



European Patent Office
80298 MUNICH
GERMANY

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



MFG Patentanwälte
Meyer-Wildhagen Meggle-Freund
Gerhard PartG mbB
Amalienstraße 62
80799 München
ALLEMAGNE

☐	☐	☐	PATENTANWÄLTE
☐	☐	☐	ERHALTEN / RECEIVED
MFG 10. Jan. 2023			
Frist	PatOrg	MFIPIHCE	

Oral Proceed.	M. 5. 23 st ⁺ M. 7. 23 st - 13.7.8 ⁺
Written Subm ^{do}	M. 5. 23 st ⁺
Draft	✓
report	23. Jan. 2023 st
Date	+ Kdecker 09.01.2023

Reference JRV/81546EP2 20444EPO	Application No./Patent No. 19170936.9 - 1216 / 3550795
Applicant/Proprietor Centripetal Networks Inc.	Vollender 20.1.23 st

Summons to attend oral proceedings pursuant to Rule 115(1) EPC

You are hereby summoned to attend oral proceedings concerning the above European patent as detailed in the box below.

The matters to be discussed are set out in the communication accompanying this summons (EPO Form 2906).

The oral proceedings will be public and will take place before the opposition division

on 11.07.23 at 09.00 hrs (CET) as a videoconference.

The date of the oral proceedings can only be changed for serious reasons (see OJ EPO 2009, 68). If you do not appear as summoned, the oral proceedings may continue without you (R. 115(2) EPC; see also OJ EPO 2008, 471).

Please see Rule 4 EPC as regards the language of the oral proceedings and the decision in Special edition No. 3, OJ EPO 2007, L.1, concerning the filing of authorisations by employees and lawyers acting as representatives before the EPO

The final date for making written submissions and/or amendments (R. 116 EPC) is 11.05.23

IMPORTANT:

Please provide us as soon as possible, preferably on a separate sheet, with the name and telephone number of a person we can contact about the oral proceedings and an email address to which we can send the details for connecting to the videoconference.

Please inform us immediately if you have not received the details for connecting to the videoconference at least ten days before the scheduled date of the oral proceedings.

You can find out more about the technical requirements and supported systems for videoconferences, making test calls and our data protection policy at www.epo.org.

1st Examiner: Pasini, Enrico

Registered Letter

EPO Form 2310Z 07.21 [ORAL03=8888] 23/12/22

ORAL4

to EPO postal service: 23.12.22
page 1 of 2

Patent Owner, Centripetal Networks, LLC - Ex. 2003, p. 1

2nd Examiner: Pohl, Daniel
Chairman: Wolters, Robert

For the Opposition Division



Annexes:
Confirmation of receipt (Form 2936)
Rule 4 EPC (EPC Form 2043)
Communication (EPO Form 2906)

Wichtige Hinweise zur mündlichen Verhandlung

Das Europäische Patentamt verfügt über keine eigenen Dolmetscher. Diese müssen im Bedarfsfall von außerhalb, teilweise sogar aus anderen Ländern, beigezogen werden, was mit einem hohen Aufwand an Kosten und organisatorischen Vorbereitungen verbunden ist. Muss ein Verhandlungstermin kurzfristig abberaumt werden, können Kosten für bestellte Dolmetscher nicht mehr vermieden werden.

Es wird daher gebeten, eine Simultanübersetzung nur bei wirklichem Bedarf in Anspruch zu nehmen. Es wäre wünschenswert, wenn sich die Beteiligten (zweckmäßigerweise gleichzeitig mit der Terminabstimmung) auf die Benutzung einer Amtssprache einigen könnten. Bei Verständigungsschwierigkeiten sind die Mitglieder der Einspruchsabteilung bereit zu helfen.

Nachstehend führen wir den Zeitpunkt auf, bis zu dem die Verfahrensbeteiligten aus organisatorischen Gründen gebeten werden, ihre bevorzugte (abgestimmte) Verhandlungssprache mitzuteilen. Bis dahin bitten wir auch bei Bedarf eine Simultanübersetzung zu beantragen. Regel 4 (1) EPU bleibt hiervon unberührt.

☐ Verfahrenssprache ist **Deutsch**

Von der/dem/den Einsprechenden wurde

☐ Englisch

☐ Französisch benutzt.

Es wird um eilige Mitteilung, möglichst per Online Filing (OLF), gebeten.

Important information concerning oral proceedings

The European Patent Office has no interpreters of its own. When interpreters are needed they have to be brought in from outside, sometimes even from other countries, which is costly and involves considerable organisation. If oral proceedings have to be cancelled at short notice, the cost of interpreters already engaged still has to be borne.

Please therefore make use of simultaneous interpreting facilities only where strictly necessary. If possible the parties should agree on an official language for the proceedings, preferably at the time when they arrange a date. The members of the Opposition Division will be willing to help should any communication problems arise.

For organisational reasons, we ask parties to inform us by the date specified below of their preferred (agreed) language for the oral proceedings. We also ask them to request any simultaneous interpreting required by the same date. This does not affect application of Rule 4(1) EPC.

☒ Language of the proceedings is **English**

The language used by the opponent/s was

☒ English

☐ German

☐ French.

Please inform us urgently, where possible by Online Filing (OLF).

Tres important Procédure orale

L'Office européen des brevets ne dispose pas de son propre service d'interprètes. Aussi faut-il appel le cas échéant à des interprètes de l'extérieur, qui viennent même parfois de l'étranger, ce qui occasionne des frais élevés et demande un grand travail d'organisation. Si la date d'une procédure orale doit être annulée au dernier moment, il n'est plus possible d'éviter les frais d'interprètes.

Les parties à une procédure sont donc priées de ne demander une traduction simultanée qu'en cas de réel besoin. Il serait souhaitable qu'elles puissent se mettre d'accord en même temps qu'elles conviennent de la date sur l'utilisation d'une langue officielle comme langue des débats. Si les parties éprouvent des difficultés de compréhension lors des débats, les membres de la division d'opposition sont disposés à leur prêter leur assistance.

Est indiquée ci-dessous la date jusqu'à laquelle, pour des raisons d'organisation, les parties sont priées de communiquer leur langue préférée (sur laquelle elles se sont préalablement mises d'accord). Les parties sont également priées, le cas échéant, de demander une interprétation simultanée avant cette date. La règle 4(1) CBE ne s'en trouve pas affectée.

☐ La langue de la procédure est le **français**

La langue utilisée par l'opposant/les opposants était

☐ l'allemand

☐ l'anglais.

Prière d'indiquer d'urgence par dépôt en ligne (OLF) si possible.

möglichst bis

Datum 11.05.23

if possible by

Date 11.05.23

si possible jusqu'au

Date 11.05.23

1. welche Sprache(n) Sie in der mündlichen Verhandlung verwenden (**Speak**)

2. aus welcher Sprache Sie eine Simultanübersetzung benötigen (**Hören**).

1. which language(s) you intend to use during the oral proceedings (**Speaking**)

2. from which language you need simultaneous interpretation (**Listening**).

1. quelle(s) langue(s) vous utiliserez au cours de la procédure orale (**pour parler**)

2. à partir de quelle langue vous aurez besoin d'une traduction simultanée (**pour écouter**).

Sollten Sie Ihren Antrag auf mündliche Verhandlung zurückziehen oder zum anberaumten Verhandlungstermin nicht erscheinen wollen bzw. aus wichtigem Grund daran gehindert sein, werden Sie gebeten,

Should you decide to withdraw your request for oral proceedings or not wish to attend on the date set, or if for some special reason you are unable to do so, you are requested

Si vous retirez votre requête tendant à recourir à la procédure orale ou si vous ne souhaitez pas vous présenter à la date fixée pour la procédure orale ou ne pouvez vous y présenter pour une raison sérieuse, veuillez

- unverzüglich das Amt - möglichst per Online Filing (OLF) - davon zu benachrichtigen, wobei das Schriftstück mit einem deutlichen Vermerk "Dringend, mündliche Verhandlung am..." oder sinngemäß gekennzeichnet sein sollte

- to notify the EPO immediately, where possible by Online Filing (OLF), marking the document clearly with the words "Urgent, oral proceedings on ..." or similar

- en faire avis sans retard à l'Office, par dépôt en ligne (OLF) si possible, en partant sur votre communication clairement la mention "Urgent, procédure orale le..." ou une indication similaire;

- in dringenden Fällen (weniger als 1 Monat vor dem Verhandlungstermin) zusätzlich auch dem/die anderen Verfahrensbeteiligten bzw. ihre(n) Vertreter auf schnellstem Weg direkt zu unterrichten.

- in urgent cases (less than one month before the date set for the proceedings), additionally to notify the other party/parties and/or their representative(s) direct as rapidly as possible.

- dans les cas urgents (moins d'un mois avant la date fixée pour la procédure orale) en faire avis également directement pas la voie la plus rapide à autre/aux autres partie(s) ou bien à son/leurs mandataire(s).

In jedem solchen Fall obliegt der Einspruchsabteilung die Entscheidung, ob die Verhandlung durchgeführt oder abberaumt wird. Es wird jedoch darauf hingewiesen, dass einem Verfahrensbeteiligten, der eine nicht rechtzeitige oder unterbliebene Benachrichtigung zu verantworten hat, die dadurch den anderen Beteiligten verursachten Kosten auferlegt werden können (Art. 104 EPÜ).

In all such cases the Opposition Division will decide whether the proceedings are to go ahead or be cancelled. You should however note that costs incurred by the other parties may be charged to a party who either fails to notify them or does not do so in good time (Article 104 EPC).

Il appartient alors à la division d'opposition de décider si la procédure orale aura lieu ou non. Il est néanmoins souligné que les frais causés aux autres parties par une partie qui est responsable de l'omission d'un tel avis ou de ce que cet avis n'a pas été fait en temps utile peuvent être mis à la charge de cette partie (art. 104 CBE).

Hinweis auf Regel 4 EPÜ

Attention is drawn to Rule 4 EPC

Rappel de la Règle 4 CBE

Regel 4

Sprache im mündlichen Verfahren

Rule 4

Language in oral proceedings

Règle 4

Langues admissibles lors de la procédure orale

(1) Jeder an einem mündlichen Verfahren vor dem Europäischen Patentamt Beteiligte kann sich anstelle der Verfahrenssprache einer anderen Amtssprache des Europäischen Patentamts bedienen, sofern er dies dem Europäischen Patentamt spätestens einen Monat vor dem angesetzten Termin mitgeteilt hat oder selbst für die Übersetzung in die Verfahrenssprache sorgt. Jeder Beteiligte kann sich einer Amtssprache eines Vertragsstaats bedienen, sofern er selbst für die Übersetzung in die Verfahrenssprache sorgt. Von diesen Vorschriften kann das Europäische Patentamt Ausnahmen zulassen.

(1) Any party to oral proceedings before the European Patent Office may use an official language of the European Patent Office other than the language of the proceedings, if such party gives notice to the European Patent Office at least one month before the date of such oral proceedings or provides for interpretation into the language of the proceedings. Any party may use an official language of a Contracting State, if he provides for interpretation into the language of the proceedings. The European Patent Office may permit derogations from these provisions.

(1) Toute partie à une procédure orale devant l'Office européen des brevets peut utiliser une langue - officielle de l'Office européen des brevets autre que la langue de la procédure, à condition soit d'en aviser l'Office européen des brevets un mois au moins avant la date de la procédure orale, soit d'assurer l'interprétation dans la langue de la procédure. Toute partie peut utiliser une langue officielle de l'un des Etats contractants à condition d'assurer l'interprétation dans la langue de la procédure. L'Office européen des brevets peut autoriser des dérogations aux présentes dispositions.

(2) Die Bediensteten des Europäischen Patentamts können sich im mündlichen Verfahren anstelle der Verfahrenssprache einer anderen Amtssprache des Europäischen Patentamts bedienen.

(2) In the course of oral proceedings, employees of the European Patent Office may use an official language of the European Patent Office other than the language of the proceedings

(2) Au cours de la procédure orale, les agents de l'Office européen des brevets peuvent utiliser une langue officielle de l'Office européen des brevets autre que la langue de la procédure.

(3) In der Beweisaufnahme können sich die zu vernehmenden Beteiligten, Zeugen oder Sachverständigen, die sich in einer Amtssprache des Europäischen Patentamts oder eines Vertragsstaats nicht hinlänglich ausdrücken können, einer anderen Sprache bedienen. Erfolgt die Beweisaufnahme auf Antrag eines Beteiligten, so werden die Beteiligten, Zeugen oder Sachverständigen mit Erklärungen, die sie in einer anderen Sprache als in einer Amtssprache des Europäischen Patentamts abgeben, nur gehört, sofern dieser Beteiligte selbst für die Übersetzung in die Verfahrenssprache sorgt. Das Europäische Patentamt kann jedoch die Übersetzung in eine seiner anderen Amtssprachen zulassen.

(3) Where evidence is taken, any party, witness or expert to be heard who is unable to express himself adequately in an official language of the European Patent Office or of a Contracting State may use another language. Where evidence is taken upon request of a party, parties, witnesses or experts expressing themselves in a language other than an official language of the European Patent Office shall be heard only if that party provides for interpretation into the language of the proceedings. The European Patent Office may, however, permit interpretation into one of its other official languages.

(3) Lors de l'instruction, les parties, témoins ou experts appelés à être entendus, qui ne possèdent pas une maîtrise suffisante d'une langue officielle de l'Office européen des brevets ou d'un Etat contractant, peuvent utiliser une autre langue. Si la mesure d'instruction est ordonnée sur requête d'une partie, les parties, témoins ou experts qui s'expriment dans une langue autre qu'une langue officielle de l'Office européen des brevets ne sont entendus que si cette partie assure l'interprétation dans la langue de la procédure. L'Office européen des brevets peut toutefois autoriser l'interprétation dans l'une de ses autres langues officielles.

(4) Mit Einverständnis aller Beteiligten und des Europäischen Patentamts kann jede Sprache verwendet werden.

(4) If the parties and the European Patent Office agree, any language may be used.

(4) Sous réserve de l'accord des parties et de l'Office européen des brevets, toute langue peut être utilisée.

(5) Das Europäische Patentamt übernimmt, soweit erforderlich, auf seine Kosten die Übersetzung in die Verfahrenssprache und gegebenenfalls in seine anderen Amtssprachen, sofern ein Beteiligter nicht selbst für die Übersetzung zu sorgen hat.

(5) The European Patent Office shall, if necessary, provide at its own expense interpretation into the language of the proceedings, or, where appropriate, into its other official languages, unless such interpretation is the responsibility of one of the parties.

(5) L'Office européen des brevets assure à ses frais, en tant que de besoin, l'interprétation dans la langue de la procédure, ou, le cas échéant, dans ses autres langues officielles, à moins que cette interprétation ne doive être assurée par l'une des parties.

(6) Erklärungen von Bediensteten des Europäischen Patentamts, Beteiligten, Zeugen und Sachverständigen, die in einer Amtssprache des Europäischen Patentamts abgegeben werden, werden in dieser Sprache in die Niederschrift aufgenommen. Erklärungen in einer anderen Sprache werden in der Amtssprache aufgenommen, in die sie übersetzt worden sind. Änderungen einer europäischen Patentanmeldung oder eines europäischen Patents werden in der Verfahrenssprache in die Niederschrift aufgenommen.

(6) Statements by employees of the European Patent Office, parties, witnesses or experts, made in an official language of the European Patent Office, shall be entered in the minutes in that language. Statements made in any other language shall be entered in the official language into which they are translated. Amendments to a European patent application or European patent shall be entered in the minutes in the language of the proceedings.

(6) Les interventions des agents de l'Office européen des brevets, des parties, témoins et experts faites dans une langue officielle de l'Office européen des brevets sont consignées au procès-verbal dans cette langue. Les interventions faites dans une autre langue sont consignées dans la langue officielle dans laquelle elles sont traduites. Les modifications apportées à une demande de brevet européen ou à un brevet européen sont consignées au procès verbal dans la langue de la procédure.

I. GENERAL

A. Parties to the Proceedings / Requests

1.

The Proprietor (**P**) of the opposed patent EP 3550B795 B1 is Centripetal Networks Inc.

2.

Against the patent an opposition has been filed:

on 02.03.2022 by the opponent **O1**, Ixia, California corporation

In the present proceedings **notices of intervention** under Article 105(1) EPC were filed by further opponents:

on 23.05.2022 by the opponent **O2**, Cisco Systems GmbH

on 27.05.2022 by the opponent **O3**, Keysight Technologies Deutschland GmbH

on 15.06.2022 by the opponent **O4**, Palo Alto Networks Inc.

3.

O1 requests revocation of the patent in its entirety based on the grounds

- under Article 100(c) EPC, extension beyond the earlier application / original application (Article 76(1) EPC / Article 123(2) EPC).

- auxiliary oral proceedings.

