

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

PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	BACKGROUND	4
A.	State of the Art	4
B.	Overview of the Relied Upon References.....	4
1.	Buruganahalli	4
(a)	Buruganahalli’s Figure 3A Whitelist Embodiment Allows an Encrypted Session Without Applying Packet-Filtering Rules to Encrypted Packets	5
(b)	Buruganahalli’s Figure 3A Blacklist Embodiment Blocks a Requested Encrypted Session Before Any Encrypted Packets are Received.....	6
(c)	Buruganahalli’s Figure 3B Blacklist Embodiment Requires that Encrypted Packets be Decrypted Before Applying any Packet-Filtering Rules	7
2.	Baehr	12
C.	The ’856 Patent’s Contributions to the Art.....	14
D.	The Claims of the ’856 Patent Have Repeatedly Been Held Valid Over Prior Art that Does Not Filter Encrypted Packets and Multiple Prior Challengers Passed on Raising Buruganahalli	23
E.	Level of Ordinary Skill	26
III.	CLAIM CONSTRUCTION	26
A.	Petitioner Fails to Apply its Own Claim Construction or the District Court’s Construction of “Network-Threat Indicators”	28
B.	Petitioner Fails to Address the District Court Claim Constructions of “Proxy System”	29

IV.	THE PRIOR ART DOES NOT RENDER THE CHALLENGED CLAIMS UNPATENTABLE.....	30
A.	Buruganahalli Does Not Teach Rule-Based Filtering of Encrypted Packets	31
1.	Buruganahalli Only Applies its Firewall Rules/Policies to Unencrypted or Decrypted Data	33
2.	The Figure 3A Embodiment Does Not Involve Applying Packet-Filtering Rules to Encrypted Packets.....	37
3.	Petitioner’s Has Not Identified a Single Instance Where Buruganahalli Teaches Filtering Encrypted Packets	40
4.	Petitioner Cannot Rewrite Buruganahalli’s Decrypt-First Approach with Conclusory Statements About a Skilled Artisan’s Understanding and Obviousness	44
B.	Petitioner Has Not Shown that Buruganahalli Teaches the Claimed “Network-Threat Indicators”	49
C.	The Prior Art Does Not Teach the Claimed Routing Filtered Packets to a Proxy System	52
1.	Buruganahalli Does Not Disclose the Claimed Routing Filtered Packets to a Proxy System.....	53
2.	The Petition Provides No Reason for Why a Skilled Artisan Would Have Been Motivated to or Would Reasonably Expect Success Modifying Buruganahalli in View of Baehr ...	55
(a)	Petitioner Never Explains How the Proposed Combination Meets the Claim Elements.....	56
(b)	Petitioner Does Not Provide Any Persuasive Reason for Why a Skilled Artisan Would Implement its Vague Combination Using Baehr.....	60
(c)	Petitioner’s Vague Allegation of Expected Success Should be Rejected	66

V. OBJECTIVE EVIDENCE OF NONOBVIOUSNESS ALSO
DEMONSTRATES THAT THE CLAIMS ARE VALID 67

A. The ’856 Patent Satisfied a Long-Felt Need in the Industry and
Received Substantial Industry Praise 68

B. Cisco Copied the ’856 Patent 69

C. The Board Should Find the Challenged Claims Patentable
Because Petitioner did not Address the *Graham* Factors 70

VI. CONCLUSION.....71

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>3Shape A/S v. Align Tech., Inc.</i> , IPR2020-00222, Paper 12 (P.T.A.B. May 26, 2020)	27
<i>Apple Inc. v. Samsung Elecs. Co.</i> , 839 F.3d 1034 (Fed. Cir. 2016) (<i>en banc</i>)	69
<i>Becton, Dickenson, and Co. v. Tyco Healthcare Grp., LP</i> , 616 F.3d 1249 (Fed. Cir. 2010)	43
<i>Becton, Dickinson & Co. v. B. Braun Melsungen AG</i> , IPR2017-01588, Paper 75 (P.T.A.B. Dec. 12, 2018)	59, 61
<i>Centripetal Networks, Inc. v. Cisco Sys., Inc.</i> , 38 F.4th 1025 (Fed. Cir. 2022)	24
<i>Cisco Sys., Inc. v. C-Cation Techs., LLC</i> , IPR2014-00454, Paper 12 (P.T.A.B. Aug. 29, 2014)	66
<i>Crocs, Inc. v. Int’l Trade Comm’n</i> , 598 F.3d 1294 (Fed. Cir. 2010)	67
<i>In re Cyclobenzaprine Hydrochloride Extended–Release Capsule Pat. Litig.</i> , 676 F.3d 1063 (Fed. Cir. 2012)	67
<i>Graham v. John Deere Co.</i> , 383 U.S. 1 (1966)	56, 57, 70
<i>Hologic, Inc. v. Enzo Life Sciences, Inc.</i> , IPR2018-00019, Paper 17 (P.T.A.B. Apr. 18, 2018)	27
<i>Infinera Corp. v. Core Optical Techs. LLC</i> , IPR2018-01259, Paper 9 (P.T.A.B. Jan. 14, 2019)	27
<i>Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.</i> , 821 F.3d 1359 (Fed. Cir. 2016)	46, 49
<i>Johns Manville Corp. v. Knauf Insulation, Inc.</i> , IPR2018-00827, Paper 9 (P.T.A.B. Oct. 16, 2018)	45, 60

