

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

U.S. Patent No. 9,917,856

PETITIONER'S REPLY TO PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	BURUGANAHALLI TEACHES RULE-BASED FILTERING OF ENCRYPTED PACKETS BEFORE SUBSEQUENT DECRYPTION BY A DECRYPT ENGINE.....	2
A.	Buruganahalli’s Disclosure Of Using A Handshake Exchange To Filter Unencrypted And Associated Encrypted Packets Is The Same As The Claimed Embodiment Of The ’856 Patent.....	3
B.	Consistent With Its Handshake Disclosure, Buruganahalli Expressly Teaches Filtering Encrypted Packets Based On Rules	7
C.	Buruganahalli’s Figure 3a Embodiment Together With Its Figure 3b Embodiment Teaches Filtering Encrypted Traffic And Routing It To A Proxy For Decryption, Just As Described On The ’856 Patent.....	11
D.	That Buruganahalli Also Teaches Decryption Of Encrypted Packets After Initial Filtering Does Not Distinguish The Challenged Claims	12
III.	BURUGANAHALLI TEACHES “NETWORK-THREAT INDICATORS” UNDER BOTH CONSTRUCTIONS	14
IV.	BURUGANAHALLI TEACHES ROUTING FILTERED PACKETS TO A PROXY SYSTEM.....	17
V.	PO’S ARGUMENTS AGAINST MODIFYING BURUGANAHALLI IN VIEW OF BAEHR’S TEACHINGS (GROUND 2) ARE UNAVAILING	19
A.	PO’s Argument That The Petition Fails To Describe “How” The Combination Meets The Challenged Claims Lacks Merit	19
B.	The Petition Provides Compelling Reasons Why A POSITA Would Have Combined The Teachings Of Buruganahalli And Baehr.....	21
VI.	PO HAS NOT MET ITS BURDEN TO ESTABLISH OBJECTIVE INDICIA OF NON-OBVIOUSNESS	23

A.	PO Fails To Show That The '856 Alleged Invention Satisfied Any Long-Felt Need Or Received Substantial Industry Praise	24
B.	PO Fails To Show Copying.....	25
C.	The Obviousness Of The Challenged Claims Cannot Be Overcome By Any Alleged Objective Indicia	25

TABLE OF ABBREVIATIONS

Document	Abbreviations
Petition	Pet.
Patent Owner's Preliminary Response	POPR
Petitioner's Preliminary Reply	PPR
Institution Decision	DI
Patent Owner's Response	POR
Patent Owner	PO

LIST OF EXHIBITS

Exhibit No.	Description
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 <i>Inter Partes</i> 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	<i>Reserved</i>
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

Exhibit No.	Description
	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”)

Exhibit No.	Description
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	<i>Cisco System Inc. v. Centripetal Networks, Inc.</i> , IPR2018-01760, Paper 41 (PTAB May 18, 2020)
EX1027	<i>Centripetal Networks, Inc. v. Cisco Systems, Inc.</i> , Case No. 2:18-cv- 00094 (E.D. Va.), Dkt. No. 621 (Opinion and Order Regarding Findings of Fact and Conclusions of Law)
EX1028	<i>Centripetal Networks, Inc. v. Cisco Systems, Inc.</i> , Case 2021-1888 (Fed. Cir.), Dkt. No. 18 (Non-Confidential Brief for Defendant-Appellant Cisco Systems, Inc.)
EX1029	<i>Centripetal Networks, Inc. v. Cisco Systems, Inc.</i> , Case No. 2:18-cv-00094 (E.D. Va.), Dkt. No. 548 (June 10, 2020 Trial Transcript)

Exhibit No.	Description
EX1030	<i>Centripetal Networks, Inc. v. Keysight Techs., Inc.</i> , 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., <i>Guidelines on Firewalls and Firewall Policy</i> , National Institute of Standards and Technology (“NIST”)
EX1037	U.S. Patent No. 8,813,228 (“Magee”)
EX1038	<i>Reserved</i>
EX1039	<i>Reserved</i>
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., <i>Design of Firewall in Router using Network Processor</i> , IEEE (Jul. 11, 2005) (“Kim”)
EX1046	Declaration of Jonathan Bradford

Exhibit No.	Description
EX1047	Declaration of Andrew Radsch in Support of Motion for <i>Pro Hac Vice</i> Admission
EX1048	Declaration of Keyna Chow in Support of Motion for <i>Pro Hac Vice</i> Admission
EX1049	Transcript of deposition of Dr. Michael Goodrich, <i>Palo Alto Networks, Inc. v. Centripetal Networks, Inc.</i> , IPR2022-00182 (September 23, 2022)
EX1050	<i>Centripetal Networks, Inc. v. Cisco Systems, Inc.</i> , No. 2021-1888, (Fed. Cir. 2022).
EX1051	Request for Comments: 3507, Internet Content Adaptation Protocol (ICAP), April 2003
EX1052	Goodrich, M. T., & Tamassia, R. (2011). <i>Introduction to Computer Security</i> , ch. 6. London, UK: Pearson.
EX1053	Declaration of Jonathan Bradford ISO Petitioner's Reply

I. INTRODUCTION

Buruganahalli filters unencrypted traffic in the same way as the '856 patent and for the same reason—to obtain plaintext information used to filter associated encrypted traffic. Like the '856 patent, Buruganahalli filters an unencrypted hello message of a handshake exchange to extract a destination domain, in order to determine (according to a security policy) whether to establish a secure session for the associated encrypted traffic and filter that encrypted traffic for routing to a proxy for further processing. *Compare* '856, 8:65-11:7 *with* Pet. 34-42 (*citing, e.g.,* Buruganahalli, 7:39-7:51, 7:60-67, 9:61-67, 10:54-12:36).