O2, O3, O4 request revocation of the patent in its entirety based on the grounds

- under Article 100(a) EPC, lack of novelty and inventive step (see Articles 52(1), 54 and 56 EPC),

- under Article 100(b) EPC, lack of a sufficient disclosure (see Article 83 EPC)

- under Article 100(c) EPC, extension beyond the earlier application / original application (Article 76(1) EPC / Article 123(2) EPC).

- auxiliary oral proceedings,

- accelerated processing (see GL E-VII, 5 and EPO OJ 2008, 221)

O3 requests exclusion from file inspection of exhibits **D39 and D40** (aka K1 and K2) under Article 128(4) EPC and Rule 144(d) EPC.

4.

P requests to

- reject the oppositions in substance and maintain the patent as granted,

- auxiliary oral proceedings.

5.

In the context of the ground of opposition under Article 100(a) EPC the following testimonies are offered under Article 117(1) EPC:

- Ms. Sarah Ehrig (by O2)
- Mr. Jacob Baugher III (by O2)

B. Uniform numbering of cited documents and of claim-features

1.

The parties are **invited to adhere to this uniform numbering in their further submissions for the rest of the proceedings.**

For the cited documents reference is made to the **EPO consolidated list** which is available in the public file and also annexed in attach. The documents are consecutively re-numbered according to the consolidated list.

2.

The feature numbering first proposed by the parties - here by O2 - is adopted also by the OD.

Claim 1

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 updated 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.

Independent claims 14 and 15 are directed to a system and computer program defined with reference to claim 1.

C. Subject of the oral proceedings.

1.

The subject of the discussion during the oral proceedings will be:

- i) whether the granted claims meet the requirements of Article 100(c) EPC
- ii) whether the granted claims meet the requirements of Articles 100(b) EPC
- iii) whether the granted claims meet the requirements of Article 100(a) EPC.

II. PROVISIONAL NON-BINDING OPINION OF THE OD

The provisional opinion of the OD is provided to underline the points which are of particular relevance for the discussion. This provisional opinion is non-binding, it is not exhaustive and it does not anticipate any decision.

A. Admissibility of the oppositions / interventions

1.

It appears that there is no disagreement among the parties on the issue of admissibility.

The OD is of the provisional view that the opposition of **O1** is admissible (Articles 99(1) and 100 EPC and Rules 3(1) and 76(1)(2) EPC).

The OD is of the provisional view that the interventions of **O2, O3, O4** are also admissible (Article 105(1),(2) EPC and 100 EPC and Rules 3(1) and 76(1)(2) EPC).

B. Extension of subject-matter, Article 100(c) EPC

1.

The opponents (Os) make Article 100(c) EPC objections in particular vs. the parent application **D1**. Os underline that granted claims are not directly corresponding to the original parent claims (see e.g. O2, notice of intervention pages 19-21). The description is identical. O4 fully adopts the arguments presented by O1-O3 but does not submit new ones.

The main objections and reply thereto by the P can be summarized according to the following points.

i)

OPPONENTS: O1 argues that a combination of **logging + routing to a monitoring device** is not disclosed. O1 refers to **feature 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** etc."* and to **feature 1.2.6** *"**routing**, by the packet security gateway, the packet to a **monitoring device** configured to store the packet for subsequent analysis"*.

Logging is disclosed in figure 12 and in paragraphs [0054] and [0084]-[0086]. According to [0054] a packet-log or digest contains selected packet information and packet logs are forwarded. O1 argues that even if forwarding was equated with the claimed routing, what is described is the forwarding of logs / digests whereas the claims covers forwarding the original packet. In addition, the destination being a monitoring device configured to store the packet for subsequent analysis is not disclosed by the logging embodiment in [0054].

Even an alternative basis in [0084]-[0086] does not disclose routing of the original packet but only a message with a subset of the packet. The destination of routing is not a monitoring device but the policy management server. See e.g. [0086].

Forwarding of packets to a monitoring device is instead only mentioned in [0053] but in the different context of multidimensional routing. This however refers to encapsulation with an IP header.

The fact that a monitoring device performs subsequent analysis - as claimed - is also not disclosed. The only analysis disclosed is in [0067]-[0070] with reference to SIP switches including an analysis application. However, the above relates to SIP or voice call related features.

A similar reasoning is proposed by **O2** indicating that **feature 1.2.6** (routing to a monitoring device) is not disclosed in combination with **features 1.2.3 to 1.2.5** (generating and reformatting a record). Generation and reformatting of a record is disclosed in parent claims 15 and 16 and [0086] but this does not disclose routing to a monitoring device. Routing to a monitoring device is disclosed in other embodiments, e.g. [0045], [0053], [0068]-[0071]. The original disclosure distinguishes between a record with a subset of information and routing a complete packet to the monitoring device. These are separate scenarios, there is no disclosure of an embodiment combining both cases.

A similar reasoning is provided by **O3** with reference to **feature 1.2.2 and 1.2.6**. For **O3** there are four problems. The **first** is a generalisation alleging that the only paragraph that discloses the routing of a full packet to a monitoring device for subsequent analysis is [0070] which is part of the description of figure 6. **O3** argues that figure 6 is limited to multi-dimensional routing and encapsulation (see e.g. [0066] and [0070]). Paragraph [0053] discloses a routing of the packet to a monitoring device but fails to mention that this is to store the packet for subsequent analysis, so for **O3** it cannot provide a basis for the claim. Nevertheless, this paragraph would also require multi-dimensional routing and encapsulation. The **second** is that routing of packets is not disclosed as being comprised in the packet digest logging function. The **third** is that routing of packets is not disclosed in combination with logging referring to separate logging disclosure ([0054], [0084]-[0086], figure 12 and OF claims 10-16 of the parent) vs. disclosure of routing of full packets to a monitoring device ([0053] and [0070]) which do not relate to packet digest. The **fourth** problem is the lack of disclosure for routing of the packet that is logged (i.e. "the" packet that matched the packet matching criterion).

O3 adds further remarks with letter of 24.10.2022 arguing that **P** has not provided a basis for a rule as claimed performing logging and also forwarding of the complete packet that is also logged. **P**'s reference to [0041] or [0043] relate at most to a general statement that does not disclose the specific feature. Moreover, based on the subsequent paragraphs this is more likely to mean that the entirety of the transformation functions can provide one or more functions on the packets. The **P**'s cited [0054] and [0084] relate to digest logging, i.e. only a subset of packet info is logged. The **P**'s cited

[0052] and [0068]-[0071] only relate to routing of complete packets. Moreover [0052] does not relate to routing to a monitoring device and [0068]-[0071] relate to VoIP calls with SIP signalling packets being encapsulated and forwarded to a monitoring device. P's cited [0085] and [0086] only relate to packet digest logging.

With letter of 14.12.2022 O3 replies to the interpretation proposed by P with letter of 29.11.2022 about the "*comprising*" feature. O3 replies that the argument is illogical because the packet transformation function "*corresponds*" to the logging function. Thus, it does not matter whether the "*comprising*" is read as referring to the packet transformation function or to the logging function and both cases extend the original disclosure. O3 refers to the common indentation of the features. Moreover, the logging features are related to the routing features. The logging is referred to the packet that matches the filtering rule that specifies logging. The further logging features refer to "*the*" same packet and it is also "*the*" packet which is routed. However, there is no original disclosure that the same packet which is logged is routed to the monitoring device. Page [0045] and figure 3 disclose a combination of accepting and routing, but not a combination of logging and routing. This is also not disclosed in [0046] which is in the context of the order in which rules are processed. P's argument that combining logging and routing would be "*technically sensible*" does not relate to direct and unambiguous disclosure.

PATENTEE: P argues that [0041] discloses that each packet transformation function can perform one or more functions. Since [0041] refers to "*on packets*" P argues that these are multiple functions on the same packet and the packet security gateway can perform one or more packet transformation functions (see [0043]). An example of such functions is packet digest logging (see [0054] and [0084]). Routing packets is also disclosed as exemplary packet transformation function (see e.g. [0052] and [0068]). So P argues that the routing ([0068] to [0071]) and packet digest logging ([0084] to [0086]) are disclosed as exemplary packet transformation function for the same packet security gateway 112. P argues that [0041] is the basis linking these two aspects to be applied to the same packet. P alleges that it is the same packet security gateway 112 that it is used for routing and logging (see respectively [0069] and [0085]).

With respect to the O's citations of [0053] as mentioning forwarding of packets to a monitoring device but not subsequent analysis or the O's citation of [0067]-[0070] disclosing analysis but in the context of SIP-switches P argues that [0070] discloses that the monitoring device is configured to perform subsequent analysis.

As to the alleged **generalisation of routing** P replies (page 13 of P's reply, point VIII) that Os neglect the allegedly general disclosure of [0045] which refers to routing of IP packets containing TCP and having accept packet transformation and in addition routing to a monitoring device, but without mentioning encapsulation or multi-dimensional routing.

P argues further with letter of 29.11.2022 that there is basis for routing a packet to a monitoring device and at the same time generating and reformatting a record of the packet. P refers to Rule 3 of figure 3 being "*accept & route to monitoring device*" in combination with [0045] as the alleged basis for replacing this with any other additional rule other than forwarding or dropping. Examples of such rules are presented throughout the disclosure. [0046] discloses a merging of rules having different transformation functions. P argues that a rule simultaneously comprising logging and routing would be technically sensible. P refers to the lawful interception case.

ii)

OPPONENTS: With reference to **1.2.2 and 1.2.6**, O1 considers that the claimed **routing to a monitoring device being comprised in the logging function** is not disclosed. This further difference applies even if - *arguendo* - one would regard routing of packets to a monitoring device being disclosed in combination with the logging functions.

A similar objection is raised by O2. The original parent do not disclose that one of the plurality of packet transformation functions "*corresponds*" to a "*packet digesting function*". Parent claim 10 and [0086] state that the packet transformation function is "*comprising*" it. Moreover, the routing is not "*comprised*" in the packet digest logging function - as instead per claim 1. The disclosure of the "*digest*" (e.g. OF claims 15, 16 and [0054],[0086]) and the routing of an entire packet to a monitoring device (e.g. [0045], [0053], [0068] to [0071]) are separate.

PATENTEE: P argues that claim 10 and [0084] establish a relation between packet transformation function and packet digest logging function. Thus, the packet transformation function allegedly corresponds to the packet digest logging function. As for point i) above P argues that packet transformation function is configured to perform multiple functions. Paragraph [0086] discloses identifying a subset of information, generating a record and reformatting the subset of information. Since the above paragraph states that these steps "*may*" be included for P it means that other steps are not excluded. P again refers to [0041] stating that a packet transformation function can perform multiple functions and routing is such a function.

P provides further arguments with letter of 29.11.2022. P argues that the interpretation of the claims should be that in feature 1.2.2 "*and comprises*" should not be referred to the "*packet digest logging function*" but instead to "*at least one of the multiple packet*

transformation function". With this second - proper according to P - interpretation the objections would be overcome. P refers to [0011] and [0048] of the B1 patent mentioning routing as part of the packet transformation function. P refers to the principle of the mind willing to understand in II.E.2.3.3 of the Case Law of the BoA of the EPO.

iii)

OPPONENTS: Automatic creation / alteration of logging filter rules for O1 is not disclosed with reference to features **1.1.3 and 1.2.2**. Automatic creation or alteration of packet filtering rules is disclosed only in [0064] describing figure 5. However this is only in combination with **new network address** associated with malicious traffic being determined. Moreover there is no disclosure of create or adapt automatically the rules corresponding to **logging functions**. Conversely, the logging disclosure in [0054], [0084]-[0086] and figure 12 does not relate to how filtering rules corresponding to logging are created or adapted. There is no original disclosure of automatic creation / adaptation of filter rules corresponding to digest / logging based on malicious traffic information from a malicious host tracker device.

O2 raises a similar point for **features 1.1.3 and 1.2.2** indicating that automatic alteration / creation of rules is only disclosed in [0064] for addresses associated with malicious traffic, not for packet digest / logging. There is no disclosure of automatic alteration / creation for rules relating to generating the record (OF claims 15-16 and [0086]) nor for rules relating to routing to a monitoring device (see [0045], [0053], [0068]-[0071]). Moreover, [0064] only discloses a specific update relating to network addresses, resulting in an intermediate generalisation, citing GL H-V, 3.2.1.

The broadest passages dealing with the creation or alteration of rules ([0049], [0064], [0065], [0087]) do not relate to the generation of records or to routing. Moreover, [0086] relates to the embodiment of figure 12 (packet digest logging) and [0087] relates to the embodiment of figure 13 (security updates).

O3 raises a similar objection, stating that the broad wording of the claim covers the case in which the packet digest logging function is automatically created or altered. Automatic creation / altering of rules is only disclosed in [0064] in the context of figure 5 but the only exemplary filtering is a blocking rule or rules for accounting for VoIP session initiation / termination. Packet logging function rules are only disclosed in the separate [0054] and [0084] to [0086] in combination with figure 12.

O3 adds further remarks with letter of 24.10.2022. The only possible basis for automatic creation / alteration of rules of feature 1.1.3 is [0064]. O3 argues that even if feature 1.1.3 does not define that the automatically generated / altered rule is logging, at least it does not exclude it. [0064] leaves open which rule is altered. A skilled person would apply this generic statement at most to blocking and passing rules for security reasons

but there is no reason to assume that a logging rule must be automatically created or altered. P cited [0041], [0044], [0045] and [0084] but these only relate to the logging function as such.

PATENTEE: P refers to [0064] as alleged basis for disclosing in a general way that rules are updated. Packet transformation functions are defined by rules (see e.g. [0041], [0044], [0045] and [0084]), the latter paragraph [0084] disclosing that rules may specify the packet transformation function relating to digest. Thus, the feature is derivable from [0064] in combination with [0084]. Moreover, [0064] relates to modifying the rules, not the network addresses. Thus for P the network addresses are not required. Moreover [0064] discloses that rules are created or altered "*as new network addresses associated with malicious traffic are determined*", these are then part of updates received from a malicious host tracker service. Thus, for P the feature is disclosed in [0064].

With letter of 29.11.2022 P argues further that [0064] relates to altering a dynamic security policy which includes rules. Paragraph [0054] indicates that a dynamic security policy includes rules which specify a packet transformation function for logging packets. Thus, the rules that are updated comprise the logging rules.

iv)

OPPONENTS: Provision of **awareness service by logging function without accessing logs** by the awareness application is not disclosed, see **feature 1.2.2**

O1 argues that a network communication awareness service is only mentioned in [0054] requiring that "*Awareness application servers may read packet logs...to produce awareness information*", i.e. the awareness service requires that the server reads the packet logs. The claim does not indicate that the network communication awareness service obtains information from the packet logs.

A similar objection is raised by O3 against **feature 1.2.2** with the only basis being [0054]. The paragraph discloses that awareness service is only provided by a "*combination of rules*" without indicating what these rules are. It is also discloses that the rules produce a digest or log of the packet. Still, this does not disclose that the log / digest alone - without any further activity - provides the awareness service. For this it is required that the logs are read and processed. The claim does not state that the logs are sent to awareness application server and read and processed therein. The claim does not state what happens with the log, thus being a generalisation.

PATENTEE: P refers to [0054] that mentions one or more rules the combination of which may implement an informational service for network communication awareness service. These rules may specify a packet transformation function that when applied to a packet matching the rule produces a digest or log of the packet. Then P states that

[0054] indicates that awareness application servers *"may"* read packet logs. Thus, for P reading the logs is optional in order to provide a network communication awareness service.

v)

OPPONENTS: External server not disclosed in isolation, with reference to **feature 1.1** *"a security policy management server external from the network"*. O1 argues that the description does not mention this feature and this is allegedly derivable only from the drawings in which the server is outside of the protected network. However, also the *"malicious host tracker service 508"* is also drawn to be outside of the protected network. So O1 argues that if it is allowed to take the *"external"* feature for the *"security policy management server"* in this way, then the other features of figure 5 cannot be omitted (i.e. external malicious host tracker service).

PATENTEE: P refers to figures 1, 6, 7, 8 of the parent showing the SPM server as external also in absence of a malicious host tracker server. Also paragraph [0064] relates to figure 5 and it does not mention the malicious host tracker service to be external.

vi)

OPPONENTS: Rewording of claim 1: O1 underlines several instances of wordings in claim 1 which were allegedly changed and indicates that such wording is not found in the original application (reference is made to page 10 of the notice of opposition of O1) alleging that this would correspond to a shift in meaning and generalisation.

PATENTEE: P replies that a mere rewording is not relevant and the point is what technical information a skilled person derives directly and unambiguously.

vii)

OPPONENTS: No disclosure of a **subset of information specified by the packet** as in **feature 1.2.4**. O2 argues that the parent application only discloses generating a record with a subset of information specified by the packet digest logging function e.g. with reference to claim 11 as filed. The same applies with reference e.g. to claims 13 to 16 or to [0086] of the parent.

