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 IPR2022-00182
Patent No. 9,917,856

PETITION FOR *INTER PARTES* REVIEW

TABLE OF CONTENTS

LIST OF EXHIBITS

EX1001	U.S. Patent No. 9,917,856 ("'856")
EX1002	File History of U.S. Patent No. 9,917,856 ("'856 FH")
EX1003	Declaration of Dr. Jon Weissman in Support of *Inter Partes* Review of U.S. Patent No. 9,917,856 ("Weissman")
EX1004	U.S. Patent No. 9,680,795 ("Buruganahalli")
EX1005	U.S. Patent No. 5,878,231 ("Baehr")
EX1006	*Reserved*
EX1007	Barry M. Leiner et al., "A Brief History of the Internet," Internet Society, 1997, available at: https://www.internetsociety.org/internet/history-internet/brief-historyinternet/ ("Leiner")
EX1008	U.S. Pat. No. 7,032,031 ("Jungck '06")
EX1009	E. H. Spafford, "The Internet Worm Program: An Analysis," Purdue Technical Report CSD-TR-823, 1988. ("Spafford")
EX1010	Eichin, M.W. and Rochlis, J.A., "With Microscope and Tweezers: The Worm from MIT's Perspective," Communications of the ACM, Volume 32 Number 6, June 1989 ("Eichin")
EX1011	T. Eisenberg et al., "The Cornell Commission: On Morris and the Worm," Communications of the ACM, Volume 32 Number 6, June 1989 ("Eisenberg")
EX1012	J. C. Mogul, "Simple and Flexible Datagram Access Controls for Unixbased Gateways," Digital Western Research Laboratory Technical Report No. 89/4, 1989 ("Mogul")
EX1013	"FireWall-1 User Interface from 3.0," PhoneBoy's Security Theater, archived at the Internet Archive Wayback Machine on January 2, 2014 at https://web.archive.org/web/20140102143305/http://phoneboy.net/ ("FireWall-1")

EX1014	"SonicWALL Global Management System: Centralized Network Monitoring and Management Solution", 2008, archived at the Internet Archive Wayback Machine on December 7, 2008 at https://web.archive.org/web/20081207003303/http:/www.sonicwall.com/downloads/EC_GMS_DS_US.pdf ("SonicWALL GMS")
EX1015	"SonicWALL ViewPoint 6.0 Administrator's Guide", 2010, archived at the Internet Archive Wayback Machine on August 21, 2010 at https://web.archive.org/web/20100821022839/http://www.sonicwall.com:80/downloads/SonicWALL_ViewPoint_6_0_Admin_Guide.pdf ("SonicWALL ViewPoint")
EX1016	Heberlein, L. T.L, et al., "A Network Security Monitor," Proceedings, 1990 IEEE Computer Society Symposium on Security and Privacy, 1990 ("Heberlein")
EX1017	"NetRanger Network Security Management System User Guide". v1.3.1 Wheelgroup Corporation, 1997 ("NetRanger")
EX1018	Roesch, M., "Snort: Lightweight Intrusion Detection for Networks," Lisa (Vol. 99, No. 1, pp. 229-238), 1999 ("Roesch")
EX1019	U.S. Pat. No. 8,370,936 ("Zuk")
EX1020	W32.hllw.Doomjuice Technical Description, Symantec Security Center, updated February 13, 2007, available at: https://www.symantec.com/security-center/writeup/2004-020909-2916-99 ("Doomjuice")
EX1021	"(Vendor Issues Fix) Re: Helix Universal Server and RealServer URL Parsing Flaw in View Source Plug-in Lets Remote Users Execute Arbitrary Code with Root Privileges" Security Tracker, September 13, 2003, available at: https://securitytracker.com/id/1007692 ("Helix")
EX1022	"Transmission Control Protocol," IETF RFC 793. J. Postel, ed., September 1981, archived at Internet Archive Wayback Machine on February 2, 2007 at

	https://web.archive.org/web/20070202201546/https://tools.ietf.org/html/rfc793 ("RFC 793")
EX1023	"Internet Protocol," IETF RFC 791, J. Postel, ed., September 1981, archived at Internet Archive Wayback Machine on February 4, 2007 at https://web.archive.org/web/20070204151303/https://tools.ietf.org/html/rfc791
EX1024	"File Transfer Protocol," IETF RFC 765, J. Postel, ed., June 1980, archived at Internet Archive Wayback Machine on February 6, 2007 at https://web.archive.org/web/20070206005843/https://tools.ietf.org/html/rfc765 ("RFC 765")
EX1025	T. B. Lee, "The Original HTTP as defined in 1991," World Wide Web Consortium, 1991, archived at Internet Archive Wayback Machine on June 5, 1997 at https://web.archive.org/web/19970605071155/https://www.w3.org/Protocols/HTTP/AsImplemented.html ("T.B. Lee")
EX1026	C*isco System Inc. v. Centripetal Networks, Inc.*, IPR2018-01760, Paper 41 (PTAB May 18, 2020)
EX1027	*Centripetal Networks, Inc. v. Cisco Systems, Inc.*, Case No. 2:18-cv- 00094 (E.D. Va.), Dkt. No. 621 (Opinion and Order Regarding Findings of Fact and Conclusions of Law)
EX1028	*Centripetal Networks, Inc. v. Cisco Systems, Inc.*, Case 2021-1888 (Fed. Cir.), Dkt. No. 18 (Non-Confidential Brief for Defendant-Appellant Cisco Systems, Inc.)
EX1029	*Centripetal Networks, Inc. v. Cisco Systems, Inc.*, Case No. 2:18-cv-00094 (E.D. Va.), Dkt. No. 548 (June 10, 2020 Trial Transcript)
EX1030	*Centripetal Networks, Inc. v. Keysight Techs., Inc.*, Case No. 2:17-cv-383 (E.D. Va.), Dkt No. 484 ("Keysight Markman")
EX1031	S. Turner & C. Polk, "Prohibiting Secure Sockets Layer (SSL) Version 2.0," IETF RFC 6176, March 2011, archived at Internet Archive Wayback Machine on March 18, 2011 at

	https://web.archive.org/web/20110318184421/https://tools.ietf.org/html/rfc6176 ("Turner")
EX1032	I. Ristic, "SSL/TLS and PKI History," April 2018, available from https://www.feistyduck.com/ssl-tls-and-pki-history/ ("Ristic")
EX1033	U.S. Pat. Appl. Pub. No. 2007/0271605 ("Le Pennec")
EX1034	U.S. Patent No. 8,504,822 ("Wang")
EX1035	U.S. Patent No. 7,793,342 ("Ebrahimi")
EX1036	J. Wack et al., *Guidelines on Firewalls and Firewall Policy*, National Institute of Standards and Technology ("NIST")
EX1037	U.S. Patent No. 8,813,228 ("Magee")
EX1038	*Reserved*
EX1039	*Reserved*
EX1040	U.S. Patent Appl. Pub. No. 2014/0283004 ("Moore")
EX1041	U.S. Patent Appl. Pub. No. 2015/0207809 ("Macaulay")
EX1042	U.S. Patent Appl. Pub. No. 2014/0089661 ("Mahadik"**)**
EX1043	U.S. Patent No. 7,849,502 ("Bloch")
EX1044	U.S. Patent No. 7,584,352 ("Boivie")
EX1045	Young-Ho Kim, et al., *Design of Firewall in Router using Network Processor*, IEEE (Jul. 11, 2005) ("Kim")
EX1046	Declaration of Jonathan Bradford

I. INTRODUCTION

Petitioner Palo Alto Networks, Inc. ("Petitioner") respectfully requests *inter partes* review ("IPR") of Claims 1 and 24-25 ("Challenged Claims") of U.S. Patent No. 9,917,856 ("'856") (EX1001) in accordance with §§311-319 and §42.100 et seq.[1]

The '856 patent is directed to determining that packets comprising encrypted data correspond to a network threat. '856, Abstract, 1:7-20. In operation, a packet-filtering system determines that packets with unencrypted data correspond to a network-threat indicator (*e.g.*, a malicious IP address), further determines that packets with encrypted data also correspond to that network-threat indicator based on their association with the unencrypted packets, and then filters both categories of packets based on criteria specified by packet-filtering rules, as partially illustrated by Figure 7. '856, 1:31-45, 23:63-24:30. Weissman (EX1003), ¶¶77-78.

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

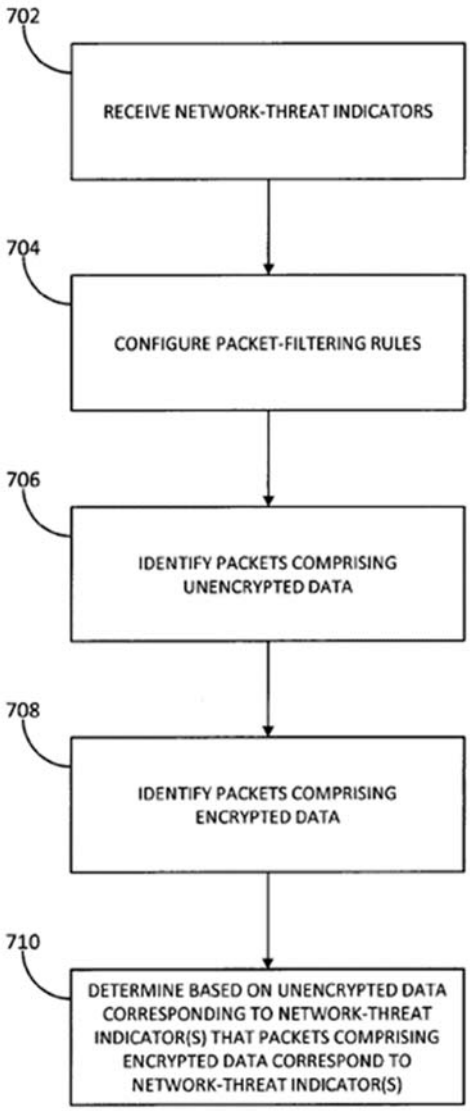


FIG. 7

The ’856 patent acknowledges that utilizing “network-threat indicators” to identify network threats was well-known. ’856, 1:12-16. The Challenged Claims utilize them for this known purpose in a rule-based packet-filtering system. The indicators are used to identify threatening packets that are to be filtered and routed to a proxy system for additional processing, and to configure the rules by which

those packets are filtered. Filtering threatening packets and routing them to a proxy system, and configuring packet-filtering rules to specify packet filtering criteria (*e.g.*, a malicious Internet Protocol (IP) address or Uniform Resource Locator (URL)) for these purposes, were also well-known. Weissman, ¶¶31-76.