PO attempts to distinguish the Challenged Claims by arguing that Buruganahalli decrypts encrypted traffic at the proxy for further filtering, *after* that encrypted traffic is routed to the proxy—but that later decryption is irrelevant because the Challenged Claims do not prohibit the unclaimed extra step of decryption *after* filtering of encrypted traffic. POR 33-37.¹ What matters, and what PO effectively concedes, is that for encrypted packets *to get to* Buruganahalli's proxy (*i.e.,* its decrypt engine), those packets are first filtered by Buruganahalli's

¹ This same unclaimed extra step—additional decryption at the proxy after filtering, as in Buruganahalli—is also described in the '856 specification, but PO and its expert ignore that description. *Compare* '856, 10:15-11:35 (describing decryption at the proxy device in steps #20-22) *with* POR 20 (describing steps 19, 23-24, but skipping steps 20-22); Ex. 2026, ¶¶64-65 (same).

security device, and then routed there, as required by the claims. Pet. 34-37; Weissman, ¶¶122-131. Buruganahalli is explicit that such routing for decryption is a rule-based action: it is “based on a firewall policy.” Buruganahalli, 9:61-65. Buruganahalli discloses filtering encrypted traffic and does so in the same manner described and claimed in the ’856 patent.

PO’s other arguments against unpatentability also lack merit. Buruganahalli teaches rules based on “network-threat indicators” under any reasonable construction of that term. Buruganahalli also teaches (both alone and as modified by Baehr) routing filtered traffic to a proxy. As to secondary considerations, PO bases its arguments on district court findings that have been vacated in their entirety, leaving PO with no evidence of secondary considerations at all—let alone any evidence, with a necessary showing of nexus, that could rebut Petitioner’s overwhelming showing of obviousness.

II. BURUGANAHALLI TEACHES RULE-BASED FILTERING OF ENCRYPTED PACKETS BEFORE SUBSEQUENT DECRYPTION BY A DECRYPT ENGINE

PO’s argument that Buruganahalli does not teach filtering encrypted packets, but discloses filtering only (i) unencrypted packets, and (ii) packets that have already been decrypted, mischaracterizes Buruganahalli. POR 33-37. In Buruganahalli, the filtering of unencrypted packets enables the firewall to filter associated encrypted packets for routing to the proxy (*i.e.*, the decrypt engine of the firewall)—*before* any

decryption occurs. Those encrypted packets are filtered based on the earlier handshake processing of unencrypted data (*e.g.*, extraction of a destination domain to determine what firewall policy to apply to associated packets), and are routed to the proxy, as required by the claims. The filtering of encrypted packets based on data from the unencrypted handshake is the purpose of Buruganahalli's process, just like in the '856 patent.

A. Buruganahalli's Disclosure Of Using A Handshake Exchange To Filter Unencrypted And Associated Encrypted Packets Is The Same As The Claimed Embodiment Of The '856 Patent

Buruganahalli filters unencrypted traffic in the same way described in the '856 patent and for the same purpose—to obtain plaintext information used to filter associated encrypted traffic. As PO acknowledges, “Buruganahalli extracts the destination domain from an unencrypted client hello message... Buruganahalli's firewall uses this destination domain to apply a whitelist/blacklist policy...” POR 4-5 (*citing* Buruganahalli, 4:45-5:10, 7:12-51). That whitelist/blacklist policy is applied to all packets of that session, including the associated encrypted packets without (*i.e.*, before) any decryption of such packets, resulting in the filtering of encrypted packets. Buruganahalli is explicit that it filters encrypted packets, based on a firewall policy, before such packets are decrypted—after all, it is the filtering of encrypted packets that separates those packets to be sent for decryption from those packets simply passed through without decryption:

In some embodiments, destination domain extraction for secure protocols further includes applying a security policy based on the destination domain ***to filter traffic*** at the security device. For example, the security policy can include... a whitelist/blacklist policy (e.g., in which a session associated with the network communications between the client and the remote server are ***not decrypted if the destination domain is included in the whitelist***, and a session associated with the network communications between the client and the remote server ***are decrypted if the destination domain is included in the blacklist***).

Buruganahalli, 7:39-50. Indeed, PO admits that if Buruganahalli’s “destination domain is on the blacklist (or unknown...),” then a secure connection is established for the subsequently received encrypted packets, and packets may be decrypted—which is performed by Buruganahalli’s decrypt engine. POR 7, 35.