PATENTEE: P argues that the claim wording *"subset of information specified by the packets"* indicates that the subset of information is in the packet. This corresponds to parent claim 12 indicating that the subset information is *"from the packet"* or *"of the packet"*. The same information is listed in [0054].

viii)

OPPONENTS: No disclosure of **performing** packet filtering **by performing** packet transformation functions as in **features 1.2 to 1.2.2**. The claims requires that packet filtering is performed at least partly by performing a packet digest logging function. In the earlier application the concept of "*packet filtering*" is only associated with the simpler packet transformation function being forwarding vs. dropping (see e.g. [0041]). This is also technically meaningful because a logging function is not the same as filtering to protect a network from malicious traffic. A packet digest logging function is not disclosed in the context of packet filtering (see e.g. OF claims 10, 11, 13-16, figure 12, [0084]-[0086] and [0054]). The content of an application is not a reservoir from which features from separate embodiments could be combined. O2 refers to Case Law of the BoA of the EPO, II-E, 1.6.1.

PATENTEE: P argues that packet filtering is based on packet filtering rules as disclosed throughout the application e.g. in [0074]. The fact that filtering based on filtering rules also includes performing at least one packet transformation function is also disclosed e.g. in figure 3 and corresponding description in which the packet transformation functions are disclosed ("*Action*") as part of the rules. O2's assertion that packet filtering only relates to forwarding or dropping is incorrect. The parent in [0040], [0041] discloses that the packet security gateway examines packets with a filter and sends them to a corresponding packet transformation function (which can perform one or more functions). As previously explained, one of such functions is packet digest logging. Thus, packet filtering is not disclosed only in connection with forwarding / dropping.

ix)

OPPONENTS: No disclosure of **first and second set of rules comprised in a security policy** referring to **features 1.1 and 1.3**. O3 alleges that a subdivision of packet filtering rules in two "*sets*" relating to initial and updated packet filtering rule forming part of a dynamic security policy is not disclosed. O3 argues that rule-sets are only disclosed in other contexts, i.e. merging (see in particular [0046]), time-shifted execution (see [0050]), rule-sets for enqueueing service (see in particular [0051]) and rule-sets for combinations of external and internal hosts (see [0057]).

PATENTEE: According to the claim feature 1.3.1 the second set of rules comprises an update to the first set of packet filtering rules. Thus, there is an initial set of rules which is then updated. There is no subdivision into a first and second set of packet filtering rules after the update. The update is disclosed throughout the original disclosure e.g. [0087].

x)

OPPONENTS: No disclosure of a **packet matching criterion specified by more than one filtering rule**. O3 argues with reference to **feature 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". O3 alleges that the second alternative, i.e. packet filtering rule with a packet matching criterion specified by a plurality of packet filtering rules is not disclosed.

PATENTEE: P refers to the basis being in [0046] stating that *"two or more rules within dynamic security policy may specify overlapping criteria"*. Thus, for P this discloses that more rules specify the same matching criterion.

xi)

OPPONENTS: Receiving updated filtering rules at the packet security gateway and filtering packets with updated filtering rules as in **features 1.3, 1.3.1 and 1.4**. O3 argues that the application only discloses that the security policy management server receives updates from a malicious host tracker service and/or more other services (see [0064]-[0065]).

PATENTEE: P refers to [0040] stating that the packet filter performs packet filtering on packets received by the packet security gateway. Thus, packet filtering is performed based on the rules of the dynamic security policy (see in particular [0041]). Thus, when the dynamic security policy is updated, filtering is performed with the updated rules.

2.

OPPONENTS: The Os also object to the original disclosure of the **dependent claims**.

Claim	Objections by Os / Reply arguments by P
2	O1 objects that <i>"a network address associated with <u>an indication</u>"</i> of malicious traffic is not disclosed P replies that [0015] of the parent discloses that network addresses are associated with malicious network traffic.
3	O1 and O2 object that a <i>"network protective action"</i> is a non disclosed and is a generalisation (e.g. of dropping, forwarding packet etc.) P replies that [0043] that PSG may perform one or more packet transformation functions and may be used to <i>"both protect"</i> a network from malicious network traffic and prevent malicious traffic from leaving it.
4	O1 objects that the parent application only discloses placing packet in different queues <u>based on network addresses</u>, which is omitted.

	O2 objects to this not being derivable from [0010] or [0051] and arguing that the rules of claim 1 relate to packet filtering and not to enqueueing service, these being different embodiments. P replies that [0051] discloses an arbitrary selector corresponding to parameters or fields associated with a packet, e.g. a DSCP selector corresponding to a DSCP field in a header. Two identical packets of the DSCP field may be queued in two different queues. As to the objection of O2 replies that this is defined in claim 4 as functionality of the PSG, not of the logging or routing. P refers to [0010].
5	O1 objects that the basis is [0014] which requires that the interface performs <u>simultaneously</u> a packet transformation function at the network layer. O2 objects that a network layer transparent manner is allegedly not disclosed in combination with the logging and routing, noting that [0042] states that for network layer transparent manner attack-packets <u>cannot</u> be routed to network interfaces. P replies that [0042] relates to network layer transparent manner without mentioning "<i>simultaneously</i>". Moreover, to the objection of O2, P refers to [0014] alleging that it discloses that the PSG in network layer transparent manner can send (route) traffic at the link layer using an interface not addressed at the network layer.
6	O1 objects that the claim defines that the "<i>network communications awareness services comprises a network security awareness service etc.</i>" whereas these three services are disclosed at the same hierarchical level in [0054] P replies that a hierarchical functionality is allegedly encompassed by the "<i>and/or</i>" on [0054].
7	O1 objects that the claims refer to the organisation that operates the network whereas [0054] refers to a "<i>secured</i>" network. P replies that claim 7 is dependent on claim 1, which already defines that the network is protected by the packet security gateway.
8, 9	O1 objects that a packet matching criterion as in the claim is not disclosed.

	P replies referring to the original claim 17 of the parent application which defined such five-tuple.
10	O1 objects that "<i>one or more <u>FDQN</u> or URI</i> " is not disclosed. P replies that a FDQN is a portion of the URL which is a type of URI. Paragraph [0044] refers to HTTP and URI. So, [0044] discloses a FDQN.
11	O1 objects that no "<i>second malicious traffic information</i>" is disclosed. O2 objects that there is no correlation of two different malicious traffic information referring to [0065]. P refers to [0052] and to [0064]-[0065] stating that the security policy management server receives updates from a malicious host tracker server and one or more other services and these services are correlated.
12	O1 objects that there is no disclosure of dropping packets of a second set of filtering rules. O2 objects that there is not combination of dropping with features 1.2.3 to 1.2.5 and 1.2.6. Figure 3 at most discloses routing + accept. P refers to [0087]-[0089] and [0083] mentioning a "<i>deny packet transformation function</i>" that drops packets. As to O2 objection, P replies that claim 12 does not define that packet digest log and routing are to be combined with dropping but merely requires dropping the packets based on the second set of filtering rules.
13	O1 objects that this claim contains a negative feature that is not disclosed. O2 objects that the subject-matter of the claim is not disclosed, referring to [0087], since the "<i>do not comprise</i>" feature is not disclosed and the description requires reception "<i>from a different computing device</i>". P refers to 1314 of figure 13 indicating to update the rule to include "<i>other network address(es) included in the different set of network addresses</i>" and to the procedure of [0087]-[0088]. To the objection of O2 P replies that [0087] states that the "<i>computing device</i>" may be associated with the malicious host tracker service, so for P the update is received - at least indirectly - from the malicious host tracker server.

14	O2 objects that there is no disclosure that the processor of the PSG causes <u>the whole system</u> to perform the claimed operations. P states that O misunderstands the claims because the steps are in fact performed by the packet security gateway. Alteration and creation of rule is instead done by the security policy management server. [0039] discloses the PSG with processor and memory.
----	---

3.

OPPOSITION DIVISION: The OD reminds that the criterion for assessing extension of subject-matter is that of a direct and unambiguous disclosure (*Gold standard* of the BoA of the EPO, Case Law of the BoA of the EPO Ed. 2022, II.E.1.3.1), either explicit or implicit. While a literal disclosure is not required, implicit disclosure has to be assessed strictly and it means the clear and unambiguous consequence of what is mentioned *expressis verbis*, i.e. what is **necessarily implied** on an objective basis (Case Law of the BoA of the EPO Ed. 2022, II.E.1.3.3). This is different from what is merely obvious to a skilled person in the light of the content of the application. This also applies when considering the originally disclosed feature combinations or the level of generalisation at which the features are disclosed (EPO GL H-V, 3.2.1).

It appears substantially undisputed among the parties that the basis for the amendments cannot be provided by the parent claims and, thus, this has to be found in the rest of the parent specification taken as a whole.

In this respect. A packet transformation function that produces a packet digest or log version is firstly introduced in general terms in [0054]. The claimed features relating to a packet digest logging function are then having the closest resemblance with the embodiment of figure 12 and [0084]-[0086]. The question is thus whether the other features as presently claimed are directly and unambiguously - i.e. explicitly or implicitly but necessarily - disclosed in combination with this specific embodiment.

The provisional view of the OD is as follows for each of the above points.

i)

For the OD the **logging** is introduced in [0054] mentioning a packet transformation function that produces "*a digest version or log of the packets*" which contains "*selected packet information*". Then the PSG "*may store and/or forward packet logs etc.*". This only discloses no forwarding or at most forwarding of the log itself. It appears also undisputed that [0086] also discloses the forwarding of the message "*comprising the subset of information (or a portion thereof)*" to a "*different computing device (e.g. security policy management server)*". While [0054] can be understood to refer to the same functionality disclosed in more detail with respect to figure 12, none of the above

seems to disclose or necessarily require the additional **routing of the very same packet that matched the filtering criteria**. It appears also that a *"monitoring"* application or the routing to a specific *"monitoring device"* is not mentioned in this context.

It also appears undisputed that the **routing embodiment** itself (e.g. [0068] to [0071]) instead mentions **routing of the packets to a monitoring device**. However, this embodiment does not refer to any logging. This embodiment appears indeed to be in unambiguously in the context (see in particular [0066]) of *"performing a monitoring service within a network environment"* which is not mentioned in the other logging embodiment. Moreover, as additionally observed by Os, it appears that if [0068]-[0069] were taken as alleged basis, this is in the specific context of VoIP and SIP signalling. P referred to [0045] as alleged alternative basis without encapsulation / multidimensional routing to a monitoring device, but this is also a more specific case clearly limited to TCP/IP, which is also not claimed (see GL, H-V, 3.2.1).

More relevantly - based on the above - for the OD it appears that the **two "logging" and "routing" embodiments are not - directly and unambiguously - disclosed in combination**. P's argument that the missing link between the two would be unambiguously provided via paragraph [0041] cannot presently be followed. Even if - *arguendo* - it was followed that *"perform one or more functions on packets"* should be interpreted as performing all the multiple functions on the same packet (although the example in [0041] seems to rather disclose alternative packet treatment, i.e. forward to network A, forward to IPsec, drop) still there is no - direct and unambiguous - disclosure that this is to be applied to **the two specific logging and routing functions and in the way claimed**. Also P's argument that the two embodiments would refer to being performed by the same packet security gateway "112" is not convincing. This at most would disclose that the two separate procedures can be performed by the same apparatus but still it does not provide any disclosure that their respective steps are to be intertwined for the same packet in the way presently claimed. Also [0043] provides a generic disclosure.

Similarly, P's reference to figure 3 with a rule *"accept & route to monitoring device"* in combination with [0045] as the alleged basis for the specific case claimed is not followed. Neither figure 3, nor [0045] mention log / digest and it is merely stated in vague terms that *"dynamic security policy 300 may include one or more rules that specify a packet transformation function other than forwarding (accepting or allowing) or dropping (denying) a packet"*. Firstly, this is a **generic** disclosure which refers to the overall policy, not to a single rule. Secondly, even if this was followed and even in combination with figure 3, this still does not disclose - or otherwise require - directly and unambiguously that the rules to be taken are *"forwarding to monitoring device"* specifically combined with *"log / digest"* on the same packet. P's reference to [0046] also

does not go beyond the generic disclosure that multiple rules can be applied in a given order or merged. Neither routing to a monitoring device nor log/digest are mentioned, even less their specific combination.

Thus, it appears that what the P argues is rather an obvious development of the original content of the parent application and not something directly and unambiguously disclosed therein as matter of necessity. **Here the OD presently sees an extension of subject-matter, in particular by an undisclosed mix of original embodiments.**

ii)

Contrary to the view of the P, it is an established principle of claims interpretation that there is no basis for excluding what is literally covered by the terms of a claim and claims have to be assessed according to their broadest technically sensible meaning. It is reminded (see Case Law of the BoA of the EPO, Ed. 2022, II-E, 1.3.9-e) that *"in the interest of legal certainty, all technically reasonable interpretations of an ambiguous claim had to be considered. If one of those interpretations contained matter that extended beyond the content of the application as originally filed, it had to be concluded that there was added subject-matter"*. The OD considers that the manner of visually presenting a claim (i.e. indenting certain features or not) is irrelevant and only the wording of the claim should be considered.

Here the claim can be interpreted in two ways which - as also indicated by P - are that *"and comprises"* can logically and syntactically refer

a) to the *"packet digest logging function"* or - in alternative -

b) to *"at least one of the multiple packet transformation function"*.

Although only the second is the one meant by P, the OD considers that the interpretation in a) is neither unreasonable nor manifestly contradictory and both interpretations are technically meaningful for a skilled person.

The OD at present concurs with the Os that - in the interpretation a) - the *"packet digest logging function"* is not originally disclosed to comprise routing. P's alternative argument that this is disclosed because paragraph [0086] discloses that the logging steps that *"may"* be included and thus other steps - as routing - are not excluded is not followed already in its logical *ratio*. This at most discloses that the logging steps are presented as - formally - optional. It does not disclose that other steps - let alone the specific routing step - are included. Similar arguments as for i) above apply to P's reference to [0041].

In conclusion, the claim can be plausibly interpreted in two technically sensible manners, one of which is not originally disclosed (Article 123(2) EPC). **Here the OD sees an extension of subject-matter.**

iii)

The embodiment of figure 12 and [0084] relates to a specific method involving a *"dynamic security policy"* with rules relating to a packet transformation function comprising a packet digest log function. The same holds for P's reference to [0054]. The meaning of this *"dynamic security policy"* is previously explained in [0064] which is also disclosing that this involves *"automatically create or alter one or more such rules as new network addresses associated with malicious network traffic are determined"*. Thus, the OD provisionally agrees with P that it is directly and unambiguously disclosed that this is the way in which the *"dynamic"* policy of the log / digest embodiment is also to be understood. Here the OD does not see an extension.

The reference to VoIP session initiation / termination at the end of [0064] is clearly presented as example of what *"may"* be provided *"additionally or alternatively"*, nor is this aspect inextricably linked from a technical point of view. Here the OD does not see an extension.

However, it is provisionally agreed with the Os that [0064] - in the context of the claimed malicious network traffic - only discloses that this relates in particular to *"rules that specify a list of network addresses known to be associated with malicious network traffic"* or *"create or alter one or more rules...to block traffic associated with the network addresses received from malicious host tracker service"*. I.e. it appears that this feature is disclosed in combination and inextricably linked with the updated rules for malicious traffic relating to such network addresses. Rules based on other aspects of the malicious traffic seem instead not to be disclosed. For this aspect **the OD here sees an extension of subject-matter**.

In conclusion, there seems to be **an extension of subject-matter by intermediate generalisation**.

iv)

It seems that the Os refer to the described feature that *"awareness application servers may read packet logs... to produce awareness information"*. As initial remark, the OD notes that granted claim 1 seems to define the steps performed by the packet security gateway (see also granted claims 14 and 15 defining that the method is to be performed by processor(s) of the sole security gateway).

Thus, it is questionable whether these steps performed at another entity would pose a limitation and whether their omission is relevant for Article 123(2) EPC. Secondly, it seems that [0054] is in the context of the *"network communications awareness service"* and it discloses that the PSG may *"store and/or forward"* (i.e. possibly just store) the

logs. Finally it seems correct that - as alleged by P - the possible use of awareness servers to read the packet logs is mentioned as an additional implementation option which "may" be used. Here the OD provisionally does not see an extension.

As to the O's objection that [0054] discloses the awareness service only provided by a "combination of rules" it seems that what is mentioned is instead that "a dynamic security policy may include one or more rules, the combination of which may effectuate an implementation of an informal service for performing a network communication awareness service, and/or network security awareness service etc.". I.e. it seems that - apart from the sub-optimal grammatical form - "one" rule is also envisaged. Moreover, it is not apparent that in this passage the "one or more rules" refers exclusively to the "network communication awareness service" - as alleged by Os - rather than to all the possible awareness services together (communication, security, threat) mentioned thereafter. Here the OD does not see an extension.

v)

It appears that the "malicious host tracker service" is indeed external to the protected network and figure 5 does not provide any other disclosure. At present the OD also cannot follow the *ratio* of P's argument referring to other figures in which the malicious host tracker service is absent. These cases are irrelevant for the question of disclosure of its location when instead present. [0065] does not mention the term "external" explicitly but it only mentions the "malicious host tracker service 508" of figure 5.