The Challenged Claims apply the same known techniques to network communications that include packets with encrypted data, relying on packets with unencrypted data to determine threats, and correlating the encrypted packets with the unencrypted packets that correspond to the threats. Determining that encrypted packets pose a threat based on their association with unencrypted packets relating to that threat was also well-known before the priority date of the '856 patent. Weissman, ¶¶64-67.

During prosecution, Patent Owner contended that the prior art failed to disclose network threat indicators and determining that encrypted packets relate to a threat based on unencrypted data. EX1002, 1351-1367. But each limitation argued during prosecution as distinguishing over the art is demonstrated herein as known, and in combination as claimed. *See* §V.B. Weissman, ¶81.

For example, **Buruganahalli** describes a packet-filtering system that determines that packets with unencrypted data correspond to a network-threat indicator, further determines that packets with encrypted data also correspond to that network-threat indicator based on their association with the unencrypted packets,

and then filters both categories of packets based on criteria specified by packet-filtering rules. The system determines that a secure client-server session comprises encrypted data corresponding to a blacklist. The system does so by first (a) determining that unencrypted data (*e.g.*, a destination domain) in a transport layer security (TLS) request packet, which initiates the secure session, corresponds to a blacklist, and (b) as a result determines that encrypted data in that same session corresponds to the blacklist. The system filters unencrypted and encrypted packets of that session based on criteria specified by one or more rules, and may split the filtered session into two half sessions, with a decryption engine providing an intermediary interface between the client and server to decrypt and monitor filtered packets containing encrypted data between the half sessions in accordance with the rules. *See* §IX.A. **Baehr** discloses a packet screening system that routes filtered packets to a proxy that is configured as a separate logical or physical entity from the packet filtering device. *See* §IX.B. Weissman, ¶¶89-95, 151-154.

As explained in greater detail herein, all the features of the Challenged Claims would have been obvious before the earliest priority date of the ’856 patent. Petitioner requests that the Board institute trial and find the Challenged Claims unpatentable. Weissman, ¶¶13-19, 161-166.

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

A. Real Party-In-Interest

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

B. Related Matters

The Challenged Claims were the subject of the following litigations that did not involve or relate to Petitioner:

- *Centripetal Networks, Inc. v. Keysight Technologies, Inc. et al*, No. 2-17-cv-00383 (E.D. Va. Filed July 20, 2017) (settled) ("Keysight suit");
- *Centripetal Networks, Inc. v. Cisco Systems, Inc.*, EDVA-2-18-cv-00094 (E.D. Va. Filed Feb. 13, 2018) ("Cisco suit") (claim 1 dropped before trial).

The Cisco suit is currently on appeal to the Federal Circuit: *Centripetal Networks, Inc. v. Cisco Systems, Inc.*, Case 21-1888 (Fed. Cir., filed April 27, 2021). Petitioner was not and is not a party to the Cisco suit or Keysight suit, had and has no control over any aspect of the Cisco suit or Keysight suit, and had and has no relation to either Cisco or Keysight with respect to those suits. Likewise, neither Cisco nor Keysight had or has any involvement in or input into this petition or proceeding.

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	Mark D. Rowland Reg. No. 32,077 James Batchelder (*pro hac vice* forthcoming) Andrew Radsch (*pro hac vice* forthcoming) Keyna Chow (*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 keyna.chow@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 §42.15(a) and any additional fees to Deposit Account No. 18-1945, under Order No. 115271-0003-666. Any additional fees are also authorized.

IV. REQUIREMENTS FOR INTER PARTES REVIEW

A. Grounds for Standing

Pursuant to §42.104(a), Petitioner certifies that the '856 patent is available for IPR and that Petitioner is not barred or estopped from requesting IPR challenging the claims of the '856 patent on the requested grounds.

B. Identification of Challenge

Pursuant to §§42.104(b) and (b)(1), Petitioner requests IPR of the Challenged Claims and that the Board cancel the same as unpatentable. The '856 patent matured from U.S. Application 14/757,638 (filed 12/23/2015). Petitioner assumes that the priority date of the '856 is 12/23/2015.[2]

1. The Specific Art on Which the Challenge is Based

Petitioner relies upon the following prior art:

Name	Exhibit	Filing Date	Issued Date	Prior art under at least[3]
Buruganahalli	EX1004	6/5/2013[4]	6/13/2017	§102(a)(2)
Baehr	EX1005	2/4/1997	3/2/1999	§102(a)(1)-(2)

[2] Petitioner takes no position on the '856 patent's priority date and assumes, for the purposes of this IPR, that the priority date is 12/23/2015.
[3] The '856 patent was filed 12/23/2015, so it is being analyzed under AIA law, and all applicable citations to statutes are to AIA versions.
[4] Buruganahalli is a continuation of an application filed on Jul. 25, 2013 and claims priority to a provisional application filed on Jun. 5, 2013.

2. Statutory Grounds on Which the Challenge is Based

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

Ground	Basis	Claim(s)	Prior Art
1	§103	1, 24-25	Buruganahalli
2	§103	1, 24-25	Buruganahalli in view of Baehr

Explanations pursuant to §42.204(b)(4)-(5) are provided in §IX-X, demonstrating that the Petitioner has at least a reasonable likelihood of prevailing on these grounds, and identifying where each element of each claim is found in the prior art.

This Petition is supported by the Declaration of Dr. Jon Weissman (EX1003) ("Weissman").

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

A. §314(a) Discretion Does Not Apply

To the extent that Patent Owner argues that the Cisco suit is relevant here, that suit is irrelevant to the Board's discretion under §314(a) because Petitioner is not a party to the Cisco suit; Petitioner neither has nor had any input or relation to that suit; trial has already concluded in the Cisco suit; and the Cisco suit did not address the same or substantially similar issues as those raised in this petition (*i.e.*, validity

based on **Buruganahalli** alone or in view of **Baehr**). EX1027, 57-67. Nor are any invalidity issues raised in the pending appeal of the Cisco suit. EX1028, 5.

B. §325(d) Discretion Does Not Apply

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 **Buruganahalli** nor **Baehr** was cited or considered in the prosecution of the ’856 patent. These prior art references address the limitations deemed missing from the prosecution prior art. For example, **Buruganahalli** discloses determining that packets with encrypted data correspond to a network-threat indicator based on unencrypted data corresponding to that network-threat indicator—which Applicant argued to be missing in prior art. EX1002, 1365; *see generally* §VI.B, §IX. Specifically, Applicant argued that the cited reference (Spies) taught filtering only “a scanned and unencrypted version of a message” and performing “processing operations such as virus scanning, spam filtering, notifications, archiving, or security policy enforcement” on the decrypted message. EX1002, 1365. Applicant concluded that Spies “does not discuss any determination regarding any encrypted data based on any unencrypted data corresponding to one or more network-threat indicators.” *Id.* Here, **Buruganahalli** discloses a packet-filtering system that determines that packets with unencrypted data (*e.g.*, in a session-initiating

handshake message) correspond to a network-threat indicator, and further determines that subsequent packets with encrypted data also correspond to that network-threat indicator based on unencrypted data. *See generally* §IX. **Buruganahalli** further discloses network-threat indicators comprising a domain name that Applicant also argued to be missing in prior art. Specifically, Applicant argued that the cited reference disclosed sending messages to a particular domain but did not teach that the domain is a network-threat indicator. EX1002, 1365. Here, **Buruganahalli** teaches including destination domains on a blacklist where they pose a risk to network security. *See generally* §IX. Additionally, the Office has not previously considered the expert testimony submitted herewith regarding the teachings of **Buruganahalli**, **Baehr**, or a combination thereof.

Accordingly, the "same or substantially the same art or arguments" were not previously presented to the Office during prosecution. *Thorne Research v. Trustees of Dartmouth College*, IPR2021-00491, Pap. 18, *8-9 (PTAB Aug. 12, 2021) (granting institution; finding first prong of *Advanced Bionics* not satisfied when prior art reference considered by Examiner was combined with references not cited during prosecution); *Advanced Bionics, LLC v. Med-El Elektromedizinische Gerate GMBH*, IPR2019-01469, Pap. 6, *8-9.

VI. BACKGROUND

A. The ’856 Patent

The ’856 patent, entitled “Rule-Based Network-Threat Detection for Encrypted Communications,” describes a “packet-filtering system” configured to use packet-filtering rules, identify packets containing unencrypted data and packets containing encrypted data, and use the unencrypted data to determine that the packets comprising encrypted data correspond to one or more network-threat indicators. ’856, *Title, Abstract*, 1:32-45. Such rule-based detection is illustrated in a flow chart diagram in Figure 7. Weissman, ¶77.

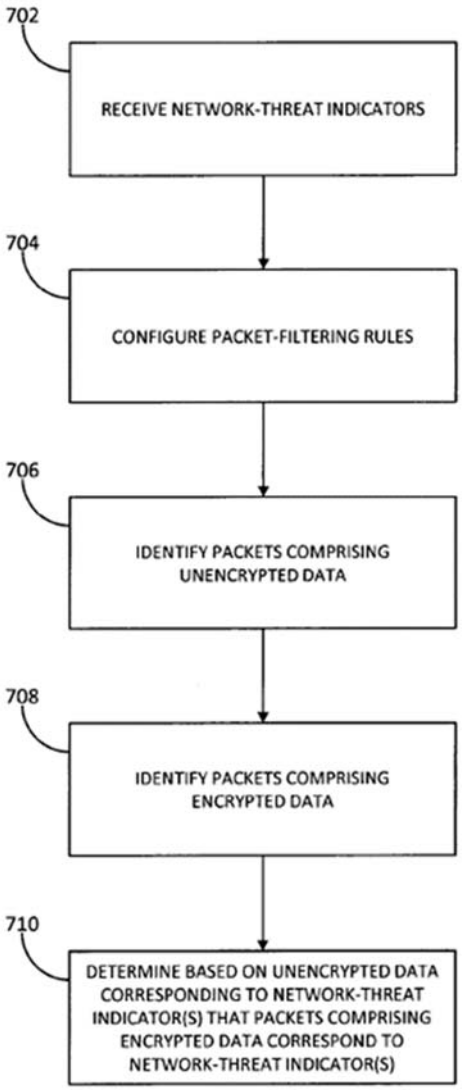


FIG. 7

'856, 23:63-65. In step 702, the packet-filtering system "may receive data indicating network-threat indicators," *e.g.*, "network addresses, domain names, uniform resource identifiers (URIs), and the like." '856, 1:11-15. 3:67-4:3. The data may be in the form of rules provided by "rule provide[rs] 138 based on network-threat indicators provided by threat-intelligence providers 140." '856, 23:66-24:4, 4:3-7.