Nevertheless, PO insists that encrypted packets are never filtered in Buruganahalli. According to PO, Buruganahalli filters encrypted packets only after they have been decrypted. POR 33-37. That is wrong. Encrypted packets are filtered based on the handshake process before they are decrypted—that is how the packets get to the proxy for decryption. The processing of the unencrypted handshake messages is used to determine whether the flow’s associated destination domain is on a whitelist or a blacklist, in order to, e.g., route associated packets to the decrypt engine in the case where the firewall policy specifies a decrypt action for packets corresponding to a blacklisted domain. E.g., Buruganahalli, 9:61-67. Other traffic may be treated differently (i.e., simply passed, or blocked), depending on the corresponding firewall policy. For example, as PO acknowledges, if the

destination domain is on a whitelist, the associated encrypted traffic would simply pass without proxy processing; or, if the destination domain is on a blacklist, the associated encrypted traffic may be blocked altogether. POR, 5-6, 35. The decision to pass, block, or route for decryption an encrypted packet is a filtering step performed on that packet.

The '856 patent filters encrypted packets in the same way as Buruganahalli. Specifically, the '856 patent describes using plaintext information (*e.g.*, a destination domain) in unencrypted packets (*e.g.*, hello message) of a handshake exchange to filter associated encrypted packets. '856, 9:19-33, cls. 18, 20 (claiming the use of domain name in handshake/hello messages configured to establish an encrypted communication session in a method for packet filtering).

The handshake process disclosed in the '856 specification is described by both PO and its expert as corresponding to the “filtering” step of the Challenged Claims. For example, PO acknowledges that in the '856 specification, “Rule gate 120 using rules may filter the handshake messages based on the domain name... Similarly, rule gate 128 using rules may filter the handshake messages for establishing encrypted communication session 308.” POR, 19-20 (emphasis removed); Ex. 2026, ¶63. PO then explains, “encrypted packets are sent from host 106, *filtered* by rule gate 120 using rules, *and delivered to proxy device* 112 (step #19).” POR, 20 (emphasis added); Ex. 2026, ¶64. In sum, PO interprets its handshake process, and subsequent

routing of associated encrypted packets, as the filtering step of the claims. *Id.*; Ex. 1049, 9:19-11:10 (PO's expert testifying that column 9 of the '856 specification describes "various filtering processes"). Indeed, the '856 specification discloses that the packet-filtering system performs an action on packets—*e.g.*, "drop the packets"—after determining whether data in the associated handshake message includes a domain name corresponding to a network-threat indicator. '856, 8:65-9:12, 9:51-65, 10:2-14; Ex. 1049, 9:19-11:10 (PO's expert testifying that "various filtering processes... including... 'log or drop of the packets.'"). That disclosure, which mirrors Buruganahalli's, also describes filtering.

PO makes the unsupported argument that "Petitioner *altered its unpatentability theory*" because Petitioner used the words "based on" the handshake processing in its PPR, but the word "after" in its Petition. POR 31-32. That argument is nonsensical as a second event that is "based on" a first event necessarily comes "after" the first event. Regardless, there was no change in theory. As both the Petition and PPR uniformly showed, Buruganahalli teaches extracting a destination domain to identify a firewall policy to apply to associated encrypted traffic—and the filtering of that encrypted traffic (*e.g.*, for routing to a proxy) is based on, and comes after, that extraction of the destination domain from the handshake. Pet. 38; PPR 5. Petitioner never relied on the subsequent processing by the proxy and application of rules to decrypted packets, as meeting the claimed

“filtering” step—which the Board recognized. *E.g.*, DI, 69 (“the ‘encrypted data communications are filtered after it is determined that information extracted from the handshake traffic matches with those on a blacklist, and thus corresponds to a network-threat indicator.’”)(quoting Weissman, ¶69); DI 69-70 (for each session packets comprising unencrypted data and packets comprising encrypted data are correlated and filtered based on the hostname (destination domain) extracted from the handshake traffic, and then the correlated and filtered packets are processed separately from packets destined for other domains.”); DI, 71.

B. Consistent With Its Handshake Disclosure, Buruganahalli Expressly Teaches Filtering Encrypted Packets Based On Rules

As the foregoing makes clear, PO’s argument that Buruganahalli never filters encrypted packets according to rules, and that Petitioner identified no such teaching in Buruganahalli, fails. Buruganahalli repeatedly discloses filtering, based on a firewall policy, encrypted packets before decryption by a decrypt engine. Indeed, the Buruganahalli packets wouldn’t be at the proxy absent filtering and routing.

