent. It was prepared as a part of practices and procedures for preparing and delivering product documentation at Sourcefire.

According to the practices and procedures at Sourcefire Inc., it was required that after the content of documentation had been approved, the corresponding document was to be saved as a PDF file that was provided with security settings to prevent future modifications to the document. Moreover, the protected document was copied to a specific folder that included the completed documents. The completed documents were then made available to the production department and to the support department for distribution. On this basis, the production department created a documentation CD-ROM or DVD and enclosed this with every Sourcefire 3D System appliance purchased by a customer. Moreover, the support department posted the completed documents to a support website for customers.

The above reflected process is evidenced for version 5.1.1 of the Sourcefire manual by an affidavit of Ms. Sarah Ehrig (document D24). Therein Ms. Ehrig confirms:

5. Based on the foregoing procedure, I can confirm that the electronic document bearing the title "*Sourcefire 3D System/User Guide/Version 5.1.1*" on its page 1 and having the timestamp "*2012-Oct-30 15:41*" on its page 2 was made available to customers of SF before March 12, 2013. The document was created in 2012 as a part of the described practices and

(D24, item 5).

The date March 12, 2013, refers to the priority date of EP 2 974 212 B1, since the declaration was prepared for an opposition against EP 2 974 212 B1. This date (March 12, 2013) is even earlier than the priority date (April 16, 2014) of the instant opposed patent.

In addition,

Evidence: Testimony of Ms. Sarah Ehrig,

pursuant to Article 117(1) EPC is offered.

- bb.** The creation of the Sourcefire manual version 5.1.1 in 2012 as well as its security settings, including protection from modifying, follow also from document properties which can be displayed with the software "*Acrobat Reader*":

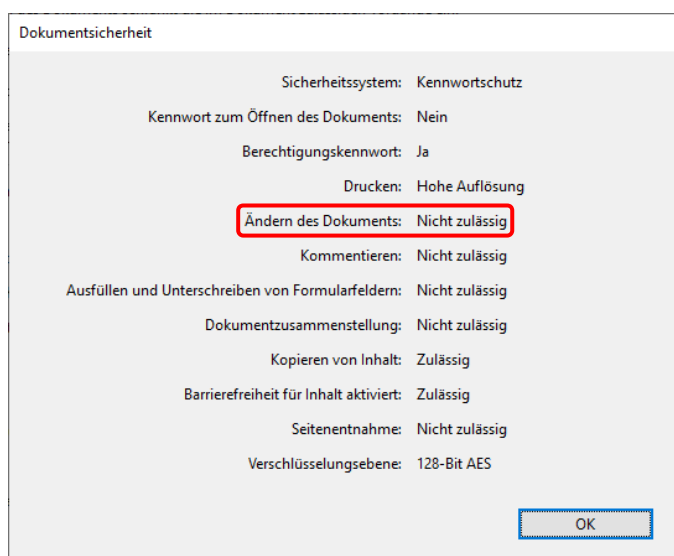
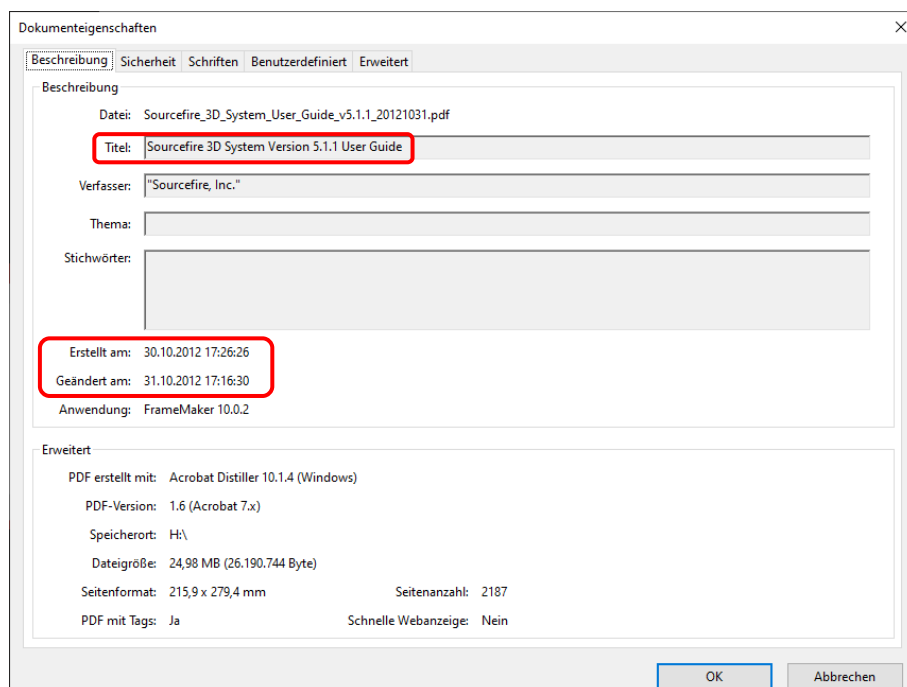


Fig. 2: Screenshots of document properties of D23 (red frames added).

In addition,

Evidence: Submission of original of D23 in pdf-format

pursuant to Article 117(1) EPC is offered.

- cc. D23 was provided to customers without any obligation for secrecy such as a non-disclosure agreement. D23 discloses that it may be distributed (provided that certain conditions are met):

Terms of Use Applicable to the User Documentation

The legal notices, disclaimers, terms of use, and other information contained herein (the "terms") apply only to the information discussed in this documentation (the "Documentation") and your use of it. These terms do not apply to or govern the use of websites controlled by Sourcefire, Inc. or its subsidiaries (collectively, "Sourcefire") or any Sourcefire-provided products. Sourcefire products are available for purchase and subject to a separate license agreement and/or terms of use containing very different terms and conditions.

Terms of Use and Copyright and Trademark Notices

The copyright in the Documentation is owned by Sourcefire and is protected by copyright and other intellectual property laws of the United States and other countries. You may use print out, save on a retrieval system, and otherwise copy and distribute the Documentation solely for non-commercial use, provided that you (i) do not modify the Documentation in any way and (ii) always include Sourcefire's copyright, trademark, and other proprietary notices, as well as a link to, or print out of, the full contents of this page and its terms.

(D23, page 2, annotations added).

- dd. Prior to the priority date of the opposed patent (April 16, 2014), Sourcefire 3D System appliances were purchased and obtained by more than 1000 customers (each of which being a large government entity or company). In accordance with the procedures explained in section 1.a. above, a documentation disc was included in the packaging with each purchased appliance. In particular, the User Guide Version 5.1.1 (document D23) was shipped to at least some customers before the priority date of the opposed patent as it was common practice to ship the latest version of the system and User Guide after it became available.

The above reflected purchases are evidenced by the declaration of Mr. Jacob H. Baugher III according to document D21.

In addition,

Evidence: Testimony of Mr. Jacob Baugher III,

under Article 117(1) EPC is offered.

Mr. Baugher is an employee of an affiliate corporation of the intervenor and was previously employed by Sourcefire, Inc. Mr. Baugher has personal knowledge of previous products and offers relating to network security systems, including the Sourcefire 3D system, as well as of practices and procedures for recording and retrieving data for the sale of such products and offers.

- ee.** Finally, in the co-pending opposition proceedings against EP 2 974 212 B1 (application number 14 719 415.3), the opposition division found in its preliminary opinion dated December 13, 2021 that the Sourcefire manual in version 5.1.1 (there: document D10) was publicly available at the priority date of EP 2 974 212 B1, which is even earlier than the priority date of the instant opposed patent (namely March 12, 2013):

10.5 It appears to be common ground between the parties that D10 was publicly available at the priority date of the application and that it discloses features 1.1, 1.2, 1.3 and 1.6 of claim 1 and, correspondingly, features 11.1, 11.2, 11.3 and 11.6 of claim 11. The opposition division sees no reason to diverge from this.

b. The claimed subject-matter is not novel over D23

aa. Features 1 to 1.1.2

1 *A method, comprising:*

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

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

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, and

- (i) The security policy management server of the Sourcefire system is called “Sourcefire Defense Center”, or “Defense Center”, in version 5.1.1 of the Sourcefire manual (document D23):

Sourcefire Defense Center

The Sourcefire Defense Center® provides a centralized management console and event database for the Sourcefire 3D System. The Defense Center aggregates and correlates intrusion, discovery, connection, and performance data, allowing you to monitor the information that your devices are reporting in relation to one another, and to assess and control the overall activity occurring on your network.

(D23, page 36, emphasis added).

The packet security gateways of the Sourcefire system are generally referred to as “*managed devices*”:

Managed Devices

Sourcefire 3D appliances, generally referred to as managed devices, are fault-tolerant, purpose-built appliances available in a range of throughputs. You can deploy these devices passively to gain insight into the users on your network and applications they use. If you deploy these devices inline, you can also block traffic based on multiple criteria, including user activity, application use, and URL requests.

(D23, page 37, emphasis added).

- (ii) Document D23 discloses that the managed devices receive an access control policy (= “*dynamic security policy*”, feature 1.1; regarding “*dynamic*”, see below) from their associated Defense Center, as is also indicated with the solid black arrow in the illustration below (which was not added by the intervenor) and the paragraph above the illustration (“*transmitted between a Sourcefire Defense Center and its managed devices*”):

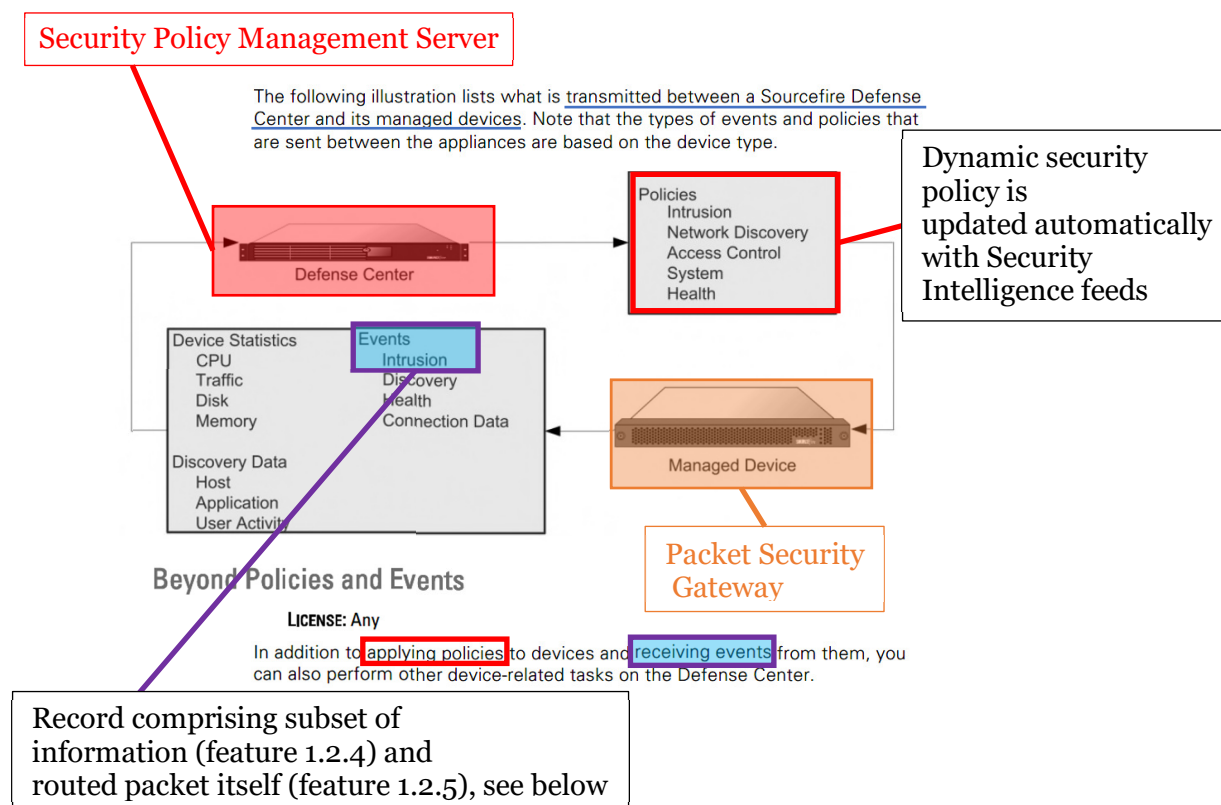


Fig. 3: D23, page 163, annotations added.

D23 also discloses that the managed devices are associated with a Defense Center located externally from the network protected by a managed device. In an example disclosed by D23, the Defense Center is located in a Home Office, and there are remote sites (New York Office, Miami Office) protected by associated managed devices:

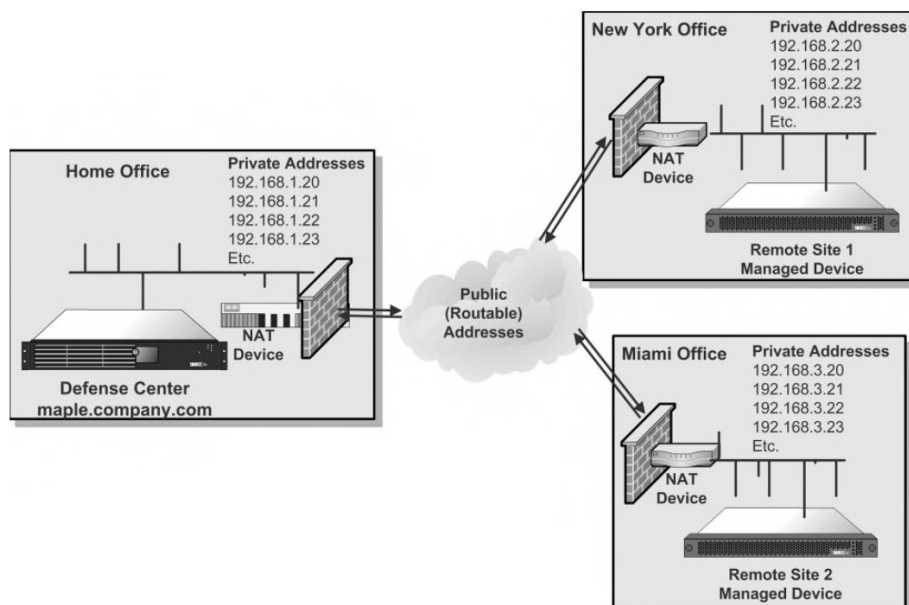


Fig. 4: D23, page 165.

- (iii) D23 furthermore discloses that the received access control policy comprises “access control rules” as well as “Security Intelligence” (= “a first set of packet filtering rules”).

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.

(D23, page 2131).

Both “access control rules” as well as the “Security Intelligence” – here: the “Security Intelligence Feed”, which forms part of the “Security Intelligence” (see above, section F.1) – specify at least one packet matching criterion. For the access control rules, several examples are given, such as IP addresses or ports; the “Security Intelligence Feed” is specifically tailored to provide a “dynamic collection of IP addresses” (emphasis added), which may comprise whitelist or blacklists (see also above, D23, page 147). Thus, D23 discloses that the first set of packet filtering rules is part of a “dynamic

security policy” and each packet filtering rule of the set comprises “*at least one packet matching criterion specified by one or more packet filtering rules*”:

access control rule

A set of conditions the Sourcefire 3D System uses to examine your monitored network traffic and which allows you to achieve granular access control. Access control rules, which populate an access control policy, may perform simple IP address matching, or may characterize complex connections involving different users, applications, ports, and URLs. The access control rule action determines how the system handles traffic that meets the rule’s conditions. Other rule settings determine how (and whether) the connection is logged, and whether an intrusion policy or file policy inspects matching traffic.

Security Intelligence feed

One of the types of Security Intelligence objects, a dynamic collection of IP addresses that the system downloads on a regular basis, at an interval you configure. Because feeds are regularly updated, using them ensures that the system uses up-to-date information to filter your network traffic using the Security Intelligence feature. See also Sourcefire Intelligence Feed.

(D23, pages 2131 and 2152, emphasis added).

(iv) Thus, D23 discloses features 1 to 1.1.2.

bb. 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;*

D23 discloses that the Defense Center (= “*security policy management server*”) downloads (= “*receives*”) a Security Intelligence Feed, which is – as shown above – a dynamic collection of IP addresses. This collection of IP addresses forms “*malicious traffic information*”, and is received from a HTTP or HTTPS server, representing a “*malicious host tracker service*”.

Moreover, D23 explicitly discloses that this feed is used by the Defense Center “*to automatically update its managed devices*” (= packet security gateways):

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.

(D23, page 142, emphasis added).

One example for a Security Intelligence Feed is the Sourcefire Intelligence Feed provided by the Sourcefire VRT (Vulnerability Research Team). According to another example of D23, it is also possible to configure third-party feeds to “*augment the Sourcefire Intelligence Feed with other regularly-updated reputable whitelists and blacklists on the internet*”. According to the disclosure of D23, this leads to the Defense Center downloading the entire feed and to “*automatically update its managed devices*”:

Working with Custom Security Intelligence Feeds

LICENSE: Any

Custom or third-party Security Intelligence feeds allow you to augment the Sourcefire Intelligence Feed with other regularly-updated reputable whitelists and blacklists on the internet. You can also set up an internal feed, which is useful if you want to update multiple Defense Centers in your deployment using one source list.

