

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PALO ALTO NETWORKS, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, INC.,
Patent Owner.

IPR2021-01150
Patent 10,530,903 B2

Before STACEY G. WHITE, JON M. JURGOVAN, and
AARON W. MOORE, *Administrative Patent Judges*.

WHITE, *Administrative Patent Judge*.

JUDGMENT

Final Written Decision on Remand
Determining No Challenged Claims Unpatentable
35 U.S.C. §§ 144, 318

I. INTRODUCTION

We address this case on remand after a decision by the U.S. Court of Appeals for the Federal Circuit in *Palo Alto Networks, Inc. v. Centripetal Networks, LLC*, 122 F.4th 1378 (Fed. Cir. 2024) (“Remand Decision”).

A. Background

Palo Alto Networks, Inc. (“Petitioner”) filed a Petition (Paper 2, “Pet.”) requesting *inter partes* review of claims 1–18 of U.S. Patent No. 10,530,903 B2 (Ex. 1001, “the ’903 patent”). We instituted review of the challenged claims on all asserted grounds. Paper 9 (“Dec.”). After institution, Centripetal Networks, Inc. (“Patent Owner”) filed a Patent Owner Response (Paper 19, “PO Resp.”), Petitioner filed a Reply (Paper 23, “Reply”), and Patent Owner filed a Sur-Reply (Paper 26). A transcript of the oral hearing held on October 31, 2022, was entered into the record (Paper 34, “Tr.”).

We issued a Final Written Decision on February 16, 2023, concluding that Petitioner had not shown by a preponderance of the evidence that claims 1–18 of the ’903 patent are unpatentable. Paper 37 (“Final Dec.”). Petitioner appealed the Final Written Decision to the United States Court of Appeals for the Federal Circuit. Paper 38.

On December 16, 2024, the Federal Circuit issued a decision vacating the Final Written Decision for “not clearly explaining its holding or rationale regarding motivation to combine and whether the proposed combination teaches the final limitation of claim 1: transmitting an indication of the first host responsive to the correlating.” *Palo Alto Networks*, 122 F.4th at 1384. In the opinion, the Federal Circuit explained that the Final Written Decision “never made a clear finding on whether a person of ordinary skill in the art

would have been motivated to modify Paxton by adding Sutton’s step of transmitting a notification of malicious activity after Paxton’s correlation step,” as proposed by Petitioner. *Id.* at 1385. The Federal Circuit stated that the Board “failed to explain why a person of ordinary skill in the art would not have been motivated to modify Paxton to provide the recited notification as taught by Sutton in response to the correlation disclosed in Paxton.” *Id.* The Federal Circuit concluded that “[b]y reading Paxton and Sutton in isolation, the Board erred,” and that

we vacate and remand for the Board to clarify and explain its holding on whether a person of ordinary skill in the art would have been motivated to transmit the identity of the first host (e.g., to an administrator) as taught by Sutton, responsive to the correlating disclosed by Paxton to improve network security.

Id. at 1386.

On February 12, 2025, a call was held with the parties and Judges White, Jurgovan, and Moore to discuss the remand proceedings. On February 20, 2025, we entered an Order authorizing the parties to submit briefing as to “whether a person of ordinary skill in the art would have been motivated to transmit the identity of the first host (e.g., to an administrator) as taught by Sutton, responsive to the correlating disclosed by Paxton to improve network security.” Paper 43, 4. The Order precluded the parties from filing additional evidence. *Id.* at 4. The parties duly filed their remand briefs. Papers 45 (“PO Remand Br.”), 46 (“Pet. Remand Br.”).

For the reasons discussed below, after considering the post-remand briefing, as well as the record previously developed during trial and the Federal Circuit’s Remand Decision, we conclude that Petitioner has not met

its burden to establish by a preponderance of the evidence that the challenged claims are unpatentable.

B. Related Proceedings

The parties indicate that the '903 patent is the subject of the following co-pending district court case: *Centripetal Networks, Inc. v. Palo Alto Networks, Inc.*, No. 2:21-cv-00137 (E.D. Va.). Paper 33, 1; Paper 3, 1. Petitioner informs us that the district court case has been stayed pending the resolution of this proceeding. Paper 12, 1.

C. The '903 Patent

The '903 patent discloses methods and systems for “correlating packets in communications networks.” Ex. 1001, 1:38–39. Figure 1, reproduced below with added coloring, shows the architecture of a system for performing the claimed technique (Pet. 9):

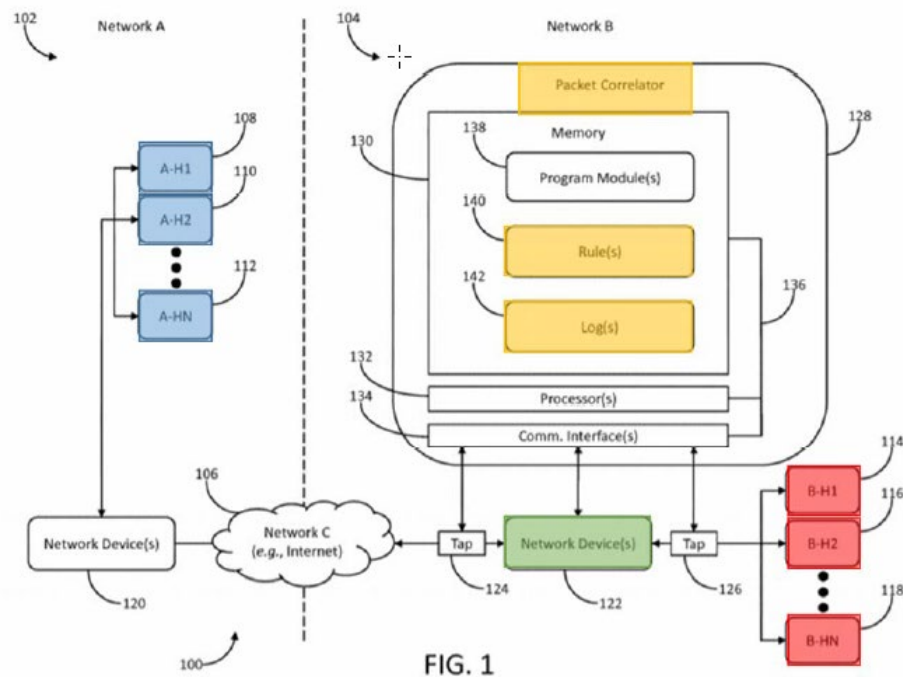


Figure 1, reproduced above (as annotated by Petitioner), depicts an environment for correlating packets in communications networks. Ex. 1001,

