UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PALO ALTO NETWORKS, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, INC.,
Patent Owner.

Case IPR2021-01151
Patent No. 10,659,573

PETITION FOR *INTER PARTES* REVIEW

TABLE OF CONTENTS

LIST OF EXHIBITS

Exhibit ("Ex.")	Description
1001	U.S. Patent No. 10,659,573 ("'573")
1002	File History of U.S. Patent No. 10,659,573
1003	Declaration of Dr. Robert Akl, D.Sc. ("Akl")
1004	U.S. Patent Application Publication No. 2014/0280778 ("Paxton")
1005	U.S. Patent No. 8,219,675 ("Ivershen")
1006	U.S. Patent No. 7,185,368 ("Copeland")
1007	U.S. Patent No. 8,413,238 ("Sutton")
1008	U.S. Patent Application Publication No. 2013/0262655 ("Deschenes")
1009	European Patent Application Publication EP 2,482,522 ("McDonald")
1010	U.S. Patent No. 8,621,556 ("Bharali")
1011	U.S. Patent No. 9,628,512 ("Prenger")
1012	U.S. Patent No. 10,931,797 ("Ahn-797")
1013	U.S. Patent Application Publication No. 2006/0048142 ("Roese")
1014	U.S. Patent Application Publication No. 2008/0163333 ("Kasralikar")
1015	U.S. Patent Application Publication No. 2012/0240185 ("Kapoor")
1016	WIPO International Publication No. WO 2014/001773 ("Jarvis")
1017	IPR2018-01654, Pap. 1 (P.T.A.B. Sep. 17, 2018) (Petition for *Inter Partes* Review of U.S. Patent No. 9,560,176)
1018	IPR2018-01655, Pap. 1 (P.T.A.B. Sep. 17, 2018) (Petition for *Inter Partes* Review of U.S. Patent No. 9,560,176)
1019	Email correspondence between the U.S. District Court for the Eastern District of Virginia and Counsel (July 14, 2021)
1020	Amended Complaint, *Centripetal Networks, Inc. v. Palo Alto Networks*, Case No. 2:21-cv-00137, Dkt. 65 (E.D.Va. July 9, 2021)
1021	U.S. Patent No. 5,303,303 ("White")
1022	Postel, J., "Transmission Control Protocol," STD 7, RFC 793, DOI 10.17487/RFC0793, September 1981, <https://www.rfc-editor.org/info/rfc793>.
1023	K. Golnabi, R. K. Min, L. Khan and E. Al-Shaer, "Analysis of Firewall Policy Rules Using Data Mining Techniques," 2006 IEEE/IFIP Network Operations and Management Symposium

	NOMS 2006, 2006, pp. 305-315, doi: 10.1109/NOMS.2006.1687561.
1024	R. Dantu, J. Cangussu and A. Yelimeli, "Dynamic control of worm propagation," International Conference on Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004, 2004, pp. 419-423 Vol.1, doi: 10.1109/ITCC.2004.1286491.
1025	T. Baba and S. Matsuda, "Tracing network attacks to their sources," in IEEE Internet Computing, vol. 6, no. 2, pp. 20-26, March-April 2002, doi: 10.1109/4236.991439.

I. INTRODUCTION

Petitioner Palo Alto Networks, Inc. ("Petitioner") respectfully requests *inter partes* review ("IPR") of claims 1-24 ("Challenged Claims") of U.S. Patent No. 10,659,573 ("'573 patent") in accordance with §§311-319 and §42.100 et seq.[1]

The '573 patent is directed to correlating packets that pass through a network device—*i.e.*, matching packets received by the network device with packets transmitted by the network device. Ex. 1001, Abstract, 1:43-57. The '573 patent provides a method of correlating the packets by logging data (choosing from a plethora of packet-related information) and matching the packets using the logged data. *Id.*, 3:56-12:58. After packets are correlated, results may be provided to an administrator, or rules may be generated to identify and drop certain packets. *Id.*, 12:59-13:67.

The '573 patent's claims are unpatentable as obvious. Correlating packets was well-known in the art. Known, too, were the various packet information and properties that the '573 patent suggests using to make correlations, as well as post-correlation activities such as notifying an administrator or provisioning filter rules.

[1] Section cites are to 35 U.S.C. or 37 C.F.R. as context indicates, and all emphasis/annotations added unless noted.

Patent Owner did not discover or invent any new packet information. It merely applied known networking characteristics and techniques to known packet correlating processes.

As demonstrated below, the prior art renders the Challenged Claims unpatentable, and Petitioner has a reasonable likelihood of prevailing with respect to the same.

II. MANDATORY NOTICES UNDER 37 C.F.R. § 42.8

A. Real Party-In-Interest

Pursuant to 37 C.F.R. § 42.8(b)(1), Petitioner identifies Palo Alto Networks, Inc. as real party-in-interest.

B. Related Matters

The ’573 patent is currently the subject of a district court litigation: *Centripetal Networks, Inc. v. Palo Alto Networks, Inc.*, Case No. 2:21-cv-00137 (E.D. Virginia, filed March 12, 2021) (“EDVA suit”).

C. Lead and Back-up Counsel, and Service Information

Lead Counsel	Backup Counsel
Scott A. McKeown Reg. No. 42,866 ROPES & GRAY LLP 2099 Pennsylvania Avenue, NW Washington, D.C. 20006-6807 Phone: 202-508-4740 Fax: 617-235-9492 scott.mckeown@ropesgray.com **Mailing address for all PTAB correspondence:** ROPES & GRAY LLP IPRM—Floor 43 Prudential Tower 800 Boylston Street Boston, Massachusetts 02199-3600	James Batchelder (*pro hac vice* forthcoming) Mark Rowland Reg. No. 32,077 Andrew Radsch (*pro hac vice* forthcoming) ROPES & GRAY LLP 1900 University Ave., 6th Floor East Palo Alto, CA 94303-2284 Phone: 650-617-4000 Fax: 617-235-9492 james.batchelder@ropesgray.com mark.rowland@ropesgray.com andrew.radsch@ropesgray.com Victor Cheung Reg. No. 66,229 ROPES & GRAY LLP 2099 Pennsylvania Avenue, NW Washington, D.C. 20006-6807 Phone: 202-508-4641 Fax: 617-235-9492 victor.cheung@ropesgray.com

Petitioner consents to electronic service of documents to the email addresses of the counsel identified above.

III. PAYMENT OF FEES

The undersigned authorizes the Office to charge the fee required by 37 C.F.R. §42.15(a) for this Petition to Deposit Account No. 18-1945. Any additional fees that might be due are also authorized.

IV. REQUIREMENTS FOR *INTER PARTES* REVIEW

A. Grounds for Standing

Pursuant to 37 C.F.R. §42.104(a), Petitioner certifies that the '573 patent is available for IPR and that Petitioner is not barred or estopped from requesting IPR of the Challenged Claims of the '573 patent on the grounds identified herein.

B. Identification of Challenge

Pursuant to 37 C.F.R. §§42.104(b) and (b)(1), Petitioner requests IPR of the Challenged Claims and that the Board cancel the same as unpatentable. The '573 patent matured from U.S. Patent Application No. 16/554,293 ("the '293 application), filed 8/28/2019. The '573 further claims priority to Application No. 14/618,967, filed 2/10/2015.[2]

1. The Specific Art on Which the Challenge is Based

Petitioner relies upon the following prior art:

Exhibit 1004 – Paxton (U.S. 2014/0280778) published 9/18/2014, and is based on application 14/208,314, filed 3/13/2014, and provisional application 61/778,820, filed 3/13/2013.

[2] Petitioner takes no position as to the propriety of the priority claims since the art presented herein pre-dates the earliest filing. Petitioner reserves the right to challenge these priority claims.

Exhibit 1007 – Sutton (U.S. 8,413,238) issued 4/2/2013, and is based on application 12/176,912, filed 7/21/2008.

Exhibit 1008 – Deschenes (US 2013/0262655) published 10/3/2013, and is based on application 13/432,847, filed 3/28/2012.

Exhibit 1005 – Ivershen (U.S. 8,219,675) issued 7/10/2012, and is based on application 12/636,144, filed 12/11/2009.

Exhibit 1009 – McDonald (European Patent Application Publication EP2482522) published 8/1/2012.

Paxton, Sutton, Deschenes, and Ivershen are prior art under AIA §§102(a)(1) and (2). McDonald is prior art under AIA §102(a)(1).

2. Statutory Grounds on Which the Challenge is Based

Petitioner respectfully requests cancelation of the Challenged Claims on the following grounds:

Ground	Statute	Claim(s)	Prior Art
1	§103	1, 7-9, 15-17, 23-24	Paxton and Sutton in view of Deschenes
2		2, 10, 18	Paxton and Sutton in view of Deschenes and McDonald
3		3-6, 11-14, 19-22	Paxton and Sutton in view of Deschenes and Ivershen

The information required by §§42.204(b)(4)-(5) is provided in Section IX.

This Petition is supported by the Declaration of Dr. Robert Akl (Ex. 1003, ¶¶1-206) ("Akl").

V. THE BOARD SHOULD NOT EXERCISE ITS DISCRETION TO DENY INSTITUTION

The Board should not exercise its discretion to deny institution under §§325(d) or 314(a).

A. §325(d)

Considering the two-part framework discussed in *Advanced Bionics, LLC v. Med-El Elektromedizinische Gerate GMBH*, IPR2019-01469, Pap. 6, *8-9, the Board should not exercise its §325(d) discretion to deny institution.

Neither the art nor the arguments in Grounds 1-3 are the same/substantially the same as those considered during prosecution. None of Paxton, Sutton, Deschenes, and McDonald was cited, let alone considered, in the prosecution of the '573 patent. While Applicant listed Ivershen, along with 322 other references, on an IDS in the '573 prosecution, Applicant did not explain its significance and Examiner did not apply or even refer to it in any rejection or notice of allowance for the '573 patent.

Further, while Applicant disclosed the petitions and expert declarations from requests for IPR filed by an unrelated party against claims of the '573 patent's grandparent patent, U.S. 9,560,176 ("'176 patent"), those petitions presented Ivershen as a primary reference, and did not rely upon any of the other art

Petitioner relies upon herein. Ex. 1017 (IPR2018-01654); Ex. 1018 (IPR2018-01655).

In contrast, here, Petitioner uses Ivershen only for certain dependent claims. The grounds of rejection with respect to the '573 patent's independent claims and remaining dependent claims do not reference Ivershen and rely on prior art not previously before the Office. These other prior art references, sans Ivershen, address the limitations deemed missing from the prosecution prior art. *See* Prosecution History, §VI.B below.

Therefore, because prior art presented herein has never been before the Office, because the combinations proposed herein have never been presented to the Office, and because the new prior art presented herein squarely addresses the limitations deemed missing from the previously applied prior art, it cannot be said that "the same or substantially the same art previously was presented to the Office" or "the same or substantially the same arguments were presented to the Office." The Board should not exercise its discretion to deny institution under §325(d).

B. §314(a)

Likewise, co-pending district court proceedings do not warrant the exercise of discretion under §314(a) based on the six factors identified in *Apple Inc. v. Fintiv, Inc*., IPR2020-00019, Paper 11. **1**: On July 9, 2021, Petitioner filed a motion to stay the EDVA suit pending the outcome of this IPR and IPRs

addressing the remaining patents asserted in that suit. EDVA courts frequently grant stays pending IPR, including pre-institution. *E.g.*, *RAI Strategic Holdings, Inc. v. Altria Clients Svcs.*, 1:20-cv-393, Dkt. 426 (E.D.Va. Dec. 4, 2020); *Centripetal Networks v. Cisco Sys.*, 2:18-cv-00094, Dkt. 58 (E.D.Va. Feb. 25, 2019); *Sharpe Innovations, Inc. v. T-Mobile USA*, 2:17-cv-351, Dkt. 41 (E.D.Va. Jan. 10, 2018). **2**: As of this filing, the court has not held a scheduling conference or set a firm trial date. The court indicated that it likely will set trial for August 1, 2022 (*see* Ex. 1019), meaning trial would be at least one year away (if suit is not stayed). Meanwhile, less than two weeks ago, PO amended its complaint to add a new patent and new allegations to the case. Ex. 1020. **3:** The court has not issued any substantive orders related to the '573. Neither party has produced any discovery or served any contentions. The court's anticipated *Markman* hearing date of March 29, 2022 (Ex. 1019) is approximately three months after the deadline for institution (if suit is not stayed). **4:** The EDVA suit likely will involve multiple grounds of invalidity, including §§101 and 112, and unique grounds under §§102 and 103 not at issue here, enabling the court to focus its limited trial time on different invalidity defenses, if the suit is not stayed. Further, this Petition addresses claims (2, 10, 18) not asserted in the Complaint in the litigation. **5:** The litigation and PTAB parties are the same. **6:** The merits of the asserted grounds in

this Petition are particularly strong as shown herein. Accordingly, the Board should not exercise its discretion to deny institution.

VI. BACKGROUND

A. Summary of the ’573 Patent

The ’573 patent is directed to using logs to correlate packets received by a network device to packets transmitted by the network device.

As shown in annotated FIG. 1 below, an exemplary system includes network device 122 (**green**) that communicates to hosts 108, 110, and 112 (**blue**) in Network A 102 as well as hosts 114, 116, and 118 (**red**) in Network B. The network device also communicates to a packet correlator 128, which includes rules 140 and logs 142 (**orange**). Ex. 1001, 2:40-3:37.