When you configure a feed, you specify its location using a URL; the URL cannot be Punycode-encoded. By default, the Defense Center downloads the entire feed source on the interval you configure, then automatically updates its managed devices.

(D23, page 147, emphasis added).

In one example, a feed concerns a so-called Zeus⁴ blacklist:

Managing Feeds and Lists

You create and manage Security Intelligence lists and feeds, collectively called Security Intelligence objects, using the object manager's Security Intelligence page. (For information on creating and managing network objects and groups, see Working with Network Objects on page 140.)

Update Feeds Add Security Intelligence Filter		
Name	Type	
Global Blacklist	List	 
Global Whitelist	List	 
MyCompany Whitelist <i>Last Updated: 2012-05-17 07:21:53</i>	List	 
Sourcefire Intelligence Feed <i>Last Updated: 2012-05-17 06:58:22</i>	Feed	 
Zeus Blacklist <i>Last Updated: 2012-05-17 07:48:05</i>	Feed	 

(D23, page 143, emphasis added).

Consequently, D23 discloses that one or more of the first packet filtering rules on the packet security gateway (= managed device) were “*automatically created or altered by the security policy management server*” (= Defense Center), based on malicious traffic information received from a malicious host tracker service (= Zeus Blacklist).

Therefore, at least if one follows the understanding of an automatic creation as expressed by the Proprietor in the parallel infringement proceedings as encompassing subscription-based updates (see D3, margin no. 65), D23 discloses feature 1.1.3.

cc. Feature group 1.2

- 1.2** *performing, by the packet security gateway and on a packet-by-packet basis, packet filtering on a first portion of packets associated with the network protected by the packet*

⁴ Zeus, ZeuS, or Zbot is a Trojan horse malware package that runs on versions of Microsoft Windows; [https://en.wikipedia.org/wiki/Zeus_\(malware\)](https://en.wikipedia.org/wiki/Zeus_(malware)); last accessed on May 9, 2022.

security gateway based on the first set of packet filtering rules by performing

1.2.1 *at least one of multiple packet transformation functions specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets,*

1.2.2 *wherein at least one of the multiple packet transformation functions specified by the at least one packet filtering rule of the first set of packet filtering rules corresponds to a packet digest logging function that provides a network communications awareness service and comprises:*

1.2.3 *identifying a subset of information specified by a packet matching the packet matching criterion of a packet filtering rule that specified the packet digest logging function;*

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;*

(i) Features 1.2, 1.2.1

First of all, D23 discloses that the managed devices perform, on a packet-by-packet basis, packet filtering based on packets associated with the protected network by performing a packet transformation function, specified by the rules of the first set of packet filtering rules (features 1.2 and 1.2.1).

For example, D23 discloses that the managed devices use the blacklists obtained as part of the “*Security Intelligence*”, such as the Sourcefire

Intelligence Feed or third-party Security Intelligence Feeds, i.e., a (dynamic) collection of IP addresses, to “*filter your network traffic*”. Thus, packets from or to a blacklisted IP address are blocked (= “*at least one of multiple packet transformation functions specified by at least one packet filtering rule*”):

Because the intelligence feed is regularly updated, the system can use up-to-date information to filter your network traffic. Malicious IP addresses that represent security threats such as malware, spam, botnets, and phishing may appear and disappear faster than you can update and apply new policies.

(D23, pages 146, emphasis added).

In addition, D23 also discloses packet filtering, by the managed devices, on a packet-by-packet basis, based on packets associated with the protected network, by the access control rules. The received access control rules specify an action, such as “*block*” or “*allow*”, or an action, where matching traffic is inspected by an intrusion policy. These actions form, in the words of the claim, “*at least one of multiple packet transformation functions specified by at least one packet filtering rule*”.

Access Control

Access control is a policy-based feature that allows you to specify, inspect, and log the traffic that can enter your network, exit it, or travel within it. An access control policy determines how the system handles traffic on your network. You can use a policy that does not include access control rules to handle traffic in one of the following ways, using what is called the default action:

- block all traffic from entering your network
- trust all traffic to enter your network without further inspection
- allow all traffic to enter your network, and inspect the traffic with a network discovery policy only
- allow all traffic to enter your network, and inspect the traffic with intrusion and network discovery policies

You can include access control rules in an access control policy to further define how traffic is handled by targeted devices, from simple IP address matching to complex scenarios involving different users, applications, ports, and URLs. For each rule, you specify a rule action, that is, whether to trust, monitor, block, or inspect matching traffic with an intrusion or file policy.

For each access control policy, you can create a custom HTML page that users see when the system blocks their HTTP requests. Optionally, you can display a page that warns users, but also allows them to click a button to continue to the originally requested site.

As part of access control, the Security Intelligence feature allows you to blacklist — deny traffic to and from — specific IP addresses, before the traffic is subjected to analysis by access control rules.

Access control includes intrusion detection and prevention, file control, and malware detection. For more information, see the next sections.

(D23, pages 38 and 39, emphasis added).

Consequently, features 1.2 and 1.2.1 are disclosed by D23.

(ii) Feature 1.2.2

Moreover, D23 discloses that at least one of the multiple packet transformation functions specified by the at least one packet filtering rule of the first set of packet filtering rules corresponds to a packet digest logging function that provides a network communications awareness service (feature 1.2.2).

In particular, D23 discloses that an intrusion policy is associated with an access control rule (= “at least one packet filtering rule”). The intrusion policy is used “to inspect matching traffic”:



Access Control

Access control is a policy-based feature that allows you to specify, inspect, and log the traffic that can enter your network, exit it, or travel within it. An access control policy determines how the system handles traffic on your network. You can use a policy that does not include access control rules to handle traffic in one of the following ways, using what is called the default action:

- block all traffic from entering your network
- trust all traffic to enter your network without further inspection
- allow all traffic to enter your network, and inspect the traffic with a network discovery policy only
- allow all traffic to enter your network, and inspect the traffic with intrusion and network discovery policies

You can include access control rules in an access control policy to further define how traffic is handled by targeted devices, from simple IP address matching to complex scenarios involving different users, applications, ports, and URLs. For each rule, you specify a rule action, that is, whether to trust, monitor, block, or inspect matching traffic with an intrusion or file policy.

(D23, pages 38 and 39, emphasis added).

Correspondingly, the section on “*Intrusion Detection and Prevention*” of D23 discloses that matching traffic, i.e., traffic matching an access control rule, is analyzed with an intrusion policy:

Intrusion Detection and Prevention

Intrusion detection and prevention allows you to monitor your network traffic for security violations and, in inline deployments, the ability to block or alter malicious traffic.

Intrusion prevention is integrated into access control, where you can associate an intrusion policy with specific access control rules. If network traffic meets the conditions in a rule, you can analyze the matching traffic with an intrusion policy. You can also associate an intrusion policy with the default action of an access control policy.

An intrusion policy contains a variety of components, including intrusion rules that inspect the protocol header values, payload content, and certain packet size characteristics; variables commonly used in intrusion rules; a FireSIGHT 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.

(D23, page 39, emphasis added).

When based on the access control rule matching traffic is identified, an intrusion policy is triggered, i.e., “*it generates an intrusion event*”. For packet-based events, a copy of the event is recorded:

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.

(D23, page 469, emphasis added).

Thus, the intrusion policy, including the intrusion rules of D23, correspond to a packet digest logging function according to feature 1.2.2. Thus, feature 1.2.2 is also disclosed.

(iii) Features 1.2.3 to 1.2.6

Moreover, the intrusion policy, including the intrusion rules of D23, also fulfill the teaching of features 1.2.3 to 1.2.6:

As already mentioned, for packet-based events, a copy of the event is recorded (feature 1.2.4: “*generating a record*”). The record comprises a subset of information (feature 1.2.3: “*identifying a subset*”) which is re-formatted (feature 1.2.5), for example in syslog format:

The Sourcefire 3D System also provides you with the tools you need to review intrusion events and evaluate whether they are important in the context of your network environment and your security policies. These tools include:

[...]

- automated alerting that you can configure for SNMP, email, and syslog

(D23, pages 469 bottom to 470 top, emphasis added).

The description of the opposed patent identifies the syslog standard as an example of how the subset of information is reformatted (opposed patent, pars. [0041], [0073]).

Moreover, intrusion events can be inspected (D23, pages 478 ff.) and include in particular the re-formatted subset of information:

Viewing Intrusion Events

LICENSE: Protection

When the system recognizes a packet that is potentially malicious, it generates an intrusion event and adds the event to the database.

The packet view includes information about the intrusion event that the packet triggered, including the event's time stamp, message, classification, priority, and, if the event was generated by a standard text rule, the rule that generated the event. The packet view also provides general information about the packet, such as its size.

(D23, pages 478 to 479, emphasis added).

For example, the “subset of information specified by the packet” (feature 1.2.3) comprises the source and destination IP address (D23, page 481). Some exemplary “subsets of information” are shown in the table view on page 489, that include the source and destination IP address of the packet:

The initial *table* view of intrusion events lists each intrusion event in its own row. The columns in the table list information such as the time, the source IP address and port, the destination IP address and port, the event priority, the event message, and more. Note that several of the columns were removed from the table view to simplify the following graphic.

	Time	Priority	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Message	Count
	2011-09-27 15:13:34	high	10.10.10.3	10.10.10.2	46485/tcp	80 (http/tcp)	ORACLE http Server mod_access restriction bypass attempt (1:15956)	1
	2011-09-27 15:13:34	high	10.10.10.3	10.10.10.2	45479/tcp	80 (http/tcp)	ORACLE http Server mod_access restriction bypass attempt (1:15956)	1
	2011-09-27 14:49:33	high	10.10.10.3	10.10.10.2	42595/tcp	80 (http/tcp)	ORACLE http Server mod_access restriction bypass attempt (1:15956)	1

Displaying rows 1-25 of 348 rows << Page 1 of 14 >>

View

Copy

Delete

Review

Download Packets

View All

Copy All

Delete All

Review All

Download All Packets

(D23, page 490, annotations added).

A detailed list of the information logged and re-formatted in an intrusion event is given on pages 480 ff. of D23.

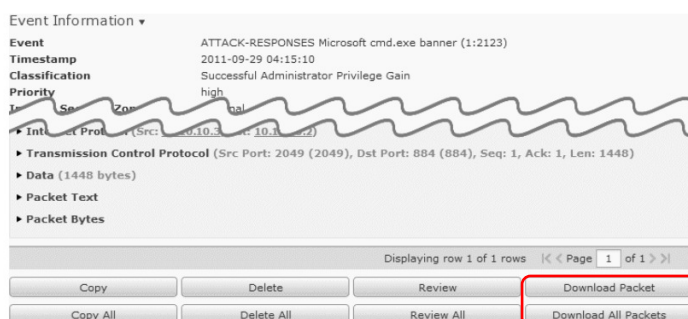
Finally, D23 also discloses that the intrusion event, including the packet, is transmitted (= "routed", feature 1.2.6) to the Defense Center. An exemplary "packet view" on a Defense Center is shown on page 498 (emphasis added):

Using the Packet View

LICENSE: Protection

A packet view provides information about the packet that triggered the rule that generated an intrusion event.

TIP! The packet view on a Defense Center does not contain packet information when the Transfer Packet option is disabled for the device detecting the event.



The packet view indicates why a specific packet was captured by providing information about the intrusion event that the packet triggered, including the event's time stamp, message, classification, priority, and, if the event was generated by a standard text rule, the rule that generated the event. The packet view also provides general information about the packet, such as its size.

Defense Center is configured to store the packet for subsequent inspection = monitoring device (feature 1.2.6)

As is clear from the citation above and from page 469 (*"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."*), the packet is routed to the Defense Center, which is configured for storing the packet and thus represents a monitoring device.

Consequently, D23 therefore also discloses features 1.2.2 to 1.2.6, and thus the entire feature group 1.2.

dd. Feature groups 1.3 and 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 up-dated malicious traffic information received from the malicious host tracker service; and*

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

Feature groups 1.3 and 1.4 concern the receipt of an updated second set of packet filtering rules and performing packet filtering based on the updated second set of packet filtering rules.

D23 discloses that the update effected by the Security Intelligence feed “takes effect” after “a few minutes”, which the skilled person will understand to mean that packet filtering is performed for a second portion of the packets (i.e. those packets received after “a few minutes”) based on the updated second set of packet filtering rules:

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.

(D23, page 142, emphasis added).

The same is also evident from the definition of a Security Intelligence feed provided in the Glossary:

Security Intelligence feed

One of the types of Security Intelligence objects, a dynamic collection of IP addresses that the system downloads on a regular basis, at an interval you configure. Because feeds are regularly updated, using them ensures that the system uses up-to-date information to filter your network traffic using the Security Intelligence feature. See also Sourcefire Intelligence Feed.

(D23, page 2152).

Thus, D23 explicitly discloses that after the update the Sourcefire system continues to perform the packet filtering function based on the update. As shown above, the packet filtering disclosed by D23 comprises the steps of feature group 1.2 and therefore also the steps of feature group 1.4.

Thus, D23 discloses feature groups 1.3 and 1.4 as well.

ee. Result

The claimed subject-matter is therefore not novel in view of D23.

2. Lack of novelty over the Sourcefire manual version 4.10 (document D19)

a. Public availability of document D19

- aa.** Document D19 is time-stamped “2011-Mar-16 14:59”, which is more than three years before the priority date of the opposed patent in April 2014. It was also made factually available to the public before the priority date, as we explained in detail above.

In addition,

Evidence: Submission of original of D19 in pdf-format

pursuant to Article 117(1) EPC is offered.

The electronic document D19 was created in 2011 as part of the practices and procedures for creating and providing product documentation for Sourcefire, Inc. (including product documentation for the Sourcefire 3D System, to which D19 relates).

Upon its creation, the Sourcefire manual version 4.10 was included on a CD-ROM or DVD in the packaging of each Sourcefire 3D System appliance purchased by a customer and was additionally made available on a support webpage for customers.

The procedure described above is proven by the affidavit of Ms. Sarah Ehrig (document D20). Therein Ms. Ehrig confirms:

5. Based on the foregoing procedure, I can confirm that the electronic document bearing the title “*Sourcefire 3D System/User Guide/Version 4.10*” on its page 1 and having the timestamp “*2011-Mar-16 14:59*” on its page 2 was made available to customers of SF before March 12, 2013. The document was created in 2011 as a part of the described practices and

(D20, item 5).

The date March 12, 2013, refers to the priority date of EP 2 974 212 B1, since the declaration was prepared for an opposition against EP 2 974 212 B1. This date (March 12, 2013) is even earlier than the priority date (April 16, 2014) of the instant opposed patent.

Additionally, we offer pursuant to Article 117(1) EPC:

Evidence: Testimony of Ms. Sarah Ehrig.

Ms. Ehrig is currently an employee of an affiliate of the intervenor and was previously employed by Sourcefire, Inc. At the time of creation of D19, Ms. Ehrig had personal knowledge of the procedures for creating and delivering product documentation.