2:7–9. The system includes network device 122, in green, that communicates with packet correlator 128. The packet correlator includes rules 140 and logs 142, shown in yellow. Taps 124 and 126 are located on either side of the network device and also communicate with the packet correlator. The components are arranged such that network traffic between, for example, host A-H1 in Network A, in blue, and host B-H1 in Network B, in red, would pass through a tap, then the network device, then the other tap.

The '903 patent explains that, in the case of packets moving from Network B to Network A, the network device “may include one or more devices that alter one or more aspects of the packets . . . in a way that obfuscates the association of the packets received from” the Network B host and the corresponding packets generated by the network device and sent to the Network A host. *See* Ex. 1001, 5:8–21. For example, the network device “may be configured to perform network address translation (NAT) for network addresses associated with [Network B],” such that “the packets received from host [B–H1] . . . may comprise network- or transport-layer header information identifying their source as a network address associated with host [B–H1],” but the corresponding packets generated by the network device “may comprise network- or transport-layer header information identifying their source as a network address associated with [the network device].” *Id.* at 5:23–37.

The '903 patent's method is described in connection with Figures 2A–D. At step 1, the packet correlator generates rules that are supplied to the taps at steps 2 and 3. *See* Ex. 1001, 3:34–51. At step 4, host B-H1 transmits data (packets P1, P2, and P3) destined for host A-H1. *See id.* at 3:52–62. At steps 5 and 6, if the packets match the rules provided to tap

126, that tap sends log data to the packet correlator. *See id.* at 3:62–4:10. At step 7, the network device 122 receives packets P1, P2, and P3, modifies them, and sends the modified packets towards host A-H1 as packets P1', P2', and P3'. *See id.* at 5:4–6:10. Those packets may, for example, have new source address information identifying the network device rather than the originating host. *Id.* at 5:23–27. As the modified packets matching the rules pass through tap 124, that tap sends log data to the packet correlator. *See id.* at 6:10–34. Steps 10–15 repeat that process, where data is being sent from host B-H2 to host A-H1. *See id.* at 6:61–8:46.

At step 16, the packet correlator “may utilize log(s) 142 to correlate the packets transmitted by network device(s) 122 with the packets received by network device(s) 122.” *Id.* at 8:47–49. This may be done by comparing “network-layer information, transport-layer information, application-layer information, or environmental variable(s)” and/or “timestamps” of the log entries. *See id.* at 8:49–9:44.

In steps 17 and 18, data sent from host B-H2 to host A-H2 does not match rules in the taps and thus, is not logged. *See id.* at 9:45–10:13. Steps 19–24 show data being sent from host B-H1 to host A-H1 that does match rules and is logged. *See id.* at 10:14–11:60.

Step 25 is another correlation, in which network-layer information, transport-layer information, application-layer information, environmental variables, and/or time stamps are used to correlate packet P10' with packet P10. *See id.* at 11:60–12:55. Then, in step 26, “[r]esponsive to correlating the packets,” the packet correlator “may determine, based on one or more of the entries in log(s) 142, a network address associated with a host located in network [B] that is associated with a packet transmitted by network

device(s) 122.” *Id.* at 12:55–62. For example, “responsive to correlating P10’ with P10,” the packet correlator “may determine . . . that the network address associated with host [B-H1] is associated with P10’ (e.g., a communication with host [A-H1]).” *Id.* at 12:62–67.

At step 27, the packet correlator “may generate one or more messages identifying [host B-H1].” *Id.* at 12:66–13:1. “For example, host [A-H1] may be associated with a malicious entity,” and the messages “may indicate that host [B-H1] communicated with host [A-H1] (e.g., the malicious entity).” *Id.* at 13:2–7. The messages are sent to a user and an administrator at steps 28 and 29. *See id.* at 13:7–15.

At step 30, the packet correlator generates and updates the rules, for example, “to configure tap devices 124 and 126 to identify and drop packets received from host [B-H1].” *Id.* at 13:16–20. The packet correlator provisions the tap devices with the rules at steps 31 and 32. *See id.* at 13:20–23. Then, at step 33, host B-H1 communicates one or more packets but, at step 34, tap 126 identifies and drops the packets to prevent the spread of malware. *See id.* at 13:23–28.

D. Illustrative Claim

Petitioner challenges claims 1–18, with claims 1 and 10 being independent. Independent claim 1 is illustrative of the challenged claims and is reproduced below.

1. A method comprising:
determining, by a computing system, that a network device has received, from a first host located in a first network, a plurality of first packets corresponding to first requests for content from a second host located in a second network, wherein the network device comprises a proxy;

determining, by the computing system, that the network device has generated a plurality of second packets corresponding to second requests, wherein the second requests correspond to the first requests, and wherein the second requests are configured to cause the second host to transmit, to the network device, the content;

generating, by the computing system, a first plurality of log entries corresponding to the plurality of first packets, wherein each of the first plurality of log entries comprises a receipt timestamp indicating a packet receipt time, and wherein the first plurality of log entries comprise first data from the first requests;

generating, by the computing system, a second plurality of log entries corresponding to a plurality of second packets, wherein each of the second plurality of log entries comprises a transmission timestamp indicating a packet transmission time, and wherein the second plurality of log entries comprise second data from the second requests;

determining, by the computing system and for each transmission timestamp, differences between at least one packet transmission time indicated by transmission timestamps and at least one packet receipt time indicated by receipt timestamps;

correlating, based on the differences and by comparing the first data and the second data, at least a portion of the plurality of first packets and at least a portion of the plurality of second packets; and

responsive to the correlating:

generating, by the computing system, an indication of the first host; and

transmitting, by the computing system, the indication of the first host.