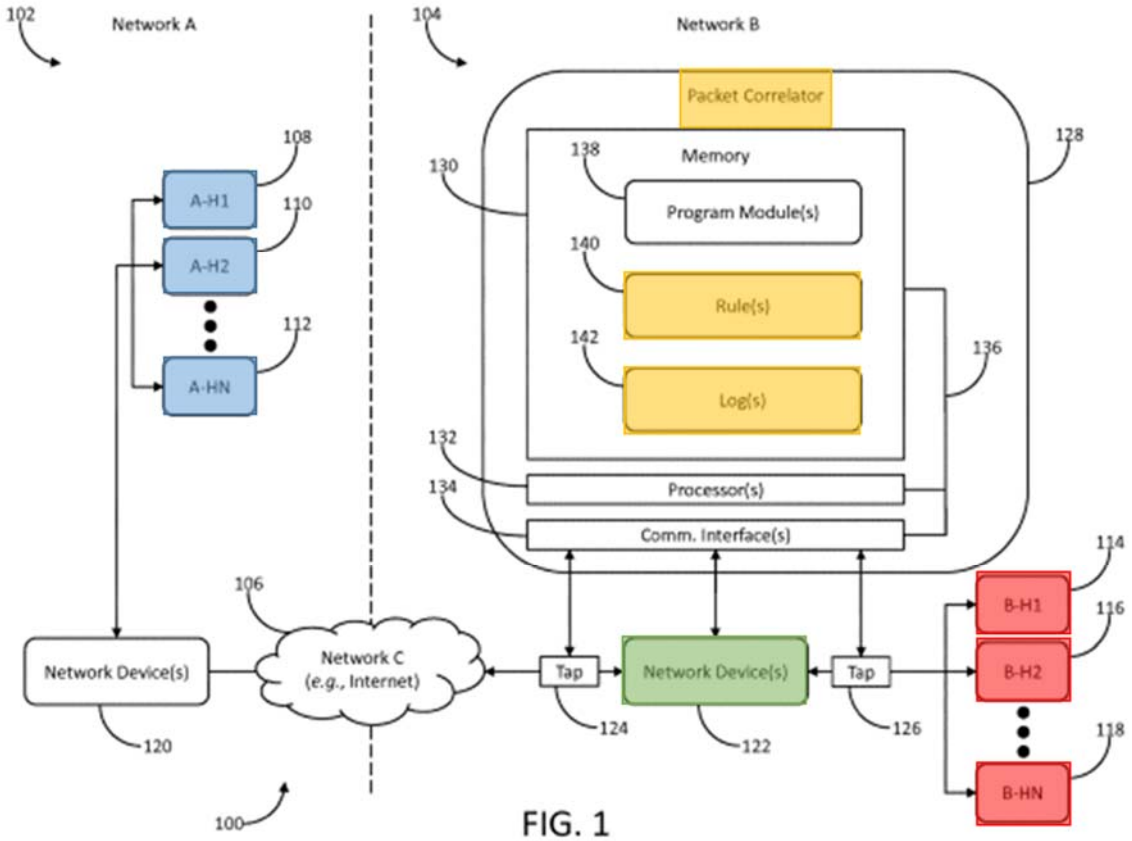


FIG. 1

As shown in the flowchart below, a network device receives packets (402) and generates log entries corresponding to the received packets (404). The network device then transmits another set of packets (406) and generates log entries corresponding to the transmitted packets (408). Finally, the network device correlates the received and transmitted packets based on their log entries (410). *See* FIG. 4 below. Ex. 1001, 14:1-24.

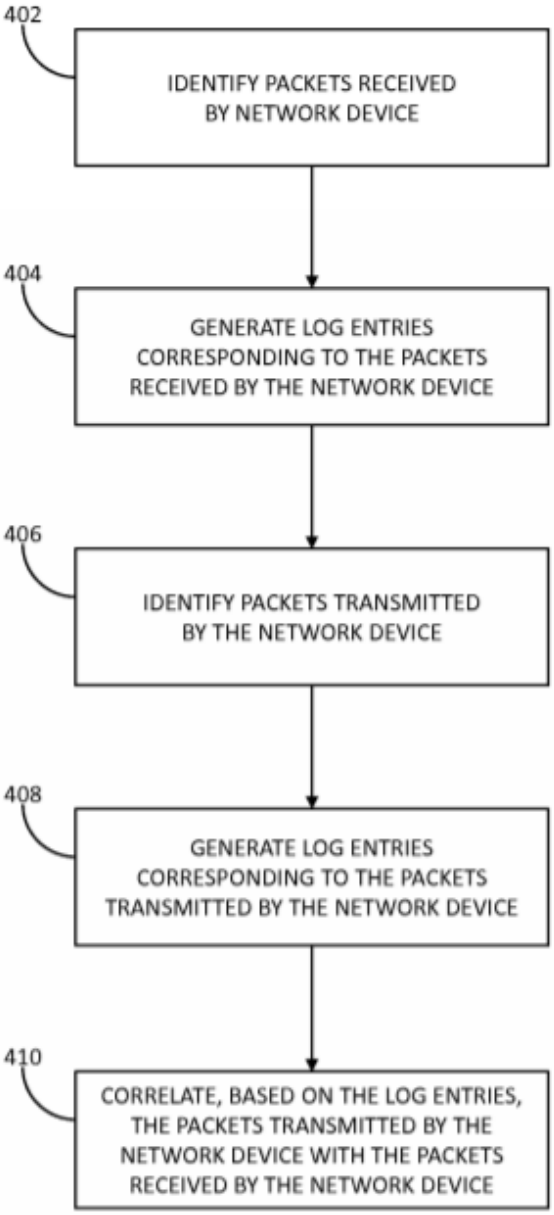


FIG. 4

Correlation may be based on any of a number of factors, such as network-layer information, transport-layer information, application-layer information, and environmental variables. *See*, *e.g.*, Ex. 1001, 4:15-5:5, 8:50-9:47. Once packets

are correlated, the system may notify an administrator of the correlation or generate rules to identify and drop packets, for example after determining that communications were with a malicious entity or if it is suspected that malware is involved. *Id.*, 12:59-13:38. Akl, ¶¶37-50.

B. Prosecution History of the '573 Patent

U.S. Application 16/554,293, which matured into the '573 patent, was filed 8/28/2019 with 24 claims. Ex. 1002, 91-99.

Examiner issued a Non-Final Office Action on 10/11/2019, rejecting a subset of the claims under obviousness-type double patenting. Claims 1-9, 11-17, and 20-24 were subject to double patenting rejections, but Examiner indicated that they would be allowable if amended or if a terminal disclaimer was filed. *Id.*, 166. Examiner did not provide a basis for rejecting claims 10, 18, and 19.

Applicant, on 11/15/2019, filed a Terminal Disclaimer to obviate the double patenting rejections. *Id.*, 237.

Examiner issued a Notice of Allowance on 1/14/2020 and indicated, as reasons for allowance, that the prior art of record failed to teach the entirety of the steps of "responsive to the correlating of the plurality of encrypted packets …generating…one or more rules configured to identify packets received from the host located in the first network; and provisioning a packet-filtering device with the one or more rules configured to identify packets received from the host located

in the first network" (i.e., claim limitation [1f] as defined in the claims charts below). *Id.*, 267-268. Akl, ¶¶51-55.

VII. LEVEL OF ORDINARY SKILL IN THE ART

The level of ordinary skill in the art is evidenced by the prior art. *See In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995) (determining that the Board did not err in adopting the approach that the level of skill in the art was best determined by references of record). The prior art discussed herein, and in the declaration of Dr. Robert Akl, demonstrates that a POSITA, at the time the '573 patent was filed, 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. Additional graduate education could substitute for professional experience, or significant experience in the field could substitute for formal education. Akl, ¶¶18-20.

VIII. CLAIM CONSTRUCTION

Claim terms subject to IPR are to 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), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent." §42.100(b).

For purposes of this Petition, Petitioner believes no terms require construction. Only terms necessary to resolve the controversy need to be construed, and should be given their plain and ordinary meaning. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017).[3] Akl, ¶¶56-57.

IX. GROUNDS OF UNPATENTABILITY

Although the ’573 patent claims correlating packets between communications networks using packet log entries, such correlation was known prior to the earliest possible priority date of the ’573 patent, and the Challenged Claims would have been obvious. Akl, ¶¶37-206.

A. Ground 1: Claims 1, 7-9, 15-17, and 23-24 are obvious over Paxton and Sutton in view of Deschenes

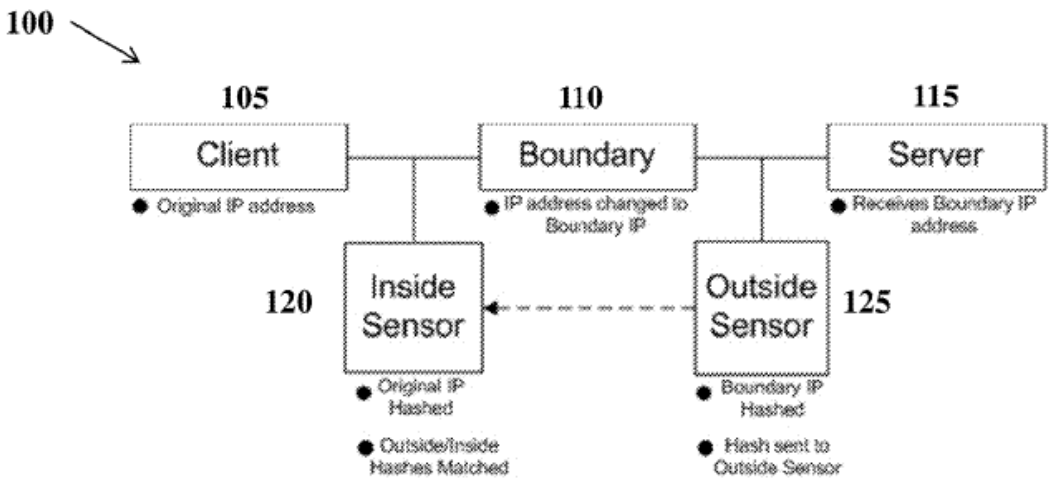
1. Overview of Paxton

Paxton is directed to a “system and method to determine the identity of network packets as they traverse boundaries that perform NAT [Network Address Translation].” Ex. 1004, ¶5. Paxton explains that analyzing an application layer payload before and after a boundary is beneficial to matching packets before and

[3] *See generally Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005); 37 C.F.R. §42.100(b). This claim-construction analysis is not a concession as to the scope of any claim term in litigation, or a waiver of any argument in any proceeding that claim terms are indefinite, invalid, or unpatentable.

after translation. *Id.*, ¶15. Matching packets and identifying the true source of packet transmissions is useful for network security, providing a way to trace malicious activity sensed at the edge of a network and identify nodes infected with malicious content. *Id.*, ¶30.

Figure 1 shows an example of a system in which packets are sent from client 105 to server 115 across a boundary 110 and vice versa. *Id.*, ¶¶15-16. Paxton's sensors and processing components may be implemented in the same server, in separate servers, and/or in a distributed fashion. *Id.*, ¶¶18, 26.



Inside sensor 120 and outside sensor 125 record traffic before and after it passes through boundary 110 and store, in a database, information including payload hashes, network layer header data, IP addresses, and timestamps of when the payloads are sensed. *Id.*, ¶¶17-20. The database storing information from the inside sensor 120 and outside sensor 125 has direct access to the sensors;

alternatively, a consolidated database may be stored at one of the sensors. *Id.*, ¶20. Payloads can then be matched using at least the hash, time, and IP address data. *Id.*, ¶21. The closest matching hashes, with respect to their timestamps, are identified as matching packets. *Id.*, ¶¶22-23.

Paxton discloses that its computer system is implemented via modules (e.g., an inside sensor module, an outside sensor module, and a matching module) that are implemented via one or more processors executing instructions. *Id.*, ¶32, claims 10-12. Akl, ¶¶58-62.

2. Overview of Sutton

Sutton is directed to "distributed security that monitors communications to identify access attempts to/from darknet addresses." Ex. 1007, Abstract, 2:41-56.

Figure 2 shows a detailed diagram of the security system.

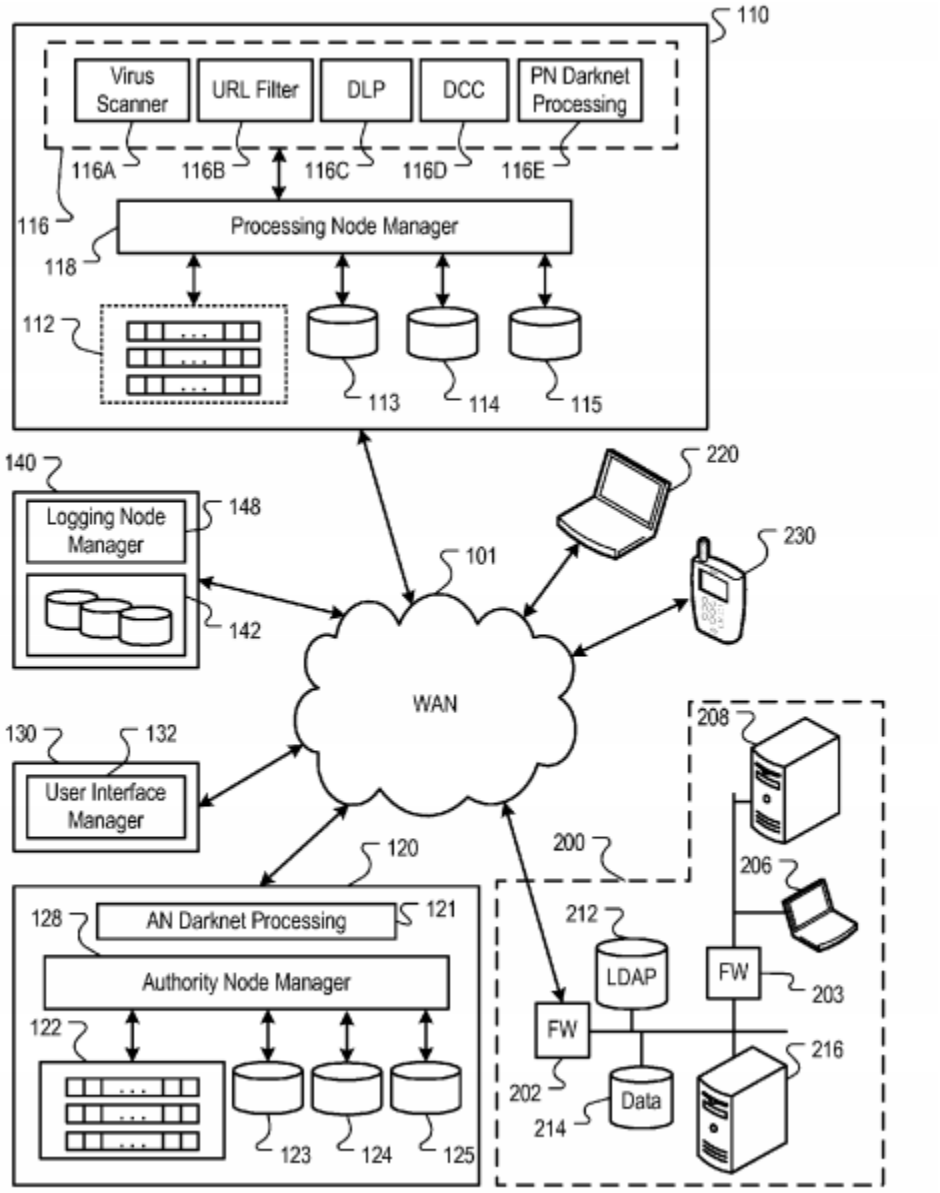


FIG. 2

A wide area network (WAN) 101, such as the Internet, connects the communication of several external systems 200, 220, and 230 through network devices (e.g., routers, gateways). *Id.*, Fig. 2, 5:22-31. Processing node 110, implemented by a plurality of devices including servers, gateways, and switches, processes data communicated through these systems, e.g., serving as a proxy. *Id.*,

3:24-4:4, 4:45-51, 5:5-21. Processing node 110 stores security policies 113 and monitors content items requested by or sent from the external systems. Processing node 110 includes, for example, a detection process filter 112, threat data 114, and data inspection engines 116, to perform threat detection processes. *Id.*, 5:45-7:17. One data inspection engine 116 is PN darknet processing 116E, which identifies communications to or from darknet addresses. *Id.*, 6:15-22.