- bb.** Creation of the electronic publication D19 in 2011, as well as its security settings, including protection against modifications, are apparent from the document properties that can be displayed with “*Acrobat Reader*”:

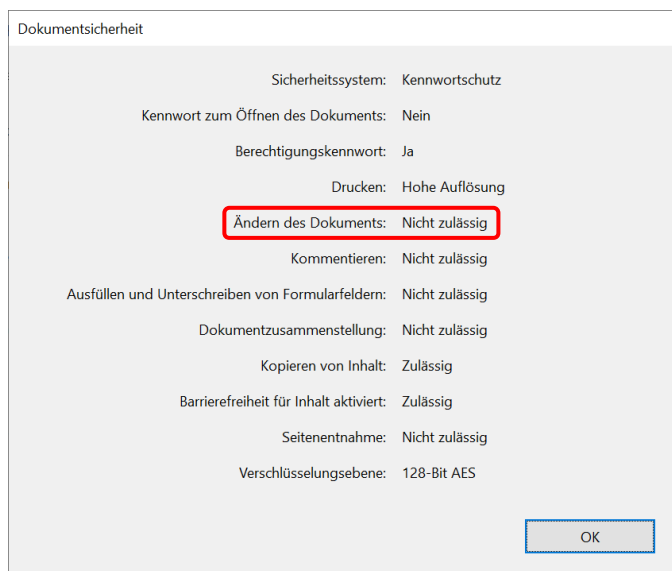
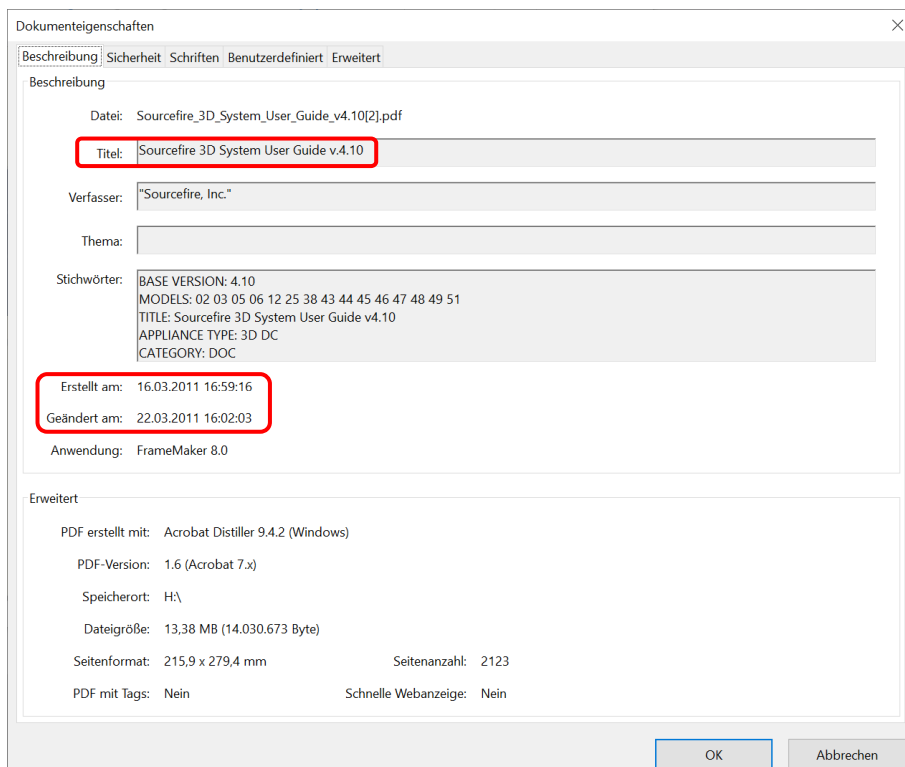


Fig. 5: Screen shots of the document properties of D19 (red frames added).

cc. D19 was made available to the customers without any obligation of confidentiality. Rather, it is explicitly stated in this document that it may be

passed on if certain conditions (e.g. no modification, inclusion of the copyright notice) are met. This is apparent from the passages on page 2 of D19, which are depicted below:

Terms of Use Applicable to the User Documentation

The legal notices, disclaimers, terms of use, and other information contained herein (the "terms") apply only to the information discussed in this documentation (the "Documentation") and your use of it. These terms do not apply to or govern the use of websites controlled by Sourcefire, Inc. or its subsidiaries (collectively, "Sourcefire") or any Sourcefire-provided products. Sourcefire products are available for purchase and subject to a separate license agreement and/or terms of use containing very different terms and conditions.

Terms of Use and Copyright and Trademark Notices

The copyright in the Documentation is owned by Sourcefire and is protected by copyright and other intellectual property laws of the United States and other countries. You may use, print out, save on a retrieval system, and otherwise copy and distribute the Documentation solely for non-commercial use, provided that you (i) do not modify the Documentation in any way and (ii) always include Sourcefire's copyright, trademark, and other proprietary notices, as well as a link to, or print out of, the full contents of this page and its terms.

(D19, page 2. Red frames added.)

- dd.** Before the priority date of the opposed patent, Sourcefire 3D System appliances had been purchased and obtained by more than 1000 customers. In accordance with the procedures described above, a documentation disc was enclosed with each purchased device. The documentation disc including the Sourcefire manual in version 4.10 was therefore actually made available to the customers (each of which being a large government entity or company) before the priority date.

The aforementioned purchases are proven by an affidavit by Mr. Jacob H. Baugher III.

Additionally, we offer:

Evidence: Testimony of Mr. Jacob Baugher III,

under Article 117(1) EPC.

Mr. Baugher is an employee of an affiliate corporation of the intervenor and was previously employed by Sourcefire, Inc. Mr. Baugher has personal knowledge of previous products and offers relating to network security systems, including the Sourcefire 3D system, as well as of practices and

procedures for recording and retrieving data for the sale of such products and offers.

- ee. The fact that the Sourcefire manual in version 4.10 was publicly available in March 2013 (i.e., well before the priority date of the opposed patent: April 16, 2014) was already found in the US Inter Partes Review proceedings (docket number: IPR2018-01436) against US patent US 9 124 552 (hereinafter: “US ‘522”; note that the Sourcefire manual in version 5.1.1, document 23, was not part of these proceedings). This decision was maintained in a final decision by the US Court of Appeals for the Federal Circuit (docket numbers: 2020-1635, 2020-1636). A petition for review by the Supreme Court of the United States was rejected. The decision of the US Patent and Trademark Office (USPTO) as well as the decision of the Court of Appeal are enclosed as document D22.

The fact that these decisions relate to version 4.10 of the Sourcefire manual follows from pages 34, 47, 50 and 105 of D22 (page numbers added at the bottom right).

In the context of the complete revocation of the patent US ‘522, the appellate court found that the USPTO had rightly recognized the Sourcefire manual in version 4.10 as being publicly available in March 2013. First of all, the Court of Appeal summarizes the decision of the USPTO as follows:

*„The Board **rejected Centripetal's argument that the cost of obtaining Sourcefire (the document) was prohibitive**; the Board found that it could be acquired by purchasing products that cost between \$1,385 and £25,000, that **586 customers actually acquired it**, and that Centripetal had not shown that an interested relevant artisan was not reasonably able to obtain the material“* (D22, page 10, our emphasis).

And then confirms it:

*„On this record, we agree with the Board that **Sourcefire was publicly accessible** and therefore qualifies as a printed publication“* (D22, page 17, by this party's emphasis).

ff. Finally, in the co-pending opposition proceedings against EP 2 974 212 B1 (application number 14 719 415.3), the opposition division found in its preliminary opinion dated December 13, 2021 that the Sourcefire manual in version 4.10 (there: document D7) was publicly available at the priority date of EP 2 974 212 B1, which is even earlier than the priority date of the instant opposed patent (namely March 12, 2013):

10.1 It appears to be common ground between the parties that D7 was publicly available at the priority date of the application and that it discloses features 1.1, 1.2 and 1.6 of claim 1 and, correspondingly, features 11.1, 11.2 and 11.6 of claim 11. The opposition division sees no reason to diverge from this.

b. The claimed subject-matter is not novel over D19

aa. Features 1 to 1.1.2

1 *A method, comprising:*

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

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

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, and*

The Sourcefire system comprises so-called 3D Sensors (= “packet security gateways”), also called “managed devices”, that are configured to protect the network:

3D Sensors

Sourcefire 3D Sensors™ are fault-tolerant, purpose-built appliances available with throughputs from 5Mbps up to 10Gbps. 3D Sensors passively aggregate network and user intelligence while defending the network against internal and external threats. Each 3D Sensor is capable of running Sourcefire IPS™, RNA® (Real-time Network Awareness), and RUA® (Real-time User Awareness).

(document D19, page 33).

The 3D sensors receive a security policy from a centralized management interface called the Defense Center (= “*security policy management server*”):

Defense Centers

The Defense Center provides a centralized management interface and database repository for the Sourcefire 3D System. You can analyze and respond to events from all your sensors consistently by doing the analysis through an interface where you can see all the data collected by the managed sensors. You can also push policies created on the Defense Center and software updates to managed sensors. If you have software sensors or Intrusion Agents on your network, you must use the Defense Center to manage them. Note that a 3D Sensor running the IPS component includes its own local web interface, but if you want to use RNA on the sensor, you must manage the sensor with a Defense Center.

(document D19, page 33, emphasis added).

The security policy comprises intrusion rules (= “*a first set of packet filtering rules*”):

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.

(D19, page 2084).

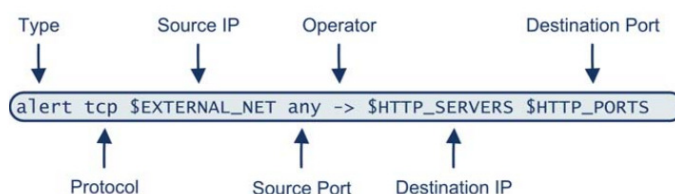
Intrusion rules comprise standard text rules and shared object rules. An exemplary intrusion rule header is shown below:

Understanding Rule Headers

Platform: DC/MDC/Standalone Sensor

Component: IPS

Every standard text rule and shared object rule has parameters and arguments that make up the rule header. For example, the following illustrates the parts of a rule header:



The [Rule Header Values](#) table describes each part of the rule header shown above.

(D19, page 764, emphasis added, the heading on page 764 is “*Understanding and Writing Intrusion Rules*”)

The intrusion rules are updated through so-called security enhancement updates (SEUs):

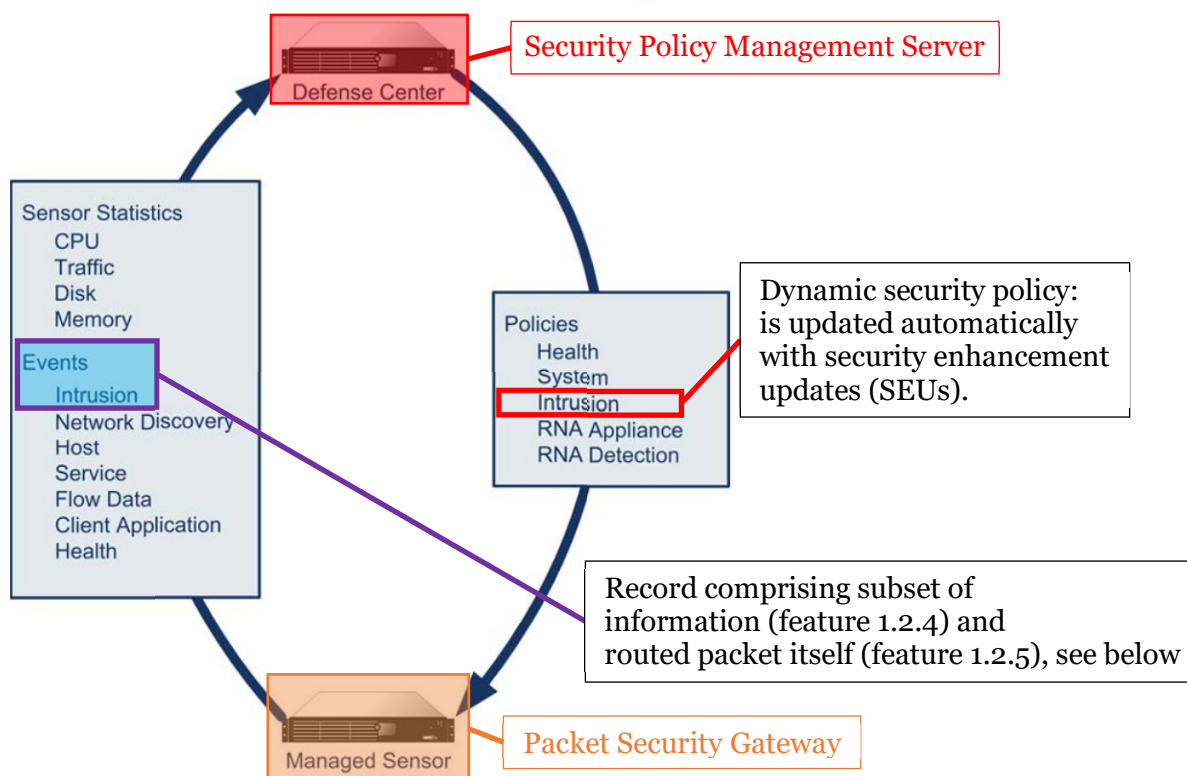
The [Sourcefire Vulnerability Research Team \(VRT\)](#) regularly sends out updates called Security Enhancement Updates, or SEUs, that can contain new intrusion rules, decoders, and preprocessors and other intrusion detection and prevention features, so you can be sure that you are detecting the most recently released attacks.

(document D19, page 254, emphasis added).

The security policy comprising intrusion rules is thus a “*dynamic security policy*”. More details are given in **section bb.** below.

The described procedure, i.e., that the dynamic security policy is received by the managed sensors from the Defense Center, is also visualized in the illustration below, with the solid black arrow (which was not added by the intervenor):

The following illustration lists what is transmitted between a Sourcefire Defense Center and its managed sensors. Note that the types of events and policies that are sent between the appliances are based on the sensor type.



If you apply a policy on a sensor before you begin managing it with a Defense Center, you can see a read-only version of the policy on the Defense Center's web interface.

Similarly, after you set up communications with a Defense Center and apply policies from the Defense Center to your sensor, you can see a read-only version of the running policies on the sensor's web interface. The following graphics

Fig. 6: D19, page 107. Annotations added.

D19 also discloses that the 3D Sensors (managed devices) are associated with a Defense Center located externally from the network protected by a 3D Sensor. In an example disclosed by D19, the Defense Center is located in a Home Office, and there are remote sites (New York Office, Miami Office) protected by the associated 3D Sensors:

In the following example diagram, when you set up the remote office 3D Sensors connections to the home office, use the Defense Center's fully qualified domain name as its host name. You can use the same registration key, you can use `snort` when adding either sensor, because the registration key does not have to be unique. However, you must use a **unique** NAT ID when adding the New York 3D Sensor to the Defense Center, and then use a different **unique** NAT ID when adding the Miami 3D Sensor. Each NAT ID has to be unique among all NAT IDs used to register sensors on the Defense Center.

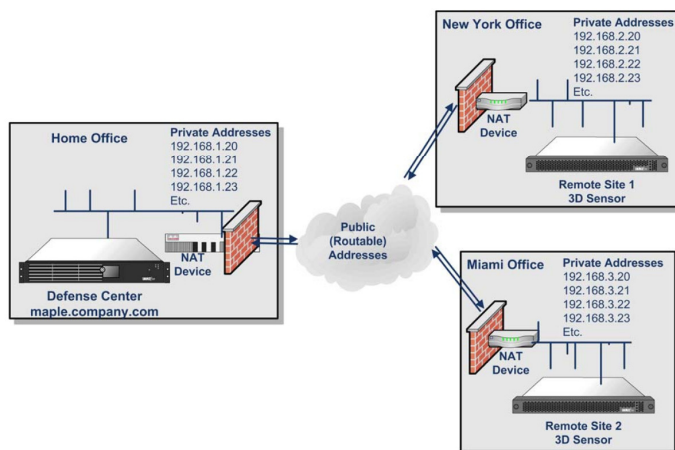


Fig. 7: D19, page 118.

Thus, features 1 to 1.1.2 are known from document D19.

bb. 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;*

D19 discloses that the Defense Center is able to automatically create or alter packet filtering rules using so-called security enhancement updates (SEUs). This process is disclosed to be fully automated. Such packet filtering rules are the standard text rules and the shared-object rules which are included in an intrusion policy (D19, pages 405 to 406, see heading „Managing Rules in an Intrusion Policy“):

Rule Types

Type	Description
shared object rule	An intrusion rule created by the Sourcefire Vulnerability Research Team (VRT) that is delivered as a binary module compiled from C source code. You can use shared object rules to detect attacks in ways that standard text rules cannot. You cannot modify the rule keywords and arguments in a shared object rule; you are limited to either modifying variables used in the rule, or modifying aspects such as the source and destination ports and IP addresses and saving a new instance of the rule as a custom shared object rule. A shared object rule has a GID (generator ID) of 3. See Modifying Existing Rules on page 864 for more information.

Rule Types (Continued)

Type	Description
standard text rule	An intrusion rule either created by the VRT, copied and saved as a new custom rule, created using the rule editor, or imported as a local rule that you create on a local machine and import. You cannot modify the rule keywords and arguments in a standard rule created by the VRT; you are limited to either modifying variables used in the rule, or modifying aspects such as the source and destination ports and IP addresses and saving a new instance of the rule as a custom standard text rule. A standard text rule created by the VRT has a GID (generator ID) of 1. Custom standard text rule that you create using the rule editor or import as local rules have a SID (Signature ID) of 1000000 or greater.
preprocessor rule	A rule associated with a detection option of the packet decoder or with one of the preprocessors included in the IPS component of the Sourcefire 3D System. You must enable preprocessor rules if you want them to generate events. Preprocessor rules have a preprocessor-specific GID (generator ID). See the Generator IDs table on page 489 for more information.

A „*standard text rule*“ and a “*shared-object rule*” (as well as so-called pre-processors) is created and updated automatically based on malicious traffic information provided by the Sourcefire Vulnerability Research Team:



Automating SEU Imports

Platform: DC/MDC/Standalone Sensor

Component: IPS

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.

The Import SEU task allows you to schedule the following subtasks separately or to combine them into one scheduled task:

1. Download the latest SEU.
2. Import the SEU.
3. Re-apply your intrusion policy so that the new SEU takes effect.

The selected subtasks present in the Import SEU task occur in the following order: download, install, rule state update, and policy re-apply. Once one subtask completes, the next configured subtask begins. Note that you can only re-apply policies applied from the appliance where the scheduled task is configured.

(D19, page 1716, emphasis added).