The packet-filtering system may then configure rules to identify packets corresponding to the network-threat indicators received in step 704. '856, 24:4-7, 4:3-7, 4:18-21. Weissman, ¶77.

In step 706, the system identifies packets comprising unencrypted data, *e.g.*, "a DNS query, a reply to a DNS query, or a handshake message configured to establish an encrypted communication session." '856, 24:8-12, 9:19-28. In step 708, the system identifies packets comprising encrypted data, such as those encrypted in accordance with parameters of encrypted communication sessions. '856, 24:14-17, 6:42-45. In step 710, the system determines "based on a portion of the unencrypted data corresponding to the network-threat indicators that the packets comprising encrypted data correspond to the network-threat indicators." '856, 24:18-21. For example, the system may determine that "packets comprise data corresponding to the network-threat indicators based on data included in the one or more handshake messages configured to establish session," and that the packets encrypted in the session correlate to the handshake messages. '856, 9:29-33, 24:18-30. Based on a determination that the packets comprise data corresponding to one or more of the network-threat indicators, filtered packets are routed to a proxy system. '856, 6:45-59. The proxy system may decrypt encrypted data, and the filter system may thereafter use unencrypted data in the packets (such as a URI, or data

indicating a protocol version, request or command) to filter the packets before the packets are re-encrypted. ’856, 10:56-11:40.Weissman, ¶¶78-79.

For example, representative Claim 1 of the ’856 patent recites:

A method comprising:

receiving, by a packet-filtering system comprising a hardware processor and a memory and configured to filter packets in accordance with a plurality of packet-filtering rules, data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprises a domain name identified as a network threat;

identifying packets comprising unencrypted data;

identifying packets comprising encrypted data;

determining, by the packet-filtering system and based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;

filtering, by the packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by the plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules:

> packets comprising the portion of the unencrypted data that corresponds to one or more network-threat indicators of the plurality of network-threat indicators; and
>
> the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and

routing, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.

B. Prosecution History

U.S. Patent Application No. 14/757,638, which matured into the '856 patent, was filed 12/23/2015. Weissman, ¶80.

During prosecution, Examiner issued a non-final rejection on 04/12/2017, rejecting the pending claims under §101 and §112, and further under §103 as obvious in view of Spies (U.S. Patent Publication 2005/0138353), Sorensen (U.S. Patent Publication 2012/0023576), and in further view of Bomer (U.S. Patent Publication 2004/0199629). EX1002, 1064-1083. On 10/11/2017, Applicant amended the claims and argued that Spies failed to teach the determining step of claim 1. EX1002, 1365. Specifically, Applicant argued that Spies taught filtering "applied to a scanned and unencrypted version of a message," and performing "additional processing operations such as virus scanning, spam filtering, notifications, archiving, or security policy enforcement" on the "decrypted message" such that "the resulting decrypted and processed version of the message may be provided to the recipient." *Id.* Accordingly, Applicant further argued that Spies failed to teach "any determination regarding any encrypted data based on any unencrypted data corresponding to one or more network-threat indicators." *Id.* Applicant also argued that Spies failed to teach network-threat indicators comprising a domain name, as recited in the claims. *Id.* Rather, Applicant argued that while Spies taught a domain name, that domain name was not identified as a network threat. *Id.* Applicant further

argued that neither Sorenson nor Bomer remedied the defects of Spies. EX1002, 1351-1367. Weissman, ¶81.

A Notice of Allowance was issued on 12/20/2017, indicating that the amended claims were sufficient to overcome the prior art of record. EX1002, 1374-1390. On 01/23/2018, Applicant requested additional amendments to the claims prior to issuance. EX1002, 1413-1422. On 02/05/2018, the amendment was entered. EX1002, 1450-1451. The '856 issued on 03/13/2018. EX1002, 1453. Weissman, ¶82.

VII. LEVEL OF ORDINARY SKILL IN THE ART

The level of ordinary skill in the art is evidenced by the prior art. *See In reGPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995) (determining Board did not err in adopting approach that level of skill in the art was best determined by references of record). The prior art discussed herein, and in Dr. Weissman's declaration, demonstrates that, on or before 12/23/2015, a POSITA would have had a working knowledge of packet-switched networking, firewalls, security policies, communication protocols and layers, and the use of customized rules to address cyber-attacks. A POSITA would have had a bachelor's degree in computer science, computer engineering, or an equivalent, and four years of professional experience. Lack of work experience could be remedied by additional education, and vice versa. Weissman, ¶¶1-12, 24-30.

VIII. CLAIM CONSTRUCTION

Claims subject to IPR are to be construed using the *Phillips* standard. §42.100(b); *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005). Only terms necessary to resolve the controversy need to be construed. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017). Only one term, addressed below, needs to be construed. All other terms should be accorded their plain and ordinary meaning. Weissman, ¶¶83-84.

A. "network-threat indicators"

Each Challenged Claim recites "receiv[e/ing . . .] data indicating a plurality of network-threat indicators." '856, cls. 1, 24-25. The term "network-threat indicators" should be construed to mean "indicators that represent the identity of a resource associated with a network threat." This construction is consistent with the '856 patent's specification, which provides examples of "network-threat indicators," including "network addresses, domain names, uniform resource identifiers (URIs), and the like." '856, 1:11-15, 3:65-4:4. This construction was adopted for this same term in IPRs filed against other of PO's patents in which this same claim term appears. EX1026, 8-10. Weissman, ¶¶85-87, 20-23.

IX. GROUNDS OF UNPATENTABILITY

A. Ground 1: Claims 1, 24-25 are rendered obvious by Buruganahalli

1. Overview of Buruganahalli

Buruganahalli is directed to firewall technologies that protect networks from unauthorized access while permitting authorized communications to pass through. Buruganahalli, 1:20-22. **Buruganahalli** discloses that firewalls may be implemented as a device, a set of devices, or software executed on a device that provides a firewall function for network access, and that the disclosed techniques can be implemented in numerous ways, including as a process, apparatus, computer program, and/or a processor. Buruganahalli, 1:21-31, 2:14-32, 2:48-60. A firewall may be implemented in a security device that includes other functions, such as proxy and routing functions. *Id.*, 1:36-38, 3:5-15. The routing functions may be based on source, destination, and protocol information. *Id.* Weissman, ¶89.

Buruganahalli discloses filtering packets by applying sets of rules (also referred to as policies) for security purposes. Buruganahalli, 2:61-66, 1:32-36. The rules may specify a domain (*e.g.*, destination domain), or other matching criteria or heuristics. Buruganahalli, 14:60-67, 4:23-30, 5:35-43. For example, destination domains may be listed on a "blacklist" (that is part of a security policy) such that destination domains extracted from packets would be compared against those on the blacklist. Buruganahalli, 7:39-67, 10:66-11:2. Packets of a session between a client

and a remote server associated with the domain name may then be filtered. Buruganahalli, 7:39-51, 7:60-67. The remote server hosting the domain may be identified by a URL or an IP address. Buruganahalli, 3:5-24, 5:6-23, 7:39-8:44, 9:25-28, 10:21-28, 13:52-14:1, 15:37-45. Weissman, ¶90.

For example, Figure 3A illustrates a firewall filtering packets in communications between a client and a remote server. Buruganahalli, 4:31-40. Weissman, ¶91.

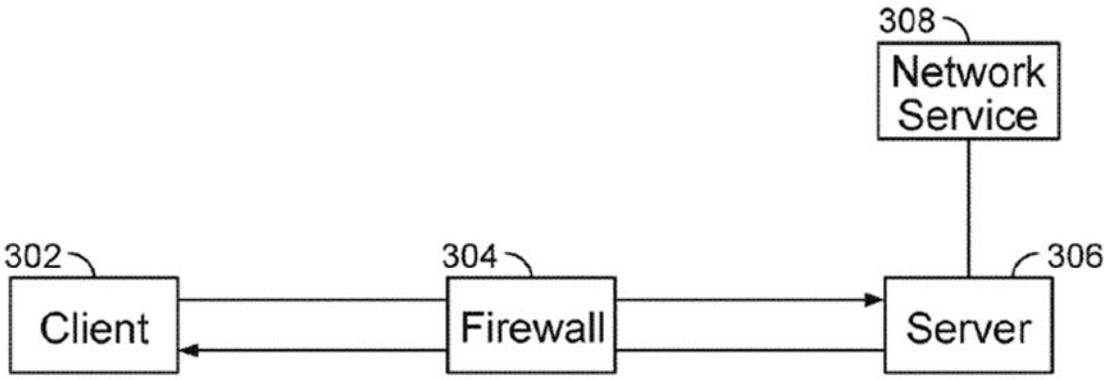


FIG. 3A

Buruganahalli discloses inspecting handshake traffic, which is an initial negotiation to set up a secure communication session between a client and a remote server. Buruganahalli, 10:54-61, 11:7-42. The firewall extracts information, such as a destination domain, from the unencrypted packets in the handshake message. Buruganahalli, 5:24-51, 7:24-25, 11:7-13. The firewall then applies rules to the extracted information, such as determining whether it corresponds to the data on a

blacklist. Buruganahalli, 5:24-36, 7:42-67, 11:7-19, 11:30-54. Based on that determination, the firewall filters the packets of the secure session. *Id.*, *Abstract*, 4:16-22, 4:31-44, 6:12-39, 6:62-7:9. For example, the firewall may intercept a client's initial request to establish an encrypted session, such as a TLS "hello" message; extract a domain name from the unencrypted request; and based on the information in the request, apply rules by which the packets, including encrypted packets, of the session between the client and the remote server are filtered. *Id.*, 15:4-21, Fig. 7. Weissman, ¶91.