<i>Kingston Tech. Co., Inc. v. Imation Corp.</i> , IPR2015-00066, Paper 19 (P.T.A.B. Mar. 24, 2016)	27
<i>KSR Int'l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007)	46, 60
<i>Lectrosonics, Inc. v. Zaxcom, Inc.</i> , IPR2018-01129, Paper 33 (P.T.A.B. Jan. 24, 2020)	70
<i>Leo Pharm. Prods., Ltd. v. Rea</i> , 726 F.3d 1346 (Fed. Cir. 2013)	67
<i>LG Elec. v. Cellular Commc'ns Equip.</i> , IPR2016-00197, Paper 7 (P.T.A.B. Apr. 29, 2016)	47, 58, 62
<i>Liqwd, Inc. v. L'Oreal USA, Inc.</i> , 941 F.3d 1133 (Fed. Cir. 2019)	67, 69
<i>In re Magnum Oil Tools Int'l, Ltd.</i> , 829 F.3d 1364 (Fed. Cir. 2016)	41
<i>Medtronic, Inc. v. Teleflex Innovations S.A.R.L.</i> , IPR 2020-01341	57
<i>Metalcraft of Mayville, Inc. v. Toro Co.</i> , 848 F.3d 1358 (Fed. Cir. 2017)	47, 56
<i>Nintendo Co. v. Genuine Enabling Tech. LLC</i> , IPR2018-00543, Paper 7 (P.T.A.B. Aug. 6, 2018)	45
<i>Oracle Corp. v. Crossroads Sys., Inc.</i> , IPR2014-01207, Paper 78 (P.T.A.B. Jan. 29, 2016)	56
<i>Plantronics, Inc. v. Aliph, Inc.</i> , 724 F.3d 1343 (Fed. Cir. 2013)	67
<i>Precision Planting LLC v. Deere & Co.</i> , IPR2019-01052, Paper 91 (P.T.A.B. Dec. 31, 2020)	66
<i>Progenity Inc. v. Natera, Inc.</i> , IPR2021-00280, Paper 10 (P.T.A.B. Jun. 25, 2021)	57

Rambus Inc. v. Rea,
731 F.3d 1248 (Fed. Cir. 2013) 67

Samsung Elects. Co. v. Elm 3DS Innovations, LLC,
925 F.3d 1373 (Fed. Cir. 2019) 66

SAS Inst., Inc. v. Iancu,
138 S. Ct. 1348 (2018).....27, 41

Winner Int’l Royalty Corp. v. Wang,
202 F.3d 1340 (Fed. Cir. 2000) 59

Regulations

37 C.F.R. § 42.104(b) 27, 30, 43, 56

PATENT OWNER'S EXHIBIT LIST

Exhibit	Description
2001	U.S. Patent Application Publication No. 2005/0138353 to Spies <i>et al.</i>
2002	U.S. Patent Application Publication No. 2012/0023576 to Sorensen <i>et al.</i>
2003	U.S. Patent Application Publication No. 2004/0199629 to Bomer <i>et al.</i>
2004	U.S. Patent Application Publication No. 2015/0207813 to Reybok <i>et al.</i>
2005	U.S. Patent Application Publication No. 2014/0317397 to Martini
2006	U.S. Patent No. 6,098,172 to Coss <i>et al.</i>
2007	U.S. Patent Application Publication No. 2004/0088542 to Daude <i>et al.</i>
2008	Internet Archive WayBack Machine – Membership – Cyber Threat Alliance from: https://web.archive.org/web/20211009155735/https://www.cyberthreatalliance.org/membership/ , captured October 9, 2021
2009	Palo Alto Networks Brief – Palo Alto Networks and Cisco ACI, dated 2019
2010	Internet Archive WayBack Machine – Scott McKeown, PTAB Denies Petition Overlooking Objective Indicia of Non-Obviousness, Ropes & Gray - Patents Post-Grant (Sept. 18, 2019), available from https://web.archive.org/web/20210303015939/https://www.patentspostgrant.com/ptab-denies-petition-overlooking-objective-indicia-of-non-obviousness/ , captured March 3, 2021
2011	Transcript of Telephonic Proceedings on Motion for Sanctions, <i>Palo Alto Networks, Inc. v. Centripetal Networks, Inc.</i> , Nos. IPR2021-01520, IPR2021-01521, IPR2022-00182, dated February 10, 2022.
2012	RESERVED