Still, the OD again notes that the claim defines the method with the steps of "a packet security gateway (112) configured for protection of a network and associated with a security policy management server external from the network". It is thus not apparent to which extent the location of a "malicious host tracker service" separately interacting only with the "security policy management server" - but not directly with the PSG - may pose a limitation to the method performed by the PSG and thus be relevant for Article 123(2) EPC.

Here the OD provisionally does not see an extension.

vi)

The OD agrees with P that, as indicated above, it is an established principle that a merely linguistic difference is not to be equated - *per se* and without further explanations - with an extension of subject-matter.

Here the OD does not see an issue of extension.

vii)

The OD at present agrees with Os that the wording "*identifying a subset of information specified by a packet*" is broadly formulated and - even in the context of the claim read as a whole - does not necessarily mean information contained in the packet that is to be taken as the subset.

I.e. in another technically meaningful interpretation, the claim can indeed be understood to define that information is identified because the packet itself "*specifies*" which information has to be identified, or which subset has to be identified. It appears undisputed that such latter case is not disclosed. **Here the OD sees an issue of extension.**

viii)

For the OD, the claim requires that filtering is "*based on the first set of packet filtering rules by performing*" the following i.e. "*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*" and "*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*".

This defines the operations for the selective treatment of individual packets (filtering) based on rules. The fact that such filtering based on rules involves additional operations defined by the associated packet transformation function (e.g. logging) is considered to be the general principle of the parent application, with which the skilled person is presented directly and unambiguously (see e.g. the P's cited [0074] or figure 3 or [0040]-[0041]). It seems correct that there is no requirement in the parent that "*packet filtering*" is exclusively associated with forwarding or dropping. It is instead disclosed unambiguously that a packet security gateway examines packets with a filter and sends them to a corresponding packet transformation function. I.e. packet filtering indeed takes place in this way "*by performing*" - as claimed - also such operations. It is reminded that literal linguistic basis is not required. Here the OD does not see an issue of extension.

ix)

For the OD the claim literally defines "*an updated second set of packet filtering rules*" wherein "*the updated second set of packet filtering rules comprises an update to the first set of packet filtering rules*" and "*performing... packet filtering ...based on the updated second set of packet filtering rules*".

The OD agrees with P that this appears to clearly define an update to a first set of rules which (not being identical since it is "*updated*") is per definition a different (= "*second*") set. The above seems thus to be derivable directly and unambiguously from the rule update disclosed in the application. It is again reminded that literal disclosure is not

required. It seems that the objection is instead based on identifying passages with a linguistic correspondences for the word "set" rather than the subject-matter of the original application which technically corresponds to the above features (rule update). Here the OD does not see an issue.

x)

With respect to the objection of O that the claimed "*one packet matching criterion specified by one or more packet filtering rules*" (i.e. a packet matching criterion specified by a plurality of packet filtering rules) is not disclosed, the OD is at present instead of the view that P's cited [0046] states that "*two or more rules within dynamic security policy may specify overlapping criteria*" and seems to disclose that more rules may specify the same matching criterion. Here the OD does not see an issue.

xi)

To the OD it seems directly and unambiguously derivable that the security policy management server provides the dynamic policy to the packet security gateway (see e.g. [0062]) and this policy can be made of updated rules based on the malicious network traffic (see e.g. [0064]-[0065]). It is inherent that - since packet filtering is performed based on the rules of the dynamic security policy (see in particular [0041]) - when the dynamic security policy is updated the filtering is performed with the updated rules. Here the OD does not see an issue of extension.

4.

For the **dependent claims** the opposition division is of the following provisional opinion.

Claim 2: Reminding that literal disclosure is not required, it seems to the OD that the parent application discloses (see e.g. [0015]) that the network addresses are associated with malicious traffic, i.e. necessarily with some information (indication) that identifies such traffic as malicious. Here the OD does not see an extension.

Claim 3: For the OD claim 3 requires that one of the packet transformation function performs a "*network protective action*". This seems to correspond to the disclosure of [0043] indicating - with the same level of generality - that the PSG uses the packet filtering and transformation functions for this purpose, i.e. "*to both protect network A 102 from malicious network traffic etc.*" Here the OD does not see an extension.

Claim 4: For the OD it appears correct that claim 4 refers to what the overall "*dynamic security policy specifies*", so this is not necessarily intertwined with the log and routing rules. However, the basis for the claim according to both parties is [0051] which defines a queuing **based on network addresses**. P refers to another alternative case based on an **arbitrary selector / DSCP field in the IP header**. Whatever basis is taken, the claim does not contain any of these original limitations as to the queuing mechanism. **Here the OD sees an extension.**

Claim 5: Also for claim 5 it appears that the functionalities are not defined to be intertwined with the logging / routing packet transformation function, so for this aspect the OD does not see an issue. As to the basis in [0014] this indeed relates to sending and receiving traffic being not addressed at the network layer and to simultaneously performing the packet transformation function at the network layer (i.e. the two functions are performed concurrently). However, it seems correct that an equivalent disclosure is provided in [0042] without this aspect. Here the OD does not see an extension.

Claim 6: To the OD it appears that [0054] only discloses three separate (network communications, network security and network threat) awareness services. It does not disclose - nor it implies - that the network communications awareness service comprises the other services. **Here the OD sees an extension.**

Claim 7: It appears that claim 1 already defines that the PSG is "*configured for protection of a network*" which network is thereby inherently be understood as protected or secured. A literal basis is not required. Here the OD does not see an extension.

Claims 8-9: The basis given by P with reference to a dependent claim of the parent application cannot be followed. As already indicated, the original parent claims do not provide a basis for the presently claimed - different - combination of features. The application is not a reservoir for isolating individual features from other embodiments (here the embodiment represented by the original parent claims). **Here the OD see an extension.**

Claim 10: As also not disputed by P, FDQN and URI are notionally and technically different. [0044] only mentions the use of the URI. **Here the OD see an extension.**

Claim 11: For the OD claim 11 leaves open which entity is meant to perform its steps. Since these are not disclosed to be steps of the PSG, already for this reason it seems that there would be an extension of subject-matter. Moreover, it seems correct that [0065] discloses correlation with "*one or more other services*" but without disclosing or requiring that this "*another service*" also relates to malicious traffic. **Here the OD sees an extension.**

Claim 12: The "*packet dropping*" of claim 12 is "*based on the updated second set of packet filtering rules*" which is an update to the first set of rules wherein - according to claim 1 - one the of the packet transformation functions of "*at least one packet filtering rule*" of the first set of rules indeed relates to digest logging / routing. I.e. according to the literal wording of the claims these can be indeed the same rules. Although [0087] discloses a "*deny packet*" rule as part of a - generic - rule update, it seems that a specific situation as covered by the claims is not disclosed. Also it seems that [0083] relates to packet discarding in a HTTP GET and PUT method and not to rule update. **Here the OD sees an extension.**

Claim 13: Figure 13 seems to disclose an entire flow-chart that only discloses *"different set of network addresses from different computing device"* and to *"determine that the set (see 1308) includes at least a portion of network addresses included in the set of network addresses"*. Then *"other network addresses"* are added to *"rule(s)"*. This seems to be notionally not the same as stating that the whole first set did not comprise the plurality of network addresses. It seems that the claimed feature is thus not disclosed. Also [0087] discloses receiving the different set of addresses only from a *"different computing device"*. The fact that a device may be - additionally - associated with the same malicious host tracker appears not to change the fact that [0087] and figure 13 both seem to clearly require *"receiving security updates from multiple sources"* (opening of [0087]), i.e. not from the same device. **Here the OD sees an extension.**

Claim 14: Although possibly being the result of an unclear formulation, the claim literally defines that the processor of the PSG causes the (whole) system to perform the claimed operations, which has no basis. **Here the OD sees an extension.**

5.

In conclusion: The OD is provisionally of the view that the main request seems to extend beyond the content of the parent application (Article 100(c) EPC).

B. Insufficiency of disclosure, Article 100(b) EPC

1.

OPPONENTS: O3 argues that in **claim 1** the **feature 1.3.1** *"automatically created or altered"* is not sufficiently disclosed. O3 argues that Article 83 EPC would require that all manners of carrying out the invention falling under the claims are disclosed. O3 refers to T2210/16 and GL F-III, 1. O argues that the invention covers a broad field since the claim refers to any *"malicious traffic information"* used for the rule updating whereas the description only relates to a simple example based on blocking certain addresses. The claim instead covers complex and non-obvious manners of determining malicious threats in a network.

O2 argues that **dependent claim 5** is not sufficiently disclosed being not clear how packets can be received transparently to the NW layer at an interface that is not addressed at the network layer and performing a packet transformation function at the network layer.

2.

PATENTEE: P replies that how to recognize malicious sources is not part of **claim 1**. The malicious host tracker service provides the information on malicious threats. Feature 1.3.1 only requires that the security policy management server automatically creates or alters the packet filtering rules based on this information.

As to **dependent claim 5**, P replies that [0014] of the patent discloses to send and receive traffic by using the link layer and to perform packet transformation functions.

3.

OPPOSITION DIVISION: It is reminded (GL F-III, 1) that when assessing sufficiency of disclosure, *"the intrinsic limitations that a sensible reading imposes on the subject-matter of the independent claims must be taken into consideration; in other words the person skilled in the art wishing to implement the claimed invention will exclude any embodiment that is meaningless and not consistent with the teaching of the application (see T 521/12)"*.

With respect to the subject-matter of **claim 1**, the PSG receives the updated rules wherein *"the updated second set of packet filtering rules comprises an update to the first set of packet filtering rules generated by the security policy management server based on updated malicious traffic information received from the malicious host tracker service"*.

It is noted that the question under Article 83 EPC is legally and conceptually separate from the question of extension of subject-matter among others because it involves the common general knowledge and routine experimentation capabilities of a skilled person. As outlined by P, the claim relates to the update of the policy rules based on malicious traffic information. The determination of properties of the malicious traffic by the malicious host tracker service is not in the scope of the claim, as outlined by P.

The skilled person would understand that what is relevant for the PSG is the reception and use of updated rules, whereas their concrete determination may vary according to circumstances. The skilled person would instead exclude those situation in which what the claim explicitly requires is not possible, i.e. establishing certain recognizable properties of the malicious traffic which can be used to generate a packet filtering rule.

For example, a person skilled in network communication protocols will know that other properties of the traffic may normally be considered relevant for packet filtering (e.g. packet size, packet type, the time of the transmissions, the content etc.) and this is not strictly limited only to associated addresses. A skilled person would thus recognize - within its normal knowledge - that various traffic properties for identifying potentially suspicious traffic in a network are possible according to circumstances and what is

relevant to carry out the claimed invention is that such traffic properties information is received from a malicious host tracker and then used for deriving an updated filtering rule, which is then passed to the PSG.

With respect to the subject-matter of **dependent claim 5**, it seems to the OD that a person skilled in network communication protocols would understand that transmission / reception of higher layer packets between devices - i.e. addressing their interfaces - can normally be implemented at a protocol layer lower than the network layer and only the packet transformation function can be then performed at this higher network layer. Multi-layer protocols are normally known and - as indicated by P - also the patent teaches as possible example to use the link layer in this respect.

Thus for the OD the skilled person is not left into doubt as to how carry out the invention.

4.

In conclusion: The OD is provisionally of the view that the ground under Article 100(b) EPC seems not to be prejudicial for the main request.

C. PATENTABILITY, ARTICLE 100(A) EPC / NOVELTY

C1. Lack of novelty vs. D23 = Sourcefire Manual version 5.1.1 of 2012

1.

OPPONENTS: As to the date of public availability of D23 O2 argues that version 5.1.1 has the time stamp of 30.10.2012 on page 2, so this is 18 months before the priority date. O argues that this document was prepared following practices and procedures of Sourcefire Inc. by being saved as non-editable PDF after approval in a specific folder and therefrom made available to production and support department for distribution. Based thereon CD-ROM or DVD with documentation where provided and enclosed with Sourcefire 3D system appliance bought by customers. In parallel it was posted to a website.

As evidence reference is made to **D24** (written testimony of Ms. Sara Ehrig). This also allegedly follows from properties of the Acrobat-PDF file. P provides screenshots in the statement of ground.

The document was offered to customers without restrictions (D23, page 2) and Sourcefire 3D system was sold before the priority date. As evidence reference is made to **D21** (written testimony of Mr. Jacob Baugher III).

The submission of the **original file of D23 in pdf-format is offered as evidence.**

The testimony of Ms. Ehrig and Mr. Baugher **is offered as evidence** under Article 117(1) EPC.

O2 also refers to the preliminary opinion of another OD in a separate case, in which however the date was apparently not contested.

With letter of 13.10.2022 O2 submits an additional affidavit of Mr. Baugher as **D50** stating that an actual sale of Sourcefire 25.02.2014 to FISHNET SECURITY without including any confidentiality obligation and confirming the customary practice of sending the latest version of the system and of the manual.

PATENTEE: P contested that the information in the **D24 and D50** affidavits suffices to prove the public availability date of D23. For D24 (Ms. Herig) P argues that it fails to state whether sales of Sourcefire with D23 version 5.1.1 occurred (e.g. sales numbers). Moreover there is no explanation on how to obtain the login credentials for the D23 manual. For D21 (Mr. Baugher) it is stated that it does not confirm that D23 was shipped to any customers, e.g. no actual facts are given about an actual sale or shipment. Even linking D24 and D21 does not establish that D23 was available before the priority date and these documents do not indicated where Sourcefire appliances could be purchased and whether this was subject to a non-disclosure agreement. In the second letter of 29.11.2022 P addresses the publication date of other documents, discussed again the content of D23 but does not comment the publication date in view of **D50**.

OPPOSITION DIVISION: Company papers - unlike scientific or technical journals - cannot be assumed to have automatically made their way into the public domain. Such cases are not to be decided based on the mere balance of probabilities or simple suppositions. This is to be established based on the particular circumstances and the evidence available considering e.g. also whether customers to whom the document was distributed could be obliged to treat it as confidential. However, it is observed that manuals for software products are these are normally considered as meant for publication (see also the GL G-IV, 7.5.3.2).

Based on the evidence provided by the Ehrig sworn statement in **D24** it is considered at present to be derivable that Ms. Ehrig testifies that D23 was created in 2012 - as consistently indicated with the date on the document - and that according to standard Sourcefire procedures it was to be included in the packaging with each SF 3D system appliances. Based on the evidence provided by the **second** Baugher sworn statement in **D50** (see point 7) it is presently considered to be derivable that Mr. Baugher testifies that an actual commercial sale including the User Guide v5.1.1 - which is here cited as D23 - was made on 25.12.2014 which did not include confidentiality obligations for the customer's normal use. With respect to the P's initial concerns on D24 + D19 (**first** Baugher sworn statement) it seems therefore to the OD that these were addressed in the second affidavit **D50**. As to the alternative retrieval using login and password it is

instead agreed with P that this has not been fully clarified. However, at least a public disclosure would be provided by the FISHNET SECURITY sale with version 5.1.1 before the priority date mentioned in **D50**.

2.

OPPONENTS: Disclosure of D23. The Os arguments can be summarized as follows.

Features 1.1, 1.1.1 and 1.1.2: **O2** refers to the Sourcefire Defense Center and to blocking traffic on managed devices based on multiple criteria (see page 36 and 37). With reference to figure 3 on page 163, **O2** argues that the "*Defense Center*" is the security policy management server which sends "*policies*" to the "*managed device*" which is equated with the PSG of the claims. The "*Defense Center*" is located externally as visible in figure 4 on page 165. The policy in figure 3 comprises "*access control*" and this specifies "*security intelligence*" (see page 2131) which **O2** equates with a first set of packet filtering rules, referring also to page 2131 which states that the access control policy may include "*multiple access control rules*". The access control rules on page 2131 "*may perform simple IP address matching or may characterize complex connections*" and the "*security intelligence feed*" on page 2152 is a "*dynamic collection of IP addresses that the system downloads on a regular basis*" and this is "*to filter your network traffic*".

Feature 1.1.3: **O2** refers to the fact that the "*Defense Center*" (= security policy management server) receives a Security Intelligence Feed which is a dynamic collection of IP addresses (being the malicious traffic information of the claim) which is received from a HTTP or HTTPS server (being the malicious host tracker device of the claim). This is used to automatically update the managed devices (= PSGs of the claim). The Security Intelligence Feed is used to build blacklists (see page 142). This can be the feed provided by the Sourcefire VRT but it is possible to add third party feeds to augment the Sourcefire Intelligence Feed (see e.g. page 147). In an example the feed is a "*Zeus blacklist*" (page 143). Automatic creation as claimed encompasses receiving subscription based updates as in D23. Thus the rules are automatically created by the Defense Center based on the Zeus Blacklist (= information from a malicious host tracker service).