Ex. 1001, 15:20–60.

E. Asserted Ground of Unpatentability

Petitioner asserts the following ground of unpatentability (Pet. 5):

Challenged Claims	Basis	References
1–18	§ 103 ¹	Paxton ² , Sutton ³ , and Ivershen ⁴

Petitioner’s challenges are supported by the Declaration of Dr. Robert Akl (Ex. 1003).

II. ANALYSIS

A. Level of Ordinary Skill in the Art

To determine whether an invention would have been obvious at the time it was made, we consider the level of ordinary skill in the pertinent art at the time of the invention. *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966). The resolution of this question is important because it allows us to “maintain[] objectivity in the obviousness inquiry.” *Ryko Mfg. Co. v. Nu-Star, Inc.*, 950 F.2d 714, 718 (Fed. Cir. 1991). In assessing the level of ordinary skill in the art, various factors may be considered, including the “type of problems encountered in the art; prior art solutions to those problems; rapidity with which innovations are made; sophistication of the technology; and educational level of active workers in the field.” *In re GPAC, Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995) (quotation omitted). Generally, it is easier to establish obviousness under a higher level of

¹ The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 285–88 (2011), revised 35 U.S.C. § 103 effective March 16, 2013. Because the ’903 patent has an effective filing date prior to the effective date of the applicable AIA amendment, we refer to the pre-AIA version of § 103.

² U.S. Pat. Application Publication No. 2014/0280778 A1 (published Sept. 18, 2014) (Ex. 1004).

³ U.S. Patent No. 8,413,238 B1 (issued Apr. 2, 2013) (Ex. 1007).

⁴ U.S. Patent No. 8,219,675 B2 (issued July 10, 2012) (Ex. 1005).

ordinary skill in the art. *Innovation Toys, LLC v. MGA Entm't, Inc.*, 637 F.3d 1314, 1323 (Fed. Cir. 2011) (“A less sophisticated level of skill generally favors a determination of nonobviousness . . . while a higher level of skill favors the reverse.”).

Petitioner asserts that a person of ordinary skill in the art at the time of the alleged invention of the '903 patent “had a bachelor’s degree in electrical engineering, computer engineering, computer science, or a related field, and approximately 2–3 years of experience in the design or development of telecommunication systems, or the equivalent.” Pet. 13 (citing Ex. 1003 ¶¶ 18–20). Petitioner further notes that “[a]dditional graduate education could substitute for professional experience, or significant experience in the field could substitute for formal education.” *Id.* Patent Owner’s proposed level of ordinary skill is similar, with Patent Owner contending that the ordinary skilled artisan “would be someone with a bachelor’s degree in computer science, electrical engineering, or related field, and either (1) two or more years of industry experience and/or (2) an advanced degree in computer science or related field.” PO Resp. 12–13 (citing Ex. 2019 ¶¶ 27–31). Similar to Petitioner, Patent Owner also states that a person of ordinary skill in the art “may have additional industry experience in lieu of a formal degree.” *Id.* at 13.

In the Institution Decision, we adopted Petitioner’s assessment of the level of skill in the art. Dec. 21. Patent Owner offers a different formulation in the Response, but neither party provides substantive argument as to why its proposed level of skill is correct. *See* Pet. 13; PO Resp. 12–13. We do not find a material difference between the parties’ proposals.

Based on this record, we apply the level of skill adopted in our Institution Decision because it is consistent with the level of ordinary skill in the art at the time of the invention as reflected in the prior art of record. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001). Accordingly, we find for the purpose of this Decision and based on the record before us, that a person of ordinary skill in the art at the relevant time would have a bachelor’s degree in electrical engineering, computer engineering, computer science, or a related field, and approximately 2–3 years of experience in the design or development of telecommunication systems, or the equivalent. We note, however, that our determinations on patentability would not change if we accepted Patent Owner’s proposed level of skill.

B. Claim Construction

In an *inter partes* review proceeding, a patent claim shall be construed using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. § 282(b). 37 C.F.R. § 42.100(b) (2020). This rule adopts the same claim construction standard used by Article III federal courts, which follow *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc), and its progeny. Under this standard, the words of a claim are generally given their “ordinary and customary meaning,” which is the meaning the term would have to a person of ordinary skill at the time of the invention, in the context of the entire patent including the specification and prosecution history. *See Phillips*, 415 F.3d at 1312–13.

Petitioner asserts “no terms require construction.” Pet. 13. Patent Owner discusses its views as to the plain and ordinary meaning of “responsive to the correlating . . . transmitting, by the computer system, the

indication of the first host,” “determining . . . differences between . . . packet transmission time . . . and packet receipt time,” “network-interface identifier,” and “encapsulating.” PO Resp. 13–25.

After review of the current record, we conclude that no express claim construction is necessary for the purposes of this Decision. *See, e.g., Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)) (“[W]e need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy.’”).

C. Obviousness of Claims over Paxton, Sutton, and Ivershen

Petitioner asserts that claims 1–18 are unpatentable under 35 U.S.C. § 103(a) as obvious over Paxton, Sutton, and Ivershen, citing the Declaration of Dr. Robert Akl for support. Pet. 5; Ex. 1003. Petitioner provides explanations as to how the prior art allegedly teaches each claim limitation. *Id.* at 14–70. Patent Owner opposes Petitioner’s contentions with the support of Michael Goodrich, Ph.D. *See* PO Resp., Ex. 2019.

i. *Paxton (Ex. 1004)*

Paxton is titled “Tracking Network Packets Across Translational Boundaries,” and “relates generally to identifying network packets, and more particularly, to determining the identity of network packets as they traverse boundaries that perform Network Address Translation (NAT).” Ex. 1004, code (54), ¶ 2. Paxton’s method for tracking network packets (i) calculates a first hash of a packet application layer payload at an inside sensor before a boundary located between a client and a server, (ii) stores a first hash data record at a device that has direct access to the inside sensor, (iii) calculates a second hash of the packet application layer payload at an

outside sensor after the boundary, (iv) stores a second hash data record at a device that has direct access to the outside sensor, (v) transmits the packet from the client to the server, or from the server to the client, and (vi) determines whether the first hash data record and the second hash data record match. *Id.* at code (57). The first hash data record and second hash data record may include a hash value, an IP address, and a timestamp. *Id.* Paxton explains that the ability to identify the true source of a packet transmission through a boundary can provide significant benefits to network security—e.g., by enabling identification of nodes that are infected with malicious content, and by enabling attribution of malicious activity sensed at the edge of a network back to its original source. *Id.* ¶ 30.