The Sourcefire Vulnerability Research Team identifies “*vulnerabilities*” (see above citation) and thus represents a malicious host tracker service (feature 1.1.3/1.3.1). For example, page 34 of D19 makes a direct connection between the updates of the intrusion rules and malicious traffic (malicious packets and malicious activity):

IPS

The Sourcefire Intrusion Prevention System (also called IPS) is one of the components of the Sourcefire 3D System that you can run on the 3D Sensor. IPS allows you to monitor your network for attacks that might affect the availability, integrity, or confidentiality of hosts on the network. By placing 3D Sensors with IPS on key network segments, you can examine the packets that traverse your network for malicious activity. Each 3D Sensor with IPS uses rules, decoders, and preprocessors to look for the broad range of exploits that attackers have developed.

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.

(D19, page 34, emphasis added).

The Sourcefire VRT provides malicious traffic information to the Defense Center (“*releases Security Enhancement Updates*”), i.e., the Defense

Center “receives”, via the Security Enhancement Updates, information on malicious traffic (see above). The Defense Center imports, as a scheduled task, i.e., without further manual interaction, the security enhancement updates comprising standard text rules or shared object rules (= “*one or more first packet filtering rules*”, see step 2 above), and re-applies these rules to the 3D Sensors (see step 3 above). Consequently, the 3D Sensors (= “*packet security gateways*”) receive rules automatically created or altered by the Defense Center (= “*security policy management server*”) based on identified vulnerabilities (= “*malicious traffic information*”) received from the Sourcefire VRT (= “*malicious host tracker service*”).

Therefore, feature 1.1.3 is disclosed by D19.

cc. Feature group 1.2

1.2 *performing, by the packet security gateway and on a packet-by-packet basis, packet filtering on a first portion of packets associated with the network protected by the packet security gateway based on the first set of packet filtering rules by performing*

1.2.1 *at least one of multiple packet transformation functions specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets,*

1.2.2 *wherein at least one of the multiple packet transformation functions specified by the at least one packet filtering rule of the first set of packet filtering rules corresponds to a packet digest logging function that provides a network communications awareness service and comprises:*

1.2.3 *identifying a subset of information specified by a packet matching the packet matching criterion of a packet filtering rule that specified the packet digest logging function;*

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;

Pages 34 and 35 of D19 disclose how packets are identified based on intrusion rules and in case of a match, a record (= “record comprising subset of information”) of the date, time, type of exploit, and context information about the source of the attack and its target is made (= “packet digest logging function”). In addition, for packet-based events, a copy of the packet that triggered the event is recorded and routed from the 3D Sensor to the Defense Center:

IPS

The Sourcefire Intrusion Prevention System (also called IPS) is one of the components of the Sourcefire 3D System that you can run on the **3D Sensor**. IPS allows you to monitor your network for attacks that might affect the availability, integrity, or confidentiality of hosts on the network. By placing 3D Sensors with IPS on key network segments, you can examine the packets that traverse your network for malicious activity. Each 3D Sensor with IPS uses rules, decoders, and preprocessors to look for the broad range of exploits that attackers have developed.

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.

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.

In a Sourcefire 3D System deployment that includes 3D Sensors with IPS and a Defense Center, the **sensors transmit events and sensor statistics to the Defense Center** where you can view the aggregated data and gain a greater understanding of the attacks against your network assets. The Defense Center can also push health, system, and intrusion policies to your sensors. You can push software updates from the Defense Center to sensors as well. For more information, see **What Can Be Managed by a Defense Center?** on page 106.

If your 3D Sensor is running IPS, you can also use a local web interface to create intrusion policies and review the resulting intrusion events. Note that if you do manage your 3D Sensors with a Defense Center, Sourcefire recommends that you use only the Defense Center's web interface to interact with the sensor and its data.

If you deploy your 3D Sensor inline on your network and create what is called an inline detection engine, you can configure your 3D Sensor to drop or replace packets that you know to be harmful.

Packet Security Gateway (feature 1.2)

Packet filtering rule (feature 1.2.3)

Matching the packet matching Criterion (feature 1.2.3)

Record comprising subset of information (features 1.2.2-1.2.5)

Routing the packet to a monitoring device (=Defense Center) (feature 1.2.6)

(D19, pages 34 to 35, emphasis and annotations added).

An intrusion event is defined as follows:

intrusion event A record of the network traffic that violated an [intrusion policy](#). Intrusion event data includes the date, time, and the type of exploit, as well as other contextual information about the source of the attack and its target.

(D19, page 2084).

Accordingly, the intrusion event that is generated comprises:

- a record comprising a subset of information specified by the packet (features 1.2.3 and 1.2.4) which is re-formatted (see below, feature 1.2.5), and
- the packet that matches the packet matching criterion.

The entire intrusion event is routed to the Defense Center, which is “*configured to store the packet for subsequent analysis*” and thus represents a “*monitoring device*” (feature 1.2.6).

An exemplary intrusion event is available for further analysis at the Defense Center and is shown on page 290 of D19:

The following graphic shows the **Defense Center** version of the packet view.

Event Information

Event : WEB-MISC Real Server DESCRIBE buffer overflow attempt (1:2411) Timestamp : 2009-10-21 11:37:18

Classification : Web Application Attack

Priority : high

Detection Engine : Fig 1 / Fig

Protocol : tcp

Source IP : 192.168.1.112

Source Port : 1468 (csdm)/tcp

Destination IP : 192.168.1.121

Destination Port : 554 (rtsp)/tcp

Rule : alert top \$EXTERNAL_NET any -> \$HTTP_SERVERS 554 (msg:"WEB-MISC Real Server DESCRIBE buffer overflow attempt"; flow:to_server,established; content:"DESCRIBE"; nocase; content:"./"; distance:1; pcre:"/^DESCRIBEs[\r\n]{300}/smi"; metadata:policy balanced-ips drop, policy connectivity-ips drop, policy security-ips drop, service http; reference:bugtraq,8476; reference:cve,2003-0725; reference:nessus,11642; reference:url,www.service.real.com/help/faq/security/rootexploit091103.html; classtype:web-application-attack; sid:2411; rev:9;)

Summary : This event is generated when an attempt is made to exploit a known vulnerability in RealNetworks Helix Media Server.

Rule Actions

Set Thresholding Options

Set Suppression Options

Packet Information

FRAME 1 (Expand All)

Frame 1 (1514 bytes captured)

Ethernet II, Src: 00:50:56:02:90:51, Dst: 00:50:56:45:20:3d

Internet Protocol, Src: 192.168.1.112, Dst: 192.168.1.121

Transmission Control Protocol, Src Port: 1468 (1468), Dst Port: 554 (554), Seq: 1, Ack: 1, Len: 1460

Packet Text

Packet Bytes

Copy Delete Review Download Packet

Copy All Delete All Review All Download All Packets

Reformatted subset (feature 1.2.5)

Routed packet (feature 1.2.6)

Defense Center is configured to store the packet for subsequent inspection = monitoring device (feature 1.2.6)

(D19, page 290; annotations added).

The re-formatting of the subset of information is described in more detail on pages 293 ff. of D19. D19 discloses, for example, a re-formatting based on the so-called syslog standard (D19, pages 752 ff., c.f. the embodiment disclosed in pars. [0041] and [0073] of the opposed patent).

Therefore, D19 discloses the entire feature group 1.2.

dd. Feature groups 1.3 and 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 up-dated malicious traffic information received from the malicious host tracker service; and*

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

Feature groups 1.3 and 1.4 concern the receipt of an updated second set of packet filtering rules and performing packet filtering based on the updated second set of packet filtering rules.

D19 discloses the automatic updating of packet filtering rules (intrusion rules comprising standard-text rules and shared-object rules) through so-called SEU updates. These updates are made “*so that the new SEU takes effect*”, i.e., such that packet-filtering is then based on the updated packet filtering rules:

Automating SEU Imports

Platform: DC/MDC/Standalone Sensor

Component: IPS

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.

The Import SEU task allows you to schedule the following subtasks separately or to combine them into one scheduled task:

1. Download the latest SEU.
2. Import the SEU.
3. Re-apply your intrusion policy so that the new SEU takes effect.

The selected subtasks present in the Import SEU task occur in the following order: download, install, rule state update, and policy re-apply. Once one subtask completes, the next configured subtask begins. Note that you can only re-apply policies applied from the appliance where the scheduled task is configured.

(D19, page 1716, emphasis added).

Thus, D19 explicitly discloses that after the update the Sourcefire system continues to perform the packet filtering function based on the update. As shown above, the packet filtering disclosed by D19 comprises the steps of feature group 1.2 which correspond to those of feature group 1.4.

Thus, D19 discloses feature groups 1.3 and 1.4 as well.

ee. Result

The claimed subject-matter is therefore not novel in view of D19.

G. Lack of inventive step (Articles 100 a), 56 EPC)

1. Lack of inventive step starting from the Sourcefire manual (document D19)

a. Background

D19 anticipates the subject-matter in a novelty destroying manner as shown above. Purely as a precaution, the following is submitted:

The proprietor had already filed an infringement complaint based on the patent EP 3 132 587 B1, which resulted from the parent application of the instant opposed patent. The competent regional court of Düsseldorf stayed the infringement proceedings until the decision on validity after the intervenor submitted that the subject-matter of EP 3 132 587 B1 is anticipated by the Sourcefire manual version 4.10 (= here: D19).

In light of the differences of claim 1 of the opposed, compared to claim 1 of EP 3 132 587 B1, the proprietor may argue that the Sourcefire manual (D19) does not disclose a malicious host tracker service. While the Sourcefire Vulnerability Research Team provides, as shown, the technical

features of a malicious host tracker service, to demonstrate that even if one were to assume such a “difference” for the benefit of the proprietor, there is at least no inventive step. Therefore, purely hypothetically, it is assumed that the corresponding features *were* not disclosed by D19:

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 up-dated malicious traffic information received from the malicious host tracker service; and*

b. Objective technical problem

The **technical effect** would be achieving an alternative method of providing automatic updates for the dynamic security disclosed by the Sourcefire manual. The **objective technical problem** is thus how to provide an alternative method of providing automatic updates for a dynamic security.

c. Obviousness

The technical solution is obvious in view of the common general knowledge of the skilled person and the developments already undertaken by numerous experts in the field of network security as we will show below:

- aa.** Firstly, it should be noted that the Sourcefire system, that is described in the manual (D19), was publicly credited for its automatic update functionality and intelligent policy tuning before the priority date of the opposed patent. Thus, the skilled person was aware of the automatic update function of Sourcefire. This is evidenced for example by following passages from D25 and D26, which were published before the priority date:

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.

(D25, page 1, emphasis added).

Note that the abbreviation NGIPS means next generation intrusion prevention system, c.f. page 33 of D19:

Sourcefire IPS™ (Intrusion Prevention System) provides best-in-class intrusion detection and prevention by harnessing the power of the industry-standard Snort® rules-based detection engine. Backed by the acclaimed Sourcefire Vulnerability Research Team™ (VRT), Sourcefire delivers its customers unrivaled protection against known and unknown threats.

See also D27, which concerns an article by Mr. Anthony Perridge, EMEA Channel Director at Sourcefire on the Sourcefire system:

Automation: Relying on manual processes to defend against modern and relentless attacks is inadequate. Attackers are taking advantage of automation and you need to as well to reduce labor intensive tasks and streamline processes. Tools that can intelligently identify and automatically alert only on relevant security events can save security teams hours investigating events that aren't real threats and prioritise those that are the most relevant. In addition, being able to automatically provision, tune and enforce security policies and rules across control points without manual intervention efficiently minimises risk of exposure to the latest threats and vulnerabilities despite dynamically changing environments.

(D27, page 1).

- bb.** At the time, a number of efforts had already been successfully made to standardize the exchange of cyber threat information. This is evidenced and summarized by document D27, published before the priority date. Document D27 in particular discloses that the so-called STIX format had been developed to standardize cyber observables and indicators (D27, pages 8 and 14). The proprietor has alleged in the infringement case that “observables” correspond to packet filtering rules (D3, marginal 148, page 74). D27 discloses in particular that the so-called Trusted Automated eXchange of Indicator Information (TAXII) effort had – before the priority

date – already been established by the US Department of Homeland Security (DHS):

- The U.S. Department of Homeland Security (DHS) is leveraging STIX in a number of critical areas including the Trusted Automated eXchange of Indicator Information (TAXII)⁴ effort which allows the Office of Cybersecurity and Communications (CS&C) and its partners in both government and the private sector to exchange data elements and relationships defined by STIX using secure automated mechanisms. Through the use of STIX, they seek to enable the rapid detection, prevention and mitigation of cyber threats and where possible, automate key elements of this process. Initial proof-of-concept efforts for TAXII are currently underway.

(D27, page 19, emphasis added).

D27 also discloses that the Financial Services Information Sharing and Analysis Center (FS-ISAC) agreed to implement the STIX architecture (including CybOX) for cyber threat information sharing amongst its constituent members in the financial services arena, which was already available by May 2013 to thousands of its members organizations:

- In Q2 2012, the Financial Services Information Sharing and Analysis Center (FS-ISAC) agreed to implement the STIX architecture (including CybOX) for cyber threat information sharing amongst its constituent members in the financial services arena. As of May 2013, FS-ISAC stood up an operational threat information repository utilizing STIX and available to all of its ~4200 member organizations.

(D27, page 19, emphasis added).

Thus, based on the common general knowledge before the priority date and the technology already put in place to do so, the skilled person would have used, for example, automatic feeds from FS-ISAC distributed via STIX and TAXII to update the dynamic security policy of Sourcefire, in addition to or alternative to the updates provided by the Sourcefire Vulnerability Research Team.

According to the proprietor, such an update, for example from FS-ISAC distributed via TAXII in the STIX format constitutes a malicious host tracker service (D3, pages 49 to 51):

■ kann die Indicators und Observables über böartige Hosts aus einer Vielzahl unterschiedlicher Quellen beziehen. Insbesondere können Indicators und Observables über böartige Hosts von Drittanbietern stammen.

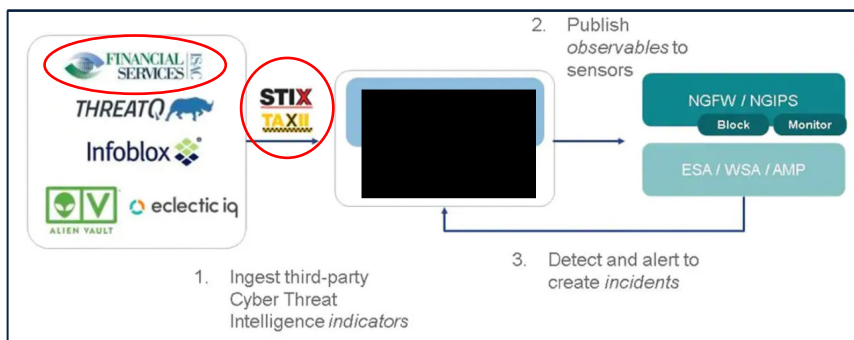


Fig. 8: Excerpt from page 49 of D3. Annotations added.

- cc. When faced with the technical problem how to provide an alternative method of providing automatic updates for a dynamic security the skilled person has a clear **incentive** to add automatic security updates based on TAXII to the teaching of D19.

D19 discloses that automatic updates are provided by the Sourcefire Vulnerability Research Team “as new vulnerabilities are identified” (D19, page 1716). Naturally, the capacity of any team is limited so the skilled person has an incentive to improve the update capabilities by widening the range of sources of malicious traffic information.

Before the priority date, the TAXII effort was common general knowledge of the skilled person and documented on the TAXII website (see documents D28 and D29). Taxii is an effort in order to standardize the automated exchange of cyber threat information. D28 is an excerpt from the so-called Wayback Machine archived on February 19, 2014 (see D29, note that the website shown in D28 and D29 is the same):



A1. What is TAXII?

Trusted Automated eXchange of Indicator Information (TAXII™) is a [U.S. Department of Homeland Security \(DHS\)](#)-led, community-driven effort to standardize the trusted, automated exchange of cyber threat information. TAXII defines a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information across organization and product/service boundaries for the detection, prevention, and mitigation of cyber threats. TAXII is not a specific information sharing initiative, and it does not define trust agreements, governance, or non-technical aspects of cyber threat information sharing. Instead, TAXII empowers organizations to achieve improved situational awareness about emerging threats, and enables organizations to easily share the information they choose with the partners they choose, while leveraging existing relationships and systems.

A2. How and why was TAXII developed?

The [U.S. Department of Homeland Security \(DHS\)](#) initiated TAXII to simplify and speed the secure exchange of cyber threat information. TAXII's standardized services and message exchanges eliminate the need for custom sharing solutions with each sharing partner, and widespread automated exchange of cyber threat information is now possible. DHS solicited community input and engaged MITRE to write the [TAXII Specifications](#).

(D28, page 1, emphasis added).

It is notable that the TAXII FAQ even incites a broad and diverse community participation:

A6. How can my organization and I be involved?

Broad and diverse community participation is an integral component of the TAXII effort. Visit the [TAXII Community](#) page for additional information.

(D28, page 1).

This is further evidenced by the fact that network security experts at Microsoft, HP, and other institutions had – before the priority date – already adopted the STIX format that is used by Taxii (D27, page 19). Therefore, the skilled person would provide an interface for Taxii feeds in the Sourcefire system of D19 when faced with the objective technical problem without inventive skill. Since the exchange via Taxii was already standardized before the priority date, only minor modifications would – if at all – be required and no incompatibilities could be expected.