Buruganahalli further discloses that a decrypt engine of the firewall is used to decrypt the encrypted packets in the secure session associated with the handshake message. Buruganahalli, 7:42-51, 7:60-67, 8:45-54, 9:61-10:9. The decryption of the encrypted packets in the secure session is handled in accordance with the description of Figure 3B, which illustrates the establishment of an SSL session between a client and a server. Buruganahalli, 9:61-10:9, 12:4-18. As shown in Figure 3B, in response to intercepting and detecting a request to establish a secure session, the firewall "effectively split[s] the SSL session between the client 312 and the remote server 316 into two half sessions shown as Session A and Session B in Fig. 3B." Buruganahalli, 12:12-18.

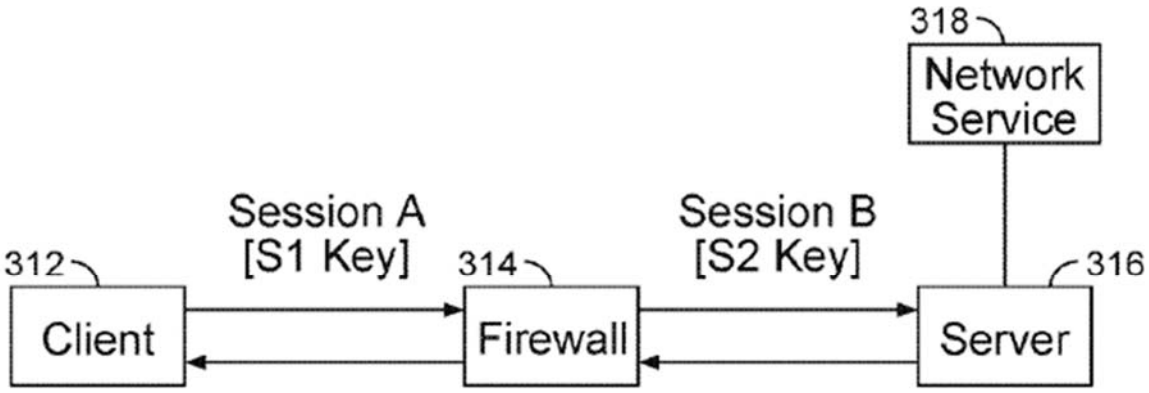


FIG. 3B

Buruganahalli explains that

> [i]n Session A, the firewall 314 acts as the remote server 316 such that it is transparent to the client 312 that it is not communicating directly with the remote server 316. Session A traffic is encrypted using the session key S1 associated with the firewall device. In Session B, the firewall 314 acts as the client 312 such that it is transparent to the remote server 316 that it is not communicating directly with the client 312. Session B traffic is encrypted using the session key S2 associated with the firewall device (*e.g.*, the firewall device can store the fingerprint from the remote server in association with that remote server IP address).

Buruganahalli, 12:14-28, 12:56-59. As a result, "any data that is communicated from the client 312 to the firewall 314 is decrypted using session key S1 and is then inspected by the firewall 314," and similarly "traffic coming from the server is decrypted with the session key S2, [and] inspected by the firewall 314." Buruganahalli, 12:29-32, 12:52-55. The firewall processes the packets in a manner "transparent" to the endpoints (*i.e.*, the client and the server) such that neither endpoint would detect the presence of the firewall applying the "trusted man-in-the-middle" decryption techniques. Weissman, ¶92.

As indicated in the preceding paragraph, **Buruganahalli** discloses that the firewall applies the "trusted man-in-the-middle" techniques "using a self-signed certificate." Buruganahalli, 9:61-67. The firewall replaces the public key in the original server certificate with its own key. The firewall then generates a new certificate (*e.g.*, "a self-signed certificate") by replacing the server certificate and signs the new certificate with its own public key (*e.g.*, "session key S1"). Buruganahalli, 5:6-23, 5:52-61, 8:25-32, 9:61-67, 12:18-36. **Buruganahalli** further discloses that such techniques may be used in addition to and/or in combination with various techniques described for destination extraction for secure protocols. Buruganahalli, 11:61-12:3. Weissman, ¶93.

In other words, **Buruganahalli** describes a system in which a firewall intercepts packets sent from (and to) a client, inspects the packets, and, in accordance

with one or more rules implementing a blacklist, identifies a request (as part of a session-initiating handshake) from the client to establish a secure session with a destination domain. Buruganahalli, 12:4-55, 7:39-67. In accordance with those one or more rules, the firewall filters the unencrypted packets establishing the session, as well as the subsequent encrypted packets of the secure session, for handling in accordance with the techniques described in relation to Figure 3B. Buruganahalli, 12:4-55. The firewall determines that the encrypted packets are part of the session established by the client request, from unencrypted information, such as IP addresses in the packets. *Id.* at 9:25-28. Weissman, ¶94.

As described in connection with Figure 3B, the firewall passes the client's secure session request to the server. Buruganahalli, 12:4-55. When the server responds, the firewall intercepts the response, decodes it, and filters it because it is determined to be a response to the request. *Id.* In particular, the firewall extracts from the response a key (*e.g.*, S2 key) that was provided by the server. *Id.* The firewall substitutes its own key (*e.g.*, S1 key) and passes the response, with the substituted key, back to the client. *Id.* As a result, the original session effectively is split into two half sessions. *Id.* In one of the two half sessions (*i.e.*, Session A), the client encrypts packets using the substituted key (S1 key), and the firewall filters and then decrypts the encrypted packets from the client (having identified those packets as being part of the secure session) using that key. *Id.* In the second of the two half

sessions (*i.e.*, Session B), the firewall re-encrypts the same information using the server's key (S2 key), and sends the encrypted packets to the server. *Id.* at 12:4-55. A similar filtering and decryption/re-encryption process happens in reverse when information is sent from the server back to the client. *Id.* Weissman, ¶95.

As would be appreciated, the intermediary interface for the session decryption and encryption is described as "transparent" to the endpoints (*i.e.*, the client and server), and as such functions as a proxy, and more specifically, a "transparent" proxy, as was known in the art. *See, e.g.*, Wang, 8:12-19 ("In particular, because the proxy device 120 is a transparent intermediary to the client-server security session, the proxy device is able to decrypt the received traffic/packets (*e.g.*, using the session key negotiated for the client-proxy or proxy-server session, as appropriate) from each sending end device, and may re-encrypt the traffic prior to forwarding it on using the respective session key with the receiving end device."); Ebrahimi, 1:48-52 ("[A] transparent proxy is neither known to nor configured by the clients; rather, the transparent proxy intercepts outgoing client requests to access origin servers/sites and transparently processes the requests on behalf of the clients."); NIST, 14. Proxies were known to operate in a manner that is invisible to an outsider, just as described in connection with Figure 3B of **Buruganahalli**. *See, e.g.*, Baehr, 4:50-63, 8:36-47, 8:65-9:7. Accordingly, although the description of Fig. 3B in **Buruganahalli** does not explicitly refer to implementing its decryption and

encryption functionality as a proxy, a POSITA would have recognized the intermediary nature of that functionality (*i.e.*, implemented in a firewall that is in line between the client and the server), and that functionality's transparent operation relative to communicating endpoints, as a proxy. Buruganahalli, 3:5-8 (stating that security devices were known to include both firewall and proxy functions); NIST 52 ("A proxy agent is a software application running on a firewall or on a dedicated proxy server . . . ."). Weissman, ¶96.

Likewise, although **Buruganahalli** does not explicitly disclose "routing" to a proxy system encrypted packets of a secure session directed to a blacklisted domain (after they have been filtered as being part of the secure session established by the initial client request), a POSITA would have understood that the filtered encrypted packets (*i.e.*, packets identified as being part of the secure session) are "routed" to **Buruganahalli**'s decrypt engine. As discussed above, a POSITA would have understood that decrypt engine to be used in implementing a proxy. **Buruganahalli** discloses that the packets corresponding to a blacklist would be decrypted, and the function of a decrypt engine is for decryption. Buruganahalli, 7:39-51, 9:61-67. Further, as **Buruganahalli** explains, a proxy is a well-known component of a security device, and a POSITA would have understood that transmitting packets between interfaces of functional components of a security device such as a firewall, using a software routing function, was also well-known. Buruganahalli, 3:5-15;

NIST, 12 ("Application-proxy gateway firewalls do not require a Layer 3 (Network Layer) route between inside and outside interfaces of the firewall; the firewall software performs the routing"), 51 ("A firewall ruleset is a table of instructions that the firewall uses for determining how packets should be routed between its interfaces."), 52 ("A proxy agent is a software application running on a firewall or on a dedicated proxy server that is capable of filtering a protocol and routing it [*sic*] between the interfaces of the device."). Weissman, ¶97.

Alternatively, at minimum, it would have been obvious to a POSITA to route the filtered packets in **Buruganahalli** to a proxy, as proxies were known, routine components of firewalls and other network security devices. Buruganahalli, 3:5-15. Further, proxies were known to be used for SSL/TLS decryption. *See, e.g.*, Wang, 8:6-27, 3:44-57, 4:21-28, 9:30-35. It was also known to route filtered packets to a proxy implemented internally to, or implemented externally from, the packet filtering device. *See, e.g.*, NIST, 12-14; Baehr, 2:25-30, 5:2-8, 8:12-18, Figs. 6-7; Wang, Fig. 1, 2:32-58; Le Pennec, Fig. 3, [0021]-[0023]. Weissman, ¶98.