Figure 1 of Paxton is reproduced below.

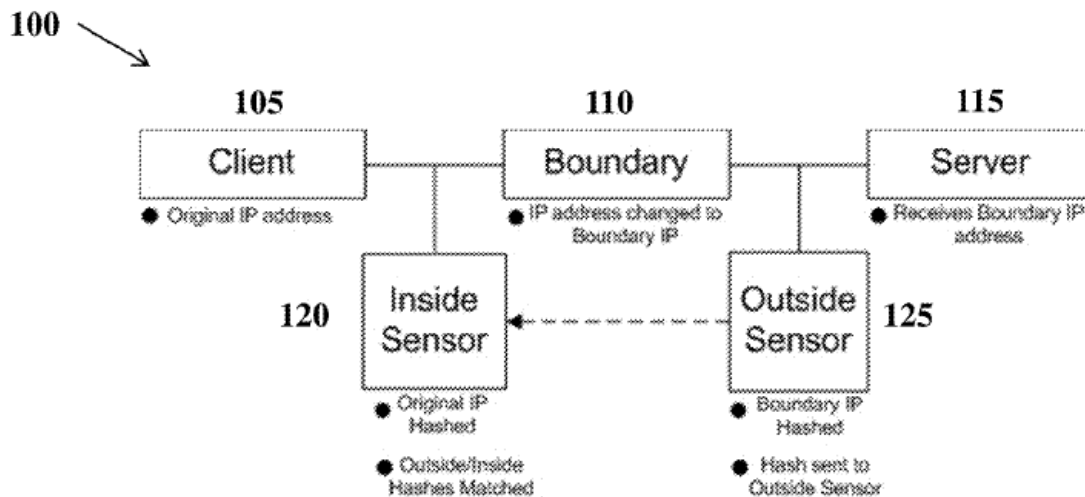


Figure 1 of Paxton, reproduced above, shows system diagram 100 for tracking packets across translation boundaries. *Id.* ¶¶ 11, 15. Packets are sent from client 105 across boundary 110 to server 115. *Id.* ¶ 16. When a packet is transmitted from client 105, inside sensor 120 calculates a hash, e.g., an MD5 algorithm hash, of the application layer payload, and stores it along with the network layer header. *Id.* ¶ 17. After the packet traverses

boundary 110, outside sensor 125 calculates a hash of the payload along with the header data of the packet. *Id.* Inside sensor 120 and outside sensor 125 can be two commodity servers running full packet capture, with inside sensor 120 passively recording traffic on client 105 network before the contents are altered by the boundary, and outside sensor 125 passively recording traffic externally after it has been modified by the boundary. *Id.*

¶ 18. Paxton explains that payloads can be matched based on at least three criteria (hash, time, and IP address), such that when an identical hash is observed on outside sensor 125 and inside sensor 120, there is a high probability that the hashes belong to the same payload. *Id.* ¶ 21. Hashes from inside sensor 120 and outside sensor 125 can be matched via a first-in-first-out queue based on recorded timestamps in the first hash data record and second hash data record. *Id.* ¶ 22. For example, after a hash is observed on the outside, the closest matching hash (with respect to the timestamp) on the inside can be identified as the corresponding match, and the combination of identifiable inside and outside header data can serve as the identity of the packet. *Id.* Figure 3 of Paxton, reproduced below, is a diagram illustrating a first-in-first-out matching approach. *Id.* ¶¶ 13, 24.

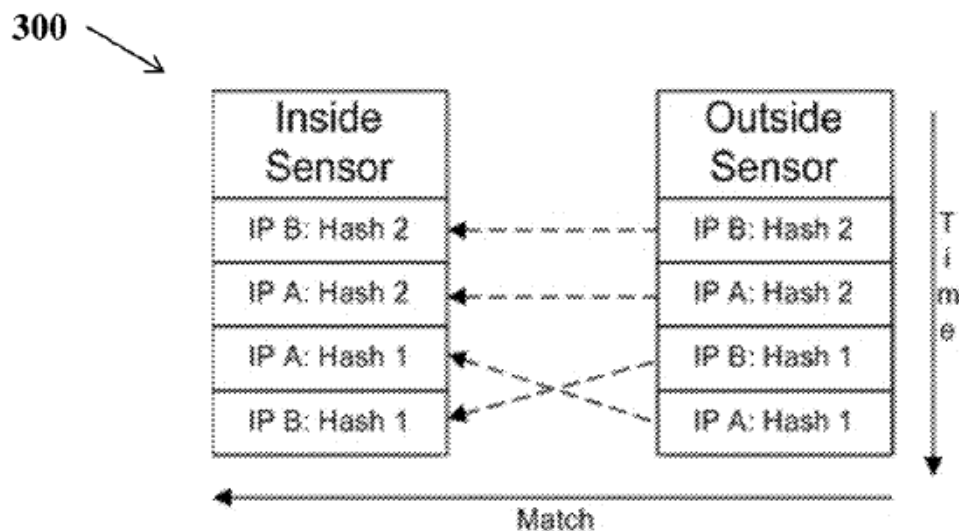


Figure 3 of Paxton, reproduced above, shows four packets that have been hashed by both inside sensor 120 and outside sensor 125, including two packets, 1 and 2, sent from both IP A and IP B (for a total of four packets).