For completeness, the intervenor refers to D30, which proves that the “*In-foblox*” service (also shown in the figure above), as another example of a malicious host tracker service, was also publicly known before the priority date.

Therefore, the subject-matter of features 1.1.3 and 1.3.1 is – in any case – obvious in view of the common knowledge of the skilled person.

2. Lack of inventive step starting from D31

a. D31 is a suitable closest prior art

Document D31 (US 2011/0072506 A1) is a US patent application published on March 24, 2011 and is thus full prior art under Article 54(2) EPC.

Document D31 is a suitable closest prior art since it has the same purpose as the underlying invention. Like the opposed patent, D31 addresses the issue of proactive network protection. D31 discloses that a problem of existing system is their vulnerability to zero-day vulnerabilities, where a threat is not known until it occurs (c.f. opposed patent, par. [0002]: *“Most existing approaches to protecting such networks are reactive rather than proactive. While reactive approaches may identify the source of an attack and assist in subsequent mitigation efforts, in most instances, the attack will have already been successfully launched.”*):

Continual patching to update the firewall as new threats are identified provides some protection, but cannot typically protect against “zero day” application layer attacks where the threat is unknown until it actually occurs. Further, because

(D31, par. [0014]), emphasis added).

D31 discloses a Unified Threat Management System (UTMS) that is capable of proactive network protection:

[0022] The security and management of process control system networks may be enhanced by providing a Unified Threat Management System (UTMS) including a UTMS-configured firewall, UTMS-configured network access device, and UTMS-configured field 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. The

[...]

tor or other workstation. The UTMS firewalls and devices may communicate with a perpetual service that proactively supplies the UTMS-configured firewalls, network access devices, and configured controllers or field devices with rulesets to meet the latest security threats, threat patterns, and control system vulnerabilities found to exist within the network. These updates are managed from within the standard

(D31, par. [0022]), emphasis added).

Document D31 is also a suitable closest prior art since it discloses the same network architecture as the opposed patent and would thus not require any structural changes. In particular, in the context of Fig. 3, D31 discloses the following system:

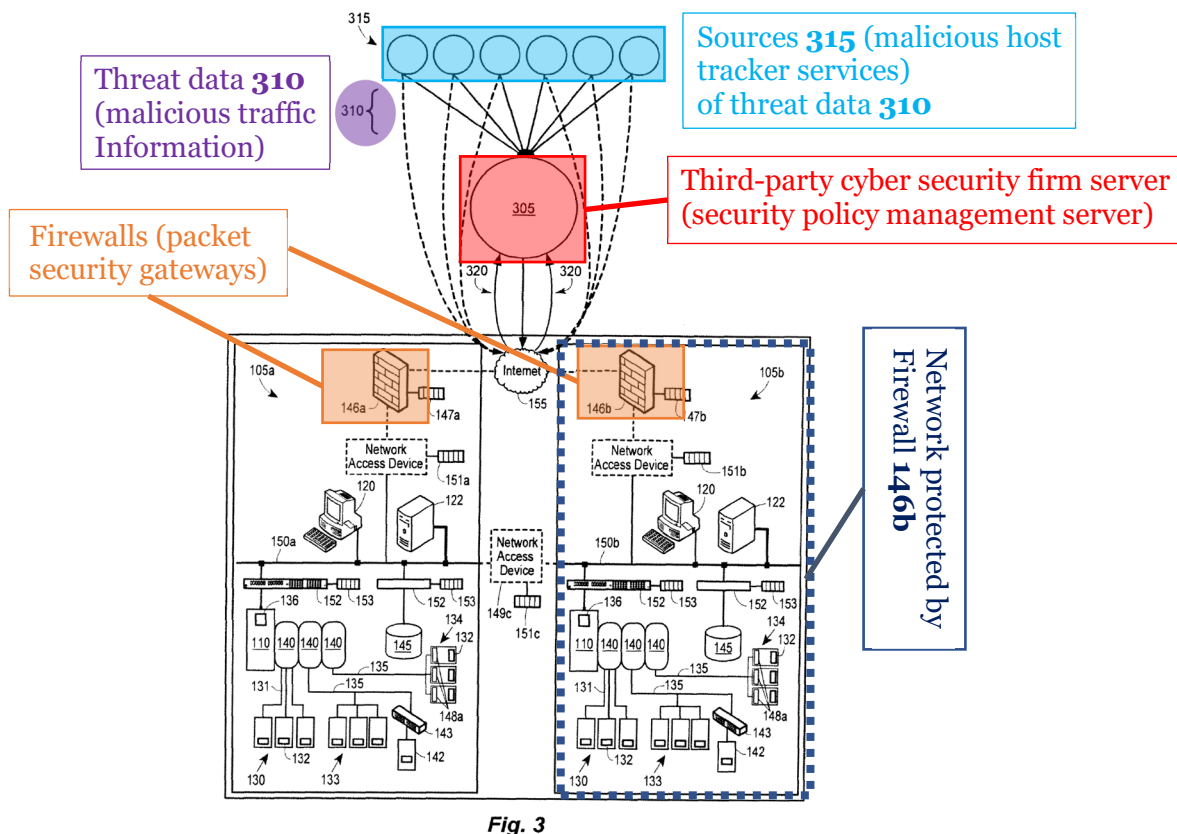


Fig. 3

Fig. 9: D31, Fig. 3. Annotations added.

This is structurally, insofar as relevant for the claim, identical to Fig. 5 of the opposed patent:

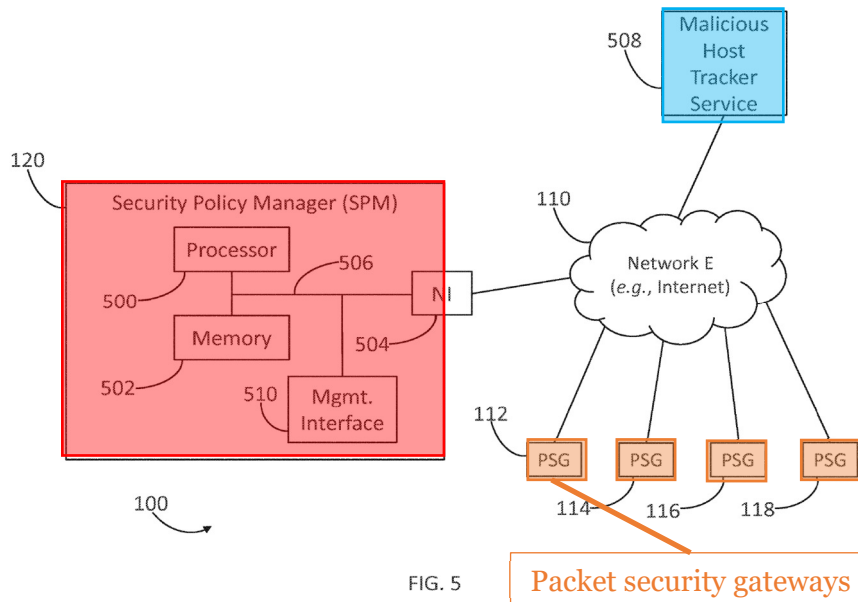


Fig. 10: *Opposed patent, Fig. 5. Annotations added.*

The subject-matter of claim 1 does not comprise an inventive step starting from D31 as will be shown below:

b. Disclosure of D31

aa. Features 1 to 1.1.2

1 A method, comprising:

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

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

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, and

Document D31 discloses a method (see D31, par. [0002]), where firewalls 146a, 146b (see D31, Fig. 3) operate based on rulesets (= security policy) comprising a plurality of rules:

function described below. Each firewall 146 or device 134, 149, 152 may include a ruleset, for example, rulesets 147a, 148a, 147b, 148b, 151a, 151b, 153 defining the communication that may be received or processed by the UTMS-configured device. Where the UTMS-configured device is a perimeter device (i.e., outside of the process control network 150a or 150b), the rulesets 147 and 151 may include a global set of rules for access to any device within the subsystems 105a, 105b. Where the UTMS-configured device is an internal

(D31, par. [0051], emphasis added).

The rules are packet filtering rules:

[0052] Generally, the UTMS may be a Network Intrusion Detection System (NIDS), a Host Intrusion Detection System (HIDS), a combination of these types of systems, or other known or future network security paradigms. For example, a NIDS-configured UTMS-configured firewall 146a, 146b and/or UTMS-configured network access device 149a, 149b, 149c or other UTMS-configured elements within the process control system 100 may use one or more rulesets to inspect and drop malicious packets from the network before the malicious packets can reach their intended destination within the process control systems and cause a fault. Additionally or

(D31, par. [0052], emphasis added).

The rulesets define a security policy:

that the system is operating normally or as expected. Each UTMS-configured firewall 146a, 146b, network access device 149a, 149b, 149c, and UTMS-configured field device 134 may include one or more rulesets or other files that define the security policy for the system 100. As further described

(D31, par. [0052], emphasis added).

These rulesets are updated to remain effective against network threats:

[0088] As previously described, the various rulesets (e.g., rulesets 147, 148, 151, 153) associated with the UTMS configured network devices 146, 134, 149, 152 require updates to remain effective against network threats. With reference to 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 rulesets to the UTMS-configured firewalls 146a, 146b, UTMS-configured network access devices 149c, other UTMS-configured network devices 146, and/or UTMS field devices 134. Ruleset collecting, constructing, validating, and distributing may be performed using any type of information technology methods suitable for performing such actions using electronic data. For example, some of the methods may include collecting the threat data 310 from the World Wide Web using various data collection techniques (e.g., robots, crawling, data feeds, collaborative forums, etc.), constructing

(D31, par. [0088], emphasis added).

The security policy is therefore dynamic.

A third-party cyber security risk management firm 305 provides the rulesets to the firewalls 146, see par. [0088] and Fig. 3 (reproduce above). The skilled person understands that this involves a server, i.e., a security policy management server at the third party cyber security risk management firm 305. Thus, the dynamic security policy is received from a security policy management server 305. As can be seen from Fig. 3, the security policy management server 305 is external to the network protected by firewall 146a or firewall 146b.

Therefore, D31 discloses features 1 to 1.1.2.

bb. 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;

As shown above, the rulesets of the dynamic security policy of D31 are updated by a server of a third-party security firm based on threat data 310 (= “malicious traffic information”) received from sources 315 (= “malicious host tracker service”), see D31, Fig. 3 (reproduced above) and pars. [0052], [0088].

These updates are performed automatically, for example, based on the detection of certain network conditions:

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.

(D31, par. [0083], emphasis added).

Therefore, D31 discloses feature 1.1.3.

cc. Feature group 1.2

1.2 *performing, by the packet security gateway and on a packet-by-packet basis, packet filtering on a first portion of packets associated with the network protected by the packet security gateway based on the first set of packet filtering rules by performing*

1.2.1 *at least one of multiple packet transformation functions specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets,*

1.2.2 *wherein at least one of the multiple packet transformation functions specified by the at least one packet filtering rule of the first set of packet filtering rules corresponds to a packet digest logging function that provides a network communications awareness service and comprises:*

1.2.3 *identifying a subset of information specified by a packet matching the packet matching criterion of a packet*

filtering rule that specified the packet digest logging function;

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;*

D31 discloses that packets are inspected based on the rules sets and malicious packets are dropped:

[0052] Generally, the UTMS may be a Network Intrusion Detection System (NIDS), a Host Intrusion Detection System (HIDS), a combination of these types of systems, or other known or future network security paradigms. For example, a NIDS-configured UTMS-configured firewall **146a**, **146b** and/or UTMS-configured network access device **149a**, **149b**, **149c** or other UTMS-configured elements within the process control system **100** may use one or more rulesets to inspect and drop malicious packets from the network before the malicious packets can reach their intended destination within the process control systems and cause a fault. Additionally or

(D31, par. [0052], emphasis added).

This is illustrated by the example shown in Fig. 13:

Packet matching criteria

Packet transformation function = packet digest logging function

Packet is re-routed (D31, par. [0103])

	1324	1302	1304	1305	1306	1308	1310	1312	1314
		PROTOCOL	FROM	THRESH.	T0	PORT	ACTION	DESCRIPTION	LOG
1326 →	☒	UDP	10.4.0.0	n/a	232.108.116.118	18515	Accept	New Multicast	NO
1328 →	☐	UDP	10.8.0.0	n/a	0-7	18516	Accept	New Multicast	NO
	☐	UDP	10.8.0.0	n/a	n/a	18517	Accept	PT_COM_RDS_IP	NO
	☐	UDP	10.8.0.0	n/a	n/a	18518	Accept	PT_COM_RDS_IP	NO
1330 →	☒	TCP	A	< x MB/hr	B	18519	Accept	PT_COM_RTRP	NO
1332 →	☒	TCP	B	n/a	A	18519	Accept	PT_COM_RTRP	NO
	☐	UDP	10.81.14.9	0-2	n/a	18520	Accept	NTP	NO
	☐	ICMP	...	...	...	18521	Accept	Remote Login	NO
	☐	ICMP	...	...	...	18522	Accept	Ping Pri-Act	NO
	☐	ICMP	...	...	...	18523	Accept	Allow SNMP Access	NO

1316	DeltaV Profile #14	LOAD	1318
1320		SAVE	1322

Fig. 13

Fig. 11: D31, Fig. 13. Annotations added.

as disclosed in par. [0103]:

[0103] In operation, each row of the example table 1300 enforces a rule if a corresponding row selector is active, as shown by an example row selection column 1324. A first

D31 thus discloses features 1.2, 1.2.1, and 1.2.3.

D31 also discloses a packet transformation function that corresponds to a packet-digest logging function, since it is possible for a log entry 1314 to be created, see Fig. 13 above. The fact that log files are created is disclosed, for example, in par. [0052] (“log files”) and in par. [0104], which discloses that packets identified based on “at least one packet matching criterion” (here: the protocol, TCP; the source IP address A; the destination IP address B; and the port number) are logged so long as a further criterion is fulfilled (here: x-megabytes traffic per hour):

imposed by that column entry. A second example row **1330** is configured to monitor TCP communications from IP address “A” (e.g., 10.4.0.0) to IP address “B” (e.g., 232.108.116.118) having port number 18519. As long as the amount of network traffic on port number **18519** is less than x-megabytes per hour, the network traffic is accepted. However, if the threshold is exceeded, a log is generated and communications are disabled for violating the threshold. On the other hand, while

(D31, par. [0104], emphasis added).

That the assessment whether the packet digest logging function is performed for a particular packet may include a further criterion (here: x-megabytes traffic per hour) is not excluded by the claim language. For example, an “*alarm*” can also be triggered by comparison of current network conditions with one or more rules (D31, par. [0076]).

Thus, D31 also discloses feature 1.2.2.

Document D31 also discloses that identified packets can also be re-routed:

server. While the example first rule **1326** identifies an action of “accept,” other actions may include, but are not limited to, block, notify, and/or re-route.

(D31, par. [0103], emphasis).

Document D31 thus discloses all features of feature 1.2 with the exception of:

- i. D31 does not disclose that a log includes a “*subset of information*” and that the subset is “*reformatted*” (part of features 1.2.4 and 1.2.5)
- ii. D31 does not disclose that the re-routing is to a “*monitoring device configured to store the packet for subsequent analysis*” (part of feature 1.2.6).

dd. Feature groups 1.3 and 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 up-dated malicious traffic information received from the malicious host tracker service; and*
- 1.4** *performing, on a packet by packet basis, packet filtering on a second portion of the packets associated with the network protected by the packet security gateway based on the up-dated second set of packet filtering rules.*

Feature groups 1.3 and 1.4 concern the receipt of an updated second set of packet-filtering rules and performing packet filtering based on the updated second set of packet filtering rules.

D31 discloses that “*the various rulesets [...] require update to remain effective*” (D31, par. [0088], recited above, emphasis added). The need for an update is detected automatically:

based on its current operating state. Additionally, the UTMS-configured process objects may access one or more rulesets **147, 148, 151, 153**, and compare detected current network conditions to one or more rules within the rulesets **147, 148, 151, 153**, to provide alarms based on detected network conditions (e.g., an unexpected increase in network traffic or type of traffic at the UTMS-configured object), to detect a software update of another element in communication with the UTMS-configured object that would require an update of the rulesets **147, 148, 151, 153**, to fully secure the system **100**, to detect a known fault-inducing attack on the network and expiration of a ruleset **147, 148, 151, 153**, etc. UTMS-configured process objects may also have a class/subclass hierarchy which enables them to be categorized in class libraries, to be collected together in a composite structure, etc. Still further,

Thus, D31 discloses that packet filtering continues after receiving an update and thus discloses feature groups 1.3 and 1.4 in their entirety.

c. Distinguishing features

Document D31 thus discloses all features of claim 1 with the exception of:

- i. D31 does not disclose that a log includes a “*subset of information*” and that the subset is “*reformatted*” (part of features 1.2.4 and 1.2.5). Note that D31 discloses the creation of a log for identified packets (see above).
- ii. D31 does not disclose that the re-routing is to a “*monitoring device configured to store the packet for subsequent analysis*” (part of feature 1.2.6). Note that D31 discloses a re-routing of identified packets (see above).

d. Technical effects / objective technical problems

The description of the opposed patent is entirely silent on any technical effect of distinguishing feature (i). Assume, *arguendo*, that a first technical effect of distinguishing feature (i) is that information is available in a particular chosen format; the only embodiment disclosed by the opposed patent (par. [0073]) concerns the – well known – syslog format.

