Internal distribution code:

(A) [-] Publication in OJ
(B) [-] To Chairmen and Members
(C) [-] To Chairmen
(D) [X] No distribution

Datasheet for the decision of 30 October 2025

Case Number: T 1907/23 - 3.5.05

Application Number: 19170936.9

Publication Number: 3550795

IPC: H04L29/06

Language of the proceedings: EN

Title of invention:
Methods and systems for protecting a secured network

Patent Proprietor:
Centripetal Limited

Opponents:
Ixia
Cisco Systems GmbH
Keysight Technologies Deutschland GmbH
Palo Alto Networks, Inc.

Headword:
Logging and monitoring packets/CENTRIPETAL

Relevant legal provisions:
EPC Art. 76(1), 123(3)

Keyword:

Added subject-matter - main request and auxiliary requests 1a, 2 to 18 (yes): combination of different embodiments not originally disclosed

Extension of scope of protection - auxiliary requests 1, 19 to 22 (yes)

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern

Boards of Appeal

Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0

Case Number: T 1907/23 - 3.5.05

D E C I S I O N
of Technical Board of Appeal 3.5.05
of 30 October 2025

Appellant: (Patent Proprietor)	Centripetal Limited Galway Technology Centre Mervue Business Park Galway (IE)
Representative:	MFG Patentanwälte Meyer-Wildhagen Meggle-Freund Gerhard PartG mbB Amalienstraße 62 80799 München (DE)
Respondent I: (Opponent 1)	Ixia 1400 Fountaingrove Parkway Santa Rosa, CA 95403 (US)
Representative:	Samson & Partner Patentanwälte mbB Widenmayerstraße 6 80538 München (DE)
Respondent II: (Opponent 2)	Cisco Systems GmbH Parkring 20 85748 Garching (DE)
Representative:	Bardehle Pagenberg Partnerschaft mbB Patentanwälte Rechtsanwälte Prinzregentenplatz 7 81675 München (DE)
Respondent III: (Opponent 3)	Keysight Technologies Deutschland GmbH Herrenberger Str. 130 71034 Böblingen (DE)
Representative:	Samson & Partner Patentanwälte mbB Widenmayerstraße 6 80538 München (DE)

Respondent IV: (Opponent 4)	Palo Alto Networks, Inc. 3000 Tannery Way Santa Clara, CA 95054 (US)
Representative:	Schmid, Andreas Hogan Lovells International LLP Karl-Scharnagl-Ring 5 80539 München (DE)
Decision under appeal:	**Decision of the Opposition Division of the European Patent Office posted on 15 September 2023 revoking European patent No. 3550795 pursuant to Article 101(3)(b) EPC.**

Composition of the Board:

Chair	K. Bengi-Akyürek
Members:	P. Tabery
	R. Romandini

Summary of Facts and Submissions

I. The appeal lies from the decision of the opposition division to revoke the opposed patent.

The opposition division found that the subject-matter of the independent claims either extends beyond the content of the earlier application as filed (main request and auxiliary requests 10 to 12) or extends the protection (auxiliary requests 1 and 19 to 22). Auxiliary requests 2 to 9 and 13 to 18 were not admitted into the opposition proceedings.

II. Oral proceedings before the board were held on 30 October 2025. The final requests of the parties were as follows:

- The appellant-proprietor (henceforth "the proprietor") requested that the appealed decision be set aside and that the oppositions be rejected (**main request**). Alternatively, it was requested that the patent be maintained in amended form in accordance with one of **auxiliary requests 1, 1a, 2 to 22.**

- The respondents-opponents O1 to O4 (henceforth "opponents") requested that the appeal be dismissed.

At the end of the oral proceedings, the board's decision was announced.

III. Claim 1 of the **main request** reads as follows (labelling as in the decision under appeal):

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 (120) 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."

Claim 1 of **auxiliary request 1** differs from claim 1 of the main request, *inter alia*, in that feature 1.2.6 has been amended as follows (additions as underlined by the proprietor, deletions not shown):

> "forwarding, by the packet security gateway, the packet log to a monitoring device configured to store the packet log for subsequent analysis".

Claim 1 of **auxiliary requests 1a and 2 to 18** differs from claim 1 of the main request, *inter alia*, in that **features 1.2.2 to 1.2.5**, relating to "packet digest logging", have been amended in various ways. On the other hand, **feature 1.2.6**, concerning "packet routing" is unamended vis-à-vis claim 1 of the main request.

Claim 1 of **auxiliary requests 19 to 22** differs from claim 1 of the main request, *inter alia*, in that feature 1.2.6 has been amended as follows (additions as underlined by the proprietor, deletions not shown):

> "forwarding, by the packet security gateway, the packet log to an awareness application server configured to store the packet [log] for subsequent analysis".

Reasons for the Decision

1. The opposed patent concerns protecting a secured network using "packet security gateways". A "security policy management server" is supposed to send a "dynamic security policy" to the packet security gateways, specifying a "packet transformation function" to be performed on the received packets. According to the patent specification, said dynamic security

policies may be applied to multiple different services (such as the so-called "blocklist", "allowlist", "VoIP firewall", "phased restoration", "enqueueing", "monitoring" or "network awareness" services; see paragraphs [0034] to [0041]).

2. Main request (patent as granted)

2.1 Added subject-matter (Article 100(c) EPC)

2.1.1 Claim 1 specifies the combination of **features 1.2.2 to 1.2.5**, relating to "packet digest logging" (associated with the "network awareness service" according to the original disclosure), with **feature 1.2.6** relating to "packet routing" to a monitoring device (associated with the "monitoring service" according to the original disclosure).