Id. ¶ 24. Figure 3 shows what happens when packets are sensed in a different order across boundaries. *Id.* In Figure 3, each of IP A and IP B sends two messages that are the same (IP A:Hash 1 and IP A:Hash 2 are equal, and IP B:Hash 1 and IP B:Hash 2 are equal). *Id.* The initial order of which the packets were sent from the original source was IP A:Hash 1, IP A:Hash 2, IP B:Hash 1, and IP B:Hash 2. *Id.* However, the order of which the packets were sensed by inside sensor 120 was IP B:Hash 2, IP A:Hash 2, IP A:Hash 1, and IP B:Hash 1, while the order of which the packets were sensed at outside sensor 125 was IP B:Hash 2, IP A:Hash 2, IP B:Hash 1, IP A:Hash 1. *Id.* Therefore, IP B:Hash 2 was the first message recorded in both inside sensor 120 and outside sensor 125, and even though this packet has the same hash value of IP B:Hash 1, since it was sensed first on both sides, the sensed packets can be matched together first. *Id.* ¶ 25. Packets IP A:Hash 1 and IP B:Hash 1 were sensed in a different order across inside sensor 120 and outside sensor 125. *Id.* ¶ 25. IP A:Hash 1 and IP B:Hash 1 have different hash values and thus, the matching module does not consider them for matching; instead, the matching module finds the match at the next available matching hash, which was IP A:Hash 1. *Id.* The matching module can then conclude with the final match IP B:Hash 1. *Id.*

Paxton explains that the system for matching cryptographically hashed payloads as described so far, assumes that the payloads sensed both inside and outside are identical. *Id.* ¶ 28. According to Paxton, if either payload has been altered (e.g., by non-transparent proxies that can make

slight modifications to the payload to perform a media type transformation, protocol reduction, or anonymity filtering), the computed hash will not be the same, and therefore, will not match. *Id.* Paxton explains that

different classes of hashing techniques could be leveraged in order to account for slight variations in payload alterations. For example, fuzzy hashing may be able to match payloads that have been slightly altered, as in the case of non-transparent proxies or deep packet inspection platforms. Fuzzy hashing is similar to traditional cryptographic hashing; with the exception that it produces a result value that is reflective of how similar the original data is to the altered data.

Id. ¶ 29.

ii. *Sutton (Ex. 1007)*

Sutton is titled “Monitoring Darknet Access to Identify Malicious Activity,” and “relates to identification of potentially malicious activity based upon access attempts to darknet addresses.” Ex. 1007, code (57), 2:7–10. Sutton discloses a technique of monitoring darknet access by: identifying a list of darknet addresses; monitoring communications originating from a protected network; comparing destination addresses of the monitored communications originating from the protected network to the list of darknet addresses; and, if a match is found between the destination addresses and the list of darknet addresses, providing notification of potential malicious activity originating from the protected network. *Id.* at 2:10–19.

Figure 2 of Sutton is reproduced below.

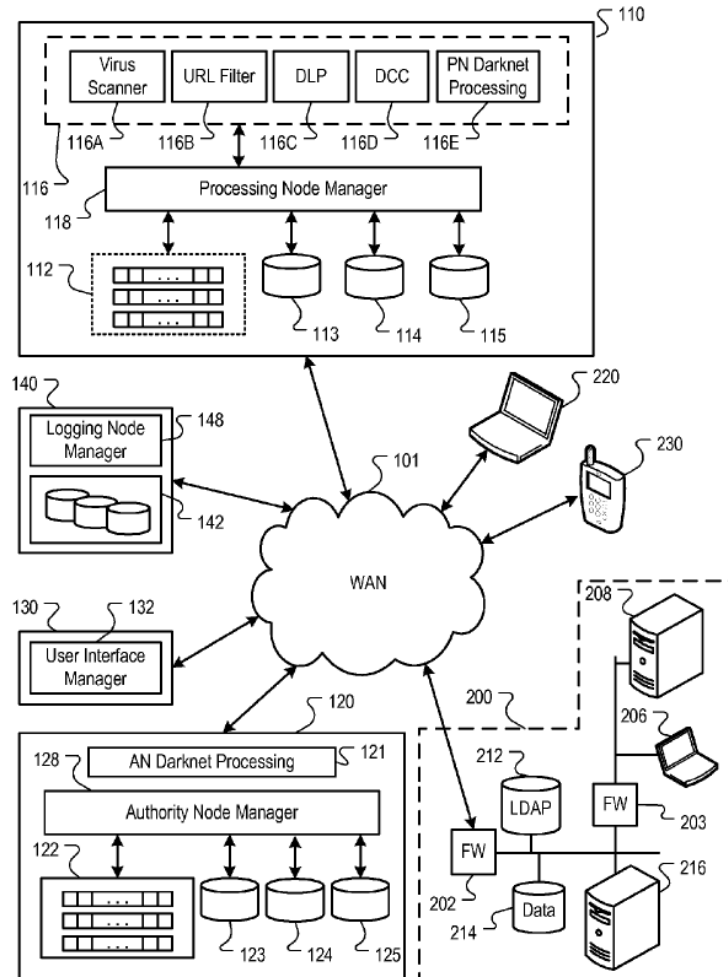


FIG. 2

Figure 2, reproduced above, is a block diagram of distributed security system 100. *Id.* at 2:29–31, 2:42–43. Distributed security system 100 includes: one or more component processing nodes 110; an authority node 120; logging node 140; external systems 200 (an enterprise), 220 (a computer device), and 230 (a mobile device); and wide area network (WAN) 101, such as the Internet, connecting the nodes and the external systems. *Id.* at 5:6–43. Each processing node 110 stores: security policies 113 received from authority node 120; detection process filter 112 and/or threat data 114 to facilitate a decision of whether a content item should be processed for

threat detection; processing node manager 118 that can manage each content item in accordance with security policy data 113, detection process filter 112, and/or threat data 114; and data inspection engines 116. *Id.* at 5:45–6:17.