Once darknet communications are detected or suspected, network administrators may be notified of such communications, devices associated with the malicious activity are identified, and rules may be implemented to prevent or filter further communications. *Id.*, 10:37-11:34, 12:57-13:14. For example, if a malicious host is outside of a network, rules may be generated to prevent communications with that host. *Id.*, 10:66-11:3. Hosts identified as running malicious code may have their communications actively filtered. *Id.*, 11:4-18. Further, other nodes may be instructed to filter and inspect communications for similar activity, and system filters may be updated. *Id.*, 12:57-13:14.

Sutton's processing node 110, which receives and analyzes packets in the overall computer system, may act as a proxy for a device or network, blocks packets when necessary, and updates and implements policies and rules used for analysis. *Id.*, 3:24-53, 4:45-5:4, 5:54-65, 10:37-11:34, 12:25-41, 12:57-13:14, 15:29-35, 15:65-16:5, 17:21-18:16. Sutton discloses using policy data to

implement rules to prevent communications, where policy data define security policies for protected systems, access privileges, disallowed websites and content, etc., and are distributed to processing nodes, which apply the rules to communications. *Id.*, 3:1-23, 3:54-4:4, 7:19-27, 8:11-16, 10:60-11:3. Those processing node functions may be implemented in a plurality of individual devices (e.g., servers, gateways, switches) and/or in a distributed manner across devices. *Id.*, 3:24-37. The various hardware and software of Sutton's system may be integrated into few components or separated into multiple components. *Id.*, 13:26-42, 14:29-57. Akl, ¶¶63-68.

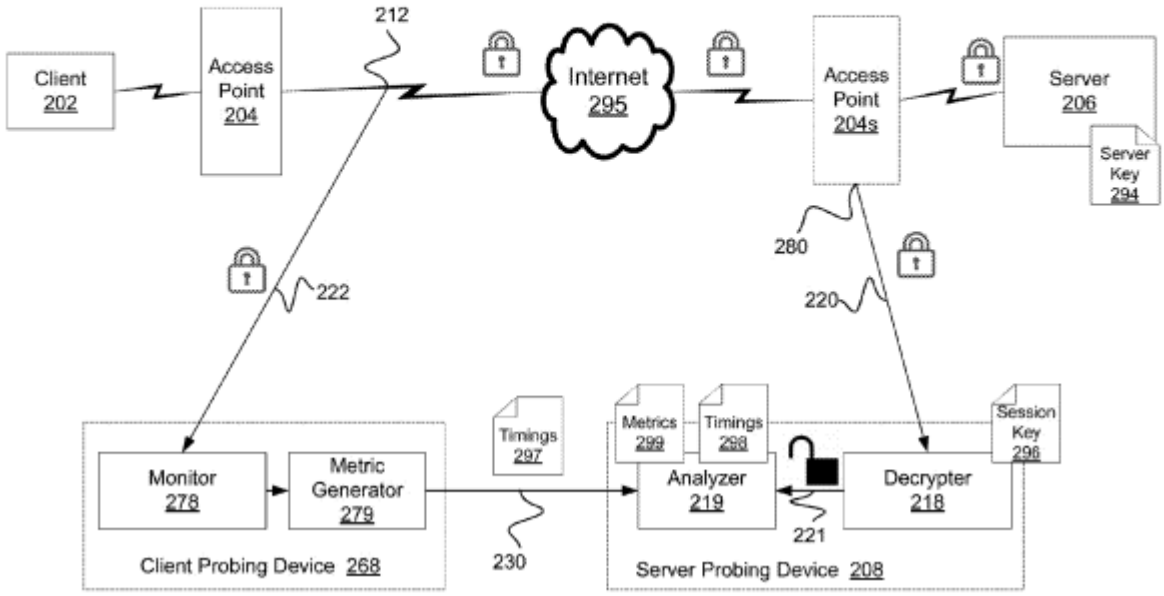
3. Overview of Deschenes

Deschenes is directed to "monitoring one or more encrypted communications sessions between a first computing device and a second computing device". Ex. 1008, ¶6. Deschenes explains that network communications between a server and client are often encrypted to secure communications between two devices. *Id.*, ¶27-28. For example, the payload portion of a packet may be encrypted. *Id.* ¶¶56-57. To monitor such communications, taps or probe points may be placed on both the client and server sides of the network. *Id.*, ¶29-31.

Figure 2 shows tap points 280 (server-side) and 212 (client-side) monitoring encrypted traffic between server 206 and client 202 using probing devices 208 and 268. *Id.*, ¶¶48-49, 52. *See also id.*, Fig. 1, ¶¶17-37 (system diagram).

FIG. 2

200



In some instances, "tap point 280 (or an associated device, such as, probing device 208, etc.) may be configured to decrypt the monitored encrypted network communication," but not client-side network tap point 212 or client probing device 268. *Id.*, ¶¶52, 55, 60. Analyzer 219 in server probing device 208 is configured to correlate encrypted client-side communications with decrypted server-side communications, regardless of whether it can decrypt the encrypted portions, using

information based upon or derived from the communications, e.g., SSL Records, TCP/IP level information, timestamps, unencrypted portions, etc. *Id.*, ¶¶42, 61-68, 70-73. The entity/entities performing decryption and analysis may be server-side (as in Figure 2) or elsewhere, e.g., at a third party. *Id.*, ¶¶85-89. Akl, ¶¶69-72.

4. Motivation to Combine (Sutton)

To the extent Patent Owner argues that Paxton does not explain in detail what actions are taken with respect to identified malicious activity, a POSITA would have been motivated to modify Paxton's computing system to, after the correlating, notify administrators of devices involved with the malicious activity (e.g., as in claims 8, 16, 24) and generate rules to be provisioned to a packet-filtering device (e.g., a gateway, server, or packet inspecting device within the system, such as, but not limited to, Paxton's sensor 120 and/or boundary 110, which are, e.g., servers, gateways, and firewalls in the first network; or, alternatively, a similar but separate device in Paxton's multi-device system performing inspecting and filtering functions that would have been included in the first network alongside Paxton's plural sensor and boundary devices to the extent Patent Owner argues a separate device is required), and used for identifying, filtering, and/or blocking host devices' future packet communications (e.g., as in claims [1f], [9g], [17f], 7, 15, 23), as taught by Sutton. Akl, ¶¶79, 116-128, 61-62. As explained above, Sutton teaches network security, including the identification

of malicious activity, such as communications with darknet addresses. Paxton discloses a method of tracing sensed malicious activity to its source via correlating packets when, e.g., a network boundary changes the source address of a packet. Sutton also teaches notifying administrators of devices suspected of association with darknet communications and malicious activity, and generating rules to prevent and/or filter future communications. Thus, when a packet is detected as communicated to/from a darknet address (post-boundary), and Paxton discloses the ability to identify the hosts transmitting/receiving the packet (pre-boundary), Sutton teaches making that identification known to administrators and/or implementing rules to identify or drop future packets to prevent further malicious communications. Accordingly, it would have been obvious to a POSITA to add Sutton's functionality, as discussed above, to Paxton's computing system (e.g., to the device implementing Paxton's matching module, which detects the sources of communications, or to a separate device in Paxton's multi-device system to perform remedial steps) to improve network security. Akl, ¶¶79, 39-40, 45-46, 61-62.

Paxton leaves, to a POSITA, remedial steps (e.g., uses of the correlation results), which are taught by Sutton. The 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) would have been obvious to a POSITA. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 415-17 (2007).

A POSITA would have had a reasonable expectation of success implementing the detecting, identifying, notifying, filtering, and blocking techniques, taught by Sutton, with Paxton's system. Paxton explains that correlation is useful for network security, and its technique is "highly modular," "can be implemented atop open source technology on commodity hardware," "can provide a stable foundation for building tiered enterprise network architectures with an inherent capability for attribution of malicious activity," and can be integrated by "[e]nterprises with significant visibility and monitoring investments into the network backbone." Ex. 1004, ¶30. Likewise, Sutton is a distributed security system over a network that "ensures…all enterprise traffic…is available for inspection," and its processing node functions are implemented via well-known devices (e.g., servers, gateways, switches, etc.). Ex. 1007, 2:41-56, 3:24-26, 10:37-11:18. The addition of techniques for specific packet detection (e.g., identifying darknet communications) and for generating notification messages and rules for existing packet-filtering devices include, generally, simple lookup and

text-based data generation routines, which would have been obvious and well within the skill of a POSITA. Akl, ¶¶80, 61-62.

5. Motivation to Combine (Deschenes)

The ’573 patent describes that packets or their underlying data may be in encrypted form—but does not describe a specific technique for analyzing or correlating packets having encrypted content. Ex. 1001, 5:50-64. Nevertheless, to the extent Patent Owner argues that Paxton does not disclose a network communications system that correlates packets with encrypted data, a POSITA would have been motivated to modify Paxton to process encrypted packets, as taught by Deschenes. As explained above, Deschenes teaches the correlation of packets analyzed at two tap points between two devices in communication. Information normally analyzed (e.g., URLs, cookies) “may be unavailable” for traffic that is encrypted, and so Deschenes teaches that other information may be used, such as timing information and unencrypted portions of the traffic. Ex. 1008, ¶¶63-68. Thus, where Paxton discloses a method of tracking packets across boundaries, but does not explicitly discuss encrypted packets, Deschenes teaches methods for correlating encrypted packets (including methods where both client and server-side packets are encrypted so that the payload is not altered, and where encrypted packets are first decrypted for analysis), which adds functionality to monitoring systems, like Paxton’s, that may otherwise discard or ignore encrypted

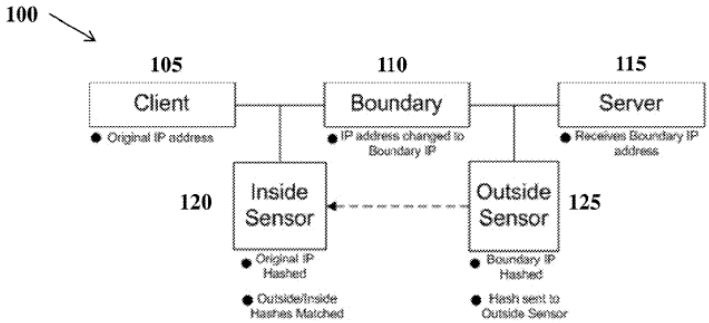
packets. *Id.*, ¶¶40, 55, 59. As encrypted communications became increasingly commonplace, correlation system such as Paxton's would have benefited from the ability to process them. Akl, ¶¶85-86, 111-115.

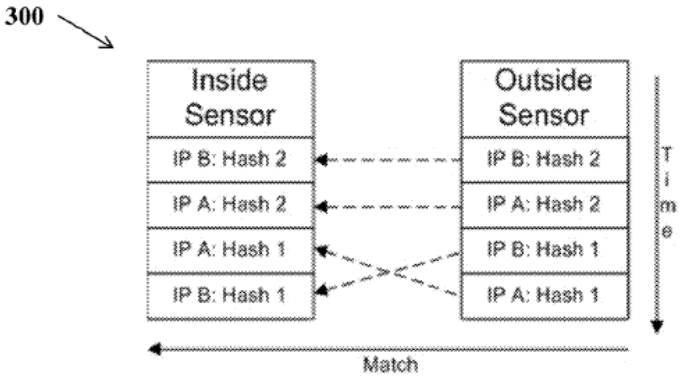
A POSITA would have had a reasonable expectation of success implementing the encrypted packet correlation methods, taught by Deschenes, with Paxton's system. Paxton and Deschenes describe components that perform similar packet monitoring and correlation functions. Ex. 1004, ¶15, Fig. 1; Ex. 1008, ¶¶48-50, Fig. 2. Furthermore, Deschenes' teaching of analyzing encrypted packets employs known protocols (e.g., SSL, HTTPS), which are merely examples. Ex. 1008, ¶20. The addition of known encryption techniques to the methods of Paxton, which is similar to the methods of Deschenes, would have been both obvious and well within the skill of a POSITA. Akl, ¶87.