The trial grounds rely on the embodiments in Buruganahalli where filtering is taught by applying to packets of a session a security policy based on the destination domain associated with that session—for example, decrypting packets if the associated destination domain is on the blacklist. Buruganahalli, 7:60-67; Pet. 19, 20, 34-35, 38-39; DI, 68. Buruganahalli expressly discloses that if a destination

domain extracted from a client hello message is “not trusted or unknown,” a secure session is still established but the associated encrypted traffic is routed to the proxy (*i.e.* “decrypt engine”) to be decrypted for further analysis. Buruganahalli, 6:12-23. Buruganahalli explains that if an encrypted communication “is initially determined to be permissible based on a policy prior to the set-up of the encrypted data communication,” then the resulting encrypted traffic may be allowed, but it would be required to be “decrypted for further analysis and ***further potential filtering based on the policy.***” Buruganahalli, 6:12-23 (emphasis added); Pet. 20, 38; Weissman, ¶¶91, 135. As this disclosure of “further... filtering” makes clear, the encrypted packets have already been filtered a first time, according to the firewall policy, before any decryption by the decrypt engine. Buruganahalli, 9:61-10:4; Pet. 20, 25, 39; DI 71. Indeed, PO’s expert describes this embodiment in Buruganahalli in the same manner. *See* Ex. 2026, ¶46 (describing the operation of Buruganahalli in connection with Figure 3B—“if the destination domain is on the blacklist (or unknown because it is not on the whitelist or blacklist), the firewall may initially allow the client hello message but require decryption thereafter”).

PO also misrepresents Buruganahalli’s Figure 1 by asserting that its policy engine 120 applies policies only after receiving results from decrypting encrypted traffic. POR, 10. But Figure 1 depicts a policy check engine 106 (Buruganahalli, 9:30-32) that precedes any decryption, and the specification expressly discloses

applying a firewall policy to encrypted packets to determine whether to decrypt them at all: “As further illustrated in FIG. 1, if the monitored traffic is encrypted... the security device can be configured (e.g., based on a firewall policy) to decrypt the monitored traffic using a decrypt engine 110 (e.g., applying trusted man-in-the-middle techniques using a self-signed certificate).” Buruganahalli, 9:61-67. This passage makes clear that the firewall applies policies to encrypted packets to filter them for decryption.

The Board also recognized that Buruganahalli describes a process for filtering both the handshake traffic *and* the encrypted packets of the session. *See* DI, 71 (“For Figure 3A’s embodiment... Buruganahalli explains that by ‘parsing the handshake traffic,’ firewall 304 may ‘apply one or more firewall policies/rules... related to destination domains’ without ‘having to decrypt’ encrypted communications.””). And PO concedes that policies are applied to encrypted traffic in Buruganahalli:

[T]he cited portion of Buruganahalli explains that *a policy may cause the firewall to initially allow a session/flow and then “require[s] that the session be decrypted* for further analysis and further potential filtering based on the policy.”

POR 41 (emphasis added), 38 (“Buruganahalli’s solution to this problem is to extract a destination domain from the unencrypted handshake traffic so that *its ‘firewall policies/rules’ may be applied ‘prior to and/or without having to decrypt the encrypted secure tunnel session traffic.’*”)(emphasis added).

Nevertheless, PO cites Figure 6 of Buruganahalli to argue that policies are applied by Figure 6's decoder only after the data has been decrypted. POR 9-10, 43-44. Again, whether policies are applied after packets have been decrypted is irrelevant; the claimed filtering step occurs before the encrypted packets are decrypted—they could not be decrypted otherwise.

PO's argument that Buruganahalli's flow lookup in Figure 6 cannot perform both the identifying step and the filtering step is similarly misplaced. POR 42-43. Specifically, PO argues that because the Petition and Board point to the flow lookup for "identifying" unencrypted and encrypted packets, it is inconsistent to rely on the same "lookup" for the "filtering" step. POR 43. But the Challenged Claims do not specify that each step must be performed by a different functional component. In any event, the act of looking up a flow is not relied on for the filtering step—the flow lookup allows the security device to associate encrypted packets with unencrypted packets (e.g., from the session initiating handshake), so that the firewall policy (e.g., blacklist or whitelist) can be applied to the received encrypted packets. Buruganahalli, 14:25-28. PO's argument misrepresents the trial grounds and the Institution Decision. *See, e.g.,* DI, 69-70 ("Hence, for each session packets comprising unencrypted data and packets comprising encrypted data are correlated *and filtered* based on the hostname (destination domain) extracted from the

handshake traffic, and then the correlated *and filtered* packets are processed separately from packets destined for other domains.”)(emphasis added).

C. Buruganahalli’s Figure 3a Embodiment Together With Its Figure 3b Embodiment Teaches Filtering Encrypted Traffic And Routing It To A Proxy For Decryption, Just As Described On The ’856 Patent

PO argues that neither Figures 3A nor 3B alone teaches the claimed embodiment (POR, 35, 37-40), but Petitioner relies on the combination of these figures, not on one in isolation. Pet. 19-24, 31, 33, 39. As the Petition explains, and the Board agreed, Buruganahalli discloses using techniques according to Figure 3A’s embodiment separate or together with techniques according to Figure 3B’s embodiment. Pet. 22-23, 40 (citing Buruganahalli, 11:61-12:3, Weissman, ¶141); DI, 71 (citing Buruganahalli, 11:7–12:3).

PO accuses the Board of combining the two figures when “Petitioner never asserts a combination of Buruganahalli’s Figures 3A and 3B.” POR, 42. That is false; the combination is explicitly relied upon in the Petition. *See, e.g.*, Pet. 22-23, 40; Weissman, ¶¶94, 141. The trial grounds rely on the disclosure of Figure 3A for applying a policy to extract a destination domain in an unencrypted hello message that is used to filter the associated encrypted traffic by comparing the domain to a blacklist, and on the disclosure of Figure 3B for routing filtered encrypted traffic to a proxy (*i.e.*, a decrypt engine). Pet. 32-41.