Each processing node 110 monitors content items requested by or sent from external systems 200, 220 and 230. *Id.* at 5:47–50. Each data inspection engine 116 can be configured to perform a threat detection process to classify content items according to a threat classification for a corresponding threat. *Id.* at 6:3–22. For example, the data inspection engines can include: a virus scanner engine 116A that can classify a content item as infected or clean; a network URL filter 1168 that can classify a URL address as allowed or restricted; a data leakage protection (DLP) engine 116C that can identify a content item as secure or leaking; a dynamic content categorization (DCC) engine 116D that can classify a content item as passed or failed; and a PN darknet processing 116E operable to identify darknet addresses. *Id.* PN darknet processing 116E identifies darknet addresses of darknets (that malicious code, such as code performing automated scanning, attempts to access) and store the darknet addresses in a darknet address database 115. *Id.* at 1:51–57, 6:14–22. PN darknet processing 116E can also interrogate communications to determine whether the communication is associated with (e.g., destined to, or originating from) an address in the darknet address database 115. *Id.* at 6:18–22.

Authority node (AN) 120 includes AN darknet processing 121 that identifies darknet address space and store a list of darknet addresses in darknet address store 125. *Id.* at 7:28–35. AN darknet processing 121 also can distribute the list of darknet addresses to processing node(s) 110. *Id.*

Figure 4 of Sutton is reproduced below.

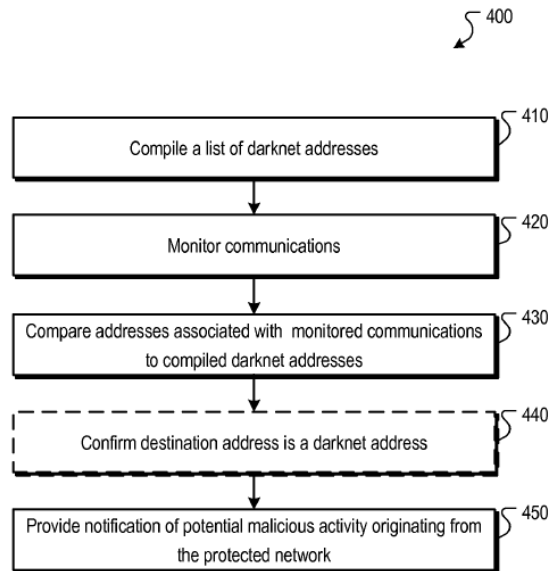


FIG. 4

Figure 4 of Sutton, reproduced above, illustrates a method for identifying malicious activity based upon darknet access. *Id.* at 1:24–25. A list of darknet addresses is compiled in step 410 by one or more authority nodes in conjunction with one or more processing nodes. *Id.* at 11:37–41. Once a list of darknet addresses is received from an authority node, processing node 110 can begin monitoring communications. *Id.* at 10:39–41. Processing node 110 inspects all or some communications for inclusion of a destination address that is included in the list of darknet addresses, and can identify communications that purport to originate from the darknet address space. *Id.* at 10:41–45. Communications are monitored in step 420 by one or more processing nodes. *Id.* at 12:25–35. The addresses associated with monitored communications in step 430 are compared to compiled darknet addresses, and if there is a match between destination addresses and the list of darknet addresses, the communication can be inferred to be indicative of malicious activity. *Id.* at 12:36–45. Optionally in step 440, the

identified destination address from step 430 can be confirmed to be a darknet address by, for example, using a scanner associated with the processing node to send a connection request to that identified the destination address. *Id.* at 12:45–56. If a device responds to the connection request, then the address is removed from the list of darknet address, but if no device responds then the address is identified as malicious. *Id.*

Notification of potential malicious activity can be provided in step 450 by one or more processing nodes and/or by an authority node. *Id.* at 12:57–13:9. This notification can be provided to (i) an administrator of a protected enterprise network, (ii) a special purpose application operable to inspect a device for malicious program code and to remove malicious program code from the device, if found, or (iii) other processing nodes with instructions to provide filtering or detailed inspection of communications identified as similar (e.g., based upon an origination address). *Id.* The communication can be also flagged as potentially malicious. *Id.* Additionally, traffic may be automatically blocked, redirected or filtered based on predefined rules. *Id.*

iii. *Ivershen (Ex. 1005)*

Ivershen is titled “System and Method for Correlating IP Flows Across Network Address Translation Firewalls.” Ex. 1005, code (54). Ivershen relates to “correlating packets in a telecommunications network and, more specifically, to correlating packets with address information that has been modified by a Network Address Translation (NAT) firewall.” *Id.* at 1:8–12. In Ivershen’s method, data packets are captured from a first interface using a monitor probe coupled to the first interface, and are correlated into a first group of session records, and for each of the first group

of session records, a correlation key is created using data in one of the packets in the session record. *Id.* at code (57). Data packets also are captured from a second interface using a monitor probe coupled to the second interface, and are correlated into a second group of session records, and for each of the second group of session records, a correlation key is created using data in one of the packets in the session record. *Id.* The correlation key for one of the first group is compared to the correlation keys for each of the second group of session records to identify session records with matching correlation keys. *Id.*

iv. *Claim 1*

In the Remand Decision, the Federal Circuit noted that we correctly identified the combination asserted: one in which ‘a packet is detected as communicated to/from a darknet address (post-boundary),’ where “Paxton discloses the ability to identify the hosts transmitting/receiving the packet (pre-boundary),’ and where “Sutton teaches making that identification known to administrators and/or implementing rules to identify or drop future packets to prevent further malicious communications. *Palo Alto Networks*, 122 F.4th at 1383. We, however, “erred by not clearly explaining [our] holding or rationale regarding motivation to combine and whether the proposed combination teaches the final limitation of claim 1: transmitting an indication of the first host responsive to the correlating.” *Id.* at 1384 (Fed. Cir. 2024). For the reasons discussed below, we find that Petitioner has not sufficiently shown that the combination of Paxton and Sutton would have taught the disputed limitation and that even if the references had taught the disputed limitation, Petitioner failed to articulate a sufficient motivation to combine Paxton and Sutton to meet the limitations of claim 1.