A POSITA would have been motivated to route filtered packets to a proxy system in implementing the split session disclosed by **Buruganahalli** for security purposes. A purpose of a proxy is to isolate potentially dangerous traffic for separate inspection, filtering, logging and/or virus detection. *See, e.g.*, NIST, 14 (describing dedicated proxy servers as providing filtering, logging and virus detection). A proxy

can perform this important security function of isolating the protected network without altering the network. Baehr, 2:38-42, 8:13-17, 8:37-47; Wang, 7:53-57, 8:12-21, 8:67-9:4 (no special client/server provisioning required, and decryption and inspection is isolated to the proxy device). Weissman, ¶99.

A POSITA would be further motivated to perform the session splitting operation by routing filtered packets to a proxy system to improve performance. Decryption and encryption are computationally intensive processing tasks, and can be optimized by being handled by dedicated proxy servers. Indeed, **Buruganahalli** recognizes the need for "workload balancing of network related resources." Buruganahalli, 3:5-15. **Buruganahalli** further discloses using "special purpose hardware" to implement firewalls "as dedicated appliances" that would "generally provide higher performance levels for application inspection than software executed on general purpose hardware." Buruganahalli, 4:7-15. **Buruganahalli** also discloses implementing firewalls as a set of devices. 1:22-25. Further, it was known that dedicated proxy servers were used to decrease the work load of a firewall. NIST, 14. A POSITA therefore would have been motivated to use dedicated proxy servers for session splitting to reduce load on a firewall and improve performance. Weissman, ¶100.

2. Claim Chart

Claim 1 is a method claim, the substance of which is representative of system Claim 24 and non-transitory media Claim 25. Weissman, ¶¶88, 146.

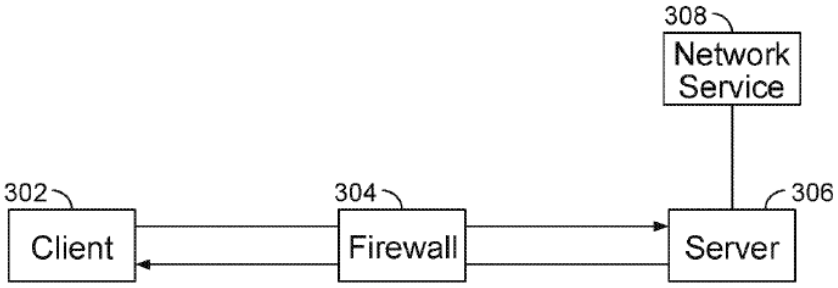
Claims	Buruganahalli
[1.pre][5] A method comprising: [24.pre] A packet-filtering system comprising: [25.pre] One or more non-transitory computer-readable media comprising instructions that when executed by at least one hardware processor of a packet-filtering system cause the packet-	**Buruganahalli discloses a method.** **Buruganahalli** is directed to a firewall that "protects networks from unauthorized access while permitting authorized communications to pass through the firewall." Buruganahalli, 1:20-22. Specifically, **Buruganahalli** discloses a method for filtering packets in communications between a client and a remote server. Buruganahalli, 4:31-40. **Buruganahalli** discloses applying a policy to packets of an initial handshake of a session to determine whether a secure connection for a new session would be allowed to be established for transmitting packets of encrypted data. *Id.* **Buruganahalli** discloses that firewalls may be implemented as a device, a set of devices or software executed on a device that provides a firewall function for network access, and that the disclosed techniques can be implemented in numerous ways, including as a process, apparatus, a computer program and/or a processor. Buruganahalli, 1:21-31, 2:14-32, 2:48-60. Weissman, ¶¶101-104, 59-60.

[5]To the extent they are limiting, the preambles of all Challenged Claims are met by the art of record.

Claims	Buruganahalli
filtering system to:[6]	
[1.a] / [25.a] [receiving, by a packet-filtering system comprising a hardware processor and a memory and configured to filter packets in accordance with a plurality of packet-filtering rules,] / [receive] data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprises a domain name identified as a network threat;	**Buruganahalli discloses receiving, by a packet-filtering system** (*e.g.*, "packet-filtering firewall," "a security device") **comprising a hardware processor** (*e.g.*, a processor) **and a memory** (*e.g.*, a memory) **and configured to filter packets in accordance with a plurality of packet-filtering rules** (*e.g.*, "set of rules… referred to as policies," "firewall policies/rules"), **data indicating a plurality of network-threat indicators** (*e.g.*, "blacklist," data that identify "threats" or "vulnerabilities"), **wherein at least one of the plurality of network-threat indicators comprises a domain name** (*e.g.*, "domain name," "destination domain") **identified as a network threat**. **Buruganahalli** discloses that its method is implemented using a "security device" such as a "packet-filtering firewall" comprising "a processor configured to execute instructions stored on and/or provided by a memory coupled to the processor." Buruganahalli, 2:14-31, 2:55-60, 3:16-24, 4:23-30. Weissman, ¶¶105-106. **Buruganahalli** discloses that firewalls were generally known to "deny or permit network transmission based on a set of rules. These sets of rules are often referred to as policies (e.g., network policies or network security policies)." Buruganahalli, 2:61-66, 1:32-36. Firewalls were also generally known to filter "inbound traffic by applying a set of rules or policies to prevent unwanted outside traffic from reaching protected devices," and "to filter outbound traffic by applying a set of rules or policies." *Id.* In **Buruganahalli's** system, these policies are "received and stored" in a security device comprising a firewall. Buruganahalli, 2:55-60, 14:58-60, Fig. 6. Weissman, ¶107 Specifically, "policies can include one or more rules, which can be specified using domain and/or host/server names… or other matching criteria or heuristics" Buruganahalli, 14:60-67, 5:35-

[6]*See also* [1.a] for additional mapping for [25.pre].

Claims	Buruganahalli
[24.a] at least one hardware processor; and memory storing instructions that when executed by the at least one hardware processor cause the packet-filtering system to: receive data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprise a domain name identified as a network threat;	43 ("domain name can be extracted… which can then be used to apply firewall policies or take responsive actions based on this information…"). For example, one of the "firewall policies/rules" may include "requirements or rules related to destination domains." Buruganahalli, 10:66-11:2, 7:27-29 ("applying a policy (e.g., a security policy) based on the destination domain to filter traffic at a security device"), 8:1-44, 15:37-45. **Buruganahalli** discloses that it is important "to extract information about the destination domain for any given new flow (*e.g.*, new session) as early as possible" because "information about the destination domain can be critical as well as relevant for security processing based on which policies and a set of actions that can be applied to the flow." Buruganahalli, 4:23-30. Weissman, ¶108. Destination domains are listed in a "blacklist policy" that is part of the "security policy." Buruganahalli, 7:42-67. A POSITA would have understood that data on the blacklist, as taught in **Buruganahalli**, comprises network-threat indicators (*e.g.*, whether a destination domain presents security risk) as the data would be compiled based on "identification of new, zero-day threats, new vulnerabilities, prevent false positives, and/or provide a feedback loop for any of such activities or trends aggregated and correlated using the security cloud service." Buruganahalli, 13:43-52. Weissman, ¶109. *See also* Weissman, ¶¶59-63.
[1.b] / [24.b] / [25.b] identify[ing] packets comprising unencrypted data;	**Buruganahalli discloses identifying** (*e.g.*, "identifies") **packets comprising unencrypted data** (*e.g.*, "unencrypted/clear text data communications exchanged as part of an initial handshake," "handshake traffic," "handshake exchange," "hello message"). **Buruganahalli** discloses that its security device contains a "Flow 608" that "identifies the packets as being part of a new session and creates a new session flow." Buruganahalli, 14:25-

Claims	Buruganahalli
	28. **Buruganahalli** further discloses "monitor[ing] the initial unencrypted/clear text data communications exchanged as part of an initial handshake to setup a secure connection for a new session between a client and a remote server…" Buruganahalli, 4:37-43. For example, the system may intercept a request to establish an encrypted session from the client to the remote server. Buruganahalli, 8:25-44, 11:47-51, 11:59-12:3, 15:22-26. With reference to Fig. 3A, **Buruganahalli** discloses "inspect[ing] the handshake traffic (e.g., the initial negotiation to setup a secure communication channel/tunnel between a client and a remote server)…" Buruganahalli, 10:54-61, 11:7-42 ("parsing the handshake traffic (*e.g.*, parsing a client hello message…)"), 12:32-36.  FIG. 3A Further, the handshake traffic is transmitted in the form of packets comprising unencrypted data. Buruganahalli, 5:43-51 (describing extracting relevant information starting from "the first packet of this handshaking process"), 7:24-25 ("the client hello message is an unencrypted communication."). A POSITA would have understood these disclosures to describe identifying packets comprising unencrypted data in an initial handshake configured to set up a new session. Weissman, ¶¶110-113, 64-67.

Claims	Buruganahalli
[1.c] / [24.c] / [25.c] identify[ing] packets comprising encrypted data;	**Buruganahalli discloses identifying** (*e.g.,* "identifies") **packets comprising encrypted data** (*e.g.*, "encrypted data communication"). **Buruganahalli** discloses that its security device contains a "Flow 608" that "identifies the packets as being part of a new session and creates a new session flow. Subsequent packets will be identified as belonging to the session based on a flow lookup." Buruganahalli, 14:25-28. **Buruganahalli** further discloses determining whether a new session violates its policy. Buruganahalli, 5:62-6:22. A session using a secure protocol involves "encrypted data communication," and the determination of how to handle the encrypted data communication(s) of the session is made by applying a security policy based on handshake traffic before the session is set up. Buruganahalli, 5:62-6:22, 4:31-44, 5:43-52, 12:33-48. A POSITA would have understood that such encrypted data communication comprises data packets. Buruganahalli, 3:16-24, 3:40-50, 8:55-60 (discussing "packet inspection of the session traffic" and that "session traffic… can include… encrypted data"), 9:25-30 (describing "a monitored traffic flow (*e.g.*, a session) based on packet analysis"); *id.*, 6:15-38, 8:11-44 (referring to a "session" as "encrypted data communications."). Accordingly, a POSITA would have understood that **Buruganahalli** teaches identifying packets comprising encrypted data that are part of a new session. *See id.* Weissman, ¶¶114-115, 64-67.
[1.d] / [24.d] / [25.d] [determining, by the packet-filtering system and] / [determine,] based on a portion of the	**Buruganahalli discloses determining, by the packet-filtering system and based on a portion of the unencrypted data** (*e.g.,* "unencrypted/clear text data communications exchanged as part of an initial handshake," "handshake traffic," "handshake exchange," "hello message", "IP address") **corresponding to one or more network-threat indicators of the plurality of network-threat indicators** (*e.g.,* destination domain on a blacklist), **packets comprising encrypted data** (*e.g.,* "encrypted data communication") **that corresponds to the one or more**