6. Claim Chart

'573 Patent	Paxton, Sutton, Deschenes
[1pre] A method comprising:	**Paxton** discloses **a method.** • "The present disclosure 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)**." (Paxton ¶2) Akl, ¶¶94-96.
[1a] identifying, by a computing system, a	**Paxton** discloses **identifying, by a computing system** (e.g., sensing by a computer system implementing modules, including a boundary, sensors, database), **a plurality of packets received by a network device from a host located**

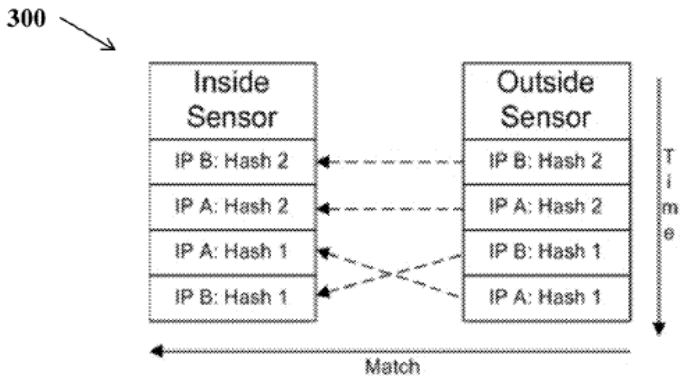
’573 Patent	Paxton, Sutton, Deschenes
plurality of packets received by a network device from a host located in a first network;	**in a first network** (e.g., packets received from client 105 at boundary 110). • “[T]he modules described herein, such as the inside sensor module, outside sensor module, and matching module, **can be implemented in a <u>computer system</u>** that comprises instructions stored in a machine-readable medium and a processor that executes the instructions.” (Paxton ¶32) • “[T]he exemplary system is described by referring to **<u>packets being sent from a client 105</u> across a boundary 110 to a server 115**. However, one of ordinary skill in the art would understand that this method could be reversed…. That is, the exemplary method could be performed when **packets are being sent from a server 115 across a boundary 110 to a client 105**.” (Paxton ¶16) • “The inside sensor 120 and outside sensor 125 can be two commodity servers running full packet capture in a promiscuous mode via a software package. **While one of ordinary skill in the art would understand that a single server with two network interfaces could suffice for the inside sensor 120 and outside sensor 125, the process can implemented in a distributed fashion as described above in order to scale to the demanding requirements of full packet capture, especially on high bandwidth links. <u>The first server, or inside sensor 120, can passively record traffic on the client 105 network before the contents are altered by a boundary.</u>** The second server, or outside sensor 125, can passively record traffic externally after it has been modified by the boundary.” (Paxton ¶18) • Fig. 1.

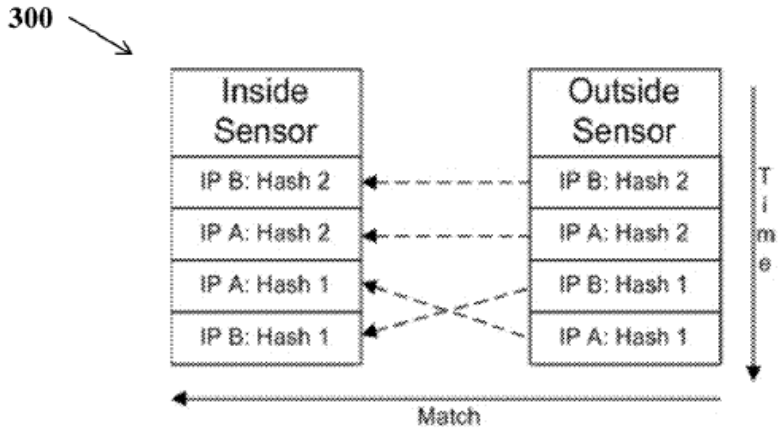
’573 Patent	Paxton, Sutton, Deschenes
	 **Figure 1** • *See also* ¶¶20, 26, 31-32, claims 10-12 (describing architectures for the sensors, boundary, database, and modules). Akl, ¶¶97-100.
[1b] generating, by the computing system, a first plurality of log entries corresponding to the plurality of packets received by the network device;	**Paxton** discloses **generating, by the computing system, a first plurality of log entries corresponding to the plurality of packets received by the network device** (generating first hash data records and storing them in a database). • “**[A]s a packet is transmitted from the client 105, the inside sensor 120 can calculate a hash, e.g., a MD5 algorithm hash, of the application layer payload and store it alongside network layer header**. After the packet traverses the boundary 110, the outside sensor 125 can calculate a hash e.g., a MD5 algorithm hash, of the payload along with the header data of the packet.” (Paxton ¶17; *see also* ¶¶28-29 regarding fuzzy hashing) • “**The hash value from each payload can be stored in a database that has direct access to the inside sensor and outside sensor and is configured to store the first hash data record and the second hash data record along with the IP address and timestamp of when it**

’573 Patent	Paxton, Sutton, Deschenes
	was sensed. Alternatively, the first hash data record and the second hash data record can be stored on the inside sensor and outside sensor, respectively. This process can occur on both the inside sensor 120 and outside sensors 125. Furthermore, a separate process can mirror the contents of each sensor's database into a single instance on the inside sensor 120, or the second hash data record can be transmitted to the inside sensor. This process can be performed in order to construct a unified location for data in order to match payloads.” (Paxton ¶20) • *See also* Paxton ¶27 (live or recorded capture modes). • Fig. 3, ¶¶24-25 (showing multiple entries for multiple packets).  **Figure 3** Akl, ¶¶101-103.
[1c] identifying, by the computing system, a	**Paxton** discloses **identifying, by the computing system, a plurality of packets transmitted by the network device to a host located in a second network** (e.g., packets sensed by

’573 Patent	Paxton, Sutton, Deschenes
plurality of encrypted packets transmitted by the network device to a host located in a second network;	the outside sensor server after passing through, and being modified by, the boundary, as transmitted packets). • *See* [1a]. • “**The first server, or inside sensor 120, can passively record traffic on the client 105 network before the contents are altered by a boundary. <u>The second server, or outside sensor 125, can passively record traffic externally after it has been modified by the boundary.</u>**” (Paxton ¶18) • “[W]hile **<u>client requests</u> are sourced from the client**, boundary requests alter the original client requests to appear from the boundary.” (Paxton ¶4) As explained in §IX.A.5 above, to the extent Patent Owner argues that **Paxton** does not explicitly disclose the packets transmitted by the network device are encrypted packets, it would have been obvious to a POSITA to apply the teachings of **Paxton** to encrypted packets, as taught by **Deschenes**. **Deschenes** discloses correlating client side and server side packets that are encrypted. • “[T]he monitored or captured **<u>network communication from one side (e.g., the server-side) may be encrypted</u>** and the probing device 108 may not be able to decrypt that portion of the monitored network communication. In such an embodiment, the **<u>traffic analyzer 120 may still be configured to match or correlate, as best it can, the two portions (e.g., server-side and client-side) of the network communication</u>**.” (Deschenes ¶42; *see also* ¶¶27-28 (client-side communications may be encrypted)) • “[T]he second or receiving **probing device (e.g., probing device 108) may be configured to <u>decrypt the encrypted network communications</u>** it monitors. In such an embodiment, **it or at least its traffic analyzer 120 may be configured to <u>match or associate the</u>**

’573 Patent	Paxton, Sutton, Deschenes
	received timing information 123b with the decrypted network communications it monitors or timing information 123 derived thereof. In such an embodiment, by combining the information provided by the received timing information 123 and 123b and the locally monitored network communications a more complete set of metrics 122 may be generated.” (Deschenes ¶46; *see also* ¶¶38-40) • “[A]nalyzer 219 may include an metric generator that is used or employed to generate a second set of metric information (e.g., timing information 298, etc.) that are based upon the decrypted network communications 221. **These [decryption]-based timing information 298 may then be compared to the encryption based timing information 297 to correlate or associate portions or transactions within the network communications**.” (Deschenes ¶73; *see also* ¶¶62, 80) Akl, ¶¶104-107.
[1d] generating, by the computing system, a second plurality of log entries corresponding to the plurality of encrypted packets transmitted by the network device;	**Paxton** in view of **Deschenes** discloses **generating, by the computing system, a second plurality of log entries corresponding to the plurality of encrypted packets transmitted by the network device** (generating second hash data records and storing them in a database). • “[A]s a packet is transmitted from the client 105, the inside sensor 120 can calculate a hash, e.g., a MD5 algorithm hash, of the application layer payload and store it alongside network layer header. **After the packet traverses the boundary 110, the outside sensor 125 can calculate a hash e.g., a MD5 algorithm hash, of the payload along with the header data of the packet**.” (Paxton ¶17; *see also* ¶¶28-29 regarding fuzzy hashing) • “**The hash value from each payload can be stored in a database that has direct access to the inside sensor and outside sensor and is configured to store…the second hash data record along with the IP address**

’573 Patent	Paxton, Sutton, Deschenes
	and timestamp of when it was sensed.” (Paxton ¶20 (full citation in [1b])) • *See also* Paxton ¶27 (live or recorded capture modes). • Fig. 3, ¶¶24-25 (showing multiple entries for multiple packets).  **Figure 3** Akl, ¶¶108-110.
[1e] correlating, by the computing system and based on the first plurality of log entries corresponding to the plurality of packets received by the network device and the second plurality	**Paxton** in view of **Deschenes** discloses **correlating** (matching), **by the computing system and based on the first plurality of log entries corresponding to the plurality of packets received by the network device and the second plurality of log entries corresponding to the plurality of encrypted packets transmitted by the network device, the plurality of encrypted packets transmitted by the network device with the plurality of packets received by the network device** (determining a closest matching hash and timestamp). • “**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.**

’573 Patent	Paxton, Sutton, Deschenes
of log entries corresponding to the plurality of encrypted packets transmitted by the network device, the plurality of encrypted packets transmitted by the network device with the plurality of packets received by the network device; and	**The combination of identifiable inside and outside header data can serve as the identity of the packet.**” (Paxton ¶22) • “FIG. 2 is a screenshot 200 of a log that illustrates a **matching payload**, in accordance with an exemplary embodiment of the invention. **The two hashes, preceded by the MD5 label, are identical in FIG. 2. Furthermore, it is also observed that the time in TimeSecs (seconds) are equal, but the time in TimeMSecs (milliseconds) differ by 814 milliseconds. In other words, the inside packet arrived 814 milliseconds before the outside packet, which is consistent with the inside packet sensing the packet first. In this case, the identity of the packet is the SrcAddr (source address) of the packet sensed from each side, which is 132.XXX.XXX.102/172.XXX.XXX.240.**” (Paxton ¶23) • Fig. 3, ¶¶24-25 (showing multiple packets being correlated).  Akl, ¶¶111-115.
[1f]	**Paxton** discloses that the correlation can be used to identify nodes infected with malicious content and identify the scope of malicious incidents.

’573 Patent	Paxton, Sutton, Deschenes
responsive[4] to the correlating of the plurality of encrypted packets transmitted by the network device with the plurality of packets received by the network device: generating, by the computing system and based on the correlating, one or more rules configured to identify packets received from the host located	• “**The ability to <u>identify the true source of packet transmission through a boundary</u> can provide significant benefits to network security.** Current technology that attempts to discover the identity of network packet suffers from authentication and integrity problems. **It can provide a way to quickly <u>identify nodes that are infected with malicious content</u>, which can <u>allow the network administrator to better identify the scope of the malicious incident</u>.** The system and method described herein can be highly modular and can be implemented atop open source technology on commodity hardware. Furthermore, it can provide a stable foundation for building tiered enterprise network architectures with an inherent capability for attribution of malicious activity. **Enterprises with significant visibility and monitoring investments into the network backbone can <u>utilize this technique to attribute malicious activity sensed at the edge of a network back to its original source</u>.**” (Paxton ¶30) As explained in §IX.A.4 above, **Paxton** discloses correlating packets to identify malicious activity and leaves specific usage and remedial steps to a POSITA. A POSITA would

[4] Steps performed “responsive” to correlating are not necessarily performed immediately after correlating. *See* Ex. 1001, 12:59-13:38 (describing a progression of steps including: (step 26) “responsive to correlating,” determining a network address associated with a transmitted packet, (step 27) determining that the packet was transmitted to a malicious entity, (steps 28-29) notifying a user of the communication with the malicious entity, and (steps 30-32) provisioning rules to drop packets and prevent the spread of malware).

’573 Patent	Paxton, Sutton, Deschenes
in the first network; and provisioning a packet-filtering device with the one or more rules configured to identify packets received from the host located in the first network.	have been motivated to generate a rule configured to identify packets received from the first host in the first network and provision a packet-filtering device with the rule, as taught by **Sutton**, responsive to the correlating disclosed by **Paxton**. **Sutton** discloses **generating, by the computing system and based on the correlating, one or more rules configured to identify packets received from the host located in the first network** (based on communications to a darknet address and identifying potential malicious code, filtering or blocking further communications from the host; preventing communications using rules; taking action to make such rules available); and **provisioning a packet-filtering device with the one or more rules configured to identify packets received from the host located in the first network** (to block further communications, rules would have been provisioned on a device that analyzes and identifies the communications, e.g., the sensors and servers already configured to analyze the packets, a gateway, proxy, firewall, etc. that is part of the first network; **Sutton** teaches that the processing nodes and functions for receiving, analyzing, and processing packets may be comprised of multiple devices with distributed hardware and software acting together). • “Systems, methods and apparatus for a distributed security that monitors communications to identify access attempts to/from darknet addresses. Such 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.**” (Sutton, Abstract) • “In those implementations where all communications 350 are inspected, the communications 350 can be processed to **identify devices which are likely associated with malicious activity. If such devices reside within the enterprise network, <u>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</u>. If**

’573 Patent	Paxton, Sutton, Deschenes
	such devices are outside of the enterprise network, the authority node policy data can be used to implement a rule preventing such devices from communicating with devices within the protected enterprise network.” (Sutton, 10:60-11:3) • “**In those implementations where only those communications 350 originating from devices within a protected enterprise network are inspected, notification 355 can be provided to the enterprise network (e.g., a network administrator) indicating that the device is potentially infected with malicious software code.** In some implementations, the processing node(s) 110 can attempt to remove the malicious program code from the device originating communications destined for the darknet address space 300. **In other implementations, communications 350 originating from the device can be actively filtered (e.g., through various application specific malware identification programs, such as, performed by processing node manager 118 and data inspection engines 116) based upon identification of the probability that malicious code exists on the device.**” (Sutton, 11:4-18) • “At stage 450, **a notification of potential malicious activity originating from the protected network is provided and/or automated blocking/filtering is implemented.... Additionally, traffic may be automatically blocked, redirected or filtered based on predefined rules.** [¶] The various data exchange and malicious activity identification processes of FIG. 4 are example **processes for which the threat data and/or detection process filters can be updated in the system 100** of FIGS. 1 and 2. Other update processes, however, can also be used.” (Sutton, 12:57-13:14) • “**[B]locking further communications from a device originating communications** with a destination address

’573 Patent	Paxton, Sutton, Deschenes
	on the list of darknet addresses and **taking appropriate additional steps to control future communications from the device** and provide notification of a potential infection.” (Sutton, 15:67-16:5) • “**Each processing node 110 can generate a decision vector D=[d1, d2,…, dn] for a content item of one or more parts C=[c1, c2,…, cm].** Each decision vector can identify a threat classification, e.g., clean, spyware, malware, undesirable content, innocuous, unknown, etc. **For example, the output of each element of the decision vector D can be based on the output of one or more data inspection engines. In some implementations, the threat classification can be reduced to a subset of categories e.g., violating, non-violating, neutral, unknown. Based on the subset classification, a processing node 110 may allow distribution of the content item, preclude distribution of the content item, allow distribution of the content item after a cleaning process, or perform threat detection on the content item.** In some implementations, the actions taken by a processing node 110 can be determinative on the threat classification of the content item and on a security policy of the external system to which the content item is being sent from or from which the content item is being requested by. A content item is violating if, for any part C=[c1, c2,…, cm] of the content item, at any processing node 110, any one of the data inspection engines generates an output that results in a classification of ‘violating.’” (Sutton, 3:1-23) • Fig. 2 (showing processing node 110 with processing node manager 118 and data inspection engines 116).