We first address whether one of ordinary skill in the art would have learned of the recited “transmitting an indication of the first host responsive to the correlating” from the cited references.

Petitioner contends Paxton discloses “generating . . . an indication of the first host” and “identify[ing] the true source of packet transmission through a boundary.” Pet. 39–40. Petitioner relies on Paxton’s disclosure “of a log that illustrates a matching payload In this case, the identity of the packet is the SrcAddr (source address) of the packet sensed from each side.” *Id.* at 40 (emphasis omitted). Further, Petitioner contends that Paxton suggests that identifying the true source of a packet can help “identify nodes that are infected with malicious content . . . sensed at the edge of the network back to its original source.” *Id.*

As to the transmitting, Petitioner relies on Sutton’s disclosure of “monitor[ing] communications to identify access attempts to/from darknet addresses” and that “[s]uch attempts can be inferred to be associated with malicious activity and a notification or other corrective action can be provided identifying such potentially malicious activity.” *Id.* at 41 (citing Ex. 1007, code (57), 10:60–11:3–18) (emphasis omitted).

As stated above, the combination asserted by Petitioner is one in which “a packet is detected as communicated to/from a darknet address (post-boundary),” “Paxton discloses the ability to identify the hosts transmitting/receiving the packet (pre-boundary),” and “Sutton teaches making that identification known to administrators and/or implementing rules to identify or drop future packets to prevent further malicious communications.” *Id.* at 22. Thus, the first question before us is whether the disclosures of these references taken together teach a transmission

responsive to a correlation. Petitioner has not persuaded us that this is taught by the references.

Patent Owner argues and we agree that “[a]t most, based on the disclosures, a [person of ordinary skill in the art] would be motivated to create a system that generated alerts (as taught by Sutton) only after malicious activity is detected on the network (as taught by Paxton), not in response to correlating.” PO Remand Br. 2. The claimed transmission is one that is responsive to the *correlation* of first packets received, and second packets generated, by a network device. Thus, there is a specific claimed relationship between the correlation and the transmission. The claim requires not just a correlation and a transmission, but a transmission that is responsive to the correlation. The claimed correlation is based on a comparison of data found in the first and second data packets. *See* Ex. 1001, 15:56–58. Petitioner alleges that this correlation is taught by Paxton’s comparison of hashes of packets with close timestamps. *See* Pet. 37. Thus, in order to meet the limitations of the claim the transmission must be responsive to the correlation of packet data. Petitioner, however, has not sufficiently shown this to be the case in the asserted combination.

Petitioner argues that the evidence is “overwhelming” that “Paxton’s correlation technique is used to identify the source of malicious activity expressly for the purpose of benefitting network security” and, therefore, one of skill in the art would have been “motivat[ed] to transmit Paxton’s identification of a host, *responsive to the process that identifies the host.*” Pet. Remand Br. 2–3 (emphasis added). We, however, are not persuaded that the reference supports this statement and it is Petitioner’s burden to

establish that each of the limitations of the claim is taught or at least suggested by the cited references.

Paxton “relates generally to identifying network packets, and more particularly, to determining the identity of network packets as they traverse boundaries that perform Network Address Translation (NAT).” Ex. 1004 ¶ 2. Paxton addresses the difficulties that may be encountered in identifying packets that have crossed “routers, proxies, gateways, firewalls, and other types of computer network components.” *Id.* ¶ 3. According to Paxton’s specification, in prior systems, servers would not know the original source of a packet because the source address would be changed as the packet crossed various boundaries. *Id.* ¶ 15. Thus, we understand Paxton’s identification of packets (the claimed correlating) to be broadly applied to identifying packets transmitted across boundaries and not narrowly for identifying malicious or harmful packets. This view of packet correlation comports with the testimony of Petitioner’s expert, Dr. Akl. *See* Ex. 1003 ¶¶ 39–40. Dr. Akl opines that “[p]acket correlation is a known network security concept that describes the process of matching and identifying packets that cross a network boundary, such as a Network Address Translation (NAT) firewall.” *Id.* ¶ 39. Sutton teaches taking remedial steps once a source of malicious activity or infected nodes has been identified. *See* Pet. 21–22; Reply 21–22. Therefore, we are persuaded that the combination of Paxton and Sutton would only teach a notification that is responsive to the identification of a packet as malicious. In our view, a notification that is responsive to the determination that a packet is malicious is not responsive to the correlation because all packets are correlated in Paxton, not just the malicious packets. The correlation is used as part of the notification to identify the source of the

malicious packet, but the Paxton-Sutton system would not be transmitting in response to the correlation, but rather in response to identification, by some other mechanism, that packet was malicious. Thus, we are not persuaded that one of ordinary skill in the art would have understood Petitioner's combination to teach or suggest the claimed transmission that is responsive to the correlation.

Even if the cited references had taught the recited transmission responsive to the correlation, we are not persuaded that one of ordinary skill in the art would have been motivated to combine the teachings of these references in the manner advocated by Petitioner. Petitioner contends that this combination would only involve “[t]he application of known techniques (e.g., Sutton’s implementation of rules and data to define security policies, disallowed websites, etc.) to improve similar devices (e.g., servers, gateways, firewalls, etc. in Sutton’s and Paxton’s systems) to provide predictable results in the same way (e.g., to provide packet-filtering functions preventing communications with potentially malicious hosts).” *Id.* at 22–23.

Petitioner argues that “Sutton discloses transmitting the indication of the first host (e.g., notifying an administrator) responsive to identifying a device associated with malicious activity.” Pet. 41. Sutton “monitors communications to identify access attempts to/from darknet addresses” and if such an attempt is found “a notification or other corrective action can be provided identifying such potentially malicious activity.” *Id.* (quoting Ex. 1007, code (57)). Sutton further states that if devices associated with malicious activity “reside within the enterprise network, a notification 355 can be provided to the enterprise network (e.g., a network administrator)

indicating that such devices are potentially infected with malicious software code.” *Id.* (quoting Ex. 1007, 10:60–11:3). Sutton identifies malicious nodes by determining whether a communication is destined or originating from an address in the darknet address database. Ex. 1007, 6:15–22. Thus, if a darknet address is found then Sutton will transmit a message indicating the malicious presence.