Exhibit	Description
2013	Cisco Press Release, “Cisco unveils network of the future that can learn, adapt and evolve,” dated June 20, 2017 – CENTRIPETAL-CSCO 472946 – 472951, Trial Exhibit PTX-1135 – (<i>Centripetal Networks, Inc. v. Cisco Sys., Inc.</i> , No. 2:18-cv-00094 (E.D. Va.))
2014	RESERVED
2015	U.S. Patent No. 9,893,883 to Chaubey <i>et al.</i>
2016	Transcript of Bench Trial Proceedings, Vol. 2B, Pages 250-324, <i>Centripetal Networks, Inc. v. Cisco Sys., Inc.</i> , No. 2:18-cv-00094, Dkt. No. 499 (E.D. Va. May 7, 2020)
2017	Transcript of Bench Trial Proceedings, Vol. 8A, Pages 1070-1156, <i>Centripetal Networks, Inc. v. Cisco Sys., Inc.</i> , No. 2:18-cv-00094, Dkt. No. 513 (E.D. Va. May 18, 2020)
2018	Transcript of Bench Trial Proceedings, Vol. 8B, Pages 1157-1230, <i>Centripetal Networks, Inc. v. Cisco Sys., Inc.</i> , No. 2:18-cv-00094, Dkt. No. 514 (E.D. Va. May 18, 2020)
2019	Amended Complaint for Patent Infringement, <i>Centripetal Networks, Inc. v. Keysight Techs, Inc., and Ixia</i> , No. 2:17-cv-00383, Dkt. No. 192 (E.D. Va. June 13, 2018)
2020	Invalidity Chart for U.S. Patent No. 9,917,856, <i>Centripetal Networks, Inc. v. Keysight Techs., Inc., and Ixia</i> , No. 2:17-cv-00383 (E.D. Va.) CENTRIPETAL-CSCO 172221 – 349
2021	Defendants Identification of Prior Art, <i>Centripetal Networks, Inc. v. Keysight Techs, Inc., and Ixia</i> , No. 2:17-cv-00383 (E.D. Va. July 5, 2018)
2022	Expert Report of Adam Sorini Regarding Invalidity (including Appendices), <i>Centripetal Networks, Inc. v. Keysight Techs., Inc., and Ixia</i> , No. 2:17-cv-00383 (E.D. Va. July 30, 2018) – CENTRIPETALCSCO 087501 – 88046

Exhibit	Description
2023	Amended Complaint, <i>Centripetal Networks, Inc. v. Cisco Sys., Inc.</i> , No. 2:18-cv-00094, Dkt. No. 29 (E.D. Va. Mar. 29, 2018)
2024	Order, <i>Centripetal Networks, Inc. v. Cisco Sys., Inc.</i> , No. 2:18-cv-00094, Dkt. No. 68 (E.D. Va. Sept. 18, 2019)
2025	Declaration of Hannah Lee in Support of Patent Owner's Opposition to Petitioner's Motion for Joinder, <i>Cisco Sys., Inc. v. Centripetal Networks, Inc.</i> , No. IPR2022-01151 (P.T.A.B. July 22, 2022)
2026	Declaration of Michael T. Goodrich, PhD in Support of Patent Owner's Response
2027	Deposition Transcript of Dr. Jon Weissman, <i>Palo Alto Networks, Inc. v. Centripetal Networks, Inc.</i> , No. IPR2022-00182 (P.T.A.B.), taken August 19, 2022

I. INTRODUCTION

The '856 Patent, also known as the Encrypted Traffic Patent in the prior litigation involving Cisco Systems, Inc. ("Cisco"), is directed to one of Centripetal's solutions for operationalizing threat intelligence to the "unsolvable" problem of cyber-attacks embedded within encrypted packets. Ex. 2013 at 1. In order to solve this problem, Centripetal developed a technique practiced by a "threat intelligence gateway"—RuleGATE®—which applies advanced packet filtering at the network edge to protect a customer's network from threats in encrypted traffic. The RuleGATE® device leverages cyber-threat intelligence in real-time to determine, based on unencrypted data, encrypted packets that correspond to network-threat indicators, and performs rule-based filtering of those encrypted packets.