Features 1.2 and 1.2.1: **O2** refers to page 146 disclosing that based on the Security Intelligence Feeds the collection of IP addresses is up-to-date information to "*filter your network traffic*". Packet-by-packet filtering is disclosed by D23 reference to the Access Control with "*access control rules in an access control policy*" which permits "*to specify, inspect and log the traffic that can enter your network, exit it or travel within it*" and this includes "*a rule action that is whether to trust, monitor, block or inspect matching traffic*" (see in particular pages 38 and 39).

Features 1.2.2: O2 refers to the claimed feature of a packet transformation function being a packet digest logging function that provides a network communications awareness service. The Access Control policy is associated with an access control rule (= a packet filtering rule) and this is used *"to inspect matching traffic"*, i.e. *"inspect and log the traffic"* (see pages 38 and 39). The *"Intrusion Detection and Prevention"* discloses that matching traffic is analyzed with an intrusion policy and this can be associated with an action of the access control policy (see in particular page 39). For such intrusions which are packet-based events, a copy of the packet that triggered the event is recorded (see in particular page 469).

Features 1.2.3 to 1.2.6: O2 refers to the group of features of identifying a subset of information from the packet matching a rule specifying a digest logging function, which is reformatted with a logging-system-standard and routed to a monitoring device for subsequent analysis. As discussed above a copy of the event is recorded. O2 indicates that the alerts of D23 can be reformatted e.g. in *"syslog"* format (see e.g. page 469 bottom to page 470 top) which is also mentioned in the patent. The intrusion events can be inspected and this includes the reformatted information. Reference is made to *"Viewing Intrusion events"* indicating that the packet view provides *"general information on the packet such as its size"* (pages 478-479).

For the specific aspect of the subset of information specified by the packet as claimed (feature 1.2.3) this is e.g. the source and destination IP addresses (see page 480 and following, e.g. 481 or also the address and port of the table on page 489).

Finally, the intrusion event including the packet is forwarded to the Defense Center (= feature 1.2.6) on page 498 referring to the packet view on a Defense Center which has the buttons *"download packet / download all packets"*. As derivable in connection with page 469, packets are routed to the Defense Center which is configured for storing and thus represents a monitoring device.

Feature 1.3, 1.3.1 and 1.4: O2 refers to the claimed features 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 by the Security Intelligence Feed *"takes effect"* after *"a few minutes"* (see in particular page 142 and page 2152 for the definition of the regular updates by Security Intelligence Feed) so this implies a second set of rules applied for subsequent filtering on a second portion of the packets (those arriving after few minutes).

PATENTEE: P contests the disclosure of the following features.

Feature 1.1.3 and feature group 1.3 + 1.3.1. For **feature 1.1.3** P indicates that the *"Security Intelligence"* was seen by O as the first set of packet filtering rules but P objects that the Security Intelligence is not a packet filtering rule. The access control policy contains the Security Intelligence as a component which is separate from the

access control rules (see the figure of page 311 showing separate blocks). The Security Intelligence block results in blacklisting predetermined IP addresses *"before the traffic is subjected to analysis by access control rules"* (see page 1251).

For P then also the *"Access Control"* rules do not correspond to feature 1.1.3 because they are not associated with malicious traffic information and also not transferred from the Defense Center to a managed device. O2 referred to page 2131 to argue that the Access Control includes Security Intelligence. P replies that a transfer of the Security Intelligence from Defense Center to the managed device is not described. It is at most disclosed that it can be used to manually build blacklists directly on the device (see page 142). The same applies to the update of the Security Intelligence which is said not to require *"reapply access control policies after you create or modify a feed"* (see page 142). Thus, there is no update of packet filtering rules by the policy management server then sent to the PSG.

As consequence of the above P also contests the disclosure of rule update as in **feature group 1.3 + 1.3.1**.

P contests disclosure of **feature 1.2.5** alleging that the syslog formatting of D23 is disclosed not as part of packet filtering rules, referring to the statement *"outside of your intrusion policies"* in page 905 of D23. For P when creating an intrusion event the information of a packet is not reformatted according to the syslog format. Messages about the intrusion are sent in syslog but this is outside of the intrusion policy and its packet filtering rules.

P contests disclosure of **feature 1.2.6**. P states that according to the claim-wording the forwarded packet must be *"the"* (same) one that matched the filtering rule. P refers to the cited passage on page 469 of D23 stating that it does not disclose that copies of events are forwarded and notes that the Defense Center was already equated with the Security Policy Management Server.

With letter of 29.11.2022 P adds further remarks. Packets blacklisted by Security Intelligence (figure of page 311) are blocked and not forwarded. So P concludes that an intrusion policy is not applied to packets blacklisted by the Security Intelligence. So there is no logging and routing of packets resulting in lack of disclosure of **all the features 1.2.3 to 1.2.6**.

OPPOSITION DIVISION:

The features on which the parties disagree are **1.1.3, 1.3 + 1.3.1 and 1.2.3 to 1.2.6**.

Feature 1.1.3: The OD presently agrees with the O that the *"Security Intelligence"* seems to be a packet filtering rule. The cited passages (e.g. page 2131) state that the access control policy may include *"multiple access control rules"* and it includes the *"Security Intelligence"*. This is confirmed by the figure of page 311 cited by P which

shows an *"incoming packet"* which is either *"traffic blocked"* or *"not black listed"* and forwarded by the *"Security Intelligence"* block i.e. there is a rule to filter incoming packets based on the address, which would be understood as a filtering rule. The claim does not exclude packet filtering based on the address and also the passage cited by P on 2151 mentions *"Security Intelligence filtering"*. As discussed by P the *"Security Intelligence"* is associated with malicious traffic update. Despite the P's view it also presently seems that page 142 literally refers to *"Security Intelligence feed"* and states that *"when the Defense Center downloads updated feed information it automatically updates managed devices"* i.e. this would be transfer of the *"Security Intelligence"* information from the Defense Center to the managed device. It seems that what may be manually performed is an alternative operation which is not using the above automatic feed and instead is based on the disabling of automatic updates or a manual Security Intelligence list. Here the OD presently does not see a difference.

For **feature 1.2.5** it seems that in D23 syslog messages can be generated in case of intrusion policy events (see e.g. page 905) but it appears that it is not disclosed that these are built by reformatted portions of the packet itself and that this is part of the policy. It is at most stated that these can be *"connection events logged by specific access control rules"* and page 905 mentions the *"syslog"* alert as something *"outside of your intrusion policy"*. It appears that also O's cited page 470 mentions only *"automated alerting that you can configure for... syslog"*. Reminding that the same direct-and-unambiguous disclosure criterion applies also for novelty, the feature seems not explicitly or implicitly disclosed. **Here the OD sees provisionally a difference.**

For **feature 1.2.6** it seems that the cited page 498 mentions that *"packet information"* including e.g. the *"packet text"* can be viewed on the *"Defense Center"* by enabling the *"Transfer Packet option"*, i.e. this would - **in general** - seem to necessarily imply a packet transfer. It appears correct - as P argues - that the same Defense Center is also mapped to *"a monitoring device"*. However, it seems that the claim does not exclude the possibility that the claimed functionalities are implemented on a same physical device. This aspect in itself does not seem to establish a difference.

However, as to **features 1.2.3 to 1.2.6** and P's argument with letter of 29.11.2022 it seems correct that page 311 and the related figure state in various places that packets blacklisted by Security Intelligence are not further inspected (figure of page 311), i.e. *"the system does not inspect... blacklisted traffic"*. The claim literally refers to *"a packet matching the packet matching criterion of a packet filtering rule"* being the one subject to further handling so - when referred to the case of page 311 and Security Intelligence - these would be the packets that match the criterion, i.e. the blacklist address. However, it seems correct that these packets are not further handled by the system of D23 (i.e. logged, forwarded etc.). Based on the passages so far cited by the parties, it seems that the explanation of the P as to the functioning of the *"Security Intelligence"* here may be

correct, i.e. it is updated based on the malicious source information but it does not lead to a rule involving packet logging and routing upon a match. **Here the OD sees provisionally a difference.**

Provisionally, it is considered that **claim 1 seems to be novel over D23.**

C1. Lack of novelty vs. D19 = Sourcefire Manual version 4.10 of 2011

1.

OPPONENTS: O2 provides similar reasoning as to the availability of D19 to the public since the document is time stamped 16.03.2011. O2 refers again to an affidavit (D20) of Ms. Ehrig and to the affidavit of Mr. Baugher III. O2 also refers to decisions of the USPTO in D22 which established the availability date to be in March 2013. O2 also refers to parallel EPO proceedings.

PATENTEE: In the reply letter of 30.09.2022 it seems that P when addressing D19 does not contest the public availability before the relevant date.

OPPOSITION DIVISION: The date on the document is much earlier than the priority date and in view of the affidavits and of the fact that this is not disputed also the OD does not see an issue here and is of the provisional opinion that this earlier version of the manual seems credibly to have been made public before the relevant date of the patent.

2.

OPPONENTS: For the disclosure of D19, Os argues as follows.

Features 1 to 1.1.2: O2 In page 33 the "3D sensors" or "managed devices" are considered to be the PSGs which received a security policy from the Defense Center (= security policy management server). The security policy includes intrusion rules (= first set of packet filtering rules) as explained in pages 2084 and 764. The intrusion rules are updated via a Security Enhancement Updates with new intrusion rules (see page 254), so this is a dynamic security policy. Figure 6 on page 107 shows that policies including "Intrusion" are sent from the "Defense Center" to the "Managed Sensor". The Defense Center is located externally as shown in figure 7 on page 118. O3 provides similar arguments with reference to page 122 and pages 404/405.

Feature 1.1.3: O2 argues that the Defense Center automatically creates or alters rules based on the security enhancement updates SEU. These rules are created based on the malicious traffic provided by the Sourcefire Vulnerability Research Team. These rules are the rules included in the intrusion policy (see pages 405-406). The SEU security enhancement updates can be automatically downloaded and installed (see page 1716). The Sourcefire Vulnerability Research Team is a malicious host tracker

service. Intrusion rules relate to malicious traffic (see page 34). The Defense Center receives via the Security Enhancement Updates information on malicious traffic and imports this as scheduled task to the managed devices.

O3 provides similar arguments in addition referring to rules being automatically created / updated by the Defense Center based on information about malicious traffic received from a Real Time Network Awareness RNA component and the Sourcefire Vulnerability Research Team. For the RNA component reference is made to page 1725 disclosing that it modifies the states of intrusion rules and also to page 468/469. RNA data is equated with malicious traffic information.

With letter of 25.10.2022 O3 argues that the Defense Center automatically applies the RNA states to the managed sensors. O3 also argues that a rule state in D19 is not only activate / deactivate as alleged by P but generate events, drop and generate events or disable (see page 435), which corresponds to changing the action of a rule in the patent. Thus considering rules for which the rule state was automatically altered by the Defense Center discloses feature 1.1.3. As to the VRT alternative, a 3D sensor can be controlled with or without the Defense Center (see page 34). In the first case the Defense Center is used to manage the SEU update which results in re-applying the intrusion policies. The SEUs are not automatically active at the 3D sensor but only activated when a policy is installed from the Defense Center (see page 1716-1717).

Features 1.2 to 1.2.6: By **O2** reference is made to pages 34-35. On the "*3D sensor*" the intrusion rules identify an intrusion event, i.e. a packet matching, and record date, time, type of exploit and contextual information. This is the record with a subset of information of the packet. For packet based events a copy of the packet or packets that triggered the event is also recorded. The 3D sensors transmit events and sensor statistics to the Defense Center. This for O2 is the routing of the packet to a monitoring device. An "*intrusion event*" is defined as a record of the network traffic that violated an intrusion policy. Thus, for O2 the event comprises a subset of information specified by the packet and the packet that matched the criterion. The entire event is routed to the Defense Center which is a monitoring device. An example event available for further analysis is shown on page 290 which for O2 displays a routed packet and also the reformatted subset of information. For reformatting O2 refers to page 293 and following which refer to "*syslog*" (see 752 and following).

O3 provides similar arguments with reference to pages 352 and 403 stating that a rule is enabled by setting its state to Generate Events or Drop and Generate Events for traffic matching the rule. For the syslog formatting O3 refers to 752 indicating that in an intrusion policy you can turn on syslog alerting and syslog alerts can be generated to the local host or to the logging host specified in the policy.

With letter of 25.10.2022 O3 argues that D19 discloses that logs can be sent to syslog facilities (see page 482) and the syslog alerts or responses contain logged data which corresponds to a subset of information which was reformatted and they contain "event data" (see page 752). So feature 1.2.5 is disclosed. In addition it is argued that copies of the packet are recorded and this is part of generating an intrusion event which is a record including a copy of the packet which is sent to the Defense Center which is a monitoring device. So feature 1.2.6 is disclosed.

Features 1.3 and 1.4: For O2 the automated updating of packet filtering rules is disclosed by the Automating SEU imports, in which an intrusion policy is reapplied so that the new SEU takes effect, (see page 1716) i.e. a second set of rules. O3 also argues that the rules are updated by the Defense Center and this is done at the RNA component, as also argued with the second letter.

3.

PATENTEE: P argues that being an earlier version, this document discloses even less information. P contests disclosure of the following features.

Feature 1.1: For P the policy is not dynamic because it is created by the Defense Center because it is not created automatically but the policy is created manually by a team of employees, i.e. the Vulnerability Research Team VRT (see page 34) and D19 states (page 24) that the policies or rules for an Intrusion Agent cannot be managed from the Defense Center.

Feature 1.1.3: For the automatic creation of rules O2 relied on the SEU including new and updated standard text rules and shared object rules published by the Sourcefire VRT (see page 1716). The rules are thus not created or modified by the Defense Center but by the VRT and the Defense Center merely downloads them at regular intervals. Moreover P argues that the VRT does not track malicious hosts (i.e. their addresses) but rather vulnerabilities (see page 1716) contained in a packet payload. Intrusion rules (see page 761) state that an intrusion is a set of keywords and of arguments that when applied to captured network traffic identify potential intrusions. Keywords and arguments are included in a rule option. Rules contain rule header and rule options (page 762). The rule header specifies which packets are to be checked (page 764). A match of the received packet with the values in the header does not trigger the effect of the rule. P argues that this is not aimed at dropping packets based on the IP address. For this P also refers to preprocessor normalizing traffic and detecting malicious packets (page 34). If the intrusion rules were concerned with IP-addresses there would be no need of normalizing traffic. As to the automating recommended rule state generation based on RNA cited by O3 (see page 1725), this relates to a rule state, i.e. whether the rule is enabled or disabled (see page 2090-2091), i.e. deactivating or activating an already existing rule. This is not what the claim requires, i.e. creating or altering the rule itself.

With letter of 29.11.2022 P adds that the Defense Center does not create or alter any rule. According to O3 a rule state can be any of "*Generate Events*", "*Drop and Generate Events*" and "*Disable*" to allege that this would be setting the action performed when a rule is triggered but P disagrees alleging that page 435 only discloses manual rule setting and automatic rule setting by the Defense Center is not disclosed on page 435. On pages 468-469 it is explained that the recommended rule state depends on i) which rule state is specified in a base policy ii) whether the rule protects the network however, it is not disclosed that the recommended state is changed with respect to the base policy and the last criteria on the pages merely disables the rule, so a change of action is not disclosed. Also with respect to the SEU update P argues that the SEU is disclosed to itself "*contain new and updated rules*" (see page 117) and it is not disclosed that the Defense Center alters such rules but only the intrusion rules provided by VRT via the SEU are used.

Feature 1.2.5: D19 does not disclose reformatting according to a logging system standard when creating an intrusion event. Only a "*packet view*" for viewing packet information is disclosed presenting the packet in tabular manner but no reformatting according to a logging system standard is disclosed. Moreover page 752 mentions syslog responses. For P reformatting is not done when intrusion events are created but in a syslog, referring to page 261-262 stating that in addition to generating intrusion events, other alerting mechanism can be used.

Feature 1.2.6: For P it is not correct that sending the intrusion event to the Defense Center means sending the packet. A copy of the packet included in the event is not the same as routing the packet to another device. It is again noted that the Defense Center was also equated with the security policy management server.

Feature 1.3.1: The updated second set of packet filtering rules according to the claim is part of the dynamic security policy as it comprises an update of the first set of packet filtering rules and is based on malicious traffic information received from a malicious host tracker service. The SEU is instead created manually by the Sourcefire VRT and just imported to the Defense Center. The updating is not done by the Defense Center but by the Sourcefire VRT. Moreover, the VRT does not identify malicious hosts but vulnerabilities.