Claims	Buruganahalli
unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;	**network-threat indicators** (*e.g.,* destination domain on a blacklist). **Buruganahalli** discloses that "a firewall can intercept and monitor data communications from a client and a remote server" to extract information corresponding to a network-threat indicator, *e.g.*, "hostname data (*e.g.*, destination domain)" in "an unencrypted data communication from the client… at the start of the handshaking process for setting up a secure TLS communication channel/session between a client and a remote server." Buruganahalli, 5:24-36, 11:7-13 ("parsing a client hello message to extract a hostname that identifies the destination domain being requested by the client to the remote server"), 11:30-52 ("the firewall can intercept and decode (*e.g.*, parse) this TLS handshake exchange to extract the hostname from the client hello message in order to apply various policies based on the destination domain"). Weissman, ¶¶116-117. The firewall determines whether the handshake traffic and the encrypted data communication(s) it seeks to set up present any threats by applying a security policy to compare the extracted information with information on a blacklist, *e.g.*, determining whether "the destination domain is included in the blacklist." Buruganahalli, 7:42-67, 11:13-19 ("the firewall 304 can apply one or more firewall policies/rules… *e.g.*, a policy that includes requirements or rules related to destination domains that may be used for secure protocol communications…"). Weissman, ¶118. Packets related to a session are correlated using "[a]n IP address" and a "port engine 104" that "determines an IP address and port number for a monitored traffic flow (e.g., a session) based on packet analysis." Buruganahalli, 9:25-28. It was well-known and conventional that IP addresses (*e.g.*, source, destination) and TCP session data associated with a packet were typically unencrypted and could be inspected without decrypting the packet information. The firewall may include a table that stores "destination domains[] and associated IP addresses and possibly other information for clients and/or remote servers identified as external sites that are monitored for implementing policies using

Claims	Buruganahalli
	destination domain extraction for secure protocols." Buruganahalli, 13:62-14:1. Weissman, ¶119. A POSITA would have understood that **Buruganahalli** teaches determining that encrypted packets correlate to a session initiated by a hello message in TLS handshake traffic. A POSITA would have further understood that this determination would have been accomplished using at least address information associated with the destination domain in the hello message. Accordingly, a POSITA would have understood that **Buruganahalli** teaches determining encrypted packets comprising data corresponding to one or more network-threat indicators (*e.g.*, a blacklisted destination domain), based on data included in the hello message (*e.g.*, destination domain and associated IP address) configured to establish the encrypted session, as both the encrypted session and the hello message would be associated with the same destination IP address of the remote server. Weissman, ¶120. **Buruganahalli**'s teachings of using a handshake message in performing the determining step are similar to those described in the specification of the '856 patent. *See, e.g.*, '856, 9:30-33 ("determine that the packets comprise data corresponding to the network-threat indicators based on data included in the one or more handshake messages configured to establish session"), 24:18-30 ("determine that one or more of the packets encrypted… correlate to one or more packets comprising … the one or more handshake messages."). Weissman, ¶121. Weissman, ¶¶61-67.
[1.e] / [24.e] / [25.e] [filtering] / [filter], [by the packet-filtering system and] based on at least one of a	**Buruganahalli discloses filtering, by the packet-filtering system and based on data indicating a request** (*e.g.*, "a request to create a secure connection") **specified by the plurality of packet-filtering rules.** *See* [1.a]—**Buruganahalli** discloses "filter[ing] inbound traffic by applying a set of rules or policies." Buruganahalli, 1:32-35, 2:61-66, 10:63-11:2 ("a network service activity that is in violation of one or more firewall policies/rules implemented by

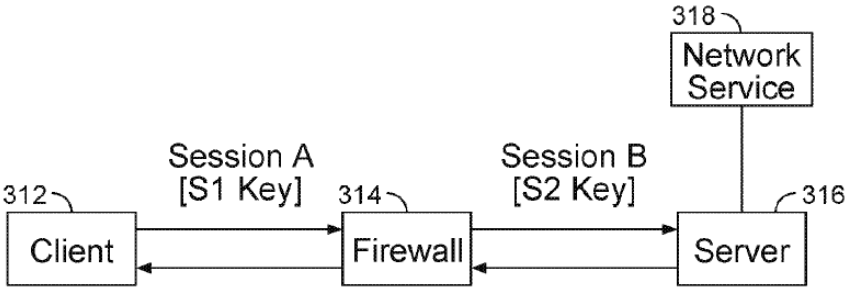
Claims	Buruganahalli
uniform resource identifier (URI) specified by the plurality of packet-filtering rules [indicating one or more of the plurality of network-threat indicators], data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of	the firewall device [] (e.g., a policy that includes requirements or rules related to destination domains…)"). As discussed in [1.d], **Buruganahalli** discloses parsing a client's SSL/TLS request (*e.g.*, packets in handshake traffic, a hello message) to create a secure connection with a remote server to determine whether the destination domain extracted from the request corresponds to data on a blacklist. Buruganahalli, *Abstract*, 5:24-52, 7:12-29, 7:39-51, 7:60-67. The system applies a security rule based on the destination domain extracted from the request to "filter traffic" from the request. Buruganahalli, 7:12-29, 8:25-44, 15:4-21. Weissman, ¶¶122-124. **Buruganahalli also discloses filtering, by the packet-filtering system and based on a uniform resource identifier (URI)** (*e.g.*, a uniform resource locator (URL)) **specified by the plurality of packet-filtering rules.** **Buruganahalli** discloses a firewall that filters packets based on identifiers for a "domain" (*e.g.*, "uniform resource locator (URL)") specified in the firewall security policies or rules. Buruganahalli, 7:39-7:51 ("a uniform resource locator (URL)/category filtering policy"), 10:21-28 ("URL/category filtering"), 15:37-45. In addition, **Buruganahalli** discloses performing "application layer filtering" and "content scanning" Buruganahalli, 3:25-39, 4:1-3, 9:16-24, 9:28-43, 10:15-20. A POSITA would have understood, as was well-known and conventional, that URLs are examples of uniform resource identifiers. *See, e.g.*, Magee, 12:25-27 ("The module will also gather a taxonomy of the uniform resource identifiers (URIs) (e.g., URLs …) associated with the target host"). A POSITA would have further understood that a firewall filters packets based on a URL by scanning content in the application layer where a URL would be found. Corresponding limitation [25.e] of Claim 25 further recites "filter[ing], by the packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by a

Claims	Buruganahalli
packet-filtering rules:[7]	plurality of packet-filtering rules ***indicating one or more of the plurality of network-threat indicators***." As discussed in [1.a], **Buruganahalli** discloses packet-filtering rules that indicate network-threat indicators. For example, the rules are implemented for security purposes to protect the network. Buruganahalli, 2:61-66, 1:32-36. They include "requirements or rules related to destination domains" and that the domains may be listed on a blacklist if they present a security risk. Buruganahalli, 10:66-11:2, 7:27-29, 7:42-67, 8:1-44, 13:43-52. Weissman, ¶¶125-128. **Buruganahalli also teaches filtering, by the packet-filtering system and based on data indicating a protocol version** (*e.g.*, "protocol information," version of TLS protocol with "server name indication (SNI)" extension) **specified by the plurality of packet-filtering rules.** **Buruganahalli** discloses that firewalls were generally known to inspect and apply rules to packets based on "protocol information" in the packets. Buruganahalli, 3:20-39, 9:16-24. It would have been obvious to a POSITA to have included the protocol version in that protocol information, such that the firewall would have applied rules based at least in part on protocol version, in order to mitigate the risks associated with widely-known security vulnerabilities of certain SSL or TLS versions. *See, e.g.*, Turner (listing SSL version 2.0 deficiencies), Ristic (identifying security issues with various versions of SSL and TLS). A POSITA would have been motivated and found it obvious to filter packets based on data indicating a protocol version, *e.g.*, SSL/TLS versions, specified by packet-filtering rules as was well-known and conventional in the art, in order to

[7]Because this limitation recites "filtering… based on at least one of" five criteria, Petitioner has the burden to show that only one of the five criteria is met.

Claims	Buruganahalli
	protect against known security vulnerabilities of certain protocol versions, and thereby enhance network security. In addition, **Buruganahalli** discloses filtering based on data indicating a version of the TLS protocol using the SNI extension. Buruganahalli, *Abstract*, 4:45-5:4, 7:12-29, 15:4-21. Weissman, ¶¶129-131. *See also* Weissman, ¶¶59-60, 61-63.
[1.f] / [24.f] / [25.f] packets comprising the portion of the unencrypted data that corresponds to one or more network-threat indicators of the plurality of network-threat indicators; and	**Buruganahalli discloses filtering packets comprising the portion of the unencrypted data** (*e.g.*, "unencrypted/clear text data communications exchanged as part of an initial handshake," "handshake traffic," "handshake exchange," "hello message") **that corresponds to one or more network-threat indicators of the plurality of network-threat indicators** (*e.g.*, destination domain on a blacklist). *See* [1.b], [1.d]-[1.e]— **Buruganahalli** discloses that it would be "desirable and efficient" to "facilitate policy-based filtering on such data communication flows (e.g., sessions) prior to the set-up of the encrypted data communication for such flows (e.g., to monitor the initial unencrypted/clear text data communications exchanged as part of an initial handshake to setup a secure connection for a new session between a client and a remote server, which is prior to the establishment of the secure communication channel/tunnel after which any data communications intercepted between the client and the remote server would be encrypted)." Buruganahalli, 4:31-44. For example, **Buruganahalli** discloses intercepting a request to establish an encrypted session from a client to a remote server. Buruganahalli, 8:25-43, 15:22-26. Furthermore, **Buruganahalli** discloses filtering unencrypted packets in the initial handshake based on the determination of whether "the destination domain is