Petitioner challenges the '856 Patent based on two pieces of prior art: Buruganahalli and Baehr. Neither reference teaches or suggests such rule-based filtering of encrypted packets. Just like the art distinguished during original prosecution of the '856 Patent and in Cisco litigation, Buruganahalli requires that encrypted packets be decrypted before applying any packet-filtering rules to filter those packets. In the blacklist embodiments relied upon in the Petition, Buruganahalli explicitly and categorically discloses that "network communications between the client and the remote server **are decrypted** if the destination domain is included in a blacklist of the whitelist/blacklist policy." Ex. 1004 at 7:65-67.

Nevertheless, the panel's Institution Decision ("ID") identified uncited disclosures with respect to Buruganahalli's Fig. 3A as allegedly teaching applying packet-filtering rules to encrypted packets, alone or in an unspecified combination with the embodiment of FIG. 3B. ID at 70-71. Respectfully, however, Buruganahalli's FIG. 3A embodiment only discloses filtering **unencrypted** packets with packet-filtering rules; subsequent encrypted packets are either passed without applying any packet-filtering rules (let alone those recited in the Challenged Claims), or the secure session is blocked before it starts (in which case encrypted packets are never received in the first place).

Petitioner also fails to show that Buruganahalli teaches the claimed "network-threat indicators." Initially, Petitioner contends without analysis that the term "network-threat indicators" should be construed differently from the construction twice adopted in the Cisco and Keysight district court proceedings. More importantly, however, Petitioner does not apply **either** construction when concluding that Buruganahalli's blacklist contains "network-threat indicators." Contrary to Petitioner's conclusory assertion, Buruganahalli's blacklisted domains represent nothing more than domains that an organization has selected for restricted access.

The cited references also fail to disclose routing filtered packets to a "proxy system." Petitioner first alleges that Buruganahalli's decrypt engine is a proxy

system, but it never attempts to demonstrate that the decrypt engine satisfies the construction of this term from the earlier Cisco litigation or any other reasonable interpretation of the term. In tacit recognition that Buruganahalli does not teach a proxy system, Petitioner asserts that a POSITA would have found it obvious to modify Buruganahalli with Baehr. There are myriad problems with this backup argument, however, including that Petitioner did not (1) carry out the required *Graham* factor analysis, (2) explain how and why a POSITA would have modified Buruganahalli with Baehr, or (3) describe how its alleged combination actually maps to the claim elements. Instead, Petitioner offers conclusory assertions riven with hindsight gleaned from the '856 Patent itself.

Each of the above three reasons alone requires that the Board find the '856 Patent claims non-obvious, but to the extent that any doubt remains, the objective indicia of nonobviousness removes all doubt. Cisco Systems, Inc., which passed over Buruganahalli in its own failed attempt to invalidate the '856 Patent and which seeks nevertheless to join this proceeding, brazenly copied Centripetal's technology and presented its cribbed work as solving the long-felt and "unsolvable" problem of detecting cyberattacks in encrypted traffic. Ex. 2013 at 1; Ex. 1027 at 61-64. Copious industry praise for Centripetal's solution further illustrates the groundbreaking nature of the patented technology. The Challenged Claims are patentable.

II. BACKGROUND

A. State of the Art

Prior to the '856 Patent, detecting cyberattacks in encrypted traffic was considered “unsolvable.” Ex. 2013 at 1; Ex. 1027 at 61-64. Typical firewalls—like Buruganahalli—could only analyze unencrypted data. Ex. 2026 (“Goodrich Decl.”), ¶¶ 31-40. With the rise in popularity of encrypted communications, cyberattacks became embedded inside encrypted communications, obfuscating the cyberattacks. Goodrich Decl., ¶ 31; Ex. 1001 at 1:17-18; Ex. 2005, ¶ 0018. Conventional wisdom addressed this problem by configuring firewalls to decrypt the encrypted communications, just like Buruganahalli (*see* §IV.A.1, *infra*). Ex. 2005, ¶ 0019; Ex. 2015 at 2:47-59. These firewalls function as a man-in-the-middle, intercepting, decrypting, analyzing, and then re-encrypting the encrypted communications. Ex. 2015 at 2:47-5:12. But decryption is difficult to perform in real-time and undesirably slows down network traffic and consumes computing power. Goodrich Decl., ¶ 31; Ex. 2027 (“Weissman Tr.”) at 53:25-54:2 (“Decryption is an expensive operation, and the firewall has to process packets very quickly.”).