’573 Patent	Paxton, Sutton, Deschenes

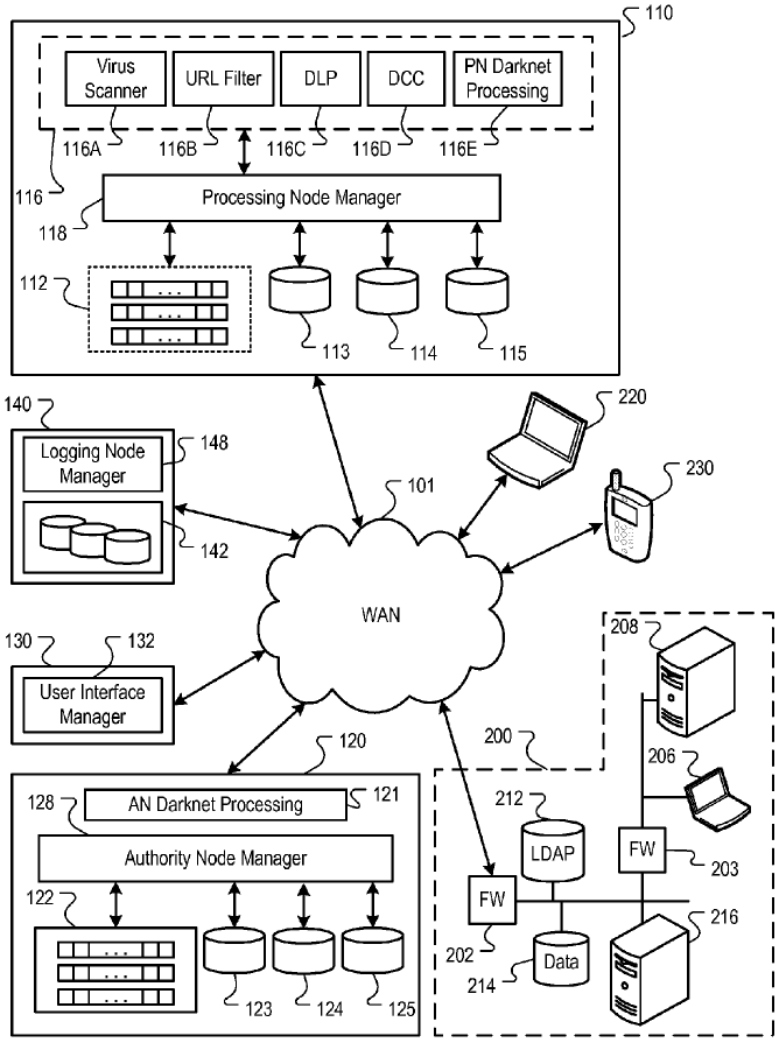


FIG. 2

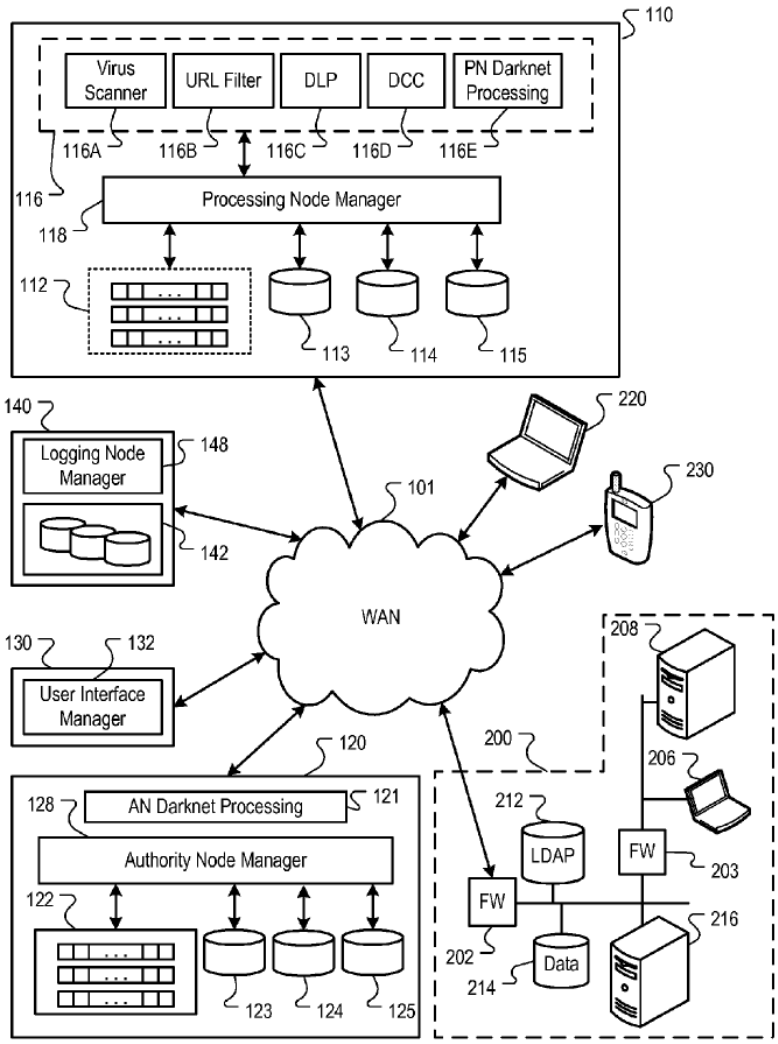
- “**Each processing node 110 can be implemented by a plurality of computer and communication devices, e.g., server computers, gateways, switches, etc.** In some implementations, the processing nodes 110 can serve as an access layer 150. The access layer 150 can, for example, provide external system access to the security system 100. In some implementations, each processing node 110 can include Internet gateways and a plurality of server computers, and the processing nodes 110 can be distributed through a geographic region, e.g., throughout a country. According to a service agreement between a provider of the system 100 and an owner of an

’573 Patent	Paxton, Sutton, Deschenes
	external system, the system 100 can thus provide security protection to the external system at any location throughout the geographic region.” (Sutton, 3:24-37; *see also* 3:38-4:4 (distributing policy data to processing nodes), 13:26-42, 14:29-57) A POSITA would have recognized, based on Sutton’s disclosure, that for a computing system to block future communications from a device (e.g., blocking a device within a network from communicating to an outside darknet address), when the device had not been previously identified as having malicious communications and/or not previously blocked, data/rules would have been generated and provisioned on a boundary or other monitoring device to identify those communications from the blocked device (i.e., a device with access to the packet or tasked with inspecting the packet would have been provisioned with rules, thereby providing a way to identify the device’s communications, and accurately block undesired communications)—or at minimum found it obvious to do so. The generation of data/rules for boundaries to drop packets of specific devices was well-known in the art. Akl, ¶¶116-124.
[7] The method of claim 1, comprising: determining, by the computing system, that the host located in the second network is associated with a malicious entity; and generating, by the computing	**Paxton** discloses that the correlation can be used to identify nodes (hosts) infected with malicious content and identify the scope of malicious incidents. • (Paxton ¶30 (*see* full citation in [1f] above)) As explained in §IX.A.4 above, **Paxton** discloses correlating packets to identify malicious activity and leaves specific usage and remedial steps to a POSITA. A POSITA would have been motivated to determine whether the second host is associated with a malicious entity, and if so to generate data to cause the first network to drop packets transmitted by the first host, as taught by **Sutton**, in **Paxton’s** system. **Sutton** discloses **determining that the second host** (outside the enterprise network) **is associated with a malicious entity** (associated with activities of a malicious actor; at a darknet

’573 Patent	Paxton, Sutton, Deschenes
system, one or more rules configured to cause the first network to drop packets transmitted by the host located in the first network.	address), and **generating, by the computing system, rules configured to cause the first network to drop packets transmitted by the first host** (causing malware identification programs to filter communications; using policy data to implement a rule to prevent all communication with malicious external host; blocking further/future communications; performed using, e.g., processing node manager 118 and data inspection engines 116 (e.g., URL filter 116B, PN darknet processing 116E) of processing node 110, a network device such as a server, gateway, or proxy). • “[T]he processing node 110 may act as a forward proxy that receives user requests to external servers addressed directly to the processing node 110.” (Sutton, 3:38-53; *see also* 4:45-51) • “The 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. The PN darknet processing 116E is described in detail at FIG. 3.” (Sutton 6:18-22) • “§4.0 Monitoring Communications to Identify Potentially Malicious Activity Once the list of darknet addresses 115 is received from the authorization node(s) 120, the processing node(s) 110 can begin monitoring communications 350. **In some implementations, the processing node(s) 110 can inspect all communications 350 for inclusion of a destination address that is included in the list of darknet addresses. In other implementations, the processing node(s) 110 can inspect only those communications 350 originating from the enterprise network 200 to determine whether those communications 350 are destined for an address on the list of darknet addresses.** In further implementations, the origin information of communications 350 can be inspected to identify

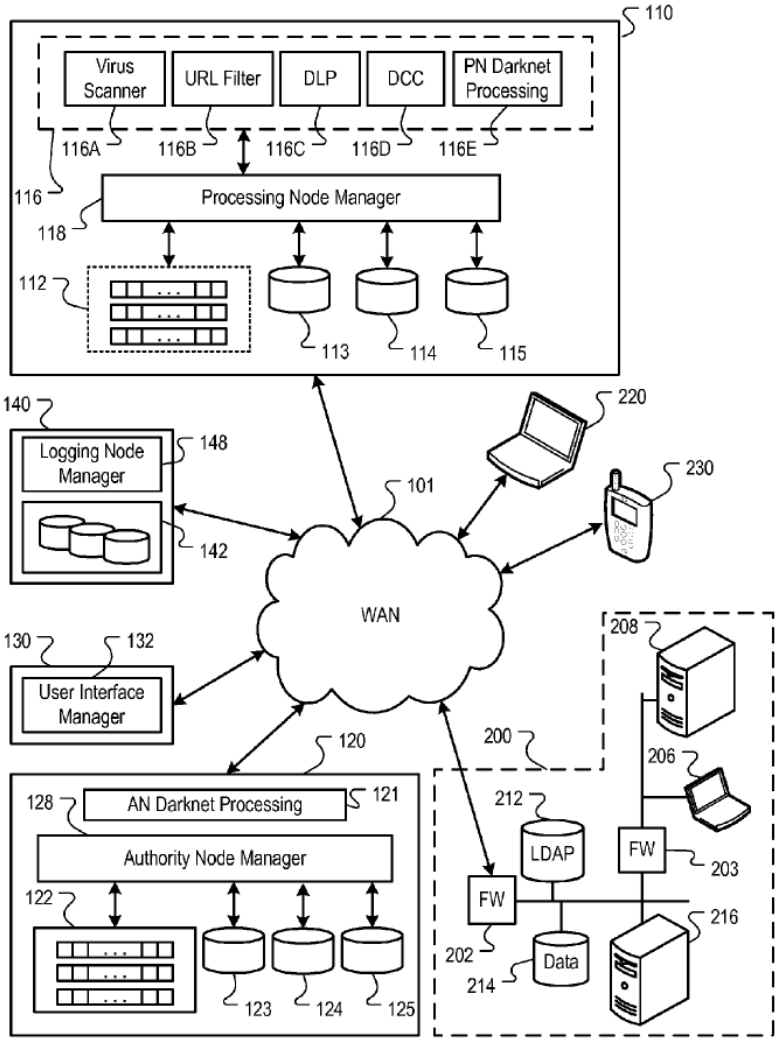
’573 Patent	Paxton, Sutton, Deschenes
	communications 350 that purport to originate from the darknet address space. Such communications 350 can be presumed to be non-legitimate as the source address has been spoofed (faked). **The determination that a destination or origination address is a darknet address can be made by comparing the destination and/or origination address on monitored communications 350 to the list of darknet addresses. If a match is found, the communication 350 is either destined to, or falsely originates from a darknet address.**” (Sutton, 10:37-59) • “In those implementations where all communications 350 are inspected, the communications 350 can be processed to **identify devices which are likely associated with malicious activity.** If such devices 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. **If such devices are outside of the enterprise network, the authority node policy data can be used to implement a rule preventing such devices from communicating with devices within the protected enterprise network.**” (Sutton, 10:60-11:3) • “In those implementations where only those communications 350 originating from devices within a protected enterprise network are inspected, notification 355 can be provided to the enterprise network (e.g., a network administrator) indicating that **the device is potentially infected with malicious software code**. In some implementations, the processing node(s) 110 can attempt to remove the malicious program code from the device originating communications destined for the darknet address space 300. In other implementations, **communications 350 originating from the device can be actively filtered (e.g., through various application**

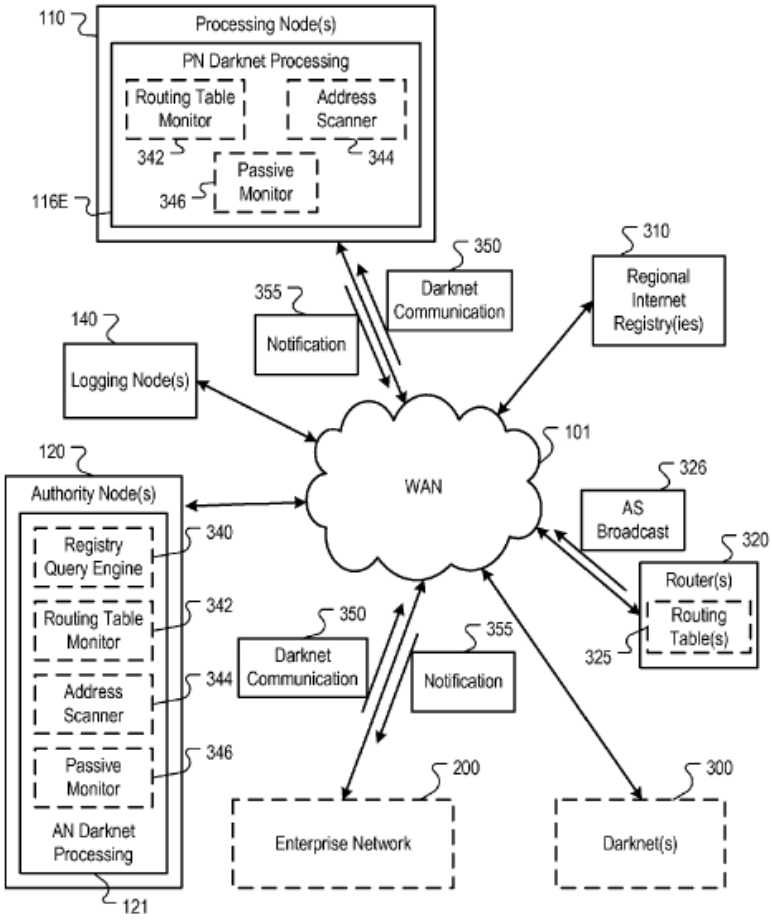
’573 Patent	Paxton, Sutton, Deschenes
	specific malware identification programs, such as, performed by processing node manager 118 and data inspection engines 116) based upon identification of the probability that malicious code exists on the device.” (Sutton, 11:4-18) • “At stage 450, **a notification of potential malicious activity originating from the protected network is provided and/or automated blocking/filtering is implemented.... Additionally, traffic may be automatically blocked, redirected or filtered based on predefined rules.** [¶] The various data exchange and malicious activity identification processes of FIG. 4 are example **processes for which the threat data and/or detection process filters can be updated in the system 100** of FIGS. 1 and 2. Other update processes, however, can also be used.” (Sutton, 12:57-13:14) • “**[B]locking further communications from a device originating communications** with a destination address on the list of darknet addresses and **taking appropriate additional steps to control future communications from the device** and provide notification of a potential infection.” (Sutton, 15:67-16:5) • Fig. 2 (showing processing node 110 with processing node manager 118 and data inspection engines 116).