In any event, PO admits that Buruganahalli itself suggests that the firewall may “switch” from operating according to Figure 3A to operating according to Figure 3B. POR, 42. Obviousness requires nothing more than this admitted teaching. And testimony from PO’s expert identifies explicit motivation to combine such techniques:

Buruganahalli discloses that encrypted packets must be decrypted in order to determine whether the extracted destination domain name matches the domain associated with the session’s URL “in order to detect malware that attempts to fool a hosting site by including false destination domain information.”

Ex. 2026, ¶100 (citing Buruganahalli, 8:11-24). That is, according to PO’s expert, a POSITA would have recognized that a destination domain extracted from the unencrypted handshake message may not be reliable (as taught in accordance with Figure 3A) such that encrypted traffic would be filtered for routing to the proxy for decryption (as taught in accordance with Figure 3B).

D. That Buruganahalli Also Teaches Decryption Of Encrypted Packets After Initial Filtering Does Not Distinguish The Challenged Claims

PO focuses its arguments on Buruganahalli’s teaching of applying firewall rules to decrypted packets (*i.e.*, to encrypted packets that were routed to, and then decrypted by, Buruganahalli’s decrypt engine), but nothing in the Challenged Claims excludes that unclaimed extra step decrypting encrypted packets after filtering.

To the contrary, the '856 specification describes this same unclaimed step of sending filtered encrypted packets to a proxy for purposes of decryption. The '856 specification explains that after domain name processing, the packet-filtering system “may communicate the [associated] packets to proxy device 112 via session 306” and “[p]roxy device 112 may receive the packets and decrypt the data in accordance with the parameters of session 306.” '856, 9:66-10:16.

Moreover, the '856 patent explains that such routing of encrypted packets for decryption is for malware detection. The '856 patent discloses that its proxy device comprises an ICAP (Internet Content Adaption Protocol) client that may communicate the packets to an ICAP server, where rules are applied to determine if the packets comprise data corresponding to the network-threat indicators. '856, 10:15-33. ICAP servers, as well known in the art, are used to detect malware by checking for viruses. *See, e.g.*, Ex. 1051, 10 (describing a common function of an “ICAP server” as performing “virus checking.”). This disclosure from the '856 patent is nearly identical to Buruganahalli’s disclosure of sending encrypted traffic to be decrypted by the decrypt engine (mapped as the claimed proxy) of the firewall for further malware processing. Buruganahalli, 9:61-10:4; Ex. 2026, ¶100 (citing Buruganahalli, 8:11-24). These identical disclosures in Buruganahalli and the '856 patent further demonstrate that the encrypted packets in Buruganahalli have been

filtered (as a result of the handshake processing) despite later being routed to a proxy for decryption.

III. BURUGANAHALLI TEACHES “NETWORK-THREAT INDICATORS” UNDER BOTH CONSTRUCTIONS

At Institution, the Board determined that no claim term requires construction, and that the claims should be given their ordinary and customary meaning. DI 47-48. Nonetheless, PO proposes a construction of “network-threat indicator” that differs from the Board’s construction of that same term appearing in other of PO’s patents. POR 28-29; Pet. 17. PO argues that the *Phillips* standard (applied here) mandates a different construction from the Board’s earlier construction under the Broadest Reasonable Interpretation (BRI) standard, but does not explain why. PO also fails to explain the difference, if any, between its proposed construction and the Board’s prior constructions. Regardless, any difference is inconsequential as Buruganahalli’s blacklist meets this term under both constructions.

Ignoring that the trial grounds are based on obviousness, not anticipation, PO incorrectly argues that Buruganahalli does not explicitly state that its blacklist addresses are associated with network threats and is silent on how the blacklist is formed. POR 49. But Buruganahalli expressly discloses an example where a destination domain on the blacklist is “not trusted,” Buruganahalli, 9:67-10:4, and that “the security device 402 can extract destination domain information... that can

facilitate 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.” Buruganahalli, 13:44-51; Pet. 30. Moreover, PO admits that, at minimum, Buruganahalli’s blacklist comprises domains that an administrator has identified for blocking. POR, 50. There is no reasonable dispute that an administrator would identify domains from the blacklist for blocking identified threats and vulnerabilities.

Buruganahalli further discloses that “destination domain extraction for secure protocols... includes applying a security policy based on the destination domain to filter traffic at the security device, in which the *security policy* includes a whitelist/blacklist policy...” Buruganahalli, 7:60-67 (emphasis added). Because the extracted destination domain information is compared against a blacklist as specified by a *security policy* at the security device, a POSITA would have understood, or at least found it obvious, that the blacklist contains a list of destination domains associated with network threats. See Ex. 2027, 59:5-13 (“[Column 7 of Buruganahalli] describes blacklist, destination domain is on a blacklist, and/or, of... talking about using URLs as a basis for filtering. So I think the person of ordinary skill could certainly reasonably read that as a network-threat indicator in Buru.”), 59:14-22 (“A blacklist are things you should be worried about as a potential network threat.”). PO is incorrect about the disclosures of Buruganahalli, and also ignores

what would have been obvious to a POSITA in view of Buruganahalli's undisputed teaching of using a blacklist—namely, that including network threats in the blacklist would have been obvious. Pet. 30; Weissman, ¶109.