B. Overview of the Relied Upon References

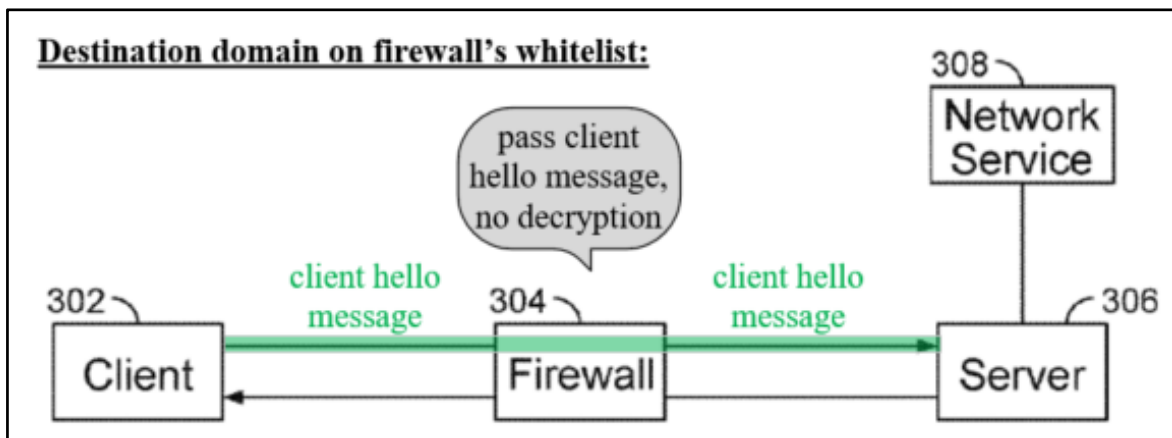
1. Buruganahalli

Buruganahalli (Ex. 1004) relates to “[t]echniques for destination domain extraction for secure protocols.” Ex. 1004, Abstract. Buruganahalli extracts the destination domain from an unencrypted client hello message of the Transport Layer

Security (TLS) protocol. *Id.* at 4:45-5:1. The unencrypted client hello message is sent by a client at the start of the TLS handshake process. *Id.* at 5:6-10, 7:19-25. The hello message includes a Server Name Indication (SNI) field indicating the destination domain. *Id.* at 4:59-5:10. Buruganahalli's firewall uses this destination domain to apply a whitelist/blacklist policy. *Id.* at 7:12-51; Goodrich Decl., ¶¶ 41-42. Buruganahalli describes three scenarios of whitelisting and blacklisting.

(a) Buruganahalli's Figure 3A Whitelist Embodiment Allows an Encrypted Session Without Applying Packet-Filtering Rules to Encrypted Packets

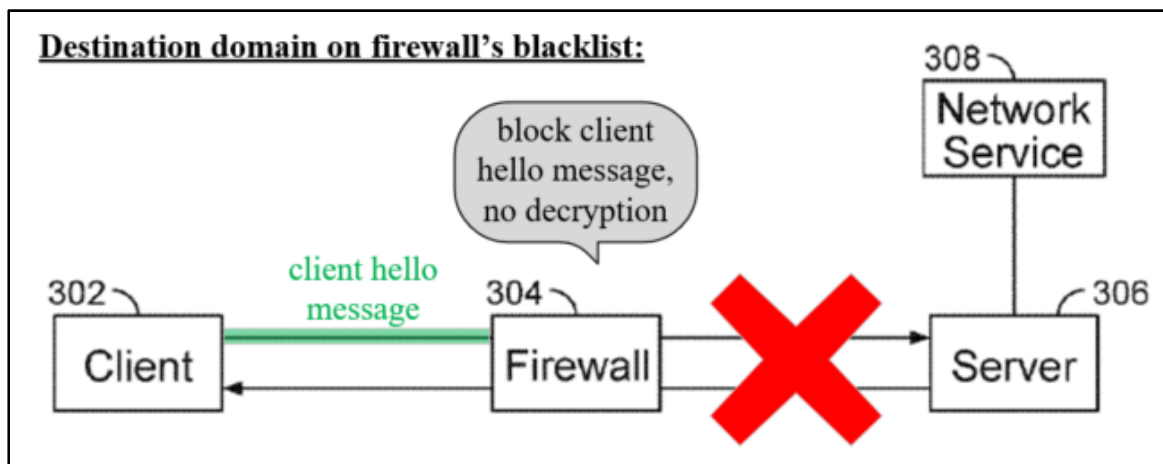
First, regarding Figure 3A (annotated below), if a destination domain is on the whitelist, the firewall allows the **client hello message** to pass through to the server and allows a secure connection to be established between the client and server. Ex. 1004 at 5:43-51, 6:1-11, 7:52-59, 10:54-11:6, 16:35-41, Fig. 3A. In this first scenario, subsequent encrypted traffic is simply forwarded without decryption or filtering. *Id.*; Goodrich Decl., ¶ 43.