’573 Patent	Paxton, Sutton, Deschenes
	 FIG. 2 • “Each processing node 110 can be implemented by a plurality of computer and communication devices, e.g., server computers, gateways, switches, etc.” (Sutton, 3:24-37 (*see* full citation in [1f] above); *see also* 3:38-4:4 (distributing policy data to processing nodes), 13:26-42, 14:29-57) Akl, ¶¶125-128.
[8] The method of claim 1, comprising:	**Paxton** discloses **generating, by the computing system, an indication of the first host** (generating a match log including the identity of the packet source address).

'573 Patent	**Paxton, Sutton, Deschenes**
generating, by the computing system, a message identifying the host located in the first network; and communicating, by the computing system and to at least one of the host located in the first network or a computing device associated with an administrator of the first network, the message identifying the host located in the first network.	• "FIG. 2 is a screenshot 200 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**, which is 132.XXX.XXX.102/172.XXX.XXX.240." (Paxton ¶23) • "**The ability to identify the true source of packet transmission through a boundary can provide significant benefits** to network security…. It can provide a way to **quickly identify nodes that are infected with malicious content, which can allow the network administrator to better identify the scope of the malicious incident**." (Paxton ¶30 (*see* full citation in [1f] above)) As explained in §IX.A.4 above, **Paxton** discloses correlating packets to identify malicious activity and leaves specific usage and remedial steps to a POSITA. A POSITA would have been motivated to generate and communicate a message, identifying the host in the first network, to an administrator of the first network, as taught by **Sutton**. **Sutton** discloses **transmitting (i.e., messaging) the indication of the first host to a computing device associated with an administrator of the first network**. • "In those implementations where all communications 350 are inspected, the communications 350 can be processed to **identify devices which are likely associated with malicious activity. If such devices 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. If such devices are outside of the enterprise network, the authority node policy data can be used to implement a rule preventing such devices from communicating with devices within the protected enterprise network.**" (Sutton, 10:60-11:3)

’573 Patent	Paxton, Sutton, Deschenes
	• “**In those implementations where only those communications 350 originating from devices within a protected enterprise network are inspected, notification 355 can be provided to the enterprise network (e.g., a network administrator) indicating that the device is potentially infected with malicious software code.** In some implementations, the processing node(s) 110 can attempt to remove the malicious program code from the device originating communications destined for the darknet address space 300. **In other implementations, communications 350 originating from the device can be actively filtered (e.g., through various application specific malware identification programs, such as, performed by processing node manager 118 and data inspection engines 116) based upon identification of the probability that malicious code exists on the device.**” (Sutton, 11:4-18)

’573 Patent	Paxton, Sutton, Deschenes
	• Fig. 2 (showing processing node 110 with processing node manager 118 and data inspection engines 116).  FIG. 2 • Fig. 3 (showing notifications 355 transmitted electronically—i.e., to devices in the computing system)

’573 Patent	Paxton, Sutton, Deschenes
	 FIG. 3 Akl, ¶¶129-133.
[9pre] A computing device comprising:	**Paxton** discloses **a computing device** (a computer system implementing modules). • *See* [1a] and [9a]. Akl, ¶¶134-135.
[9a] at least one processor; and memory comprising instructions that, when executed	**Paxton** discloses **at least one processor and memory** (machine-readable media) **storing instructions for execution by the processors** to perform a method. • “In particular regard to the various functions performed by the above described **components (processor-executed processes, assemblies, devices, systems, circuits, and the like)**, the terms…used to describe such

’573 Patent	Paxton, Sutton, Deschenes
by the at least one processor, cause the computing device to:	components are intended to correspond…to any component, such as **hardware, processor executed software, or combinations thereof**, which performs the specified function….” (Paxton ¶31) • “Portions of the invention can comprise a computer program that embodies the functions described herein. **Furthermore, the modules described herein, such as the inside sensor module, outside sensor module, and matching module, can be implemented in a computer system that comprises instructions stored in a machine-readable medium and a processor that executes the instructions.** However, it should be apparent that there could be many different ways of implementing the invention in computer programming, and the invention should not be construed as limited to any one set of computer program instructions.” (Paxton ¶32) • “A computer implemented system, comprising: an inside sensor module…implemented in a computer system that comprises instructions stored in a machine-readable medium and a processor that executes the instructions; an outside sensor module…implemented in a computer system that comprises instructions stored in a machine-readable medium and a processor that executes the instructions; a matching module…implemented in a computer system that comprises instructions stored in a machine-readable medium and a processor that executes the instructions.” (Paxton, claim 10) Akl, ¶¶136-137.
[9b] identify a plurality of packets received by a network	*See* [1a]. Akl, ¶138.

’573 Patent	Paxton, Sutton, Deschenes
device from a host located in a first network;	
[9c] generate a first plurality of log entries corresponding to the plurality of packets received by the network device;	*See* [1b]. Akl, ¶139.
[9d] identify a plurality of encrypted packets transmitted by the network device to a host located in a second network;	*See* [1c]. Akl, ¶140.
[9e] generate a second plurality of log entries corresponding to the plurality of encrypted packets transmitted by the network device;	*See* [1d]. Akl, ¶141.
[9f] correlate, based on the first plurality of log entries	*See* [1e]. Akl, ¶142.

’573 Patent	Paxton, Sutton, Deschenes
corresponding to the plurality of packets received by the network device and the second plurality of log entries corresponding to the plurality of encrypted packets transmitted by the network device, the plurality of encrypted packets transmitted by the network device with the plurality of packets received by the network device; and	
[9g] responsive to the correlating of the plurality of encrypted packets transmitted by the network device with the plurality of packets received by the network device:	*See* [1f]. Akl, ¶143.

’573 Patent	Paxton, Sutton, Deschenes
generate, based on the correlating, one or more rules configured to identify packets received from the host located in the first network; and provision a packet-filtering device with the one or more rules configured to identify packets received from the host located in the first network.	
[15] The computing device of claim 9, wherein the instructions that, when executed by the at least one processor, further cause the computing device to: determine that the host located in the second network is associated with a malicious entity; and	*See* [7]. Akl, ¶144.

’573 Patent	Paxton, Sutton, Deschenes
generate one or more rules configured to cause the first network to drop packets transmitted by the host located in the first network.	
[16] The computing device of claim 9, wherein the instructions that, when executed by the at least one processor, further cause the computing device to: generate a message identifying the host located in the first network; and communicate, to at least one of the host located in the first network or a second computing device associated with an administrator of the first	*See* [8]. Akl, ¶145.

’573 Patent	Paxton, Sutton, Deschenes
network, the message identifying the host located in the first network.	
[17pre] One or more non-transitory computer-readable media comprising instructions that, when executed by one or more processors of a computing system, cause the computing system to:	**Paxton** discloses **one or more non-transitory computer-readable media** (machine-readable media) **comprising instructions that, when executed by one or more processors of a computing system, cause the computing system to** perform a method. *See* [9pre] and [9a]. Akl, ¶¶146-147.
[17a] identify a plurality of packets received by a network device from a host located in a first network;	*See* [1a]. Akl, ¶148.
[17b] generate a first plurality of log entries corresponding to the plurality of packets received by the network device;	*See* [1b]. Akl, ¶149.
[17c]	*See* [1c].

’573 Patent	Paxton, Sutton, Deschenes
identify a plurality of encrypted packets transmitted by the network device to a host located in a second network;	Akl, ¶150.
[17d] generate a second plurality of log entries corresponding to the plurality of encrypted packets transmitted by the network device;	*See* [1d]. Akl, ¶151.
[17e] correlate, based on the first plurality of log entries corresponding to the plurality of packets received by the network device and the second plurality of log entries corresponding to the plurality of encrypted packets transmitted by the network	*See* [1e]. Akl, ¶152.

’573 Patent	Paxton, Sutton, Deschenes
device, the plurality of encrypted packets transmitted by the network device with the plurality of packets received by the network device; and	
[17f] responsive to the correlating of the plurality of encrypted packets transmitted by the network device with the plurality of packets received by the network device: generate, based on the correlating, one or more rules configured to identify packets received from the host located in the first network; and provision a packet-filtering device with the one or more	*See* [1f]. Akl, ¶153.

’573 Patent	Paxton, Sutton, Deschenes
rules configured to identify packets received from the host located in the first network.	
[23] The one or more non-transitory computer-readable media of claim 17, further comprising instructions that, when executed by the one or more processors of the computing system, cause the computing system to: determine that the host located in the second network is associated with a malicious entity; and generate one or more rules configured to cause the first network to drop packets transmitted by the host located	*See* [7]. Akl, ¶154.

’573 Patent	Paxton, Sutton, Deschenes
in the first network.	
[24] The one or more non-transitory computer-readable media of claim 17, further comprising instructions that, when executed by the one or more processors of the computing system, cause the computing system to: generate a message identifying the host located in the first network; and communicate, to at least one of the host located in the first network or a computing device associated with an administrator of the first network, the message identifying the	*See* [8]. Akl, ¶155.

’573 Patent	Paxton, Sutton, Deschenes
host located in the first network.	

B. Ground 2: Claims 2, 10, and 18 are obvious over Paxton and Sutton in view of Deschenes and McDonald

1. Overview of McDonald

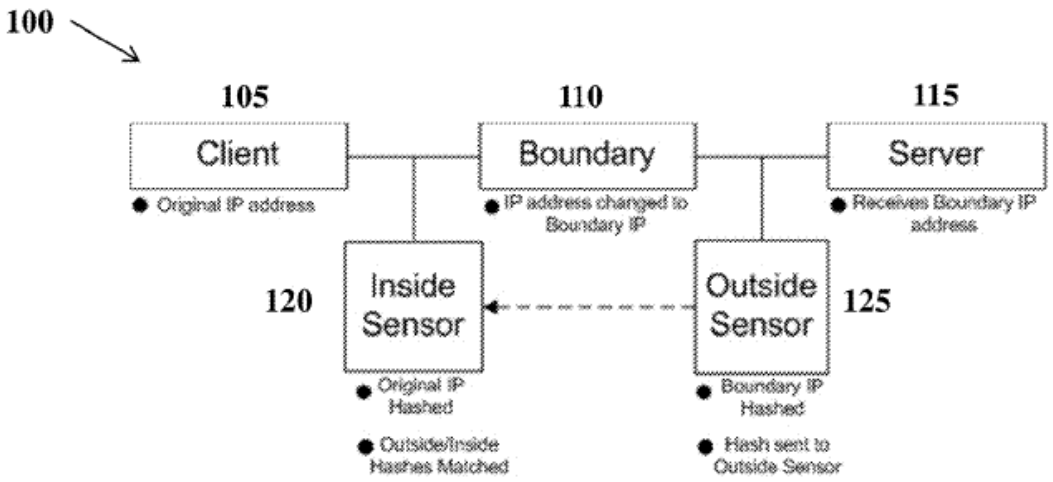
McDonald is directed to correlating packets based on their identifier information (e.g., ports). McDonald describes “correlating at least one identifier from the first packet which is different to a corresponding identifier of the second packet.” Ex. 1009, Abstract. The system employs packet selectors “for selecting a first packet from a first side of the identifier translator prior to transmission through the identifier translator” and “for selecting candidate packets from a second side of the identifier translator after transmission through the identifier translator.” *Id.*, ¶7. Akl, ¶¶77-78.

2. Analysis and Motivation to Combine (McDonald)

As discussed in §IX.A, Paxton and Sutton, in view of Deschenes, discloses the method, computing device, and computer-readable media of claims 1, 9, and 17.