The second technical effect of distinguishing feature (ii) is that the identified packet itself is made available for subsequent analysis. In an embodiment, the stored packet can be subsequently reviewed by a law enforcement or national security authority (opposed patent, par. [0039]).

The first and second technical effects are completely unrelated, there is no synergy effect between them. The claim is a juxtaposition (see Guidelines G-VII, 7) of features. In fact, as was shown above, the distinguishing features concern distinct and unrelated embodiments of the opposed patent. The embodiment of par. [0039] concerning the monitoring device does not make any reference at all to a packet digest logging function let alone a reformatting of a subset of information. *Vice versa*, the embodiment of par.

[0073] does not make any reference whatsoever to a monitoring device. Therefore, the partial problems approach is applicable (see Guidelines G-VII, 5.2; G-VII, 6).

The first partial problem is how to provide a method of packet filtering that allows a structured log entry to be created.

The second partial problem is how an identified packet can be made available for subsequent analysis, for example for law-enforcement purposes.

e. Obviousness

The claimed solution is obvious in view of the general knowledge of the skilled person. It is obvious that a log entry comprises some sort of format and is thus “*re-formatted*”. The claim does not specify any particular type of format and even the description only relates to the commonly known syslog format.

It is also obvious that a re-routing, as disclosed by D31, is only meaningful if the destination of the re-routed packet is configured to store the packet (otherwise the packet may as well be dropped and not re-routed).

Purely exemplary, intervenor refers to the following documents:

aa. Obviousness in view of D32

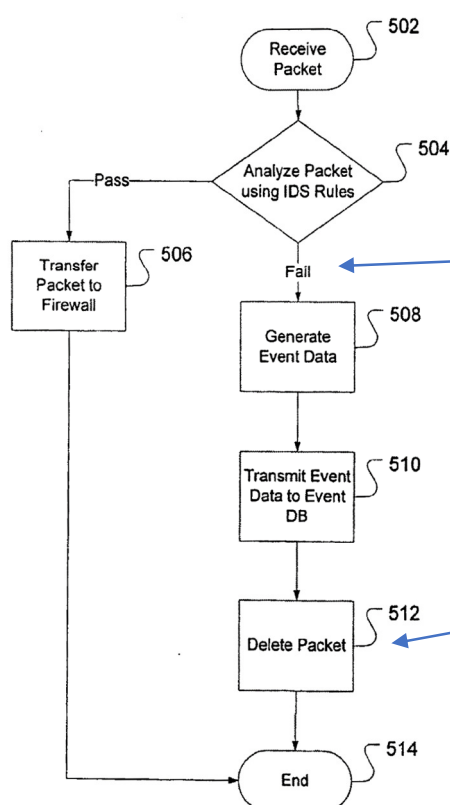
Document D32 is a US patent application published on October 7, 2020 and is thus full prior art under Article 54(2) EPC.

Document D32 discloses the solution to both partial problems within a single document.

Starting from D31, the skilled person would consider document D32 as it relates to the same technical field, i.e., a data traffic monitoring system

(D32, abstract). D32 even concerns a method of automatically generating rules for use by a monitoring module (D32, par. [0044]).

Document D32 discloses the following workflow in the context of Fig. 5 (similar workflows are disclosed in Figs. 6 and 9, and the corresponding passages from the description:



[0106] However, if the set of IDS rules contains at least one rule that indicates that the communication packet should be prevented from entering the protected network, the packet “fails” the IDS rules analysis operation 504. Upon determination that a packet has failed the IDS rules analysis operation, a generate event data operation 508 is performed. The generate event data operation 508 includes collecting certain information from the failed packet. This information includes at least the source of the packet and may include some or all of the event data described in Table 1 that is directly available from the packet. The event data may also identify the IDS rule or rules that the packet failed and may identify the IDS module as the module that failed the packet.

[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 exact order of the operations described above with respect to the IDS analysis may be varied and that the delete packet operation 512 could be performed before the transmit event data operation 510.

Fig. 12: D32, Fig. 5, annotations added.

Thus, document D32 discloses a packet is analyzed (step 504) and based on a packet matching criterion a packet is rejected (fail) which leads to:

- i. The generation of event data (= subset of information), which is transmitted to an event database (e.g. event database 310, see D32, Fig. 3).

D32 discloses that the event data is re-formatted, for example based on the XML or HTML format:

[0069] The event data reported, of course, are dictated by the implementation of the reporting monitor module. Such event data may include, for example, data identifying the monitor module generating the event data, the event type, a priority associated with the event determined by the monitor module, a timestamp for the event, and one or more identifying details of the message that is the source of the event, such as the source IP address, port, URL or MAC of the message, an identifier indicating if the source is internal to the computing system, the destination IP address, port, URL or MAC of the message, an identifier indicating if the destination is internal to the computing system, and information concerning whether the message is coming from a known “bad” or “good” host. The event data may be provided as a simple ASCII file with a known format, as XML that include data type definitions, in an HTML file, or in any other form, as long it is known to and useable by the SSI.

(D32, par. [0069], emphasis added.)

Starting from D31, the skilled person would thus take the log (D31, par. [0104]) and re-format it in XML format (D32, par. [0069]) without inventive skill.

- ii. The deleted packet is stored in a “*deleted packet database for further analysis*”. The deleted packet database is thus “*configured to store the packet for subsequent analysis*” and thus represents a “*monitoring device*”.

Starting from D31 and in view of the second partial problem, the skilled person would thus “*re-route*” (D31, par. [0103]) the packet to the “*deleted packet database*” (D32, par. [0111]) for further analysis without inventive skill.

The subject-matter of claim 1 thus lacks an inventive step starting from D31 in view of D32. The same applies *mutatis mutandis* to claims 14 and 15, which therefore do not comprise an inventive step either.

bb. Obviousness in view of common general knowledge and D36

The solution to the first partial problem is obvious in view of the common general knowledge of the skilled person. The solution to the second partial problem is obvious in view of document D36.

i. First partial problem

It was common general knowledge of the skilled person before the priority date that a log has to be re-formatted according to some sort of logging standard. In an embodiment, the opposed patent refers to the syslog standard (par. [0073]). Syslog was standardized years before the priority date as is evidenced by documents D33 (RFC 5424) and D34 (change history of the standard). Document D33 discloses the syslog standard as an important tool to avoid compatibility issues:

„Without this document, each other standard needs to define its own syslog packet format and transport mechanism, which over time will introduce subtle compatibility issues” (D33, page 2).

Thus, the very purpose of the syslog standard is to provide a compatible tool to the skilled person that he can simply use without any inventive skill.

That syslog was commonly used for firewalls protocols is also evidenced by document D35. D35 even discloses the same network architecture as the opposed patent, see Fig. 6:

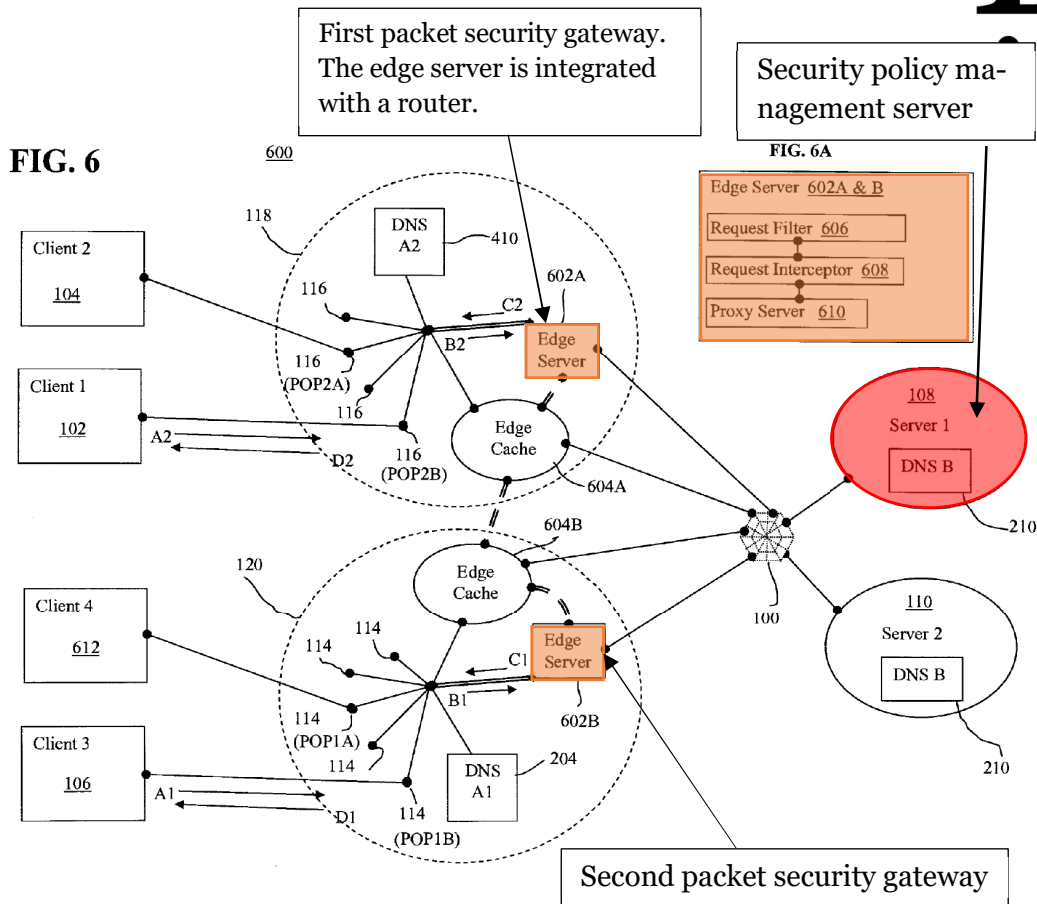


Fig. 13: Fig. 6 of NK 4. Annotations added.

D35 discloses that Server 108 (=security policy management server) is located external to the networks 118, 120 protected by the edge server (=packet security gateway). Server 180 serves as a security policy management server that can transmit a dynamic security policy identifying malicious computer program code from a virus watch service (malicious host tracker service) to the edge servers 602A and 602B (= packet security gateways) as a dynamic security policy so that forged packets are identified and prevented from reaching the network 100 from any of the clients 102, 104, 106:

Once traffic is intercepted, the edge server **602** can perform many value added services. As described above, the edge server **602** can perform DNS translations and redirect clients **102, 104, 106, 612** to make their content requests to the edge cache **604**. The edge server **602** can also monitor the data transmission being generated by clients **102, 104, 106, 602** for malicious program code, i.e. program code that has been previously identified (by the server **108** or a third party such as a virus watch service) as unwanted, harmful, or destructive such as viruses or other unauthorized data being transmitted. For example, if the edge server **602A** detects a data packet whose origin address could not have come from the downstream network or POP's **114** to which it is connected, the edge server **602A** knows that this data packet must be a forgery and can eradicate it or prevent it from reaching the network **100**. For example, where a computer hacker surrep-

(NK 4, column 28, lines 17 to 32, emphasis added).

D35 discloses that packets are examined based on packet filtering rules (D35, Col. 38, ll. 55 to 61). A comparison can include, for example, comparing the port address of the received packet with a stored port address "80" to identify if it is an HTTP packet⁵ (D35, Col. 38, ll. 64 to 67).

Once the function of a rule has been evaluated, the packet analyzer performs the desired action or actions determined by the rule (D35, Col. 39, ll. 13 to 15).

For example, information about the packet is logged (D35, Col. 39, ll. 15 to 36, highlighting added by this party) in syslog format

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

(D35, col. 35, lines 34 to 36; see also col. 35, lines 52 to 57).

Thus, the solution to the first partial problem is obvious in view of the common general knowledge of the skilled person.

⁵ The port address 80 is used for the http protocol.

ii. Second partial problem

The solution to the second partial problem is obvious in view of document D36. D36 (US 2011/0314177 A1) is a US patent application that was published on December 22, 2011 and which therefore is full prior art pursuant to Article 54(2) EPC.

If, starting from D31, in view of the second partial problem, how an identified packet can be made available for subsequent analysis, for example for law-enforcement purposes, the person skilled in the art will consider D36. D36, like the D31, deals with network security in general. Specifically, D36 concerns technologies that redirect traffic associated with a target entity for the purpose of lawful interception:

“Technologies for redirecting traffic associated with a target entity for purposes of lawful intercept are presented herein” (D36, abstract).

D36 discloses that Internet Service Providers (ISPs) may be required by law enforcement agencies to collect data traffic from a specific target person, e.g. a device on the network associated with a specific location or person, for law enforcement and cyber-security purposes:

“Internet service providers (ISPs) may be required by local, state or federal law enforcement agencies to capture data traffic from a particular target entity, such as a network device associated with a particular location or person for purposes of law enforcement and cyber-security” (D36, paragraph [0002]).

Since D36 is thus concerned with routing packets for law enforcement purposes, the person skilled in the art would have reason to use D36 to solve the problem when starting from NK 6.

D36 discloses

- 1.2.3** *identifying a subset of information specified by a packet matching the **packet matching criterion** of a packet filtering rule that specified the packet digest logging function; [...]*
- 1.2.6** *routing, by the **packet security gateway**, the packet to a **monitoring device configured to store the packet for subsequent analysis**;*

as is illustrated, for example, by the embodiment in Fig. 4:

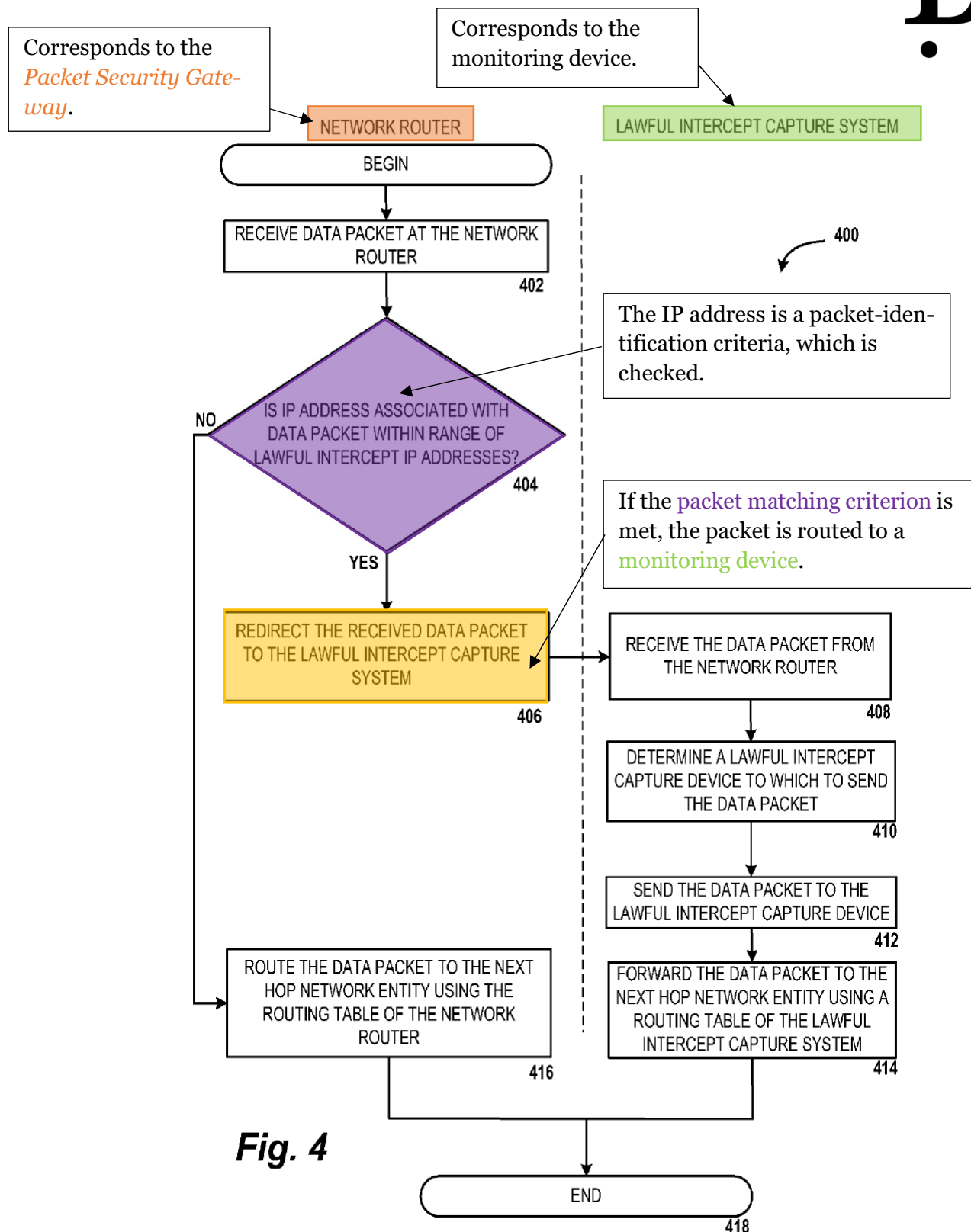


Fig. 14: Fig. 4 of D36. Annotations added.