Ex. 1004, Fig. 3A (annotated)

**(b) Buruganahalli's Figure 3A Blacklist Embodiment
Blocks a Requested Encrypted Session Before Any
Encrypted Packets are Received**

Second, if the destination domain is on the blacklist, the firewall blocks the unencrypted **client hello message** from passing through to the server. *Id.* at 5:64-6:11, 10:54-11:19; *see id.* at 4:31-44; Goodrich Decl., ¶ 44. Thus, no secure connection is established and no encrypted packets are received by the firewall, as depicted in annotated Figure 3A below. Ex. 1004 at 5:64-6:11, 10:54-11:19; *see id.* at 4:31-44; Goodrich Decl., ¶ 44.



Ex. 1004, Fig. 3A (annotated)

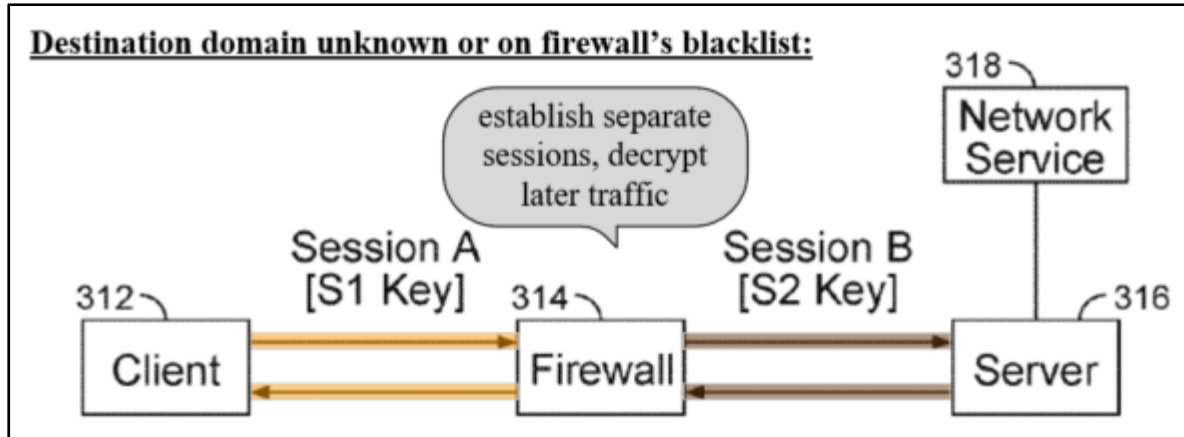
Buruganahalli thus unsurprisingly states that the firewall can apply a policy “without having to decrypt” (*id.* at 11:18) traffic because no secure, encrypted session is ever started, and no encrypted packets are received. *Id.* at 11:7-19; *see id.* at 4:31-44; Goodrich Decl., ¶ 45. Petitioner readily acknowledges this fact in its argument about how Buruganahalli discloses filtering packets comprising unencrypted data. Pet. 37-38 (arguing that unencrypted traffic is filtered “based on the determination of

whether ‘the destination domain is included in the blacklist’” which occurs “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”) (citation omitted). Buruganahalli further clarifies that because firewall 304 does not perform decryption of encrypted packets, it “cannot detect such firewall policy/rule violation(s)” (Ex. 1004 at 11:5-6) in the encrypted packets. *Id.* at 11:2-6; Goodrich Decl., ¶ 45.

**(c) Buruganahalli’s Figure 3B Blacklist Embodiment
Requires that Encrypted Packets be Decrypted Before
Applying any Packet-Filtering Rules**

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. Ex. 1004 at 6:12-38, 7:60-67, 8:25-44, 11:59-12:64. In this third scenario, the secure connection is established, but split into two sessions: **Session A** and **Session B**, as depicted in annotated Figure 3B below. *Id.* This allows the firewall to **decrypt** encrypted packets for further analysis. *Id.* at 12:29-32 (, *id.* at 12:50-55 (“[s]imilarly, traffic coming from the server is **decrypted** with the session key S2, inspected by the firewall 314, and then encrypted using the session key S1 and forwarded to the client 312”)¹; Goodrich Decl., ¶ 46.