Paxton further discloses that “a communication path that interfaces the network device and the first network comprises a first tap configured to identify packets received by the network device” (inside sensor 120, e.g., a server, records traffic on the communication path between client 105’s network and the boundary

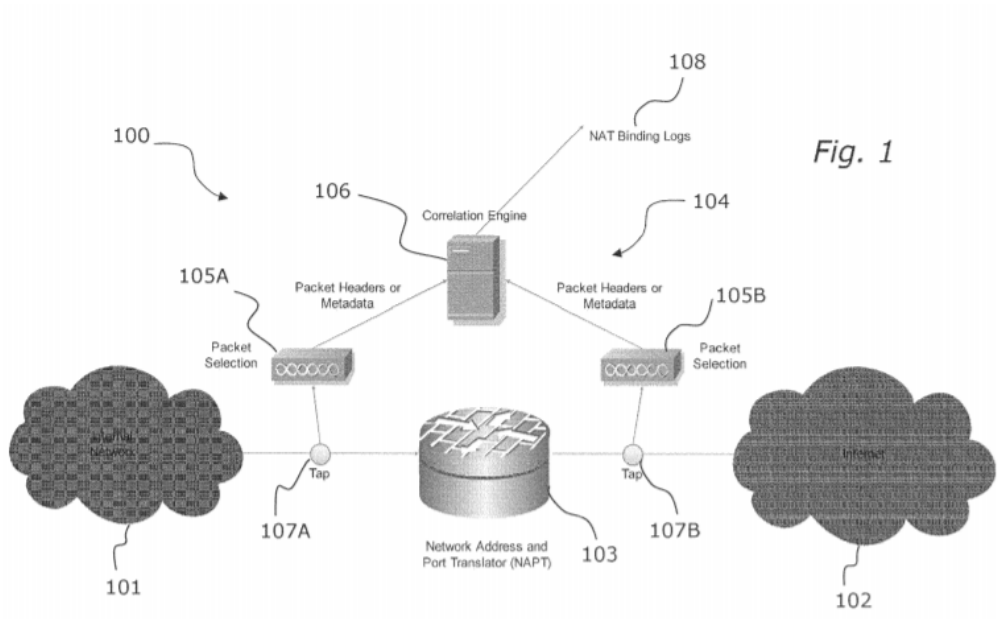
110) and "a communication path that interfaces the network device and the second network comprises a second tap configured to identify packets transmitted by the network device" (outside sensor 125, e.g., a server, records traffic on the communication path between boundary 110 and server 115's network), as recited in claims 2, 10, and 18. Ex. 1004, ¶18; *see also* §IX.A above (discussions regarding Paxton's system operation). The sensors may, e.g., be separate servers, or network interfaces on a single server. *Id.* *See* Paxton Fig. 1.



Akl, ¶¶87-88, 157.

Paxton discloses that its taps passively record traffic but does not explicitly disclose steps or programming instructions causing the computing system to provision the first and second taps with rules configured to identify the plurality of packets received and transmitted, respectively, by the network device, as recited in claims 2, 10, and 18. Akl, ¶¶89, 158.

McDonald similarly discloses a correlation system with taps in communication paths around a NAT and teaches configuring the taps with rules. For example, McDonald discloses that candidate packets for correlation by Address Correlation Engine (ACE) 104 are selected by "two packet selectors 105A and 105B which each select a subset of packets from the network traffic on each side of the NAT 103." Ex. 1009, ¶11. *See* Figure 1.



Akl, ¶¶90, 159.

The packet selectors are programmed with rules configured to select packets that have a higher chance of successful correlation, e.g., packets with certain flags, TCP packets, packets that pass through the tap points during certain time windows. Ex. 1009, ¶¶13, 14, 21, Fig. 3. McDonald further discloses that "selection criteria" may be dynamically created or updated as desired. *Id.*, ¶35. Akl, ¶¶91, 160-161.

It would have been obvious to a POSITA to modify Paxton's taps (e.g., servers) to include rules for selecting candidate packets for correlation and to have the computing system provision such rules onto the taps, as recited in claims 2, 10, and 18. Paxton discloses that its taps record traffic passively, but Paxton also recognizes that full packet capture on high bandwidth links may be demanding of resources. Ex. 1004, ¶18. McDonald likewise acknowledges that "packet selectors 105A and 105B could select all packets, but this would be unlikely in practice." Ex. 1009, ¶11. Thus, while the packet selectors analyze every packet passing through the tap points, it would have been obvious to limit deeper correlation analysis to a subset of packets satisfying rule-based criteria—i.e., packets for which there would be higher chances of identifying matching packets—avoiding the need to inspect all the traffic passing through the network device. *Id.*, ¶¶13, 35; *see also* ¶¶14-20. Additionally, McDonald discloses that the selection criteria (i.e., selection rules) may be static or dynamically created or updated. *Id.*, ¶35. Further, a POSITA would have recognized that rules "dynamically" created and/or updated for use by the taps are provisioned onto the taps by the computing system because the rules are implemented in a digital computing system, such that the act of provisioning the rules obviously, if not necessarily, involves the computing

system.[5] *See, e.g.*, Ex. 1007, 6:32-7:17, 7:48-55, 13:10-14 (describing processing filters), 7:36-47, 7:56-67, 8:11-15 (describing management of filters, push/pull processes). Akl, ¶92.

A POSITA would have had a reasonable expectation of success provisioning rules in Paxton's taps, as taught by McDonald. Paxton and McDonald both describe taps that perform similar packet monitoring and selection functions. Ex. 1004, ¶¶18-20, Fig. 1; Ex. 1009, ¶¶11-13, Fig. 1. Furthermore, Paxton's taps (inside and outside sensors 120 and 125) are "implemented in a computer system that comprises instructions." Ex. 1004, ¶32, claim 10. A POSITA would have recognized that provisioning and implementing rules to identify packets, on a server in a computing system, would have used, for example, basic data storage, retrieval, and evaluation routines (e.g., storing rules, reading rules, evaluating

[5] Steps performed "by the computing system," such as the "provisioning" recited by claims 2, 10, and 18, do not preclude user input to or interaction with the computer system in performing those steps. *See* Ex. 1012 (U.S. Patent 10,931,797, a continuation of the '573 patent) at 15:45-47 and 16:48-50 (representing that "generating, by the computing system…, one or more rules" comprises "receiving user input defining the one or more rules").

packet information), which would have been obvious and well within the skill of a POSITA. Akl, ¶93.

C. Ground 3: Claims 3-6, 11-14, 19-22 are obvious over Paxton and Sutton in view of Deschenes and Ivershen

1. Overview of Ivershen

Ivershen is directed to systems and methods for correlating IP flows across a NAT firewall. Ex. 1005, Abstract. Figure 2 shows the components of the system used to correlate IP flows.

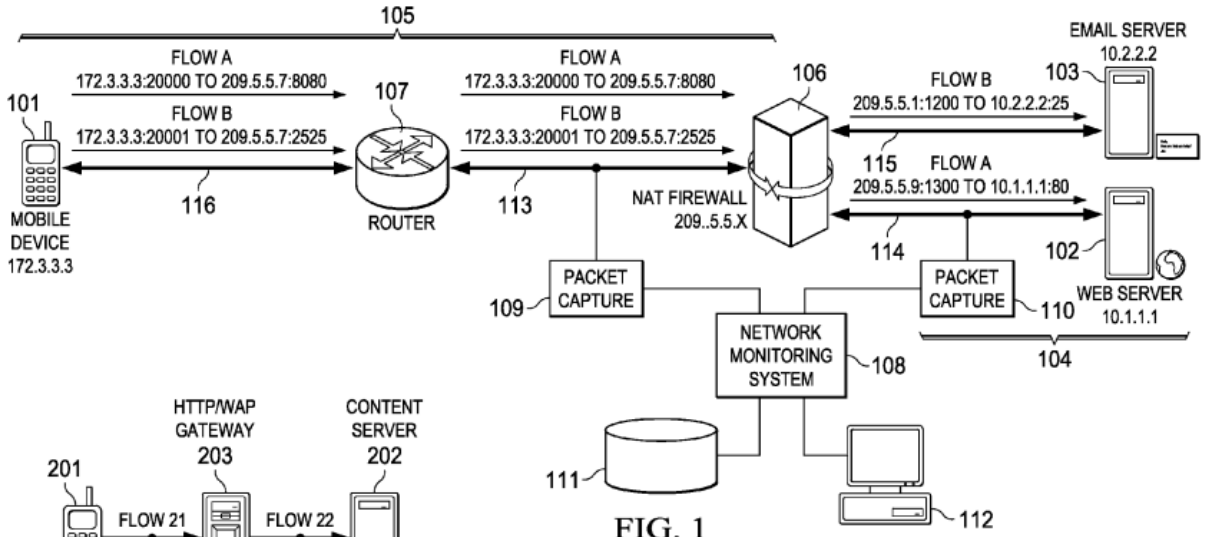


FIG. 1

FIG. 2

Packet capture devices 109 and 110 capture data before and after packets cross a NAT firewall 106. *Id.*, 5:11-13. The network monitoring system 108 then matches (correlates) the packets at both capture devices by searching for flows

within close time windows having similar timestamps (differences of a few milliseconds) and determining whether they have matching information. *Id.*, 2:43-51, 5:62-6:11, 8:4-10.

A variety of information may be used to correlate the packets, including L5/L7 data, flow starting timestamps, L7 protocols, HTTP URIs, flow duration, and HTTP header information. *Id.*, 5:36-7:3. This information is typically unmodified through NAT traversal. *Id.*, 5:27-35. Additionally, Ivershen discloses that while a NAT modifies address information passing between networks, a routing table (e.g., containing IP addresses and ports) could be used to correlate packets if it is available and updated. *Id.*, 2:3-8, 4:19-41, 5:11-26. Akl, ¶¶69-72.

2. Motivation to Combine (Ivershen)

With respect to claims 3-4, 11-12, and 19-20, to the extent Patent Owner argues that Paxton does not explicitly disclose correlating based on a comparison of ports (claims 3, 11, 19) or network-interface identifiers (claims 4, 12, 20), a POSITA would have been motivated to log and use these parameters in Paxton's correlation system, as taught by Ivershen. Akl, ¶¶81, 164-176. Both Paxton and Ivershen seek to use typically invariant information to correlate packets; for example, Paxton identifies the application layer payload and Ivershen identifies L5 and L7 data as examples of such information. Ex. 1004, ¶15; Ex. 1005, 5:27-35. Paxton also utilizes other packet information and, in some embodiments, varies

hashing functions to make the best match—making use of "**at least** three criteria: hash, time, and IP address" and employing fuzzy hashing in embodiments where identically matching payload hashes are not expected. Ex. 1004, ¶¶21, 28-29. Ivershen similarly teaches that additional packet properties, beyond a calculated checksum, are used to find matches, narrow match results, and discard false positives—using checksum keys, flow starting timestamps, L7 protocols, flow durations, HTTP URIs, and "other properties." Ex. 1005, 5:62-6:12. A POSITA would have thus recognized that the specific information used to correlate packets is not limited in number or type, and Paxton's correlation system would produce results with increased confidence—e.g., by narrowing multiple potential results as taught by Ivershen—by comparing additional types of packet information. As such, Ivershen teaches that information known to be used for correlation includes ports and network-interface identifiers. *Id.*, 2:3-8, 2:52-63, and 7:40-8:3. Port information, for example, is packet information that systems at network boundaries already inspect to route packets to their proper destinations, and so it would have been an obvious choice for conducting correlation analysis, which also relates to the routing of those packets. It would have been obvious to a POSITA to utilize this information in addition to the information in Paxton to increase the likelihood of correlating the correct packets. Akl, ¶¶81, 41-44.

With respect to claims 5-6, 13-14, and 21-22, to the extent Patent Owner argues that Paxton finds matches "based on at least three criteria: hash, time, and IP address," and does so by finding the "closest matching hash (with respect to the timestamp)," but does not explicitly disclose comparing times/timestamps, a POSITA would have been motivated to log and compare times/timestamps of packet receipt times and packet transmission times, as taught by Ivershen. Akl, ¶¶82, 177-186. As discussed above, Ivershen discloses correlating by determining which packets are within a close time window, matching a "CHKEY, flow starting timestamp, and L7 protocol," "look[ing] for a flow start timestamp that is within a few milliseconds of the beginning of the flow on the first probe," and by comparing flow durations. Ex. 1005, 5:62-6:11, 8:4-10. Matching times within a certain threshold or window accounts for timestamp drift and travel time across interfaces. *Id.*, 2:43-51, 5:62-6:4. A POSITA would have been motivated to apply Ivershen's function of matching for flow starting timestamps (and its accounting for drift and travel time) to Paxton's receipt and transmission timestamps, and/or to apply Ivershen's function of matching flow starting timestamps and comparing flow durations in addition to Paxton's timestamp matching, in order to utilize additional information and increase the likelihood of correlating the correct packets. Akl, ¶82.

While Paxton discloses that a first-in-first-out ("FIFO") routine for matching timestamps is an "approach [that] can be leveraged" in order to match hashes with respect to their timestamps, Paxton leaves to the POSITA exact implementation details and preferences for matching packets based on times. Ex. 1004, ¶¶21-22. For example, while Paxton discloses matching packets based on hashes, Paxton does not disclose a preference for where or how to begin searching for a matching hash. As Ivershen teaches that a search for matching timestamps should be within a few milliseconds of the timestamp to be matched, a POSITA would have been motivated to implement Ivershen's matching functions to provide both a determinable starting point to match packets as well as an increased likelihood of matching the correct packets, as Ivershen's functions account for timestamp drift and packet travel time. A POSITA would have recognized that narrowing the field of comparisons to be made increases the overall speed of correlating. Ex. 1005, 7:36-39, 8:4-10. In situations where multiple potential matching hashes and timestamps exist, Paxton's FIFO approach may still be used toward making a final correlation determination. A POSITA would have recognized that there exist many such approaches and packet characteristics at their disposal to resolve ambiguities between potential correlation matches. Ex. 1016, 9:25-10:11. The search for matching packets having similar timestamps, as taught by Ivershen,

serves to increase the likelihood of a unique and correct correlation result. Ex. 1009, ¶¶21-26, 37. Akl, ¶83.

The application of known techniques (e.g., Ivershen's correlation via comparison of packet timestamps, durations, ports, network-interface identifiers, etc.) to improve similar devices (e.g., Paxton's and Ivershen's correlation systems) to provide predictable results in the same way (e.g., to provide additional packet information in order to make accurate correlations) would have been obvious to a POSITA. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 415-17 (2007).

A POSITA would have had a reasonable expectation of success using the various packet information taught by Ivershen, in Paxton's system. Paxton's system already maintains a database of hash values, timestamps, and IP addresses, and other header data for correlation. Ex. 1004, ¶¶17, 20. The inclusion of other logged packet information, and the processing of such information, involves little more than the same data processing techniques existing in Paxton (e.g., saving and recalling information, comparing values, etc.), which would have been obvious and well within the skill of a POSITA. Akl, ¶84.