2.1.2 The proprietor cited paragraphs [53], [54], [40], [47] and [70] of the earlier application (WO 2015/160567 A1, the "parent" application) to support this combination. In view of the well-established "disclosure test" according to the case law of the Boards of Appeal, which was to be applied in an equal way for both novelty and added-matter assessments alike, the skilled reader of the original application would have, without any difficulties, picked up one or several embodiments relating to the multiple services supported (see point 1 above) and would have readily combined them. Those embodiments would thus have been considered *complementary* rather than *alternative* implementation options. No new technical information would have thus arisen from such a "selection from a list".

2.1.3 The board is not persuaded. In fact, paragraph [53] relates to an embodiment, where a "dynamic security

policy" includes a "packet transformation function" for "routing" packets to a "monitoring device". On the other hand, paragraph [54] relates to an embodiment, where a "dynamic security policy" includes a "packet transformation function" for producing a "digest version, or log, of the packet". It is common ground that paragraphs [40], [47] and [70] of the parent application as filed disclose that a packet may also be subject to several "packet transformation functions". However, none of these paragraphs specifies that this includes a particular packet being subject to both, the "routing to a monitoring device" as well as a "packet digest logging function". The board considers that the skilled person would understand from paragraphs [53] and [54] of the parent application as filed that they relate to *alternative* (rather than *complementary*) solutions for storing selected aspects of packets. Both solutions relate to extracting information from packets (paragraph [53]: "*copy the packets or data contained within them*"; paragraph [54]: "*produces a digest version, or log, of the packet*", wherein the "*packet log (or digest) may contain selected packet information*") and forwarding this information to another entity (paragraph [53]: "*to route or switch packets [...] to a monitoring device*"; paragraph [54]: "*may store and/or forward packet logs*").

2.1.4 The fact that paragraph [53] names "*review by law enforcement*" as a benefit, whereas the subsequent paragraph [54] mentions "*access by client applications*", cannot change this understanding. Notably, the expression "*access by client applications*" is vague and broad enough to also comprise client applications used for law enforcement.

2.1.5 The board does not subscribe to the proprietor's argument that paragraphs [53] and [54] of the parent application related to complementary functions which thus presented themselves to the skilled reader as being readily combinable. Contrary to what is argued by the proprietor, the original parent application neither discloses that *logging* "generates compact, indexable records for real-time visibility and correlation, nor that the *routing to the monitoring device* "preserves high-fidelity content for retrospective analysis".

2.1.6 Lastly, the board is not convinced by the proprietor's argument that the combination of "logging" a packet and "routing" it to a monitoring device constituted a mere selection from a list of "packet transformation functions" disclosed in the parent application and were thus to be considered as originally disclosed. Rather, the board holds that, for the reasons provided *supra*, the two functions under scrutiny offer themselves as *alternatives* which the skilled reader would thus not consider implementing in combination. In other words, the skilled person would not have directly and unambiguously deduced from the original teaching that (at least) two services (i.e. the "network awareness" and "monitoring" services) amongst the available services (see point 1 above) could be simply combined - not least due to the existence of a multitude of - possibly contradictory or colliding - rules underlying the respective "dynamic security policies" of the available services to be eventually applied to the data packets received at the "packet security gateway". Thus, only by mere speculation one could assume that the skilled person would have directly and unambiguously selected two items from a list and considered combining the rules associated with separate services to the same data packet received at the

respective "gateway". Moreover, contrary to the proprietor's allegation, supporting multiple, modular "packet transformation functions (PTFs)" does not mean that the claimed "logging" and "routing" steps are indeed performed for the very same data packet.

2.1.7 In view of the above, the skilled person is faced with new technical information vis-à-vis the disclosure of the parent application as filed when reading the combination of features 1.2.2 to 1.2.5 with feature 1.2.6 of present claim 1.

2.2 Consequently, the main request is not allowable under Article 100(c) EPC as it extends beyond the content of the parent application as filed.

3. Auxiliary requests 1 and 19 to 22

3.1 Extension of protection (Article 123(3) EPC)

3.1.1 As to claim 1 of **auxiliary request 1**, the board concurs with the opposition division and the opponents that the amended feature "*forwarding [...] the packet log*" introduced into **feature 1.2.6** constitutes a shift in scope and thus an illicit extension of the protection conferred by this claim. In particular, said "log" may consist of information different from that contained in the received data packet, e.g. "arrival times" (see e.g. paragraph [54] of the application as filed). This is due to the fact that "forwarding" of the packet's arrival time does not fall within the definition of feature 1.2.6 while it falls within that of feature 1.2.6 as amended.

3.1.2 The same objection applies to claim 1 of **auxiliary requests 19 to 22**.

3.2 In view of the above, auxiliary requests 1 and 19 to 22 are not allowable under Article 123(3) EPC.

4. Auxiliary requests 1a and 2 to 18

4.1 The objection raised in points 2.1.1 to 2.1.7 above (combination of "packet digest logging" and "packet routing") with respect to claim 1 of the main request applies likewise to claim 1 of each of auxiliary requests 1a and 2 to 18.

4.2 In view of the above and irrespective of admittance considerations, auxiliary requests 1a and 2 to 18 are not allowable under Article 76(1) EPC.

5. With no allowable claim request on file, the appeal must be dismissed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chair:

B. Brückner K. Bengi-Akyürek

Decision electronically authenticated