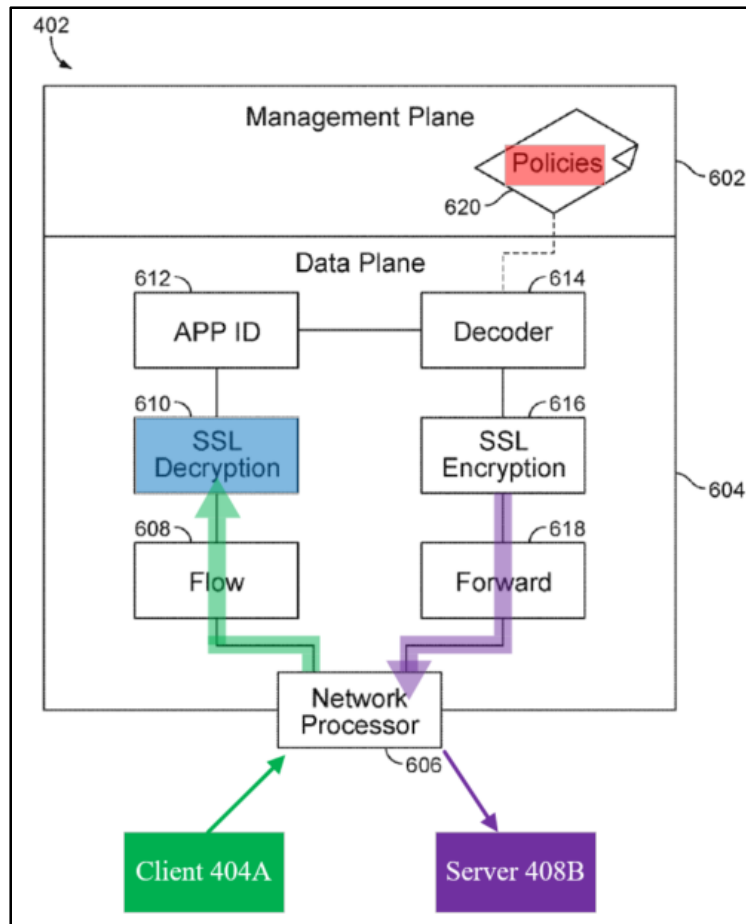
¹ Unless otherwise noted, all emphasis is added.



Ex. 1004, Fig. 3B (annotated)

None of these three scenarios involves rule-based filtering of encrypted packets. Goodrich Decl., ¶ 47. In every scenario, Buruganahalli only applies packet-filtering rules to unencrypted packets or decrypted packets. *Id.* Indeed, Buruganahalli explicitly states that “techniques for decrypting such secure communications are **needed** in order to monitor such encrypted data communications **and to apply filtering based on a policy.**” Ex. 1004 at 4:20-22; Goodrich Decl., ¶ 47.

Buruganahalli reinforces this fundamental fact about how encrypted communications were handled before the '856 Patent throughout its disclosure. For example, in Figure 6, security device 402 (*e.g.*, firewall) has a management plane storing **policies 620** and a data plane for handling packets. Ex. 1004 at 14:8-20, 14:58-60, Fig. 6; Goodrich Decl., ¶ 47.