3. Claim Chart[6]

’573 Patent	Paxton, Sutton, Deschenes, Ivershen
[3] The method of claim 1, wherein correlating the plurality of encrypted packets transmitted by the network device with the plurality of packets received by the network device comprises: comparing **[11]** The computing device of claim 9, wherein the instructions, when executed by the at least one processor, cause the computing device to correlate the plurality of encrypted packets transmitted by the network device with the plurality of packets received by the network device	**Paxton** does not explicitly disclose the correlating based on **comparing ports indicated by the first and second plurality of log entries corresponding to the packets received and transmitted by the network device**. • *See* Paxton ¶¶4-5. As discussed in §IX.C.2 above, it would have been obvious for a POSITA to correlate received and transmitted packets by **comparing ports indicated by the first and second plurality of log entries corresponding to the packets received and transmitted by the network device**. **Ivershen** teaches this correlation of packets by comparing port information of portions of received and transmitted packets (e.g., using a NAT translation table to match an [address:port] of a transmission received at the interface on one side of a NAT with an [address:port] of a transmission transmitted from the interface on the opposite side of the NAT). • “Packet capture device 109 captures substantially all of the packets on interface 113, and packet capture device 110 captures substantially all of the packets on interface 114. **As discussed above, NATF/WAPG 106 modifies the address information in the data packets that is passes between networks. As a result, monitoring system 108 cannot use the source or destination address to correlate the packets on interfaces 113 and 114 since the IP addresses and ports are quite different on[] each interface for related messages.**

[6] Claims 3-6 (methods) are substantially similar to claims 11-14 (computing device) and are substantially similar to claims 19-22 (computer-readable media) apart from their preambles. Similar claims (e.g., 3, 11, and 19) have been grouped together.

’573 Patent	Paxton, Sutton, Deschenes, Ivershen
by causing the computing device to: compare **[19]** The one or more non-transitory computer-readable media of claim 17, wherein the instructions, when executed by the one or more processors of the computing system, cause the computing system to correlate the plurality of encrypted packets transmitted by the network device with the plurality of packets received by the network device by causing the computing system to: compare **[3, 11, 19]** one or more ports indicated by the first plurality of log entries corresponding to the plurality of packets received by the network device with one or more ports indicated by the second plurality of log entries	**The routing table used by NATF/WAPG 106, such as Table 1, could be used to correlate messages on interfaces 113 and 114, but this information may not be available to monitoring system 108. Even if the NAT translation table data was available, monitoring system 108 would require immediate notification of updates or changes to the translation table in order to correlate the packets on legs 113 and 114.**” (Ivershen, 5:11-26) A POSITA would have understood that correlating using the NAT translation table includes comparing ports (and IP addresses) of packets received/transmitted on interfaces 113/114 (e.g., comparing a first packet identified as 209.5.5.7:8080 with second packets to find the corresponding value 10.1.1.1:80), or at minimum would have found such correlation obvious because the NAT table, e.g., as shown Ivershen Table 1, distinguishes the public addresses (i.e., relating to the transmitted packets) by port numbers (e.g., 8080 vs 2525). Akl, ¶¶170-173. • “NATF/WAPG 106 uses a NAT translation table, such as Table 1 below, to determine the IP address to use on network 104 for the incoming packets in flows A and B. TABLE 1 NAT Translation Table Destination IP address/port number in incoming packets from network 105 | Corresponding destination IP address/port number on private network 104 209.5.5.7:8080 | 10.1.1.1:80 209.5.5.7:2525 | 10.2.2.2:25 As illustrated in FIG. 1, NATF/WAPG 106 modifies the source and destination address information in the packets of flows A and B. For example, in flow A, the source and destination IP address is 172.3.3.3 and 209.5.5.7, respectively, in network 105.

’573 Patent	Paxton, Sutton, Deschenes, Ivershen
corresponding to the plurality of encrypted packets transmitted by the network device.	However, in network 104, the source and destination IP address for packets in flow A are changed by NATF/WAPG 106 to 209.5.5.9 and 10.1.1.1, respectively. The port numbers for the incoming and outgoing packets at NATF/WAPG 106 are also changed.” (Ivershen, 4:19-41) Akl, ¶¶164-173, 187, 194.
[4] The method of claim 1, wherein correlating the plurality of encrypted packets transmitted by the network device with the plurality of packets received by the network device comprises: comparing **[12]** The computing device of claim 9, wherein the instructions, when executed by the at least one processor, cause the computing device to correlate the plurality of	**Paxton**, in view of **Ivershen**, discloses the **correlating** based on **comparing network-interface identifiers**[7] (e.g., ports) **of the network device indicated by the first and second plurality of log entries corresponding to the packets received and transmitted by the network device**. *See* [3]. Akl, ¶¶174-176, 188, 195.

[7] *See* Ex. 1001, 4:49-53 (network-interface identifiers include identifiers of physical or logical ports).

’573 Patent	Paxton, Sutton, Deschenes, Ivershen
encrypted packets transmitted by the network device with the plurality of packets received by the network device by causing the computing device to: compare **[20]** The one or more non-transitory computer-readable media of claim 17, wherein the instructions, when executed by the one or more processors of the computing system, cause the computing system to correlate the plurality of encrypted packets transmitted by the network device with the plurality of packets received by the network device by causing the computing system to: compare **[4, 12, 20]** one or more network-interface identifiers of the network device indicated by the first plurality of log	

’573 Patent	Paxton, Sutton, Deschenes, Ivershen
entries corresponding to the plurality of packets received by the network device with one or more network-interface identifiers of the network device indicated by the second plurality of log entries corresponding to the plurality of encrypted packets transmitted by the network device.	
[5] The method of claim 1, wherein correlating the plurality of encrypted packets transmitted by the network device with the plurality of packets received by the network device comprises: comparing **[13]** The computing device of claim 9, wherein the instructions, when executed by the at least one processor, cause the computing	**Paxton** discloses wherein **correlating the plurality of encrypted packets transmitted by the network device with the plurality of packets received by the network device comprises comparing one or more times indicated by the first plurality of log entries corresponding to the plurality of packets received by the network device with one or more times indicated by the second plurality of log entries corresponding to the plurality of encrypted packets transmitted by the network device** (each first hash data record is matched with a second hash data record, which includes determining a second hash data record closest in time, i.e., comparatively a smallest difference). • “**After a hash is observed on the outside, <u>the closest matching hash (with respect to the timestamp)</u> on the inside can be identified as the corresponding match.**” (Paxton ¶22) • “FIG. 2 is a screenshot 200 of a log that illustrates a matching payload…. The two hashes, preceded by the MD5 label, are identical in FIG. 2. **Furthermore, it is also observed that <u>the time in</u>**

’573 Patent	Paxton, Sutton, Deschenes, Ivershen
device to correlate the plurality of encrypted packets transmitted by the network device with the plurality of packets received by the network device by causing the computing device to: compare **[21]** The one or more non-transitory computer-readable media of claim 17, wherein the instructions, when executed by the one or more processors of the computing system, cause the computing system to correlate the plurality of encrypted packets transmitted by the network device with the plurality of packets received by the network device by causing the computing system to: compare **[5, 13, 21]** one or more times indicated by the first	**TimeSecs (seconds) are equal, but the time in TimeMSecs (milliseconds) differ by 814 milliseconds. In other words, the inside packet arrived 814 milliseconds before the outside packet, which is consistent with the inside packet sensing the packet first.**” (Paxton ¶23) As explained in §IX.C.2 above, to the extent Patent Owner argues that **Paxton** does not explicitly disclose comparing times, a POSITA would have been motivated to perform correlation in **Paxton’s** system by determining differences between packet receipt times and packet transmission times, or between flow start times of received and transmitted packets, as taught by **Ivershen**. **Ivershen** discloses **correlating packets** including **comparing times** (e.g., determining whether two timestamps are within a few milliseconds of each other; determining whether two timestamps are within a close time window to another timestamp; determining matching flow durations) **between packets received by the network device and packets transmitted by the network device** (e.g., times of a first-side packet in relation to a NAT and times of a second-side packet in relation to a NAT). • “Using a known checksum key from a packet on the first side of the NAT firewall, the checksum keys for all packets with a timestamp within a specified time on the second side of the NAT firewall can be analyzed. For example, **to account for packet transit time, firewall delay and clock errors, the checksum keys for all packets on the second side of the NAT firewall having a timestamp within milliseconds of the first-side packet are analyzed**.” (Ivershen, 2:43-51) • “**Monitoring system 108 can then pull together two or more legs of the session on demand.**

’573 Patent	Paxton, Sutton, Deschenes, Ivershen
plurality of log entries corresponding to the plurality of packets received by the network device with one or more times indicated by the second plurality of log entries corresponding to the plurality of encrypted packets transmitted by the network device.	**Starting with a first one of the legs,** such as the session flow and CHKEY created by probe 109 on interface 113, **the other probe 110 is queried with the** CHKEY, **flow starting timestamp**, and L7 protocol **from the first leg of the flow. The second probe 110, searches for a session that matches these parameters. The search on the second probe should look for a flow start timestamp that is within a few milliseconds of the beginning of the flow on the first probe. This allows for timestamp drift among the probes and network travel time across interfaces 113,114 and NATF/WAPG 106. If a match is found, two session flows are successfully correlated together into a single call record.** [¶] If more than one match is found, then false positives can be identified and discarded by comparing other properties of the flow, such as, for example, the **closest flow duration** or an exact HTTP URI match.” (Iversheh, 5:62-6:11) • “In step 405, the checksum key for an IP flow on the first side of the NAT firewall is compared to the checksum keys for flows on the second side of the NAT firewall. **The flows that are used for comparison on the second side may be limited by using only flows or packets occurring within a time window that is close to or similar to the timestamp of the first-side packet.**” (Iversheh, 8:4-10) Akl, ¶¶177-182, 189, 196.
[6pre] The method of claim 1 wherein: **[14pre]**	*See* discussions of claims 1, 9, and 21 in §IX.A above. Akl, ¶¶184, 191, 198.

’573 Patent	Paxton, Sutton, Deschenes, Ivershen
The computing device of claim 9, wherein: **[22pre]** The one or more non-transitory computer-readable media of claim 21, wherein:	
[6a, 14a, 22a] the first plurality of log entries corresponding to the plurality of packets received by the network device **[6a, 22a:** comprises**]** **[14a:** comprise**]** **[6a, 14a, 22a]** a plurality of timestamps indicating times corresponding to receipt, by the network device, of the plurality of packets received by the network device;	**Paxton** discloses wherein the first plurality of log entries corresponding to the plurality of packets received by the network device comprises a plurality of timestamps indicating times corresponding to receipt (timestamp of when the payload was sensed),[8] by the network device, of the plurality of packets received by the network device. *See* [1b] in §IX.A.6, [5]. Akl, ¶¶184, 191, 198.
[6b, 14b, 22b] the second plurality of log entries	**Paxton** discloses the second plurality of log entries corresponding to the plurality of encrypted packets transmitted by the network device comprises a plurality

[8] *See* Ex. 1001, 4:60-67 (receipt times include, e.g., a time when the packet is received, identified, logged, or the like).

’573 Patent	Paxton, Sutton, Deschenes, Ivershen
corresponding to the plurality of encrypted packets transmitted by the network device comprises a plurality of timestamps indicating times corresponding to transmission, by the network device, of the plurality of encrypted packets transmitted by the network device; and	of timestamps indicating times corresponding to transmission (timestamp of when it was sensed),[9] by the network device, of the plurality of encrypted packets transmitted by the network device. *See* [1d] in §IX.A.6, [5]. Akl, ¶¶185, 192, 199.
[6c: correlating**]** **[14c:** the instructions, when executed by the at least one processor, cause the computing device to correlate**]** **[22c:** the instructions, when executed by the one or more processors of the computing system, cause the computing system to correlate**]** **[6c, 14c, 22c]** the plurality of encrypted packets	**Paxton** discloses that **correlating the plurality of encrypted packets transmitted by the network device with the plurality of packets received by the network device comprises comparing one or more times indicated by the plurality of timestamps indicating times corresponding to receipt with one or more times indicated by the plurality of timestamps indicating times corresponding to transmission** (e.g., correlating by comparing the timestamps to determine whether two timestamps are within a few milliseconds of each other; determine whether timestamps are within a close time window). *See* [1e] in §IX.A.6, [5]. Akl, ¶¶186, 193, 200.

[9] *See* Ex. 1001, 6:50-57 (transmission times include, e.g., a time when the packet is transmitted, identified, logged, or the like).

’573 Patent	Paxton, Sutton, Deschenes, Ivershen
transmitted by the network device with the plurality of packets received by the network device **[6c:** comprises comparing**]** **[14c:** by causing the computing device to compare**]** **[22c:** by causing the computing system to compare**]** **[6c, 14c, 22c]** one or more times indicated by the plurality of timestamps indicating times corresponding to receipt with one or more times indicated by the plurality of timestamps indicating times corresponding to transmission.	

X. SECONDARY CONSIDERATIONS

Petitioner is unaware of any secondary considerations relevant to the Challenged Claims. Akl, ¶202.

XI. CONCLUSION

Substantial, new, and noncumulative technical teachings have been presented for each Challenged Claim, which are disclosed and/or rendered obvious for the reasons set forth above. There is a reasonable likelihood that Petitioner will prevail as to each of these Challenged Claims. *Inter partes* review of claims 1-24 of the ’573 patent is accordingly requested.

Respectfully submitted,

Dated: July 20, 2021

By: /Scott A. McKeown/
Scott A. McKeown
Registration No. 42,866

Counsel for Petitioner Palo Alto Networks, Inc.

CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. § 42.24(a) and (d), the undersigned hereby certify that the Petition For *Inter Partes* Review complies with the type-volume limitation of 37 C.F.R. § 42.24(a)(i) because, exclusive of the exempted portions, it contains 13,990 words as counted by the word processing program used to prepare the paper.

Dated: July 20, 2021

By: /Scott A. McKeown/
Scott A. McKeown
Registration No. 42,866

CERTIFICATE OF SERVICE

The undersigned certifies service pursuant to 37 C.F.R. §§ 42.6(e) and 42.105(b) on the Patent Owner by Priority Mail Express of a copy of this Petition for Inter Partes Review and supporting materials at the correspondence address of record for the ’573 patent:

BANNER & WITCOFF, LTD.
1100 13th STREET N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

Dated: July 20, 2021

By: /Scott A. McKeown/
Scott A. McKeown
Registration No. 42,866