Further rebutting PO's argument, PO's expert published a textbook in 2011 linking a blacklist to malicious traffic. He described a "*blacklist* approach, or *default-allow* ruleset" as one where "all packets are allowed through except those that fit the rules defined specifically in a blacklist" and "from a security perspective... it assumes the network administrator can enumerate all of the properties of *malicious traffic*." Ex. 1052, 22 (final emphasis added). Accordingly, there can be no reasonable dispute that a POSITA would have recognized that a blacklist is associated with network threats.

PO's argument that Petitioner's expert, Dr. Weissman, characterized Buruganahalli's blacklist as a list of domains that represent "potential threats" is both incorrect and irrelevant. POR, 50 (citing Ex. 2027, 60:12-22, 59:14-22). Dr. Weissman did not testify that the blacklist in Buruganahalli is limited to only potential network threats. For example, he testified that URLs on a blacklist "are not good" and are "a threat." Ex. 2027, 58:15-23. Moreover, neither of the proposed constructions of "network-threat indicator" distinguishes between actual and potential threats, and neither construction should be narrowed to exclude one over the other. Indeed, by their nature, threats have degrees of confidence.

Buruganahalli's blacklist contains data that indicates a plurality of "network-threat indicators," as claimed.

IV. BURUGANAHALLI TEACHES ROUTING FILTERED PACKETS TO A PROXY SYSTEM

PO first argues that Buruganahalli does not disclose routing filtered packets to a proxy system because no filtering occurs until after the packets have been decrypted. POR 53. As discussed above, this argument fails because Buruganahalli discloses filtering unencrypted and encrypted packets before they are routed to the proxy (*i.e.*, decrypt engine).

PO next argues that "Buruganahalli's decrypt engines 110, 610 are not a proxy" because they perform only decryption. POR 53-55. That argument contradicts the '856 specification and the knowledge of a POSITA. Buruganahalli's decrypt engines perform the same functions as the '856 patent's disclosed proxy that receives and decrypts encrypted packets. *Compare* '856, 10:15-16 ("Proxy device 112 may receive the packets and decrypt the data in accordance with the parameters of session 306), *with* Buruganahalli, 9:61-67 ("... the security device can be configured (*e.g.*, based on a firewall policy) to decrypt the monitored traffic using a decrypt engine 110 (*e.g.*, applying trusted man-in-the-middle techniques using a self-signed certificate)."); Pet. 40 (*citing* Buruganahalli, 9:61-67, 12:18-36); Weissman, ¶140.

PO also argues without merit that Buruganahalli's decrypt engine does not meet its construction of the term "proxy system" requiring "interven[ing] to prevent threats in communications between devices." POR, 53-54. PO points to the SSL decryption engine 610 in Figure 6 as performing decryption without intervening in communications to prevent threats. *Id.* But PO ignores the mapping in the Petition that points to Buruganahalli's decrypt engine applying trusted man-in-the-middle techniques, which intervenes in the communication between a client and remote server precisely to prevent threats via decryption. Pet. 39-40 (citing Buruganahalli, 9:61-10:4). The Petition explains that a POSITA would have understood that Buruganahalli's disclosures in connection with Figure 3B "describe a firewall containing functionality acting as a proxy for both the remote server and the client by *standing in line of their communications...*" Pet. 40-41 (emphasis added). Applying trusted man-in-the-middle techniques (*i.e.*, standing in line of communications) meets even PO's narrow construction of "interven[ing] to prevent threats in communications between devices." PO's own expert characterizes a "trusted man-in-the-middle" technique as involving "intercepting" of communications. Ex. 2026, ¶31. And Buruganahalli expressly discloses that its decryption is used "to detect malware." Buruganahalli, 8:11-24. Buruganahalli meets PO's argued-for construction, and PO simply ignores Buruganahalli's

teaching of applying trusted man-in-the-middle techniques that describe a transparent proxy function for detecting, *e.g.*, malware. Pet. 20-22, 24-25, 40-41.

There can be no reasonable dispute that a POSITA would have understood that applying a trusted man-in-the-middle technique describes the function of a proxy. Pet. 40-41; Weissman, ¶¶140-142. Indeed, PO's expert, Dr. Goodrich, cites a patent (*see* Ex. 2026, ¶31 (citing Ex. 2015 ("Chaubey"), 2:47-5:12)), explaining that a security device acts as a man-in-the middle by implementing a proxy technique. Ex. 2015, 2:66-3:2 ("When implementing the SSL forward proxy technique, the security device may split the secure session into two parts and act as a man-in-the-middle (*e.g.*, between the client device and the server device)."), 4:52-55 ("... by acting as a man-in-the-middle using the SSL forward proxy technique..."). The decrypt engine of Buruganahalli's firewall applying trusted man-in-the-middle techniques (which PO does not dispute) meets the claimed proxy, as would have been understood by a POSITA.