Claims	Buruganahalli
	included in the blacklist." Buruganahalli, 7:39-51, 7:60-67, 10:54-11:54. Weissman, ¶¶132-133, 61-67.
[1.g] / [24.g] / [25.g] the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and	**Buruganahalli teaches filtering the determined packets comprising the encrypted data** (*e.g.*, "encrypted data communication") **that corresponds to the one or more network-threat indicators** (*e.g.*, destination domain on a blacklist). *See* [1.c]-[1.e]—**Buruganahalli** discloses that the encrypted data communications are filtered based on data specified in the firewall policies/rules described above. Buruganahalli, 4:16-22. For example, the firewall filters encrypted data communications after a determination that the handshake traffic corresponds to a network-threat indicator (*e.g.*, whether the extracted destination domain is on a blacklist). Buruganahalli, 6:12-39 (encrypted data communications associated with a secure session monitored for filtering based on a firewall policy); *see also id., Abstract* (applying a policy based on the destination domain to filter traffic), 4:31-44 (policy-based filtering on a session with encrypted data communications), 6:62-7:9 (applying policy to a resumed session), 7:12-29 (applying a policy based on the destination domain to filter traffic), 7:39-51 (same), 7:60-67 (same), 15:4-21 (same). To the extent it is argued that **Buruganahalli** does not explicitly disclose filtering the packets with encrypted data that corresponds to a network-threat indicator, a POSITA would have understood that the packets communicated as part of a secure session are filtered after a determination that a handshake message that initiates the session includes data that corresponds to the network threat indicator (*e.g.*, a blacklisted destination domain). This is because the handshake message comprises data (*e.g.*, destination domain) that also applies to the encrypted data of the session, such that the security risks associated with the handshake message and encrypted data are correlated. At minimum, a POSITA would have been motivated and found it obvious in view of

Claims	Buruganahalli
	Buruganahalli to filter the encrypted data of a secure session that was initiated by a handshake message with data corresponding to a network-threat indicator in order to monitor transmission, into or out of a protected network, of data that potentially presents a security risk. Weissman, ¶¶134-135, 61-67.
[1.h] / [24.h] / [25.h] [routing] / [route], by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.	**Buruganahalli teaches routing, by the packet-filtering system, filtered packets to a proxy system** (*e.g.*, a "decrypt engine… applying trusted man-in-the middle techniques," a "proxy" that is one of the "security functions") **based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators** (*e.g.*, destination domain on a blacklist). **Buruganahalli** discloses that if the filtered packets correspond to a network-threat indicator, *e.g.*, "if the destination domain is included in the blacklist," then the encrypted data communications are sent to a "decrypt engine" of the firewall to be "decrypted." Buruganahalli, 7:39-51, 7:60-67, 9:61-67. Weissman, ¶¶136-137. The process of decrypting the encrypted data is described in connection with Figure 3B, which illustrates a process of establishing an SSL session. Buruganahalli, 12:4-18.  FIG. 3B

Claims	Buruganahalli
	The firewall detects and intercepts an SSL session request. Buruganahalli, 12:12-14. It splits "the SSL session between the client 312 and the remote server 316 into two half sessions." Buruganahalli, 12:14-18. "In Session A, the firewall 314 acts as the remote server 316 such that it is transparent to the client 312 that it is not communicating directly with the remote server 316. Session A traffic is encrypted using the session key S1 associated with the firewall device. In Session B, the firewall 314 acts as the client 312 such that it is transparent to the remote server 316 that it is not communicating directly with the client 312. Session B traffic is encrypted using the session key S2 associated with the firewall device…" Buruganahalli, 12:14-28. As discussed in §IX.A.1, this disclosure describes that the packets of a secure session are processed in a manner "transparent" to the client and the server such that these endpoints would not detect the presence of the firewall applying the "trusted man-in-the-middle" techniques. Buruganahalli, 12:14-15. Weissman, ¶¶138-139. Also, as discussed in §IX.A.1, **Buruganahalli** explicitly discloses that the decrypt engine of the firewall applies "trusted man-in-the-middle techniques using a self-signed certificate." Buruganahalli, 9:61-67. In connection with Figure 3B, a POSITA would have understood that the firewall replaces the server certificate and signs a new certificate (*i.e.*, the "self-signed certificate") with its own public key (*e.g.*, "session key S1"). Buruganahalli, 5:6-23, 5:52-61, 8:25-32, 9:61-67, 12:18-36. Weissman, ¶140 A POSITA would have understood that these techniques are used by the decrypt engine of the firewall in addition to and/or in combination with the various techniques described for destination extraction for secure protocols, such as the example provided in Figure 3A above. *Id.*, 11:59-12:3. Weissman, ¶141. Based on this description, a POSITA would have understood that Figure 3B and its accompanying disclosures describe a firewall containing functionality acting as a proxy for both the remote server and the client by standing in line of their communications

Claims	Buruganahalli
	in a "transparent" manner, as was known in the art. *See, e.g.*, Wang, 8:12-19; NIST, 14; Baehr, 4:50-63, 8:36-47, 8:65-9:7; *see also* §IX.A.1. **Buruganahalli**'s teachings are further consistent with the description of a proxy in the '856 specification. *See* '856, 10:62-63 (discussing "proxy devices" as being the "the man in the middle"). Weissman, ¶142. **Buruganahalli** further discloses that it was known that a firewall may be implemented in a security device that includes other functions, such as a routing function that may be based on source and destination information, and a "proxy" function that is one of the "security functions." *Id.*, 1:36-38, 3:5-15 ("Security devices… can include various security functions…e.g., … proxy"). A POSITA would have understood that the encrypted packets would be routed to the decrypt engine of the firewall (used as part of the proxy function, as discussed above) such that they would be "decrypted using a session key S1 and then inspected by the firewall 314," which **Buruganahalli** explicitly discloses as the action taken "[a]fter the session set-up handshaking is completed." Buruganahalli, 12:29-32, 15:22-44. A POSITA would have further understood that routing may be implemented as a software process that may be internal within a firewall. *See, e.g.*, NIST, 12; *see also* §IX.A.1. In view of this understanding, these additional disclosures support that a POSITA would have understood, or at minimum would have been motivated and found it obvious, to ***route*** filtered packets to a proxy system (*i.e.*, the decrypt engine of the firewall used as part of the proxy function) when applying the "trusted man-in-the-middle" techniques. Weissman, ¶143. To the extent it is argued that **Buruganahalli**'s session splitting disclosure in connection with Figure 3B does not explicitly teach routing filtered packets to a proxy system, a POSITA would have been motivated and found it obvious to perform the session splitting by routing filtered packets (*e.g.*, using software or the routing function, as discussed above) to a proxy system for security purposes, whether implemented together with other firewall functionality in the same device or in one or more

Claims	Buruganahalli
	separate devices, as was well-known and conventional in the art. *See, e.g.*, NIST, 12-14; Baehr, 2:25-30, 5:2-8, 8:12-18, Figs. 6-7; Wang, Fig. 1, 2:32-58; Le Pennec, Fig. 3, [0021]-[0023]. Isolation of potentially dangerous traffic for separate inspection, filtering and/or logging is a purpose of a proxy associated with a security system interconnecting networks. *Id.* It was well-known and conventional that a proxy system provides security protection by intercepting communications to and from a protected network, thereby isolating the network from direct access by an outsider that may pose security risks. *See, e.g.*, Baehr, Abstract, 8:37-40. In addition, Buruganahalli confirms that it was known to implement a firewall as a set of devices. 1:22-25; 2:50-52. Weissman, ¶144. It would have been advantageous to implement the proxy as one or more devices apart from other firewall functionality to reduce the work load on the firewall, and allow computationally intense processing required for decryption and encryption to be performed by proxy devices dedicated to these tasks. Either way the firewall would minimize security risks by routing threatening packets to the proxy function. Specifically, **Buruganahalli**'s firewall acts as a trusted man-in-the-middle by using the proxy to decrypt the encrypted data posing security risks (based on its correspondence to a network threat indicator) such that the client within the protected network would be protected against malware or other security attacks. Buruganahalli, 3:5-8, 7:39-51, 7:60-67, 8:20-24, 10:15-20, 13:43-52. *See also* §IX.A.1. Weissman, ¶145. *See also* Weissman, ¶¶61-63, 68-76.

B. Ground 2: Claims 1, 24-25 are rendered obvious by Buruganahalli in view of Baehr

Claims 1, 24 and 25 would have been obvious to a POSITA based on the disclosure of **Buruganahalli**—*see* Ground 1. Alternatively, these claims would

have been obvious over **Buruganahalli** in view of **Baehr**, which discloses a packet filtering system sending packets aside to a proxy network. Weissman, ¶147.

Buruganahalli discloses a firewall for filtering packets in communications between a client and a remote server. Buruganahalli, 4:31-40. **Buruganahalli** further discloses that if the filtered packets from a handshake message configured to set up a session correspond to data on a blacklist, then the packets from the encrypted session would be decrypted. Buruganahalli, 7:39-51, 7:60-67, 12:29-32. The decryption is performed by a decrypt engine of the firewall applying "trusted man-in-the middle techniques." Buruganahalli, 9:7-8, 9:61-67. **Buruganahalli** discloses that the firewall acts as the remote server such that the client is not communicating directly with the server, and that it acts as the client such that the remote server is not communicating directly with the client. Buruganahalli, 12:13-33. Weissman, ¶148.