The method of Fig. 4 is summarized as follows:

„A routine 400 begins at operation 402, where the network router 104 receives a data packet“ (D36, paragraph [0060]).

The network router 104 constitutes a *packet security gateway*. This step corresponds to feature 4 of claim 1, which is thus also disclosed by D36.

The method proceeds as follows:

„From operation 402 the routine 400 continues to operation 404, where the network router 104 may determine whether either the origination IP address or the destination IP address associated with the data packet is within the range of lawful intercept IP addresses 262 that correspond to the lawful intercept routing policy 260 for redirecting the data packets of the lawful intercept capture system 108.“

This means that a *packet matching criterion* is checked, namely the source IP address or the destination IP address. This corresponds to feature group 5, which is thus also disclosed by D36.

If the *packet matching criterion* is met, the method proceeds as follows:

*„If, however, at operation 404, the network router 104 determines that the origination IP address or the destination IP address associated with the data packet lies within the range of lawful intercept IP addresses 262, the routine 400 proceeds from operation 404 to operation 406, **where the network router 104 redirects the data packet to the lawful intercept capture system 108.** According to embodiments, the data packet may be redirected to the lawful intercept capture system 108 based on the lawful intercept routing policy 260 associated with the lawful intercept IP address. The lawful intercept routing policy 260 may indicate the redirection IP address 264 associated with the lawful intercept capture system 108 to which to route the data packet associated with the lawful intercept IP address“ (D36, paragraph [0062], highlighting added by this party).*

This means that the *packet security gateway*, i.e., the network router 104, routes the data packet, which matches the *packet matching criterion*, i.e. a certain IP address, to the Lawful Intercept Capture System 108 for further analysis. The Lawful Intercept Capture System 108 in turn forwards the packet to a certain “*lawful intercept capture device 110A*” (D36, pars. [0063]-[0064]), which thus constitutes a monitoring device.

Starting from D31 and in view of D35, the skilled person would thus “*re-route*” (D31, par. [0103]) the packet to the “*lawful intercept capture device 110A*” (D36, pars. [0063]-[0064]) for further analysis, when faced with the problem of how an identified packet can be made available for subsequent analysis, for example for law-enforcement purposes, without inventive skill.

iii. Summary

Thus, claim 1 is not based on an inventive step.

The same applies accordingly to claims 14 and 15, which therefore do not involve an inventive step either.

H. Dependent claims

None of the dependent claims fulfills the requirements of the EPC. The dependent claims comprise added-matter and are not sufficiently disclosed (Articles 100b), 83 EPC). Moreover, the subject-matter of the dependent claims is not novel or at least not inventive:

1. Claim 2

2. *The method of claim 1, wherein the at least one packet matching criterion comprises at least one network address associated with an indication of malicious network traffic.*

The subject-matter of claim 2 is not novel over each of D19 or D23.

- a. D23 discloses that a Security Intelligence Feed (whether this is the Sourcefire Intelligence Feed or a third-party feed does not matter) is a dynamic collection of IP addresses (a network address) with a poor reputation:

Comparing Feeds and Lists

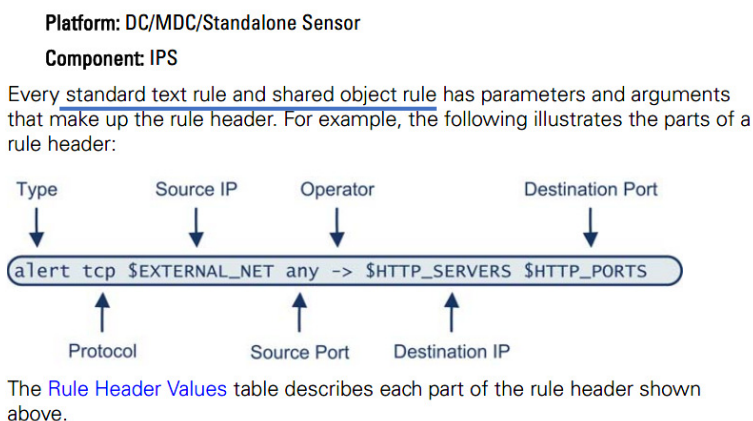
A Security Intelligence *feed* is a dynamic collection of IP addresses that the Defense Center downloads from an HTTP or HTTPS server at the interval you configure. Because feeds are regularly updated, the system can use up-to-date information to filter your network traffic. To help you build blacklists,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

(D23, page 142, emphasis added).

D23 also explicitly refers to “malicious IP addresses” in this context (D23, page 146, penultimate paragraph.

- b. D19 discloses that a standard text rule or standard objection rule (comprised in the intrusion rule) comprises source and destination IP addresses of the packet:

Understanding Rule Headers



(D19, page 764, emphasis added, the heading on page 764 is “*Understanding and Writing Intrusion Rules*”)

The standard text rule or standard objection rule is created and updated automatically based on malicious traffic information provided by the Sourcefire Vulnerability Research Team (see above, especially D19, page 34 and page 1716).

2. Claim 3

3. *The method of any one of claims 1 or 2, wherein at least one packet transformation function comprises a network protective action.*

- a. The subject-matter of claim 3 is not disclosed by the parent application as filed (document D6) or the application as filed (document D5). Claim 3 was drafted from scratch with the response of the (then) applicant dated April 3, 2020:

3. The method of any one of claims 1 or 2, wherein at least one packet transformation function comprises a network protective action~~wherein the subset of information comprises at least one of an arrival time of the one or more packets, a flow direction of the one or more packets, an identifier of an interface of the packet security gateway that received the one or more packets, an identifier of at least one packet filtering rule associated with the one or more packets, or metadata associated with at least one packet filtering rule associated with the one or more packets.~~

Neither D6 nor D5 disclose “a network protective action” anywhere contrary to Articles 76(1) and 123(2) EPC.

b. Moreover, the subject-matter of claim 3 is not novel over D19 or D23:

Document D23 discloses:

You can also deploy a managed device as an inline, switched, or routed intrusion system, which allows you to configure the device to drop or replace packets that you know to be harmful.

(D23, page 469).

Document D19 discloses that the intrusion policy may drop harmful packets:

If you deploy your 3D Sensor inline on your network and create what is called an inline detection engine, you can configure your 3D Sensor to drop or replace packets that you know to be harmful.

(D19, page 35).

3. 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.

- a. Claim 4 is not disclosed by the parent application as filed (document D6) or the application as filed (document D5). It was added with the (then) applicant's response dated April 3, 2020.

As claim 4 is worded now it does not correspond to the disclosure of pars. [10] and [51] of document D6. These paragraphs disclose that the

“dynamic security policy may also include one or more rules, the combination of which may effectuate an enqueueing service within a network environment” (D6, par. [51]; D5, par. [51]).

However, the “rules” of claim 1 are “packet-filtering rules” that do not “effectuate an enqueueing service within a network environment”. It is not disclosed anywhere in documents D5 or D6 that a packet-filtering rule as claimed can define first and second forwarding queues. These are distinct embodiments. The “enqueueing service” does not relate to a packet digest logging function (features 1.2.2 to 1.2.5) or routing of the packet (feature 1.2.6).

Thus, different embodiments were combined contrary to the requirements of Articles 123(2) and 76(1) EPC.

- b. Claim 4 is not novel over D19 or D23. Both D19 and D23 disclose rules that forward packets based on their type of service (ToS) value or, for the IP header protocol, based on their Differentiated Services Code Point (DSCP) field. For example, document D19 discloses:

Inspecting a Packet's Type of Service

Platform: DC/MDC/Standalone Sensor

Component: IPS

Some networks use the type of service (ToS) value to set precedence for packets traveling on that network. The `tos` keyword allows you to test the packet's IP header ToS value against the value you specify as the keyword's argument. Rules using the `tos` keyword will trigger on packets whose ToS is set to the specified value and that meet the rest of the criteria set forth in the rule.

IMPORTANT! Argument values for `tos` must be numeric.

The ToS field has been deprecated in the IP header protocol and replaced with the Differentiated Services Code Point (DSCP) field.

(D19, page 815).

Similar disclosure is found on page 9750 of D23. The opposed patent identifies the DSCP field as an embodiment of the subject-matter of claim 4 (opposed patent, par. [0038]).

Thus, the subject-matter of claim 4 is not novel over D19 or D23.

Moreover, it is noted that the use of DSCP to provide differentiated quality of service was already standardized before the priority date, see documents D37 and D38:

“The differentiated services architecture is based on a simple model where traffic entering a network is classified and possibly conditioned at the boundaries of the network, and assigned to different behavior aggregates. Each behavior aggregate is identified by a single DS codepoint. Within the core of the network, packets are forwarded according to the per-hop behavior associated with the DS codepoint” (D37, section 2, page 12).

As well as:

„Packet classifiers select packets in a traffic stream based on the content of some portion of the packet header. We define two types of classifiers. The BA (Behavior Aggregate) Classifier classifies packets based on the DS codepoint only. The MF (Multi-Field) classifier selects packets based on the value of a combination of one or more header fields, such as source address, destination address, DS field, protocol ID, source port and destination port numbers, and other information such as incoming interface. Classifiers are used

to ‘steer’ packets matching some specified rule to an element of a traffic conditioner for further processing” (D37, section 2.3.1, page 14).

and:

DS codepoint	a specific value of the DSCP portion of the DS field, used to select a PHB.
--------------	---

(D37, page 4).

Per-Hop-Behavior (PHB)	the externally observable forwarding behavior applied at a DS-compliant node to a DS behavior aggregate.
------------------------	--

PHB group	a set of one or more PHBs that can only be meaningfully specified and implemented simultaneously, due to a common constraint applying to all PHBs in the set such as a queue servicing or queue management policy. A PHB group provides a service building block that allows a set of related forwarding behaviors to be specified together (e.g., four dropping priorities). A single PHB is a special case of a PHB group.
-----------	--

(D37, page 6).

4. 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.*

- a. Claim 5 extends beyond the application as filed (document D5) and the parent application as filed (document D6). It was added with the (then) applicant’s response dated April 3, 2020.

Neither D5 nor D6 disclose that the operation of the PSG “in a network layer transparent manner” may be combined with the packet digest

logging function as claimed, in particular with the generation of a record (feature 1.2.3 to 1.2.5) and routing of the packet (feature 1.2.6). In particular, the application as filed (and correspondingly the parent application as filed) teaches at par. [42] that, by operating in a network layer transparent manner, attack packets cannot be routed to network interfaces. However, the claim requires routing of (identified) packets (feature 1.2.6). Therefore, two different, and in fact even incompatible, embodiments have been combined contrary to Articles 123(2) and 76(1) EPC.

- b. The subject-matter of claim 5 is insufficiently disclosed (Article 83 EPC) as the opposed patent does not disclose how *“packets [can be received] 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”*.
- c. The subject-matter of claim 5 is not novel over D19 and D23, which both disclose a *“transparent inline mode”* (D19, pages 226 and 227; D23, page 233).

5. 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.*

The subject-matter of claim 6 is not novel over D19 or D23.

According to par. [0041] of the opposed patent, *“a network security awareness service or a network threat awareness service”* may, for example, be effected by a packet digest logging function that stores, for example, *“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)” (opposed patent, par. [0041]).

As shown above, D19 and D23 discloses a packet digest logging function, see e.g. D19, pages 258, 259, and 290; D23, page 469. Thus, D19 and D23 disclose “a network security awareness service or a network threat awareness service”.

6. Claim 7

7. *The method of any one of claims 1-6, wherein 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.*

The subject-matter of claim 7 is not novel over D19 and D23:.

- a. D23 discloses that an intrusion policy (and thus the logged information) is chosen to fit the need of an organization:

The default intrusion policies that you can use are:

- Balanced Security and Connectivity
This policy is built for both speed and detection. It serves as a good starting point for most organizations. It is also a good starting point for any type of deployment.
- Connectivity Over Security
This policy is built for organizations where connectivity (being able to get to all resources) takes precedence over network infrastructure security. This policy enables far fewer rules than those enabled in the Security over Connectivity policy. Only the most critical rules that block traffic are enabled.

(D23, page 566, emphasis added).

The “*table view*”, for example, presents information “of interest” to the user of the system:

table view

A type of workflow page that displays event information, with one column for each of the fields in the database table. When performing event analysis, you can use drill-down pages to constrain the events you want to investigate before moving to the table view that shows you the details about the events you are interested in. The table view is often the next-to-last page in workflows delivered with the system.

(D23, page 2155, emphasis added).

- b. Similarly, D19 discloses that the events (which contain the “*record*” created by the packet digest logging function) are used to indicate communications that are “*of interest to an organization that operates the network*”, for example they may already be prioritized:

Investigation and Qualification

Your incident handling process should specify how, after a security incident is detected, an investigation is conducted. In some organizations, junior members of the team triage all the incidents and handle the less severe or lower priority cases themselves. High severity and high priority incidents are handled by more senior members of the team. You should carefully outline the escalation process so that each team member understands the criteria for raising an incident's importance.

Part of the escalation process is tied to understanding how a detected event can affect the security of your network assets. For example, an attack against hosts running Microsoft SQL Server is not a high priority for organizations that use a different database server. Similarly, the attack is less important to you if you use SQL Server on your network, but you are confident that all the servers are patched and are not vulnerable to the attack. However, if someone has recently installed a copy of the vulnerable version of the software (perhaps for testing purposes), you may have a greater problem than a cursory investigation would suggest.

The Sourcefire 3D System is particularly well suited to supporting the investigation and qualification process. With standalone 3D Sensors with IPS, you can create your own event classifications, and then apply them in a way that best describes the vulnerabilities on your network. When traffic on your network triggers an event, it is automatically prioritized for you. If you also deploy a 3D Sensor with RNA on the same network segment and use a Defense Center to correlate the information from both sensors, then events are automatically qualified for you with special indicators showing which attacks are directed against hosts that are known to be vulnerable.

(D19, page 322, emphasis added).

The intrusion event workflows are set up so that information that is of interest to the user is displayed, which are customized as desired according to the user's needs:

If the predefined workflows do not meet your specific needs, you can create custom workflows that display only the information you are interested in. Custom intrusion event workflows can include drill-down pages, a table view of events, or both; IPS automatically includes a packet view as the last page. You can easily switch between the predefined workflows and your own custom workflows depending upon how you want to investigate events.

(D19, page 283).

See also the table view of intrusion events (an example is shown above):

table view

A type of [workflow](#) page that displays [event](#) information. Table views include a column for each of the fields in the database. For example, the table view of [intrusion events](#) includes columns such as Time, Priority, Impact Flag, Source IP, Destination IP. As another example, the table view of RNA [network discovery events](#) includes such columns as Time, Event, IP Address, MAC Address, and so on. Generally, you use [drill-down pages](#) to constrain the events you want to investigate before moving to the table view that shows you the details about the events you are interested in. The table view is the next to last page in predefined workflows; advancing from the table view leads to the [packet view](#) (for workflows based on intrusion events), the [host view](#) (for workflows based on [RNA events](#)), the [vulnerability detail page](#) (for workflows based on vulnerabilities), or the [user identity view](#) (for workflows based on [RUA events](#)).

(D19, page 2095, emphasis added).

7. Claim 8

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.*

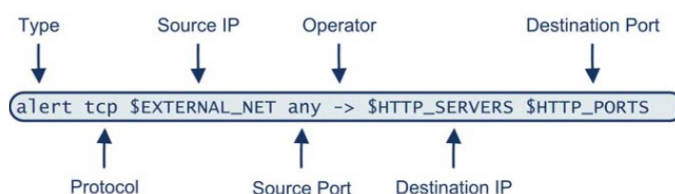
The subject-matter of claim 8 is not novel over D19 and at least not inventive over D23. D19 discloses an exemplary intrusion rule header as shown below:

Understanding Rule Headers

Platform: DC/MDC/Standalone Sensor

Component: IPS

Every standard text rule and shared object rule has parameters and arguments that make up the rule header. For example, the following illustrates the parts of a rule header:



The [Rule Header Values](#) table describes each part of the rule header shown above.

(D19, page 764, emphasis added, the heading on page 764 is “*Understanding and Writing Intrusion Rules*”)

See also D19, page 400 and page 402, wherein IP ranges and port ranges as well as the protocol (“*tcp*”) are used to define an intrusion rule. The intrusion rule thus comprises a five-tuple comprising protocol, source IP, source port, destination IP, and destination port.