V. PO'S ARGUMENTS AGAINST MODIFYING BURUGANAHALLI IN VIEW OF BAEHR'S TEACHINGS (GROUND 2) ARE UNAVAILING

A. PO's Argument That The Petition Fails To Describe "How" The Combination Meets The Challenged Claims Lacks Merit

PO repeats its failed POPR argument that the Petition fails to explain "how" the combination in trial ground 2 meets the claims. *Compare* POR 55-56 *with* POPR 35-36. As the Board already recognized, the Petition specifies where each claim

element is found—trial ground 2 specifies that Buruganahalli alone teaches all limitations except [1.h] of Claims 1, 24 and 25, and the Petition further relies on the teachings in Baehr for limitation [1.h]—and the reasons for the combination. DI, 87-88 (rejecting arguments at POPR 36); Pet. 42-50.

PO's POR argument continues to be baseless. As an example of the Petition's purported lack of specificity, PO argues that the Petition "does not explain how the claimed 'routing' in Baehr's 'sending packets aside to a proxy network' [] would be [] 'based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.'" POR 57. First, that argument's framing is an attempt to attack Baehr individually, and not in the combination of the trial grounds. Second, trial ground 2 relies on Buruganahalli, not Baehr, for the determining step and the routing of the filtered packets. Baehr is cited for nothing more than its teachings about implementing a proxy system separate from a packet screening system acting as a firewall, and the advantages regarding the same. Pet. 44-48. Third, PO's arguments also improperly suggest that bodily incorporation of Buruganahalli into Baehr is required. *See, e.g.*, POR 58 ("Petitioner never states what in Buruganahalli would be implemented in Baehr's proxy system..."). Bodily incorporation is not required, and in any event the ground's foundational reference is Buruganahalli, not Baehr.

PO's argument that the Petition does not specify whether the proxy would be implemented as a physically separate device or merely a logically separate device is irrelevant. POR 58-59. The Claims do not require the proxy to be implemented in one form or the other, and either implementation meets the claim language. The only requirement is that the claimed proxy receive packets. Furthermore, a proxy is a basic component in any network system. It is merely a matter of implementation as to which approach would be desired in a given system. Arguing a lack of expectation of success to implement a decades-old computer building block according to its known function has no merit.

B. The Petition Provides Compelling Reasons Why A POSITA Would Have Combined The Teachings Of Buruganahalli And Baehr

PO next argues that the Petition does not provide a reason “why” a POSITA “would combine Buruganahalli with Baehr in the claimed manner.” POR 60-65. PO first raises the strawman argument that Baehr “does not provide a reason for offloading encryption from a firewall to a proxy” to “fix the issues with Buruganahalli.” POR 60-61. But Baehr does not need to supply such a reason: the suggestion that the art itself must provide the express teaching, suggestion, or motivation was rejected years ago. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398 (2007).

Moreover, the Petition provided multiple rationales for why a POSITA would have been motivated to modify Buruganahalli with the teachings of Baehr's separate proxy. Pet. 47-48. As Dr. Weissman testified, these advantages include preserving computer resources, achieving load balancing, maximizing performance, isolating a private network from an outsider, strengthening security, and limiting any potential security vulnerability to only one component of a larger system. Weissman ¶¶155-156. PO does not dispute these advantages, but argues that they are not advantages over Buruganahalli. POR 61. But, at the same time, PO repeatedly argues that "Buruganahalli's firewall does not route filtered packets to a proxy system." POR 52-54. Because Buruganahalli does not explicitly state that the decrypt engine of the firewall is a proxy, any stated advantage to implement a separate proxy would provide motivation to modify Buruganahalli with Baehr's teachings of routing packets to a proxy.

PO again attacks the references individually and focuses on Baehr's use of its proxy, without addressing the combination of the prior art grounds. POR 62. PO's assertion that the cost and complexity of adding a proxy system to Buruganahalli would "far outweigh any benefit," is unsupported, conclusory, and is based on bodily incorporation. POR 65. Regardless, the modification to implement the decrypt engine as a proxy would be obvious despite economic costs. *In re Farrenkopf*, 713 F.2d 714, 718 (Fed. Cir. 1983)(affirming the Board's finding that the additional

expense associated with a modification would not discourage a POSITA from seeking the advantage provided by the modification); *see also Medichem, S.A. v. Rolabo, S.L.*, 437 F.3d 1157, 1165 (Fed. Cir. 2006)(“The fact that the motivating benefit comes at the expense of another benefit, however, should not nullify its use as a basis to modify the disclosure of one reference with the teachings of another...”)(citation omitted).