Feature 1.4: P argues that the second set of packet filtering rules is not disclosed, so no packet filtering based on it can be performed. As to the arguments of O3, P adds that the statement by O3 that intrusion rules can be updated by the Defense Center are unsubstantiated assertions.

3.

OPPOSITION DIVISION: The OD is of the following provisional view.

Feature 1.1: For the OD, irrespectively of how this is originated, the policy of D19 is explicitly disclosed to be changeable by downloading changes on the managed devices. In this respect the policy is *"dynamic"* (e.g. as opposed to a fixed policy). Here the OD does not see that this would be excluded by the claim wording, i.e. no difference is seen at present.

Feature 1.1.3: It appears correct that D19 does not disclose that the SEU is automatically created or altered by the Defense Center, which Os have equated with the security management server but by the VRT. It seems also correct that the SEU itself is explicitly stated to already contain the "updated intrusion rules" (see page 117). As to P's allegation of a further difference based on excluding malicious IP addresses, the OD is however not convinced. The claim broadly refers to *"malicious traffic information"* which does not exclude other aspects. Moreover, the claim does not require that packets are dropped. On these aspects P seems to argue beyond the wording of the claims.

As to the alternative alleged disclosure based on the automated recommended rule state generation based on RNA it appears - after considering the passages so far cited by both parties - that as argued by P e.g. the cited passages on pages 468-469 mention a change from *"Generate Events"* or *"Disable"* to *"Generate Events"*, a change from *"Drop and Generate Events"* to *"Drop and Generate Events"* or as a third option a change to *"Disable"*. According to the provisional understanding of the OD, this does not seem to disclose that an action associated with the rule or the rule itself is changed but only the selection of the same action (which is not a change) or the change between disable and enable of the rule (which is a change of state, but not a change of the rule). For the purposes of novelty assessment, none of the above seems notionally and technically the same as creating or modifying a rule. So neither the SEU nor the RNA seem to anticipate this feature. **Here the OD provisionally sees a difference.**

Feature 1.2.5: The citation from page 290 seems to disclose that event information is displayed but this is only related to source and IP address and port and it is not apparent that this would be reformatted according to a logging standard. Moreover, this is what is displayed at the Defense Center, so it is not apparent that such reformatting is done by the PSG. Page 254 discloses that an intrusion event (date, time, source of the attack) is generated as record. Page 752, cited by both Os, discloses that *"you can send syslog alerts which are intrusion event notifications"* and this can be sent to the logging host specified in the policy. I.e. it seems that what is sent is indeed put in syslog format. It is however reminded that the criterion is that of a direct and unambiguous disclosure. Based thereon, it seems that the above still does not necessarily require that a portion of the packet itself is sent in syslog format. **Here the OD provisionally sees a difference.**

Feature 1.2.6: For the OD the document discloses that the whole packet is recorded and sent (i.e. routed) to the Defense Center. The claim does not restrict this further. Here the OD does not see a difference based on the wording of the claims. This also applies for the fact that the Defense Center is equated also with the security policy management server (the fact that these functionalities may be on a same hardware is not excluded by the claim). Here the OD does not see a difference.

Feature 1.3.1: As explained above, the OD agrees with P that the updating is not generated by the Defense Center but by the Sourcefire VRT. As to P's alleged further difference, the OD notes again that the claim-feature just defines "*malicious traffic information*" and vulnerabilities inherently relate to some malicious host so this aspect does not seem to establish a further difference. **Here the OD provisionally sees a difference.**

Feature 1.4: For this specific feature, although this is done differently, as discussed above, it is considered that the VRT update also results in performing packet filtering with an updated rule as defined in this feature. Here the OD does not see a difference.

Provisionally, it is considered that **claim 1 seems to be novel over D19.**

C3. Lack of novelty vs. D41 = Juniper

1.

OPPONENT: With letter of 14.12.22 **O3** replies to P that **D41** is prior-art according Article 54(2) EPC. The date on the document is indicated as publication date, i.e. 10.12.2012. O3 refers to GL G-IV, 7.5.3.2 relating to other print-equivalent publications and to Dec.BoA T1668/12, point 3.4. Thus O3 concludes that D41 is prior-art and the same applies for **D41b**.

O3 refers to **D41** disclosing the use of policies to define which traffic is blocked or allowed by Juniper Networks security devices. The JN security devices are managed by a remote Network Security Manager NSM. Intrusion Detection and Prevention IDP applies on the policy level. IDP - known also as firewall - is used to detect and prevent attacks in network traffic and drop malicious packets before they enter the network. Multiple security policies can be defined in NSM but a security device can only have an active security policy at a time. Security policies contain multiple rules which can be created in "*rulebases*", i.e. sets of rules that are combined to define a security policy. IDP rules contain "*attack objects*" to identify malicious activity and the rule defines the attack object, i.e. a known pattern of attack, and the action you want the IDP to take when the monitored traffic matches the rule's attack objects.

JN regularly updates predefined attack objects to keep up-to-date with newly discovered attacks. The attack databases updates are downloaded to the NSM GUI server. The updates contain new description or severities for existing attack objects, new attack objects and group and deletion of obsolete attack objects. New attack objects are available for selection in an IDP rulebase in a security policy. When you install the security policy on the managed device only the attack objects that are used in the IDP rules for the device are pushed from the GUI server to the device. An automatic update is possible in which JN regularly updates the signature pack with newly discovered attack patterns. The security device automatically replaces its database with the newer version. Hence at least some rules are automatically and not manually created and altered at the NSM. For logging, each time a rule is matched, the IDP system creates a log record that appears in a log viewer. Individual packets that match the rule can be captured to determine the extent and purpose of the attack. Event and traffic logs can be stored externally in a syslog server. Thus, O3 explains that messages have to be reformatted in syslog standard before being sent. The security device sends syslog reports to the remote NSM and this includes *"traffic data"*.

With reference to the specific claim features:

Features 1 to 1.1.3: The PSG is the JN security device. They are associated with the security policy management server which is the NSM with the NSM-GUI on an external host. The security device sends the syslog reports to the NSM (see page 20, 312/313 and 1148). The security device receives dynamic security policies with a plurality of rules from the NSM (see page 588).

The rules contain matching criterions defined in the attack objects (see pages 593-594). The JN Web server provides regular updates to the attack object database in the NSM GUI server on malicious traffic information and NSM is therefore a malicious host tracker device (see page 647).

With reply of 25.10.2022 O3 refers to **feature 1.1** and argues that the fact that the security policies are configured in the NSM and installed on the managed device and thus must necessarily come from the NSM. O3 refers to D41b.

O3 refers to the **additional document D41b / Juniper Administration Guide and to D41c** (printout of Juniper documentation website indicting that D41b was published on 18.5.2010. D41 refers to in page 589 to the link to the administration guide D41b thus forming a single document. D41b on pages 504-505 discloses that *"during policy installation, NSM installs the rules in the policy on the security devices"* and also updates. In D41b these are made using Abstract Data Models ADM and Data Models DM files. As shown in figure 76 on page 310 of D41b the DM files include the security policy, i.e. a set of rules for each device. Since the policies are updatable, they are dynamic.

For **feature 1.1.3** it is added that D41 discloses that predefined attack objects are periodically updated (see page 647) and attack objects are used for Intrusion Detection and Prevention IDP or for Deep Inspection DI to identify malicious traffic and represent pattern of attacks, i.e. information associated with malicious traffic as claimed. Thus the Juniper's service for attack objects is a malicious host tracker service. With letter of 14.12.2022, O3 adds that P's arguments on the automatic creation / alteration of rules alleging a difference based on the fact that the NSM does not change the "*attack objects*" is incorrect because the claim does not define any particular process for rule creation and the inclusion of malicious addresses in the rule would suffice. I.e. it is sufficient that the received network addresses, i.e. the attack objects, are included in the rules, i.e. without changes to the attack object itself but thereby changing the rule.

Features 1.2 and 1.2.1: The IDP rulebase uses the attack objects to identify malicious attacks and to take an action when the monitored traffic matches a rule's attack object (see pages 593-594).

With letter of 25.10.2022 it is argued that for the update of the attack objects and attack objects database D41 (see pages 530, 648) refers to D41b Administration Guide, thus forming a single prior-art item. D41b explains that new attack objects are downloaded to the GUI Server and then to the management device (see page 290 of D41b). When the security policy already exists on the device but an object in the policy is changed on the NSM, the update un-sets the current policy on the device and then it installs the policy again (see page 505 of D41b).

Features 1.2.2 to 1.2.6: The IDP notification function corresponds to the packet digest logging function. If a packet matches a criterion, the notification function logs the packet - which for O3 means capturing a subset of the information defined in the packet (see page 610 and page 650 for the content of the log viewer). The subset of information is reformatted to fit different standards e.g. syslog e.g. to store event and traffic logs externally in a syslog server (see page 347). The IDP function also captures full packets of traffic data (see page 610) and routes them - additionally to normal logs - to a syslog server or sends the syslog reports to the NSM (see page 348 and 1148).

With letter of 25.10.2022 O3 argues for **feature 1.2.6** that besides creating and viewing logs in the Log Viewer, D41 discloses logging full individual packets that match a rule by capturing the packet data for the attack (see page 610). For more information about the Log Viewer it is again referred (see page 616) to D41b. Log data which is sent to the NSM comprises packet data, i.e. the full packet that matched the rule (see D41b, page 734, 742 and 762). Thus the NSM server is a monitoring device for subsequent analysis to which the packet is sent. In addition, event logs including the full packet are routed to the syslog server (see D41b, page 787), which is also a monitoring device.

Features 1.3 to 1.4: D41 discloses the update of the policy as discussed above. The updates are received by the JN security device from the NSM and the update comprises new or updated rules generated based on information on new attacks received from the JN Web server periodically and the filtering after the update uses the new rule.

With letter of 25.10.2022 O3 refers to what explained previously in the same letter, i.e. rules of security policies being at least partially automatically updated based on the updated attack database provided by Juniper. This involves resetting and installing the updated rules at the managed device.

2.

PATENTEE: With letter of 29.11.2022 P contests that **D41 and D41b** were publicly available before the priority date and questions that it was not shown that the download link was already established before the priority date of the patent and alleges that the document could have been confidential.

In addition, P is contesting the disclosure of the following features.

Feature 1.1: For P there is no disclosure in D41 that the security device receives the policy from the NSM. Page 580 cited by O3 merely states that multiple security policies are configured by the NSM but for P this still fails to indicate how a security policy is applied to the security device.

Feature 1.1.3: P states that O3 referred to the regular updates for "*attack databases*". The attack database updates are provided by Juniper Networks and include - inter alia - intrusion prevention and detection IDP attack objects (page 647). The attack object is used by a rule to identify the malicious traffic (see pages 593 and 594). O3 argues that the automatic update of attack databases leads to an automatic update of rules but does not substantiate why this is the case. However, it is merely stated that the new attack objects are available for selection and only the attack objects used by the IDP rules for the device are pushed from the GUI server to the device (see page 647).

Also page 532 does not disclose automatic generation of rules by the NSM but only an attack database for deep inspection DI. Firstly the security device (and not the NSM) downloads the attack database from an attack object server. Secondly, the security device replaces its attack object database with the newer version (see pages 532-533 and figure 144).

With letter of 25.10.2022 P argues that the claim requires that malicious traffic information is used by the security policy management server to create / alter the rules. O3 has shown that attack database updates are used for updating attack objects. This is done by downloading new attack objects to the GUI server and downloading new attack objects to the managed device (see e.g. D41b, page 290). This is however not

the automatic creation / alteration of a rule. The NSM receives and forwards the attack objects (which were equated to the packet matching criterion by O3). The NSM does not modify the attack objects at all and these are forwarded to the managed devices.

Feature 1.2.6: P states that O3 equated logged traffic data included in a syslog report with a packet, however for P this is not correct. Claim 1 requires a subset of information of a packet. The logged traffic data is not the traffic data itself. The cited 1148 discloses sending syslog reports but not packets.

Features 1.3, 1.3.1 and 1.4: P states that O3 referred to the previous arguments but as explained for feature 1.1.3 an automatic creation or alteration of rules by the NSM is not disclosed.

3.

OPPOSITION DIVISION: As to the public availability of **D41 Juniper** being a manual directed to customers it seems at present established that the publication date is indicated to be in 2012, which also corresponds to the copyright indication on page 1. A similar remark appears to be valid for the manual **D41b** which has an indication of publication and copyright in 2011. Both documents are manuals directed to actual or potential customers without any indication of confidentiality and the indicated dates are well in advance of the priority date, so the OD considers at present that the above indications appears to credibly indicate - also with reference to D41c - the actual publication date (see also the GL G-IV, 7.5.3.2).

As to the disputed features the OD is of the following provisional view.

Features 1 to 1.1.3: The OD presently agrees with the Os that D41b is referenced in D41 for further explanations. Already from D41 it seems that the fact that multiple security policies are configured by the NSM seems to imply that it is therefrom that these are obtained at the security device. This is then explicitly mentioned in D41b on pages 504-505 disclosing that "during policy installation, NSM installs the rules in the policy on the security devices". It is also agreed that the Juniper's service for attack objects falls under the terms of a malicious host tracker service. As for example explicitly shown by the cited figure 76 on page 310 of D41b the policies are updatable, i.e. dynamic.

It appears correct that the claim merely requires that the rule "*was automatically created or altered by the security policy management server based on malicious traffic information received from a malicious host tracker service*" without further specifying how. In this respect Juniper network provides periodic attack-database updates with new or modified IDP attacks (see page 647), the attacks or attack objects of D41 corresponding to the matching criterion of a rule. These are downloaded to the GUI Server and then downloaded to the managed device (see e.g. the cited D41b, page

290). It is also explained that then *"NSM must reset the policy when the security policy you are installing already exists on the physical device but an object within the policy has changed in the NSM. The update first unsets the current policy on the device, deletes the old object, adds the new changed object, then installs the entire security policy again on the physical device"* (see D41b, page 505). I.e. although it is agreed with P that the updated received object itself is not modified by the NSM - in the present understanding of the OD - it appears that the insertion by the NSM of different / updated objects nevertheless necessarily updates the resulting rules and this is done by the NSM based on information on malicious traffic. Here the OD does not see a difference with the claim wording.

Feature 1.2.6: The feature relates to *"routing, by the packet security gateway, the packet to a monitoring device configured to store the packet for subsequent analysis"*. P argues that the forwarding of logged traffic data included in a syslog report is not a packet. It is agreed with P that the claim requires that *"the (= full) packet"* is forwarded.

The cited passages of D41b however refer to (see page 610) *"you can record individual packets in network traffic that match a rule by capturing the packet data for the attack"* and *"to send the packet data to NSM with the log data double click etc."* (see page 734) or that the *"log has associated packet data"*. O3 alternatively refers to event-logs routed to the syslog server which also mentions the inclusion of packet data, i.e. *"hasPacketData"* (with reference to D41b page 787). According to the present understanding of the OD, it seems that the above means that individual packets are captured and forwarded as data to a monitoring device. I.e. this would mean that the recorded *"individual packet"* is indeed sent (= routed) to a monitoring device (the claim does not require a particular form of routing it). Here the OD presently does not see a difference.

Features 1.3, 1.3.1 and 1.4: Both parties refer to the difference or disclosure argued for the previous features, in particular as for feature 1.1.3. With a similar reasoning as above, here the OD provisionally does not see a difference.

Based on the above, the **OD is of the provisional opinion that claim 1 appears to lack novelty in view of D41 / D41b.**

C4. Lack of novelty vs. D43 = US 2013/0263247 A1

1.

OPPONENTS: O3 alleges lack of novelty based on **D43** disclosing a packet interceptor adapter / DPPM which is mapped to the PSG (reference is made to the abstract, figures 1 and 7-8 and to [0045], [0050], [0053], [0058], [0059], [0062], [0083]-[0085], [0088], [0090]-[0091], [0118], [0183]).

Below, the arguments for the **disputed features** are summarized.

Feature 1.1.3: O3 argues that the packet interceptor adapter - mapped to the PSG - and the management device - mapped to the policy management server - are both external to the network they protect (see figure 7). The rule or rule sets are re-defined or re-set from the management interface. The rules are implemented dynamically taking historical traffic (see in particular [0085]).

Features 1.2.4, 1.2.5 and 1.2.6: O3 argues that examples of the action include logging information and forwarding the packet to an external device for subsequent processing with reference to the abstract and the skilled person does not need any further information since it is understood that logging requires reformatting using a logging system standard as syslog mentioned in [0183] of D43.

Features 1.3, 1.3.1 and 1.4: O3 states that this does not add anything beyond the fact that the updated rules are received and packets are filtered based thereon and D43 discloses dynamically redefining rules.

2.

PATENTEE: P contests the disclosure of the following features.