Document D23 discloses that access control rules may comprise a number of conditions, including source and destination IP address ranges (networks), ports, and, for example, URLs:



Understanding Rule Conditions

LICENSE: Any

You can set an access control rule to match traffic meeting any of the conditions described in the following table:

Access Control Rule Condition Types

Condition	Description
Zones	A configuration of one or more interfaces where you can apply policies. Zones provide a mechanism for classifying traffic on source and destination interfaces, and you can add source and destination zone conditions to rules. See <i>Working with Security Zones</i> on page 158 for information on creating zones using the object manager.
Networks	Any combination of individual IP addresses, CIDR blocks, and prefix lengths, either specified explicitly or using network objects and groups (see <i>Working with Network Objects</i> on page 140). You can add source and destination network conditions to rules.
VLAN Tags	A number from 0 to 4094 that identifies traffic on your network by VLAN. See <i>Working with VLAN Tag Objects</i> on page 152 for information on creating individual and group VLAN Tag objects using the object manager.
Users	Individual LDAP users and user groups retrieved from a Microsoft Active Directory Server. See <i>Understanding LDAP Authentication</i> on page 1709 for information on specifying and retrieving the users and groups you want to use for user control.
Applications	Applications provided by Sourcefire, user-defined applications, and application filters you create using the object manager. See <i>Working with Application Detectors</i> on page 1519 and <i>Working with Application Filters</i> on page 154 for more information.

Access Control Rule Condition Types (Continued)

Condition	Description
Ports	Transport protocol ports, including individual and group port objects you create based on transport protocols. See <i>Working with Port Objects</i> on page 151 for information on creating individual and group transport protocol objects using the object manager.
URLs	Sourcefire-provided URLs grouped by category and reputation, literal URLs, and any individual and group URL objects you create using the object manager. See <i>Enabling Sourcefire Cloud Communications</i> on page 1886 and <i>Working with URL Objects</i> on page 153 for more information.

(D23, pages 366 to 367.

Thus, document D23 discloses the subject-matter of claim 8 except for the indication of the transport layer protocol in the context of access control rules. However, D23 discloses that in the context of intrusion rules, the transport protocol may be used in the rule header (D23, page 921). Moreover, it is noted that packet filtering in firewalls based on this five-tuple, which is also known as flow id to the skilled person, is generally known to the skilled person. Purely by means of example, intervenor refers to document D11, Fig. 21:

FIG.21

IDENTIFYING/PROCESSING POLICY STORING PORTION: DEVICE POLICY (FILTERING SETTING)

14a DEVICE NAME /SERVICE NAME	14b IDENTIFYING POLICY					14c PROCESSING POLICY (FILTERING SETTING)
	14b1 DESTINATION IP ADDRESS (Dst.IP)	14b2 SOURCE IP ADDRESS (Src.IP)	14b3 Protocol	14b4 DESTINATION PORT NO. (Dst.Port)	14b5 SOURCE PORT NO. (Src.Port)	
Media Renderer	*	.	.	.	.	PASS
Media Server	EXTERNAL NETWORK (INET)	*	.	.	.	DISCARD
:						:

Thus, the subject-matter of claim 8 is not inventive over D23 alone and D23 in view of the common general knowledge of the skilled person as exemplified by D11.

8. Claim 9

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

The subject-matter of claim 9 is not novel over D19 or D23. Document D19 devotes an entire chapter to the inspection of application layer header information (Chapter 13: “Using Application Layer Preprocessors”) in the context of preprocessor rules. Note that preprocessors can also be updated automatically by the VRT (features 1.1.3 and 1.3.1):

The Sourcefire Vulnerability Research Team (VRT) regularly sends out updates called Security Enhancement Updates, or SEUs, that can contain new intrusion rules, decoders, and preprocessors and other intrusion detection and prevention features, so you can be sure that you are detecting the most recently released attacks.

(D19, page 254).

Moreover, intrusion rules can also be used to inspect application layer header information:

Inspecting Application Layer Protocol Values

Platform: DC/MDC/Standalone Sensor

Component: IPS

Although preprocessors perform most of the normalization and inspection of application layer protocol values, you can continue to inspect application layer values using the keywords described in the following sections:

- [RPC](#) on page 828
- [ASN.1](#) on page 829
- [urilen](#) on page 830
- [DCE/RPC Keywords](#) on page 832

(D19, page 828, emphasis added; note that the page is in the section:

“Understanding and Writing Intrusion Rules”).

For example, a URI may be inspected using the keyword “*urilen*” (see next section; D29, pages 830 and 831).

Document D23 comprises the same disclosure insofar as D19, except that it goes even further and includes further keywords for application-layer value inspection by intrusion rules:

Inspecting Application Layer Protocol Values

LICENSE: Protection

Although preprocessors perform most of the normalization and inspection of application layer protocol values, you can continue to inspect application layer values using the keywords described in the following sections:

- RPC on page 988
- ASN.1 on page 989
- urilen on page 990
- DCE/RPC Keywords on page 991
- SIP Keywords on page 996
- GTP Keywords on page 1000
- Modbus Keywords on page 1017
- DNP3 Keywords on page 1020

(D23, page 988, emphasis added).

Thus, the subject-matter of claim 9 is not novel over D19 or D23.

9. 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).*

- a. The subject-matter of claim 9 extends beyond the application as filed and the parent application as filed, at least because the application and parent application as filed do not disclose the dependency of claim 9, being dependent on any of claims 1 to 8. Claims 1 to 8 do not relate to “*application-layer packet-header information*”.
- b. The subject-matter of claim 10 is not novel over D19 or D21. D19 discloses:

urilen**Platform:** DC/MDC/Standalone Sensor**Component:** IPS

You can use the **urilen** keyword in conjunction with the HTTP Inspect preprocessor to inspect HTTP traffic for URIs of a specific length, less than a maximum length, greater than a minimum length, or within a specified range.

After the HTTP Inspect preprocessor normalizes and inspects the packet, the rules engine evaluates the packet against the rule and determines whether the URI matches the length condition specified by the **urilen** keyword. You can use this keyword to detect exploits that attempt to take advantage of URI length vulnerabilities, for example, by creating a buffer overflow that allows the attacker to cause a DoS condition or execute code on the host with system-level privileges.

(D19, pages 830 and 831, emphasis added; note that the page is in the section: “*Understanding and Writing Intrusion Rules*”)

Similarly, document D23 discloses:

urilen**LICENSE:** Protection

You can use the **urilen** keyword in conjunction with the HTTP Inspect preprocessor to inspect HTTP traffic for URIs of a specific length, less than a maximum length, greater than a minimum length, or within a specified range.

After the HTTP Inspect preprocessor normalizes and inspects the packet, the rules engine evaluates the packet against the rule and determines whether the URI matches the length condition specified by the **urilen** keyword. You can use this keyword to detect exploits that attempt to take advantage of URI length vulnerabilities, for example, by creating a buffer overflow that allows the attacker to cause a DoS condition or execute code on the host with system-level privileges.

(D23, page 990, emphasis added; note that the page is in the section: “*Understanding and Writing Intrusion Rules*”)

Thus, the subject-matter of claim 10 is not novel over D19 or D23.

10. 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.*

- a. The subject-matter of claim 11 extends beyond the application as filed and the parent application as filed. Claim 11 was added with the (then) applicant's response of April 3, 2020 from scratch:

11. The method of any one of claims 1-10, further comprising:
~~routing, by the packet security gateway and on a packet-by-packet basis, to a monitoring device each of the one or more packets corresponding to the at least one packet matching criterion in response to the performing the packet digest logging function~~
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.

The application as filed (document D5) and the parent application as filed (document D6) do not disclose anywhere the presence of more than one malicious traffic information and correlating two (different) malicious traffic information. Par. [65] of D5/D6 discloses, on the contrary, the correlation of updates from “services”, which refers back to the previous sentence and relates to a “*malicious host tracker service 508 and/or one or more other services*”:

“For example, 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). For example, a network address received from host tracker service 508 may be a duplicate of a network address received from another (e.g., different) service (e.g., a range of network addresses received from host tracker service 508 may overlap with a range of network addresses received from another service)” (D5, par. [65], emphasis added).

Neither par. [65] not anywhere else in D5 or D6 is it discloses that the other “service” provides second “malicious traffic information”.

Moreover, neither D5 nor D6 disclose that second malicious traffic information is correlated with first malicious traffic information in order to perform a packet digest logging function as claimed. As shown above for claim 1, creation or alteration of rules is not disclosed in combination with a packet digest logging function even generally, and especially not in the context of the very specific correlation required by claim 11.

Thus claim 11 does not comply with Articles 123(2) and 76(1) EPC.

- b.** The subject-matter of claim 11 is also not novel over D23. D23 discloses that second malicious traffic information (e.g. a ZeUs blacklist) is “*correlated*” with the Sourcefire Intelligence Feed in order to “*augment the Sourcefire Intelligence Feed with other regularly-updated reputable whitelists and blacklists on the internet*”:

Working with Custom Security Intelligence Feeds

LICENSE: Any

Custom or third-party Security Intelligence feeds allow you to augment the Sourcefire Intelligence Feed with other regularly-updated reputable whitelists and blacklists on the internet. You can also set up an internal feed, which is useful if you want to update multiple Defense Centers in your deployment using one source list.

When you configure a feed, you specify its location using a URL; the URL cannot be Punycode-encoded. By default, the Defense Center downloads the entire feed source on the interval you configure, then automatically updates its managed devices.

(D23, page 147, emphasis added).

In one example a feed concerns a so-called Zeus blacklist:

Managing Feeds and Lists

You create and manage Security Intelligence lists and feeds, collectively called Security Intelligence objects, using the object manager's Security Intelligence page. (For information on creating and managing network objects and groups, see Working with Network Objects on page 140.)

Update Feeds Add Security Intelligence Filter		
Name	Type	
Global Blacklist	List	 
Global Whitelist	List	 
MyCompany Whitelist <i>Last Updated: 2012-05-17 07:21:53</i>	List	 
Sourcefire Intelligence Feed <i>Last Updated: 2012-05-17 06:58:22</i>	Feed	 
Zeus Blacklist <i>Last Updated: 2012-05-17 07:48:05</i>	Feed	 

(D23, page 143, emphasis added).

- c. The subject-matter of claim 11 is also not inventive over D19 in view of the general knowledge of the skilled person for essentially the same reasons given above for claim 1. In particular, it was not only known but “Taxii”, had been specifically developed before the priority date “to standardize the trusted, automated exchange of cyber threat information” (see, e.g. D28, page 1) and allows multiple subscriptions to malicious host tracker services (see D28, page 3, F1) which implies the “correlation” of malicious traffic information from multiple services (which is simplified by Taxii because of the standardization of the way in which malicious traffic information is exchanged). Further reference is made to **section G.1.c.** to avoid repetitions.

11. 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.*

- a. Claim 12 extends beyond the application as filed (document D5) and the parent application as filed (document D6). It was drafted from scratch with the (then) applicant's response dated April 3, 2020:

12. The method of any one of claims 1-11, wherein the packet transformation function comprises an accept packet transformation function; and
 wherein the performing the packet digest logging function comprises:
 forwarding, by the packet security gateway, the each of the one or more packets corresponding to the at least one packet matching criterion toward its respective destination; 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.

Neither D5 nor D6 discloses 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. On the contrary, the D5 and D6 only disclose a routing in combination with an “*accept*”:

five-tuple

300

Rule #	Protocol	Source Address	Source Port	Destination Address	Destination Port	Action
1 (302)	TCP	140.*	*	130.*	20	Accept
2 (304)	TCP	140.*	*	*	80	Accept
3 (306)	TCP	150.*	*	120.*	90	Accept & Route to Monitoring Device
4 (308)	UDP	150.*	*	*	3030	Accept
5 (310)	*	*	*	*	*	Deny

FIG. 3

Fig. 15: D5/D6 Fig. 3. Red box added.

Therefore, D5 and D6 were impermissibly treated as a reservoir to artificially create a new embodiment contrary to the requirements of Articles 123(2) and 76(1) EPC.

- b. The subject-matter of claim 12 is also not novel over D19 or D23.

Document D19 discloses that a “drop rule” is set up that simultaneously drops the packet and creates an intrusion event, thus also creating a “record comprising the subset of information” (features 1.2.3 to 1.2.5) and routing the packet to the monitoring device, i.e. the Defense Center (feature 1.2.6):

Setting Drop Behavior in an Inline Deployment

Platform: DC/MDC/Standalone Sensor

Component: IPS

A *drop rule* is an intrusion rule or preprocessor rule whose rule state is set to Drop and Generate Events. You can use the **Drop when Inline** option in your intrusion policy to determine how IPS handles drop rules in an inline deployment; see Setting Rule States on page 435 for information on setting rule states in your intrusion policy.

[...]

When you set your intrusion policy to drop packets in an inline deployment, and you apply your policy to a detection engine on a Sourcefire 3D Sensor with an inline or inline with failopen interface set, IPS drops packets that trigger enabled drop rules and generates events for the triggered rules.

(D19, pages 358 and 359, emphasis added).

Document D23 similarly discloses:

Setting Drop Behavior in an Inline Deployment

LICENSE: Protection

A *drop rule* is an intrusion rule or preprocessor rule whose rule state is set to Drop and Generate Events. You can use the **Drop when Inline** option in your intrusion policy to determine how the system handles drop rules in an inline deployment; see Setting Rule States on page 617 for information on setting rule states in your intrusion policy.

[...]

When you set your intrusion policy to drop packets in an inline deployment, the system drops packets that trigger enabled drop rules and generates events for the triggered rules.

(D23, page 563, emphasis added).

12. 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.*

- a.** Claim 13 extends beyond the application as filed (document D5) and the parent application as filed (document D6). It was added from scratch by the (then) applicant with his response dated April 3, 2020:

13. The method of any one of claims 1-12, wherein the packet transformation function comprises a deny packet transformation function; and
 ——— wherein the performing the packet digest logging function comprises:
 dropping, by the packet security gateway, the each of the one or more packets
corresponding to the at least one packet matching criterion 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.

Neither D5 nor D6 disclose claim 13. Par. [87] of D5/D6 reads:

“For example, security policy management server 120 may receive a security update comprising a set of network addresses (e.g., {network address A, network address B, and network address C} from malicious host tracker service 508 (or a computing device associated therewith) [...] At step 1306, the security policy management server may receive a security update comprising a different set of network addresses from a different computing device. 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)”. (D5/D6, par. [87], emphasis added).

Firstly, par. [87] discloses that network address B and network address C are comprised in both the set {network address A, network address B, and network address C} and the set {network address B, network address C, network address D, and network address E}.

Secondly, par. [87] uses the open wording “*comprises*”, i.e. security update comprising a set of network addresses (e.g., { network address A, network address B, and network address C}). Therefore, the original disclosure in par. [87] does not directly and unambiguously disclose that the “*first set of packet filtering rules do not comprise the indications of the plurality of network addresses*”. The set of network addresses comprising { network address A, network address B, and network address C} is not defined to exclude network addresses D and E.

Thirdly, par. [87] requires that the “*different set of network addresses*” is received “*from a different computing device*”, whereas according to the claim wording, this is not the case (“*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 up-dated malicious traffic information received from the malicious host tracker service*”, feature 1.3.1, emphasis added).

Moreover, par. [87] does not disclose a “*plurality of network addresses*”, in a manner that is inextricably linked to the remaining features of the embodiment that merely two network addresses are not contained in the first set, while two other network addresses are contained in the first set.

b. Claim 13 is not novel over D19 or D23.

Document D19 discloses that updated standard text rules (plural) and shared object rules (plural) are released by the Sourcefire VRT (D19, page 1716). Since, each standard text rule and shared object rule contains at least one network address (see above), the skilled person will understand that the update contains a plurality of new malicious network addresses.

D23 discloses that a Security Intelligence Feed is a “*dynamic collection of IP addresses*” (plural, D23, page 142).

Thus claim 13 is not novel over D19 or D23.

13. 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.*

- a.** Claim 14 extends beyond the parent application as filed (document D6). The parent application as filed does not disclose “*a system comprising at least one processor of a packet security gateway and a memory*”. In particular, the application documents as filed do 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 (features 1.1.3 and 1.3.1). Thus, claim 14 violates Article 76(1) EPC.
- b.** The subject-matter of claim 14 is not novel over D19 or D23.

D19 discloses a system comprising Defense Center and 3D sensor (D19, page 107), which comprises a processor of a packet security gateway (“CPU”, see D19, pages 2050 ff.) and a memory (“disk”, D19, page 2052).

D23 discloses a system comprising Defense Center and 3D sensor (D19, page 163), which comprises a processor of a packet security gateway (“CPU”) and a memory (“RAM”), see, for example, D23, page 90.

- c.** The subject-matter of claim 14 does not comprise an inventive step starting from D32. D32 discloses a system comprising a processor of a packet security gateway (firewalls 146a, 146b; D3, Fig. 3) and a memory, see D32, par. [0117].

14. 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.*

The subject-matter of claim 15 is not novel over D19 or D23. The Sourcefire manuals (D19 and D23) describe the Sourcefire computer program which runs on the Sourcefire system.

The subject-matter of claim 14 does not comprise an inventive step starting from D32. D32 discloses that the process may be implemented in software (D32, par. [0117]).

Tobias Kaufmann
European Patent Attorney

Bardehle Pagenberg Partnerschaft mbB
Patentanwälte Rechtsanwälte
Association No. 1029

Enclosures:

Documents D2 to D38