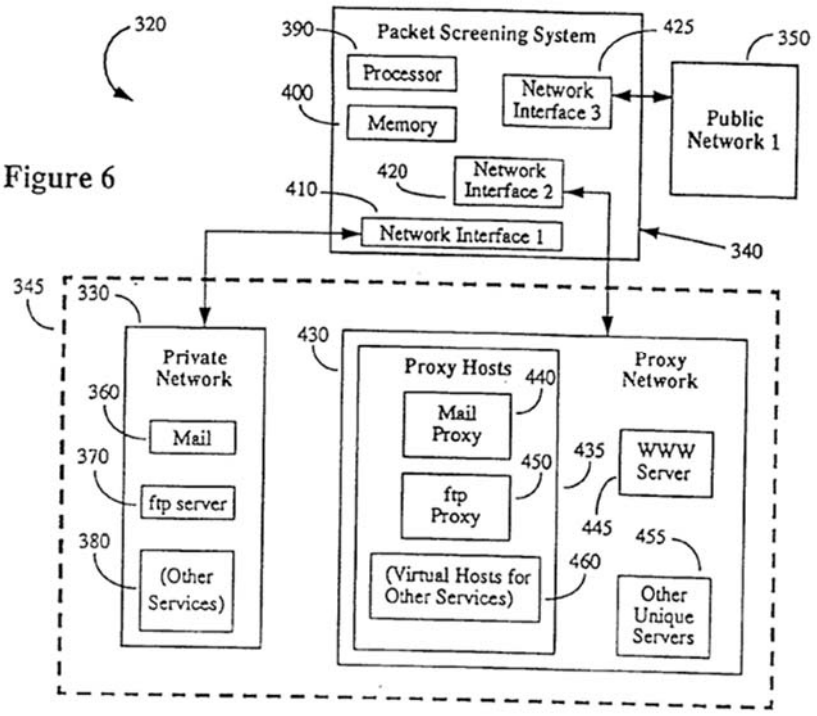
Buruganahalli further discloses that a security device may have "various security functions" such as "firewall" and "proxy," and also other functions, such as a routing function based on source and destination information. Buruganahalli, 3:5-15. As discussed above, a POSITA would have recognized that **Buruganahalli**'s disclosures relating to Figure 3B describe a proxy function, and it would have been obvious from **Buruganahalli**'s disclosure to route filtered packets to this proxy

function, *i.e.*, by passing the packets between software functions of a security device implementing a firewall. Buruganahalli, 3:16-24. Weissman, ¶149.

Buruganahalli recognizes the need for "workload balancing of network related resources." Buruganahalli, 3:5-15. **Buruganahalli** further discloses using "special purpose hardware" to implement firewalls "as dedicated appliances" that would "generally provide higher performance levels for application inspection than software executed on general purpose hardware." Buruganahalli, 4:7-15. **Buruganahalli** also discloses implementing firewalls as a set of devices. 1:22-25. A POSITA would have known that to reduce load on a firewall, the firewall would "hand off" filtered traffic to dedicated proxy servers as an alternative performing the proxy functions internally. NIST, 14. Accordingly, a POSITA would have been motivated and found it obvious to incorporate **Baehr**'s teaching to implement a proxy system separate from a packet screening system acting as a firewall, in the security system disclosed by **Buruganahalli**. Weissman, ¶150.

Baehr is directed to a packet screening system of data packets at a network interface that acts as a firewall. Baehr, Abstract, 2:10-12. Figure 6 of Baehr illustrates such "packet screening system." Baehr, 2:66-67. Weissman, ¶151.

Figure 6



The system positions a "screen" between a public network and a private network to protect the private network that may be targeted for attacks. Baehr, 2:10-17. The screen includes a packet filtering module that inspects incoming and outgoing packets and sends them to an engine to determine appropriate routing actions based upon predetermined criteria (*e.g.*, source and destination) to enable the screen to make a determination whether a packet is coming from or going to a network location that may indicate a security problem. Baehr, 2:18-23, 6:37-7:7. Weissman, ¶151.

Baehr teaches using a "proxy network" to protect the private network. **Baehr** discloses that "[w]hen a packet is sent by a host on, for instance, public network 350, it is received at port (interface) 425 of the screen 340." Baehr, 10:2-5, 9:63-67. The

screen 340 filters packets using a set of predetermined "screening criteria." Baehr, 6:37-7:10. Based on the screening, the screen 340 takes "one or several predefined actions" on the packets to "prevent attacks on the system." Baehr, 7:8-25. One of such actions is "sending packets aside to the proxy network 430" for "security purposes" even if their intended destination is the private network. Baehr, 2:25-30, 8:12-18 ("An important action for security purposes is that of sending packets aside to the proxy network…"), 10:43-49. For example, if a packet's intended destination is on the private network, it would be sent instead to the proxy network, which would execute the appropriate operations. Baehr, 2:25-30. The proxy network may include proxy hosts and other servers. Baehr, 4:26-63. Weissman, ¶152.

Baehr explains that sending the filtered packets to the proxy network is advantageous for various reasons. The proxy network is "isolated from the private network, so it cannot be used as a jumping off point for intruders." Baehr, *Abstract*. It has the "advantage of preventing outsiders from ever actually entering the private network []; once a user has been allowed access or a connection to a private network, it is much more difficult to restrict his/her actions than if no access at all is allowed." Baehr, 8:37-40. In addition to preventing outsiders from entering the private network, the proxy network communicates with the outsiders seamlessly, as if the outsiders are communicating with the private network. Baehr, 4:50-63, 8:36-47, 8:65-9:7. Weissman, ¶153.

The proxy network may be a separate computer system (*e.g.*, as shown and described in connection with Fig. 6), or it may be a separate logical entity, but not physically separate from the screen (*e.g.*, as shown and described in connection with Fig. 7). Baehr, 4:26-31, 5:2-8. **Baehr** discloses that the proxy network may be "implemented entirely in the program instructions" stored in memory of the packet screening system, or as one or more additional processors and memories. Baehr, 4:64-5:2. Weissman, ¶154.

A POSITA would have been motivated and found it obvious to implement **Buruganahalli**'s system in view of the teachings of **Baehr** to route the filtered packets to a proxy system separate from the firewall, such that **Buruganahalli**'s techniques characterizing a transparent proxy function would have been implemented in a proxy system separate from and external to the firewall. As discussed above, a POSITA would have been motivated and found it obvious to implement **Buruganahalli**'s techniques describing a proxy in a dedicated system for the advantages of preserving computing resources, achieving load balancing, and maximizing performance, as recognized in **Buruganahalli** (Buruganahalli, 3:5-15, 4:7-15) and in the prior art generally. *See, e.g.*, NIST, 14 ("Typically, dedicated proxy servers are used to decrease the work load on the firewall…" and "can be used to secure less time-sensitive services…").The teachings of **Baehr** further provide the added advantages of isolating the proxy system, which handles high-risk or

suspicious packets and is particularly vulnerable to attacks, from the private network. Baehr, *Abstract* ("The proxy network is isolated from the private network, so it cannot be used as a jumping off point for intruders"). For example, Baehr explains that "[t]he proxy network has the additional advantage of preventing outsiders from ever actually entering the private network," and this is crucial because "once a user has been allowed access or a connection to a private network, it is much more difficult to restrict his/her actions than if no access at all is allowed." Baehr, 8:36-47. Weissman, ¶155.

Separating the proxy network from the screen/firewall facilitates isolating the proxy network from the private network by placing the screen/firewall between the two networks (e.g., so that the networks do not communicate directly with one another, instead each communicating separately with the screen/firewall via a separate network interface, and allowing the screen/firewall to inspect any packets sent to or from by a proxy host). Indeed, it would have been advantageous to isolate one security function (*e.g.*, a firewall that filters packets) from another security function (*e.g.*, a proxy function that processes packets) such that any security vulnerability would be limited to only one component of the system (*e.g.*, even if the proxy was compromised, the screen/firewall would be unaffected). Weissman, ¶156.

A POSITA would have found it routine, straightforward and advantageous to modify **Buruganahalli** to incorporate **Baehr**'s teachings of routing to an external proxy system, and would have known that such a combination (yielding the claimed limitations) would predictably work and provide the expected functionality. *See KSR Int'l Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1731 (2007). Specifically, **Buruganahalli** discloses that the firewall "acts as the remote server" such that it is "transparent" to the client, while **Baehr** explicitly describes the function of a transparent proxy such that "the outside user's requests are met while invisibly preventing him/her from ever actually accessing the private network." Buruganahalli, 12:17-21; Baehr, *Abstract*, 4:50-63 (describing the proxy and network forming "a single apparent domain from the point of view of outsiders… without any indication being given to the user" that the proxy network is involved in processing the user's request), 8:36-47 ("invisibly preventing him/her from ever actually accessing the private network"), 8:65-9:7 ("no IP address for the proxy host exists, and none is appended to any packets"). A POSITA would have had a reasonable expectation of success in implementing **Buruganahalli**'s system in view of the teachings from **Baehr**. For example, when a firewall implemented in accordance with **Buruganahalli's** teachings receives an encrypted packet in a session associated with a suspect domain, the firewall would route the packet to an interface (*e.g.*, network interface

2 in **Baehr**'s Figure 6) for processing by a proxy network external to the firewall. Weissman, ¶157.

Buruganahalli and **Baehr** are in the same field of endeavor—data communications and security in a computer network—and are analogous art to the '856 patent. And both **Buruganahalli** and **Baehr** are specifically directed to a packet-filtering system to prevent unauthorized access to a network by applying a set of rules for security purposes. Buruganahalli, 1:20-39, 2:48-3:24; Baehr, Title, Abstract, 2:10-17. Weissman, ¶158.

X. SECONDARY CONSIDERATIONS

The Challenged Claims of the '856 patent are overwhelmingly demonstrated as obvious by the grounds presented herein that cannot be overcome by any alleged objective indicia. While the trial transcript in the Cisco suit references purported secondary considerations for the '856 patent (EX1029, 3215:4-3240:4), the underlying evidence is not publicly available and Petitioner does not have access to such evidence. From what little can be discerned from the public record, the evidence fails to show nexus. Petitioner reserves the right to respond to any secondary considerations Patent Owner may assert in this proceeding. Weissman, ¶¶159-160.

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. *IPR* of Claims 1, 24-25 of the '856 patent is accordingly requested. Weissman, ¶¶161-166.

Respectfully submitted,

Dated: November 18, 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 10,735 words as counted by the word processing program used to prepare the paper.

Dated: November 18, 2021 By: /*Keyna Chow*/
Keyna Chow

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 Fedex of a copy of this Petition for *Inter Partes* Review and supporting materials at the correspondence address of record for the '856:

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

Dated: November 18, 2021 By: /*Scott A. McKeown*/
Scott A. McKeown
Registration No. 42,866