Feature 1.1.3: P argues that O3 considered the historical packet activity to be the malicious packet information from the protected networks. However, P is of the view that it was not shown how the rules are created / altered and that this is done dynamically. However the historical packet activity consists of packets stored in a memory e.g. SDRAM (see [0085], [0090], [0099] and figure 8) of the packet interceptor adapter (mapped to the PSG by O3). A rule processor capable of redefining / resetting the rules of the packet interceptor adapter uses the historical information. Thus, this is in the PSG and not in any external device as required by the claim. Also paragraph [0085] refers to a malformed packets being stored and if a second such packet is received, determining that malicious activity is ongoing and delete the second packet. However, this does not correspond to the alteration or creation of a rule.

Features 1.2.4, 1.2.5 and 1.2.6: P is of the view that O3 did not provide any reason going beyond alleged implicit disclosure, nor where the generation of a specific subset of information is disclosed, nor to logging / storing. Moreover, it is not specified that the external device is a monitoring device. With respect to syslog reference was made to [0183] but this is in the context of an arbitrary enterprise firewall, not with reference to the packet interceptor adapter that O3 has mapped to the PSG.

Features 1.3, 1.3.1 and 1.4: P disagrees that these features are disclosed by the mere re-definition of rules. As discussed above P is of the view that automatic creation and alteration (i.e. updating) of rules is not disclosed.

3.

OPPOSITION DIVISION: The OD is of the following provisional view for the contested features.

Feature 1.1.3 It is agreed with the Os that it seems correct that rules are re-defined or reset, i.e. treated dynamically, via the management interface (see in particular [0083]). However, this seems not to be in connection with the *"historical packet activity"* mentioned by O3 referring to [0085]. Quite to the contrary, this paragraph literally states that this *"allows stateful processing, i.e. state based rules"*, so this is presently understood as something notionally and technically different from creating or changing the rule itself, which is thus not *"automatically created or altered by the security policy management server based on malicious traffic information received from a malicious host tracker service"*. **Here the OD provisionally sees a difference.**

Features 1.2.4, 1.2.5: It appears correct that none of the cited passages discloses or requires that a subset of of the information is recorded, nor that the subset is reformatted according to a logging standard. While syslog may be known, it seems correct that the reference in [0183] to syslog is not disclosed in combination with the reformatting of a portion of the captured packet by the packet interceptor adapter. So features 1.2.4 and 1.2.5 seem not disclosed. **Here the OD provisionally sees a difference.**

Features 1.2.6: It is agreed with the O3 that the abstract literally discloses the option of *"logging / storing information about the packet or forwarding the packet to an external device for subsequent processing"* thus it seems that at least feature 1.2.6 is disclosed. Here the OD does not see a difference.

Features 1.3 and 1.4: As outlined above it seems that D43 discloses that the rules can be re-defined via the management interface. Re-defining a rule seems to imply that the rule is changed which also means that thereafter filtering is done with the updated rule. So features 1.3 and 1.4 seem in principle to be disclosed. Here the OD does not see a difference.

Feature 1.3.1 requires however a specific content of the updated rules, namely *"the updated second set of packet filtering rules comprises an update to the first set of packet filtering rules generated by the security policy management server based on updated malicious traffic information received from the malicious host tracker service"*. As outlined above, it is agreed with the P that this does not seem to be what D43 discloses. **Here the OD provisionally sees a difference.**

Based on the above, the **OD is of the provisional opinion that claim 1 appears to be novel in view of D43.**

Overall, according to the present opinion of the OD, **D43** seems to be of lesser relevance.

C5. Lack of novelty vs. D44 = US 7966659 B1

1.

OPPONENTS: O3 argues lack of novelty based on **D44** disclosing a "*central management tool*" (mapped to the security policy management server), a distributed source with a firewall (mapped to the packet security gateway) and including the dynamic creation of rules for security devices (reference is made to the abstract, figures 2-3, column 1, lines 27-39 and column 1 line 65 to column 2 line 1; column 2, lines 35-36 and 48-56, column 10, lines 1-4 and 32-37). The arguments for the **disputed features** are summarized below.

Feature 1.1.3: The distributed devices having a firewall (PSG) are in communication with the central management tool (security policy management server) and are external to the network protected by the firewall. The central management tool creates firewall and security rules based on aggregating gathered information from the distributed sources and the rules can be automatically modified by the central management tool (column 7, lines 39-42 and 59-65).

Features 1.2.4, 1.2.5 and 1.2.6: O3 argues that the firewall filters incoming or outgoing data and other typical actions can be to log (see e.g. column 7, lines 3-14) and an intrusion log can be monitored by a learn component 212 (column 8, lines 58-61). For O3 a log is typically not a full packet but a record that only contains a subset of a packet, so they must be formatted according to a logging system standard. Moreover, D44 discloses that the firewall decides whether the packet should be transmitted to the intended destination, blocked, dropped or re-routed (column 1, lines 34-39 or column 12, lines 18-22 or column 7, lines 7-14). It is evident that a packet is re-routed to be analysed.

2.

PATENTEE: P contests the disclosure of the following features.

Feature 1.1.3: P states that O3 asserts that malicious traffic information from a malicious host tracker device is used as a basis for the "*central management server*" to create or alter the rules referring to a rule builder module 322 (column 7, lines 39-42). However, the rule builder module 322 belongs to the central management tool 302, which is a different embodiment (with reference to column 6, lines 52-55 for the first embodiment of figure 2 and with reference to column 9, lines 16-18 for the second embodiment of figure 3). Irrespectively thereof, none of 202 or 302 that O3 equated with a "*security policy management server*" uses i) malicious traffic information which is ii) received from a malicious host tracker device. It acquires "*industrial protocol communication information*" from distributed sources which in turn collect the

information on the communications they receive or send, i.e. traffic information (see column 7, lines 31 to 43). The same applies to central management tool 303 which collects information from distributed devices and then from this correlated information the rules are created (column 9, lines 33-45). Moreover, the distributed source 206 and distributed device 304 were equated with the "*malicious host tracker service*" whereas the distributed source 204 and the distributed device 306 were equated with "*packet security gateways*". However, it is not disclosed that 206 and 304 identify malicious traffic, so they do not represent malicious host tracker devices.

Features 1.2.4, 1.2.5 and 1.2.6: P argues that O3 has referred to scattered passages mentioning some sort of logging and routing. These passages mention routing and logging without any apparent relation to each other, whereas the claims require that this is performed on the same packet. It is disclosed that the detection system can log unauthorized accesses (see column 7, lines 10-14) or that there is an intrusion log that records observed traffic (see column 8, lines 58-61) but this fails to disclose a subset of information being logged, so this does not disclose feature 1.2.4. O3 argues an implicit disclosure of the use of a logging standard but this is not necessarily the case (e.g. the reformatting could be done at the central management tool). Firewalls may route or re-route packets in D44 but there is no connection with the intrusion log.

3.

OPPOSITION DIVISION: The OD is of the following provisional opinion.

Feature 1.1.3: It appears correct that while a "*central management tool*" is indeed updating the rules, this is disclosed to be on a different basis, i.e. also the passage cited by the O3 on column 7, line 39 and following, refers instead to "*information reported by (both) distributed sources 204 and 206*", so that a mapping of these identical devices - which both contribute to the reported information - to be one the PSG and the other the malicious host tracker of the claims seems artificial. Moreover, it is correct that D44 only discloses that the "*central management tool*" performs a correlation of traffic information from multiple sources. I.e. while the claimed aspect of "*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*" seems disclosed in D44, this is not done "*based on malicious traffic information received from a malicious host tracker service*" but on the basis of correlating traffic information from multiple distributed sources, which seems at present to be notionally and technically not the same. **Here the OD provisionally sees a difference.**

Features 1.2.4, 1.2.5 and 1.2.6: The OD presently cannot recognize the disclosure of these features, since D44 seems to disclose only in general terms that logging can be done or that re-routing towards another destination can be done. In the cited passages it is not stated whereto the packet is re-routed. The same applies to the "*subset*" of

information, its formatting according to a "*logging system standard*" or for the routing to a monitoring device for subsequent analysis. Even if the traffic aggregation were considered to be a kind of re-routing, it appears that P is correct that based on the passages cited so far in D44 it seems not disclosed that routing to a monitoring device and logging of a subset of information are performed in combination for one and the same packet. It is reminded that a same disclosure criterion is uniformly applied by the EPO also to the prior-art and it is always the same *Gold Standard* of the BoA - directly and unambiguously derivable - which is to be used for the question of novelty. None of the features seems disclosed. **Here the OD provisionally sees a difference.**

Based on the above, the **OD is of the provisional opinion that claim 1 appears to be novel in view of D44.**

Overall, according to the present opinion of the OD, **D44** seems to be of lesser relevance.

C6. Conclusion on Article 100(a) EPC, novelty

1.

In conclusion: The OD is provisionally of the view that the ground under Article 100(a) EPC, novelty, seems to be prejudicial for the main request. This is at least based on D41 & D41b.

D. PATENTABILITY, ARTICLE 100(A) EPC / INVENTIVE STEP

1.

In view of the above, it seems that other grounds may be already prejudicial for the main request. The following provisional remarks on the presented inventive step attacks are thus included mainly for completeness and to streamline an eventual discussion in the OP.

D1. Inventive step in view of D19 combined with D25, D26, D27, D28, D30

1.

OPPONENTS: O2 assumed that P may argue novelty in the sense that **D19** does not disclose a malicious host tracker service. Assuming such difference would result in the **differentiating features** being **features 1.1.3 and 1.3.1**.

The **technical effect** and **objective technical problem** would be to provide an alternative method for automatic updates for dynamic security.

For O2 the solution is obvious stating that the skilled person is aware of the automatic update capabilities of Sourcefire D19, e.g. referring to statements in **D25, D26**

Also **D27** relates to efforts to standardize the exchange of cyber threat information using the STIX format and the TAXII trusted automated exchange of indicator information. Thus, it would be obvious to use feeds based e.g. on STIX and TAXII to update the dynamic security policy. **D28** is an excerpt from the wayback machine archived on 19.02.2014 and mentioning that TAXII is an effort to standardize the trusted automated exchange of cyber threat information.

D30 discloses another example of malicious host tracker service called "*Infoblox*" in **D30**. Thus for O2 the claim is obvious.

2.

PATENTEE: P replies that the formulation of the problem contains a pointer to the solution since it refers to providing automatic updates, referring to GL G-VII, 5.2. P argues that the solution is anyway inventive.

P argues that FirePOWER of **D25** is used to prevent next generation intrusion prevention systems but it is not related to "*3D sensors*" as in the Sourcefire Manual D19. **D26** allegedly does not refer to the 3D sensors or to D19.

P argues that **D27** does not render obvious the addition of feature 1.1.3 because it does not disclose that packet filtering rules are automatically created by the security policy management server. However, the "*observables*" of D27 are not the packet filtering rules for P but "*stateful properties or measurable events*" as e.g. information about a file, registry key value, HTTP request being sent etc. Thus the TAXII system alone does not provide the missing features. There is no explanation how an interface to such feeds would be provided in Sourcefire.

P argues that **D30** relates to the Infoblox DNS Firewall, i.e. it relates to a firewall and not to a malicious host tracker device.

3.

OPPOSITION DIVISION: To start with, the OD was of a **different provisional view** on the question of disclosure of D19, i.e. that **features 1.1.3 and 1.3.1 but also feature 1.2.5** are not disclosed, so a full discussion of the problem solution approach appears not possible until the novelty discussion has been completed. Based on these different premises feature 1.2.5 would still be missing.

Provisionally, it is observed that **D19** only discloses the SEU created by the VRT team, as discussed above. In this respect O2's alleged problem of "*providing an automatic update for a dynamic security*" seems indeed a problem formulated with foreknowledge of the solution.

D25 and D26 do not seem to disclose the claimed solution and only mention the possibility of automatic updates of rules or policies in general terms without specifying how, on which basis and by which network elements. Moreover, **D25 and D26** are all published in 2014, i.e. after **D19**, so they are not part of the disclosure of D19. A combination with these documents still does not lead to the claimed solution.

D27 refers to STIX format and TAXII. O2 refers to the exchange of "*observables*" as the alleged filtering rules. O2 alleges that this was a feature mapping made by the proprietor in infringement proceedings. This is not relevant here to prove disclosure, since it refers to unrelated proceedings and in any case neither the parties nor the OD are bound by such kind of alleged statement made by a party, even more so in separate proceedings. Based on the citation of D27 made here by P the "*observables*" appear to be "*stateful properties or measurable events*" as e.g. information about a file, registry key value, HTTP request being sent etc. and not rules, so it is at present not apparent whether / how this **would** be combined by a skilled person with the teaching of D19 without *ex-post facto* analysis.

D28 refers to TAXII standardizing the trusted automatic exchange of cyber threat information and O2 argues that a skilled person would thus add a TAXII interface in D19 since this was standardized before the priority date. However, for the OD it seems correct that there is still no explanation as to how this should be used for concrete rule generation, e.g. it is not apparent to the OD that - even if such an automatic feed were provided somewhere in D19 - the skilled person would have a rule update based thereon placed in the "*Defense Center*" (e.g. noting that the SEU rules in D19 are just forwarded via the Defense Center, not actively altered therein).

D30 is referred to without citing particular passages. However, according to what is stated by O2 it just discloses the existence of malicious host tracker service and not its concrete use to generate rules. Secondly, it seems correct - as cited by P - that D30 refers to such "*Infoblox*" in the specific context of DNS-firewalls, so it is not presently clear whether and how a skilled person would concretely combine a DNS-firewall within the "*3D-Sensors*" architecture of D19.

In conclusion the OD is provisionally not convinced by this inventive step argument.

D2. Inventive step in view of D31 = US 2011/0072506 A1 in view of common general knowledge

1.

OPPONENTS: O2 argues that D31 relates to firewalls which include rulesets for inspecting and dropping traffic. The rulesets can be updated to remain effective against network threats. A *"third party cyber-security risk management firm"* collects threat data from a plurality of *"sources"* (reference is made to figure 3). For O2 this means that a server is used to provide the rulesets and the *"sources"* are the claimed malicious host tracker devices. Packets may be logged as shown in figures 11 and 13 and [0103] and log files are used (see [0052]). Paragraph [0103] states that *"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"*.

For O2 D31 discloses all the features of claim 1 except that

- i) a log includes a subset of information which is reformatted (**features 1.2.4 and 1.2.5**) and
- ii) that re-routing is to a monitoring device configured to store the packet for subsequent analysis (**feature 1.2.6**)

which are treated by O2 as non-synergetic features citing GL G-VII, 7 with corresponding **separate problems**

- i) how to provide packet filtering that allows a structured log entry
- ii) how to make the packet available for subsequent analysis

O2 alleges that both solutions as claimed are obvious with reference to common general knowledge and refers to two patent documents.

- **Combination with D32:** For i) figure 5 and [0106] + [0111] disclose collecting event data as the information from a packet that fails an analysis using rules and failure results in a delete packet operation. Saving a copy of the packet to an event database for further analysis is possible. The event data is provided in simple format, e.g. ASCII XML etc. i.e. it is reformatted.

For ii) storing the packet in the deleted packet database of [0111] means that it is re-routed thereto.

- **Combination with common general knowledge and D36:**

For i) O2 refers to any of **D33, D34 and D35** as alleged common general knowledge documents disclosing the syslog standard. **D35** in figure 6 and 6A discloses edge-servers (= mapped to PSG) connected to a DNS server 108, which for O2 is the external policy management server. The edge server monitors data generated by clients for malicious program code, i.e. program code that has been previously identified by the server as harmful (see column 28, lines 17-32). Packets are examined according to

packet filtering rules, e.g. port address (column 38). An enterprise firewall may implement rule-sets and report alert logs to a central station via methods as syslog or SNMP (see column 35, lines 34-36 or 52-57).

For ii) **D36** discloses that Internet Service Providers may be required to capture data traffic for purposes of law enforcement and cyber security. With reference to the embodiment of figure 4 this discloses that if an IP address matches the range for lawful interception the packet is directed to the lawful intercept capture system, i.e. the packet is routed thereto for further analysis. Thus a skilled person would re-route the packet of D31 for further analysis.

2.

PATENTEE: In addition to the above acknowledged difference P also disputes disclosure of the following features.

Feature 1.1: P disagrees with the disclosure of a server. It is not said that cyber-security risk management firm implements a server.

Feature 1.1.3: P indicates that the cited passage on [0083] merely states that detecting certain network conditions may trigger an automatic update of the rulesets, however this is just a general update of rulesets and [0085] just states that the cyber security firm collects threat data from various sources to construct the rulesets, i.e. the cyber security firm already constructs the rulesets without indicating that this is done automatically in a server. Moreover, the "*sources*" of figure 3 are equated with the malicious host tracker but in [0092] it is only disclosed that the sources create "*threat data*" by analyzing potential or known threats. However for P this does not relate to information on malicious hosts and [0022] and [0014] rather refer to application layer attacks when a new device or code application is introduced, such as expose to bugs and other vulnerabilities.