VI. PO HAS NOT MET ITS BURDEN TO ESTABLISH OBJECTIVE INDICIA OF NON-OBVIOUSNESS

PO’s objective indicia of non-obviousness arguments are based on a *vacated* district court opinion, and fail for that reason alone. PO argues that “[o]bjective evidence of nonobviousness, including satisfaction of a long-felt need and industry praise, contributed to the court’s validity determination and enhanced verdict of willful infringement in the Cisco litigation.” POR 68 (citing vacated district court opinion and order). But the district court’s cited findings (ECF No. 621) in the Cisco litigation have been vacated by the Federal Circuit in their entirety. Ex. 1050, 27; *see also, id.*, 2-3 (vacating “all order and opinions of the court entered on or after August 11, 2020, including the final judgment” in Case No. 2-18-cv-00094 (EDVA)). PO’s other purported evidence fails, too.

A. PO Fails To Show That The '856 Alleged Invention Satisfied Any Long-Felt Need Or Received Substantial Industry Praise

Without merit, PO relies on a Cisco press release (Ex. 2013) as evidence of long-felt need and industry recognition and argues that “the nexus between this evidence and the '856 patent claims was [] established by way of the court’s finding that Cisco’s Encrypted Traffic Analytics technology, which claimed to solve the unsolvable problem, infringed the '856 Patent. Ex. 1027 at 30-57.” POR 68-69. But the district court’s opinion has been vacated. Other than pointing to that vacated opinion, PO made no effort to establish the requisite nexus between Cisco’s Encrypted Traffic Analytics and the Challenged Claims. Indeed, the press release describes Cisco’s Encrypted Traffic Analytics only in general terms. For example, the press release states that Cisco’s Encrypted Traffic Analytics “detect threats in encrypted traffic,” but does not state how the threat detection is performed. The article makes no reference to the '856 Patent and does not describe any claimed step or technique of the '856 Patent. And there has been no showing that Cisco’s Encrypted Traffic Analytics solution is coextensive with the Challenged Claims. *See Fox Factory, Inc. v. Sram, LLC*, 944 F.3d 1366, 1373 (Fed. Cir. 2019).

Because PO fails to establish the requisite nexus between Cisco’s Encrypted Traffic Analytics, any generic statements that such product allegedly satisfied a long-felt need or received industry praise are insufficient, as such “need” or “praise”

is not shown to be tethered to the purportedly inventive features of the '856 patent. POR 67-69.

B. PO Fails To Show Copying

PO also argues that “the district court found that the '856 Patent had been copied by Cisco” (POR 69), but again that finding was vacated and cannot provide evidence of copying. Ex. 1050, 2-3, 27. PO offers no other evidence to show alleged copying.

C. The Obviousness Of The Challenged Claims Cannot Be Overcome By Any Alleged Objective Indicia

PO argues that because Petitioner’s expert did not examine a trial transcript from the Cisco litigation, Petitioner fails to address the objective evidence of non-obviousness. POR 70-71. But the entirety of PO’s objective indicia of non-obviousness is based on a district court opinion that has been vacated. Accordingly, that opinion, and the trial transcript that led to that opinion (which is, after all, subject to credibility determinations, and some of which is under seal and not publicly available), does not provide a basis for establishing objective indicia here. PO’s attempt to shift the burden to Petitioner to rebut non-existent evidence of objective indicia fails.

Dated: November 18, 2022

Respectfully submitted,

By: /Scott A. McKeown/
Scott A. McKeown (Lead Counsel)
USPTO 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

*Attorneys for Petitioner, Palo Alto
Networks, Inc.*

CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. § 42.24(c) and (d), the undersigned hereby certify that Petitioner's Reply to Patent Owner's Response complies with the type-volume limitation of 37 C.F.R. § 42.24(c)(1) because, exclusive of the exempted portions, it contains **5,599** words as counted by the word processing program used to prepare the paper.

Dated: November 18, 2022

By: /Keyna Chow/
Keyna Chow

CERTIFICATE OF SERVICE

The undersigned certifies that the foregoing PETITIONER'S REPLY TO PATENT OWNER'S RESPONSE, was served in its entirety by filing through the Patent Trial and Appeal Case Tracking System (PTACTS), as well as providing a courtesy copy via e-mail to the following attorneys of record for Patent Owner listed below:

James Hannah (Lead Counsel)
Reg. No. 56,369
KRAMER LEVIN NAFTALIS & FRANKEL LLP
jhannah@kramerlevin.com
svdocketing@kramerlevin.com

Jeffrey H. Price (Back-up Counsel)
Reg. No. 69,141
KRAMER LEVIN NAFTALIS & FRANKEL LLP
jprice@kramerlevin.com

Jenna Fuller (Back-up Counsel)
Reg. No. 74,212
KRAMER LEVIN NAFTALIS & FRANKEL LLP
jfuller@kramerlevin.com

Bradley C. Wright (Back-up Counsel)
Reg. No. 38,061
BANNER & WITCOFF, LTD.
bwright@bannerwitcoff.com

Scott M. Kelly (Back-up Counsel)
Reg. No. 65,121.
BANNER & WITCOFF, LT.
skelly@bannerwitcoff.com

John R. Hutchins (Back-up Counsel)
Reg. No. 43,686.
BANNER & WITCOFF, LTD.
jhutchins@bannerwitcoff.com

Counsel for Patent Owner Centripetal Networks, Inc.

Dated: November 18, 2022

By: /Dara Del Rosario/
Name: Dara Del Rosario
ROPES & GRAY LLP