Petitioner’s assertion that the combination of Paxton and Sutton would “improve network security” is insufficient to demonstrate that one of ordinary skill in the art would have been motivated to combine the references such that that Sutton’s transmission would be responsive to Paxton’s correlation. As discussed above, Paxton discloses a system for correlating packets that cross network boundaries. *See* Ex. 1004 ¶ 15. Sutton discloses a technique of monitoring darknet access by: identifying a list of darknet addresses; monitoring communications originating from a protected network; comparing destination addresses of the monitored communications originating from the protected network to the list of darknet addresses; and, if a match is found between the destination addresses and the list of darknet addresses, providing notification of potential malicious activity originating from the protected network. Ex. 1007, 2:10–19. The known technique articulated in Sutton is matching the destination of a packet with the list of darknet addresses and then providing a notification of potential malicious activity. If this technique were applied to Paxton’s system for identifying packets, then one of ordinary skill in the art would have been motivated to combine the prior art references to transmit a notification in response to the identification of a potentially malicious packet. Petitioner has not explained why one of ordinary skill in the art

would have been motivated to combine the references to transmit in response to correlating the packets.

A fundamental problem is that Paxton does not disclose that its correlating can be used to identify malicious activity.⁵ There would be no reason to add Sutton’s notifications to Paxton without something to identify malicious activity that should be the subject of a notification. And if some other way to identify malicious packets were to be added, the notification would be in response to that other way, not “responsive to the correlating,” as claimed.

As the Federal Circuit has held, “[t]he question in an obviousness inquiry is whether it would have been obvious to a person of ordinary skill in the art to combine the relevant disclosures of the two references, not whether each individual reference discloses all of the necessary elements.” *Palo Alto Networks, Inc.*, 122 F.4th at 1386 (quoting *Game & Tech. Co. v. Wargaming Grp. Ltd.*, 942 F.3d 1343, 1352 (Fed. Cir. 2019)). The Federal Circuit has charged us with determining “whether the particular combination argued by the Petitioner—modifying Paxton by adding Sutton’s notification step after Paxton’s correlation step—would meet the claim limitations at issue.” *Id.* at 1386. We are not persuaded that Petitioner has established that one of ordinary skill in the art would have combined the teachings of the references in a manner that would have yielded the claimed system. This is

⁵ In its claim chart, Petitioner asserts that “Paxton discloses correlating packets to identify malicious activity.” Pet. 40. The only citation for that, however, is to Section IX.A.4 of the Petition (pages 21-23) which offers Petitioner’s proposed motivation to add Sutton, but does not provide any support for the idea that Paxton identifies malicious activity by correlating packets across the boundary.

true because the claimed system does not require mere notification, but rather it requires a transmission responsive to the correlation. Thus, Petitioner is required to establish that one of ordinary skill in the art would have not just made a notification, but that the transmission/notification would be responsive to the correlation. Petitioner has not sufficiently articulated a reason why one of ordinary skill would have learned of the recited responsiveness to the correlation. As noted above, Sutton teaches transmission responsive to maliciousness. Missing from Petitioner's argument is an explanation as to why would one of ordinary skill in the art want to transmit in response to the act of correlation. Petitioner's arguments indicate that Sutton's identification of darknet communications would trigger the need for transmission. Thus, the transmission would be responsive to that identification of potential maliciousness and not Paxton's correlation of packet data. Petitioner has not articulated a rationale that would explain why one of ordinary skill in the art would seek to transmit responsive to the correlation.

In view of the above, Petitioner has not provided us with argument and evidence sufficient to establish by a preponderance of the evidence that claim 1 would have been obvious over the teachings of Paxton, Sutton, and Ivershen.

v. Claim 10

Independent claim 10 is an apparatus claim that recites similar limitations to claim 1. Petitioner asserts that the combination of Paxton, Sutton, and Ivershen teaches the limitations of independent claim 10. Pet. 58–63. We have reviewed the record and find that Petitioner's arguments and evidence are insufficient for substantially similar reasons as articulated

above in regards to claim 1. As such, Petitioner has not demonstrated by a preponderance of the evidence that claim 10 would have been obvious over the teachings of Paxton, Sutton, and Ivershen.

vi. Dependent Claims 2–9 and 11–18

Petitioner asserts that the combination of Paxton, Sutton, and Ivershen teaches the limitations of dependent claims 2–9 and 11–18. Pet. 43–58, 63–70. Dependent claims 2–9 depend from claim 1 and dependent claims 11–18 depend from claim 10. Petitioner’s arguments and evidence regarding the additional limitations of these dependent claims do not remedy the above discussed deficiency with the independent claims. As such, Petitioner has not demonstrated by a preponderance of the evidence that claims 2–9 and 11–18 would have been obvious over the teachings of Paxton, Sutton, and Ivershen.

III. CONCLUSION

Based on the evidence presented with the Petition, the evidence introduced during the trial, and the parties’ respective arguments, Petitioner has not shown by a preponderance of the evidence that each of claims 1–18 of the ’903 patent are unpatentable.

In summary:

Claim(s)	35 U.S.C. §	Reference(s)/ Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1–18	§ 103	Paxton, Sutton, Ivershen		1–18
Overall Outcome				1–18

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that Petitioner has not shown by a preponderance of the evidence that claims 1–18 are unpatentable; and

FURTHER ORDERED that, because this is a Final Written Decision, parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

IPR2021-01150
Patent 10,530,903 B2

PETITIONER:

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

PATENT OWNER:

James Hannah
Jeffrey Price
KRAMER LEVIN NAFTALIS & FRANKEL LLP
jhannah@kramerlevin.com
jprice@kramerlevin.com

Bradley Wright
Scott Kelly
John. R. Hutchins
BANNER & WITCOFF, LTD
bwright@bannerwitcoff.com
skelly@bannerwitcoff.com
jhutchins@bannerwitcoff.com