Feature 1.3, 1.3.1 and 1.4: As indicated above [0088] fails to discloses automatic creation or alteration of the rules by a server.

- combination with D32: For P D32 discloses an integrated monitoring system which monitors traffic on an internal network or received from an external network but it does not disclose features 1.1, 1.1.3 and features 1.3 to 1.4 with the automatic creation / alteration of rules which in [0044] of D32 are created on the basis of event data in a database which is in an integrated monitoring system (see [0064], [0072] and [0100]). Thus for P this is not a creation by the security policy management server based on malicious traffic information received from a malicious host tracker service.

For P also feature 1.2.6 is not disclosed because [0111] discloses that failing a rule results in the packet being deleted and saving a copy to a deleted packet database for further analysis. So P argues that deleting the packet is contrary to what feature 1.2.6 requires.

- **combination with D36:** P argues that it does not disclose feature 1.2.6. An IP router compares packets with source / destination address for lawful interception and in case redirects it to a lawful intercept capture system. However, for P the router does not perform security functions as a firewall and thus is not a packet security gateway. Moreover, this routing is not performed as part of packet digest logging.

3.

OPPOSITION DIVISION: The lack of disclosure of features 1.2.4 to 1.2.6 in D31 is undisputed by the parties and also the OD agrees.

As to the argument of P that the cyber security risk management firm "305" would not use a server, it seems to the OD that figure 3 shows that the NE "305" is connected to the Internet and [0088] states that this can be "*constructing*" and "*distributing*" the rulesets for which threat data are collected e.g. "*from the world wide web using various data collection techniques*", i.e. even if not literally disclosed, using a server is still a normal and straightforward option. Paragraph [0088] refers to collecting "*threat data*". However, reference is made to generic data and it seems correct what P states, i.e. that it is not disclosed or required that a malicious host tracker service is used. So **feature 1.1.3** seems not disclosed. For the same reason it seems that also this aspect of **feature 1.3.1** is not disclosed.

Moreover, while **D31** mentions logging and rerouting as possible actions, it is questionable for the OD whether it is disclosed - directly and unambiguously - that both are necessarily to be applied **to the same packet**.

Since the above provisional view on D31 is different from the respective assessment made by both parties, it is at present difficult for the OD to make a complete inventive step assessment. The OD provides at least the following provisional remarks.

Combination with the teaching of D32: It seems that D32 in figure 5 + [0106] + [0111] discloses that a packet-analysis based on rules includes the step of "*collecting certain information*" (= subset) *from the failed packet*" and that this may be "*event data*" resulting in the step "*transmit event data to event DB*", so this would mean that a subset of data is logged. This event data may be provided as "ASCII", "XML" etc. (see [0069]) i.e. reformatted. Then [0111] is in the same context of figure 5 and it discloses that packet deletion may indeed involve "*saving a copy of the packet to a deleted packet database for further analysis*" (which could evidently be a separate device and it seems different from the event database). I.e. it seems that this would disclose operations as in all of

features 1.2.4 to 1.2.6 and figure 5 + [0111] seems also disclose that both actions of reformatted-subset logging to event database and packet storing to a deleted packet database can be performed for the **same** packet. As said, this however does not yet address all the differentiating features according to the above view of the OD (e.g. host tracker aspect apparently still missing).

Combination with common general knowledge & the teaching of D36: This combination seems at present less convincing. Firstly it seems that for i) the cited documents do not go beyond stating that syslog is known which appears undisputed. However, there is no mention of syslog being applied to a subset of data. For ii) it seems that **D36** in figure 4 discloses rule-based rerouting of a packet to lawful intercept for further analysis. However, even taking all the above, it is not apparent whether the skilled person **would** make all the above choices according to what is defined in the claims (e.g. apply both routing and logging to the same packet, which seems not disclosed in any of **D31 + D33/D34/D35 and D36**). This combination at present seems more artificial.

A full opinion on inventive step cannot be formed at present in view of the diverging view of the OD on the differentiating features vs. closest-prior-art D31, as already discussed above.

D3. Inventive step in view of D44 = US 7966659 B1

1.

O3 in addition to the novelty argument for **D44**, argues inventive step considering as potential differences the steps of logging packets (including reformatting the logged subset of packet information according to a logging system standard) and routing such packets to a monitoring device to store the packet for subsequent analysis. For **O3** it would be obvious to apply the teaching of **D44** to a policy according to the common general knowledge.

O3 refers to **D41** Juniper and **D19** Sourcefire 4.10 and alleges that the above differences would anyway be obvious in view of these two documents.

2.

PATENTEE: P replies referring to the previous assessment for these documents indicating that has been made by P and concluding that the combination is still missing some of the claimed features.

3.

OPPOSITION DIVISION: As indicated above, also the OD was of the provisional opinion that more features are missing for D44 than argued by O3 and D44 was considered to be of lesser relevance. So it is not possible to anticipate a preliminary opinion without first completing the discussion on the disclosure of the closest-prior-art D44. However, the OD notes that it was preliminarily considered that **D41 / Juniper** taken alone was anticipating the subject-matter of the claims.

D4. Inventive step in view of D45 = WO 2012 / 164336

1.

OPPONENTS: O3 objects based on D45 taken as closest-prior-art. It discloses cyber threat intelligence data generated by intelligence headquarter IHQ. This is refined cyber threat intelligence data produced by the IHQ which is then sent to the gateways (mapped to the claimed PSG). The gateways process the traffic entering or exiting the network based thereon. O3 equates this refined cyber threat intelligence data with the claimed rules. D45 states literally that IHQ "*collects raw cyber threat intelligence data from the cyber threat intelligence sources*" e.g. seed information or logs and the IHQ produces a "*comprehensive threat report*" based thereon which is e.g. shown in the table of figure 7 with an IP address value and a corresponding reputation indicator. The gateway will use this customized threat report when processing future packets. O3 proposes a combination with aspects of **D41 Juniper** or **D19 Sourcefire 4.10**, allegedly obviously resulting in the claimed subject-matter.

PATENTEE: P argues that the combination with D41 and D19 is not obvious and also that **feature 1.1.3** and consequently **feature 1.3, 1.3.1 and 1.4** are at least not disclosed in D45 since it just discloses creation of a "*customized threat report*" which is not the creation or alteration of packet filtering rules.

2.

OPPOSITION DIVISION: According to the present view of the OD, D45 is less relevant than most of the other cited documents and therefore it seems a less likely choice as credible closest-prior-art. It appears questionable whether any packet filtering rule update is disclosed in this document. As outlined by P, it mentions *expressis verbis* that the IHQ just "*collects raw cyber threat intelligence data*" and these are refined in a "*customized threat report*" that is passed to the gateways. However the latter (i.e. a table with IP address & reputation) seems more to correspond to the mere malicious host information of the claims than to a rule based thereon. For the OD most of the claimed features seem not disclosed. In addition to the undisputed differences conceded by O, as argued by P, it seems correct that at least **feature 1.1.3** and

consequently **feature 1.3, 1.3.1 and 1.4** are also not disclosed. D45 thus adds very little to the disclosure of D19 which was already discussed above. It is however noted again that **D41 alone** was provisionally considered to anticipate the claimed subject-matter.

To the OD presently considers D45 to be a less suitable starting point as closest-prior-art and it appears that when starting therefrom a skilled person would not obviously arrive to the subject-matter of the claims.

D5. Inventive step in view of D19 alternative feature mapping and D19a

1.

OPPONENTS: With letter of 25.10.2022 **O2** argues lack of inventive step based on introducing the **late filed D19a** Sourcefire Whitepaper published at the latest on 03.03.2013 based on the web archive printout **D19b**.

This relies on an **alternative feature mapping for D19** in which the claimed packet filtering device is still mapped to the "*3D sensors*" but the "security policy management server" is mapped to the "*VRT server*" which provides updated rules in the SEUs and updated vulnerabilities for rules in VDBs to the "*3D sensors*".

The "*3D sensor*" receives from the VRT server a set of updated rules in the provided SEU from the VRT, so that the policy corresponding to these rules is a dynamic security policy and the rules evidently comprise a matching criterion, so this discloses features **1 to 1.1.2**. For **feature group 1.2** the mapping remains the same and these are considered disclosed.

For **feature group 1.3 and feature 1.4** when an update of the SEU is installed on the "*3D sensor*" (= PSG) the new updated rules will be used and they were created by the VRT based on updated malicious traffic information.

For **O2** the **difference** is that **D19** does not disclose how the VRT derives the new rules provided in the SEU. The proprietor alleges that this would only be done manually. However this is incorrect because D19 just leaves it open. The **technical problem** is thus how to provide updates of the rules to a packet filtering device.

The solution is obvious in view of **D19a** relating to the VRT for Sourcefire which refers to a "*technology that automatically fine tunes and enforces security policies and that can be adapted in real time to the current threat situation*" and that this is based on intelligence gathering e.g. by "*looking at public vulnerability feeds*" (see pages 1-2). Hence these feeds are malicious host trackers as required by the alleged difference above. The SEU is such an updated content (see page 5).

2.

PATENTEE: In addition to the undisputed difference above being **feature 1.1.3**, with letter of 29.11.2022, P disputes that **feature 1.1** is not disclosed with the alternative feature mapping since this requires that the whole dynamic security policy is received from the security policy management server.

In **D19** the whole policy is applied by the "*Defense Center*" to the "*3D sensor*", not by the VRT, so the VRT cannot correspond to the "*security policy management server*".

Moreover, the VRT does not transmit the SEU to the 3D sensor, but to the Defense Center. Also the cited passages (pages 1-2) of **D19a** literally indicate "*customers to take control... with technology that automatically fine tunes and enforces security policies*". Also the statement on acting on information in real time does not mean that updated rules are created automatically and D19a has to be considered in the context of the other teaching of D19, i.e. the VRT digesting the information in the public vulnerability feeds.

3.

OPPOSITION DIVISION: To start with, the provisional view of the OD on the disclosure on D19 (see section C1 above) is not identical with the allegation of any of the parties, so a full provisional opinion on inventive step seems not possible before the discussion on disclosure in the closes-prior-art has been completed.

It seems however correct, as also mentioned in section C1 above, that the SEU is stated explicitly to contain "*updated intrusion rules*" (see page 117). The claims require that rules are "*automatically created or altered by the security policy management server based on malicious traffic information received from a malicious host tracker service*". In this respect it seems that the "*Defense Center*" forwards SEU updated by the VRT to the PSG. However, it seems correct that it is not apparent whether this also means that a whole policy (rather than individual rules) is disclosed to be created or altered by the VRT (as required by the claim in feature 1.1 to be from the "*security policy management server*"), although this may nevertheless still be obvious.

It appears that **D19a** is *prima facie* relevant to clarify VRT-aspects of D19 to which it relates. According to the provisional opinion of the OD, then it seems that **D19a** clearly refers to "*public vulnerability feeds*" and "*acting on that information in real time*". Based thereon, it seems that - in the context of inventive step - considering malicious hosts information and acting on the information automatically would not go beyond what a skilled person would regard as possible concrete implementation of what is stated in D19a since automation of tasks is one normal concern of the skilled person and vulnerability would normally be considered e.g. to likely involve information on malicious IP addresses or similar.

Datum
Date 09.01.2023
Date

Blatt
Sheet 56
Feuille

Anmelde-Nr:
Application No: 19 170 936.9
Demande n°:

In conclusion, no complete opinion on inventive step starting from D19 is expressed since the conclusion on the question of disclosure of the claimed features in D19 as closest-prior-art has to be first concluded.

III. FURTHER SUBMISSIONS

1.

Any further submission by the parties should be made within the time limit of Rule 116.

Late filed facts, evidence, requests may be disregarded by the OD (see Rule 116, Article 114(2) EPC; Guidelines E-VI, 2.1 and 2.2).

2.

In view of the amount of the submissions made, the OD issues the present summons for **three consecutive days**. It is however anticipated that this is only made as a precaution in case this is actually required. No rights can be derived therefrom and it is possible that - according to the circumstances - the actual duration will be shorter.

19170936.9

CONSOLIDATED LIST – KONKORDANZLISTE - LISTE DE CONCORDANCE

P: Centripetal Networks Inc.

1 : IXIA

2 : Cisco Systems GmbH (INTERV)

3 : Keysight Technologies Deutschland GmbH

4 : Palo Alto Networks, Inc.

EPO	CITATIONS-ENTGEGENHALTUNGEN-ANTÉRIORITÉS	P	1	2	3	4
D1	WO2015/160567 A1		D2			
D2	EP3550795 (B1)			D2		
D3	Copy of infringement complaint			D3		
D4	Court Order served on March 15, 2022			D4		
D5	Documents of application underlying the opposed patent			D5		
D6	Documents as filed with the parent application			D6		
D7	WOUS14,253,992 (A)			D7		
D8	Feature analysis			D8		
D9	Markup copy of the claim amendments			D9		
D10	US2004/123220 (A1)			D10		
D11	US2006/136987 (A1)			D11		
D12	US2007/240208 (A1)			D12		
D13	US2006/146879 (A1)			D13		
D14	US8,306,994 (B2)			D14		
D15	US2005/138204 (A1)			D15		
D16	US2006/195896 (A1)			D16		
D17	US2006/248580 (A1)			D17		
D18	US2011/055916 (A1)			D18		
D19	"Sourcefire 3D System User Guide" Version 4.10, published in 2011			D19	K4	
D19a	Sourcefire VRT™: Focused on Protecting "Your" Network, 2011		D19a			
D19b	Snapshot of the Snort Website www.snort.org in the Wcbarehive taken on 03.03.2013		D19b			
D20	Affidavit-1			D20		
D21	Affidavit-2			D21		
D22	Final Decision by The US Court of Appeals of the Federal Circuit			D22		
D23	"Sourcefire 3D System User Guide" Version 5.1.1, published in 2012			D23		
D24	Affidavit-3			D24		

D25	Espinoza, Mireya, "Frost & Sullivan Recognizes Sourcefire for Next-Generation IPS" Frost & Sullivan; PR Newswire, 14 May 2013			D25		
EPO	CITATIONS-ENTGEGENHALTUNGEN-ANTÉRIORITÉS	P	1	2	3	4
D26	Perridge, Anthony, "For CyberSecurity Professionals, is the Concept of "Control" a Pipe Dream?" Daily News Egypt, 16 January 2014			D26		
D27	Barnum, Sean, "Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™)" The Mitre Corporation, 20.02.2014			D27		
D28	Excerpt from Wayback Machine with TAXII Website excerpt showing FAQ, dated February 19, 2014			D28		
D29	Excerpt from Wayback Machine showing the date of archival of the TAXII Website excerpt, dated February 19, 2014			D29		
D30	Terrapinn, Limited, "Infoblox gives global businesses greater network control" Total Telecom, 24 January 2013			D30		
D31	US2011/072506 (A1)			D31		
D32	US2010/257598 (A1)			D32		
D33	"Syslog", RFC 5424, published in March 2009			D33		
D34	"Syslog" change history			D34		
D35	US8,204,082 (B2)			D35		
D36	US2011/314177 (A1)			D36		
D37	"An Architecture for Differentiated Services", RFC 2475, published in December 1998			D37		
D38	Publication history of "An Architecture for Differentiated Services"			D38		
D39	Action for alleged infringement dated 1 January 2022 (partly blackened version)				K1	
D40	Proof-of-service document, dated 26 February 2022				K2	
D41	Juniper Networks, Concepts & Examples Screen OS Reference Guide, Release 6.3.0, Rev. 02 (10.12.2012)				K3	
D41a	Print-out of document properties of pdf-version of K3/Juniper downloaded from https://www.juniper.net/documentation/software/screensos/screensos6.3.0/630_ce_all.pdf				K3a	
D41b	Juniper Networks Network and Security Manager, Administration Guide". 2011		D41b			
D41c	Print-out of Juniper documentation Website https://www.juniper.net/documentation/software/management/security-manager/index.html		D41c			
D42	Website www.sourcefire.com/security-technologies/cyber-security-products/3d-system archived in web.archive.org/web/20110502063459/http://www.sourcefire.com/security-technologies/cyber-security-products/3d-system on 02.05.2011				K4a	
D43	US 2013/0263247 A1 (03.10.2013)				K5	
D44	US 7,966,659 B1 (21.06.2011)				K6	
D45	WO 2012/164336 A1 (06.12.2012)				K7	
D46	Complaint_EP3550795_Redacted					E1

D47	Notice_of_delivery_of_the complaint					E2
D48	US 8,572,717 B2, published 29 October 2013					E3
D49	US 7,095,716 B1, published 22 August 2006					E4
D50	Affidavit of Mr Jacob H. Baugher			D50		