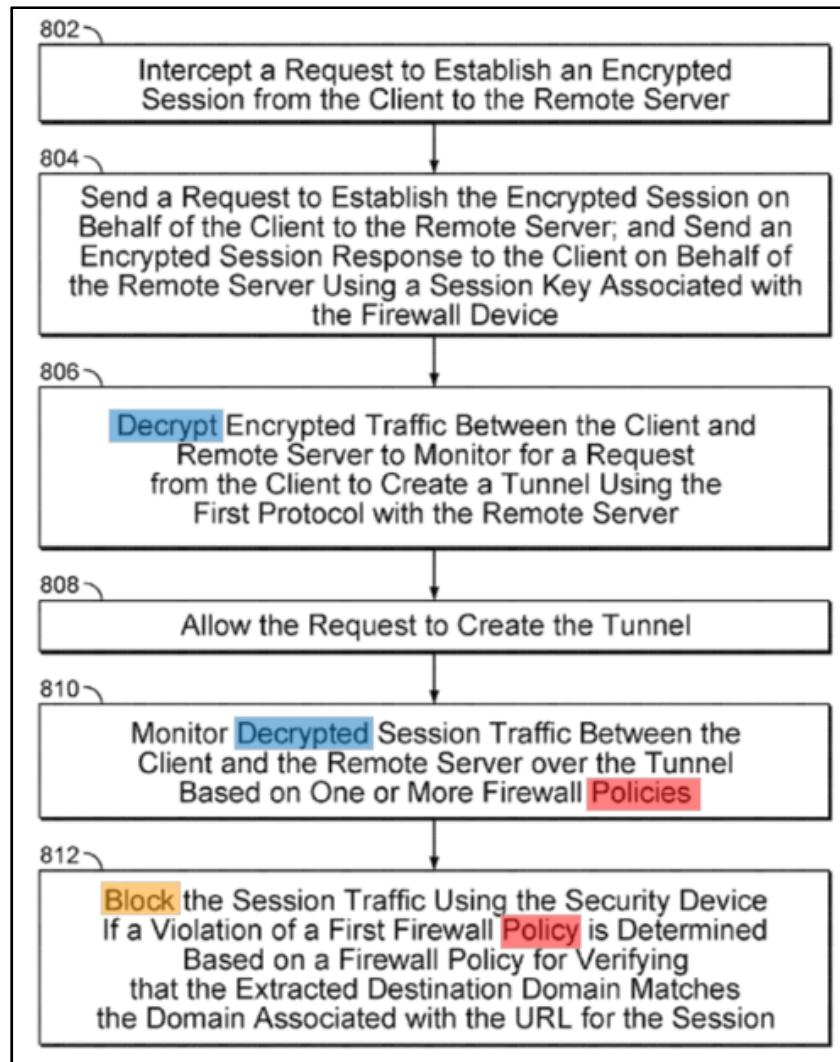


Ex. 1004, Fig. 6 (annotated)

Network processor 606 receives a packet from **client 404A** intended for **server 408B**. Ex. 1004 at 14:21-22. The packet may be assigned to a flow 608 that is newly created (*e.g.*, if the packet is an unencrypted packet for a new session/flow) or previously created (*e.g.*, if the packet is a subsequent packet like an encrypted packet) based on a flow lookup (using an IP address—not a domain name). *Id.* at 14:25-28; *see id.* at 9:25-30 (describing use of IP address); Goodrich Decl., ¶ 48; Weissman Tr. at 35:4-25 (acknowledging that a packet is correlated to a particular flow using “the IP address and port”). If an encrypted packet does not belong to a

whitelisted flow/session, it is decrypted by an **SSL decryption engine 610** before applying any policies. Ex. 1004 at 14:33-38. **Policies 620** to allow or block that decrypted data are not applied until the decrypted data is decoded by decoder 614, as evidenced by the dashed line in Figure 6 connected to the decoder. Goodrich Decl., ¶ 48; Ex. 1004 at 14:50-58, 14:21-22, Fig. 6; *see id.* at 9:44-10:28, Fig. 1 (policy engine 120 applies policies after receiving results from decrypting and decoding encrypted traffic).

Finally, regarding Figure 8, Buruganahalli provides a flow diagram showing that encrypted traffic is **decrypted** and the **decrypted** traffic is monitored using **policies**, which may result in **blocking** the traffic. Ex. 1004 at 15:22-45, Fig. 8; Goodrich Decl., ¶ 49.

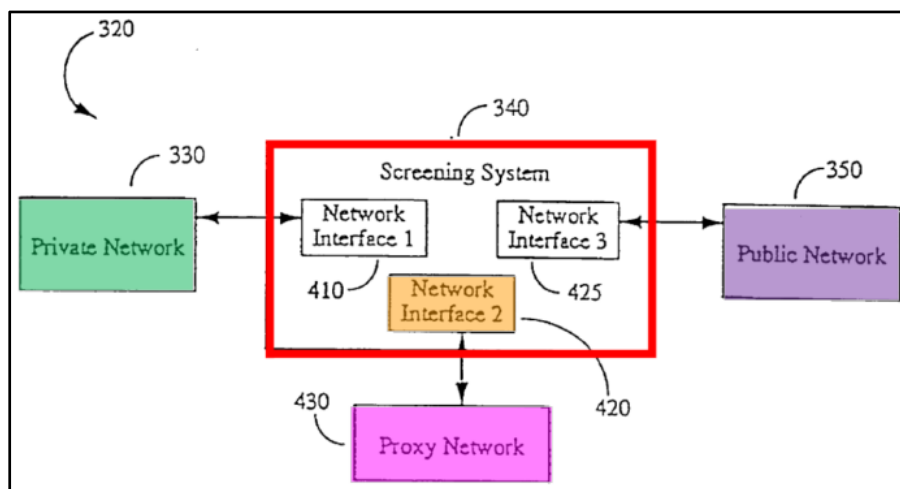


Ex. 1004, Fig. 8 (annotated)

In every instance Buruganahalli only applies policies to unencrypted packets or decrypted data—never to encrypted packets. Goodrich Decl., ¶ 50. Decryption is fundamental to Buruganahalli's firewall, which is designed to split a secure session so the firewall can act as a man-in-the-middle to decrypt encrypted packets. Ex. 1004 at 4:16-22, 11:59-13:4, claims 1, 6-10.

2. Baehr

Baehr (Ex. 1005) relates to a system for screening packets transmitted between a **private network** and a **public network**. Ex. 1005 at Abstract, 1:9-17, 2:10-17, Fig. 5 (annotated below). Baehr describes adding **network interface 420** to **screening system (or “screen”) 340** for coupling it to **proxy network 430**. *Id.* at 3:51-64; Goodrich Decl., ¶ 51.

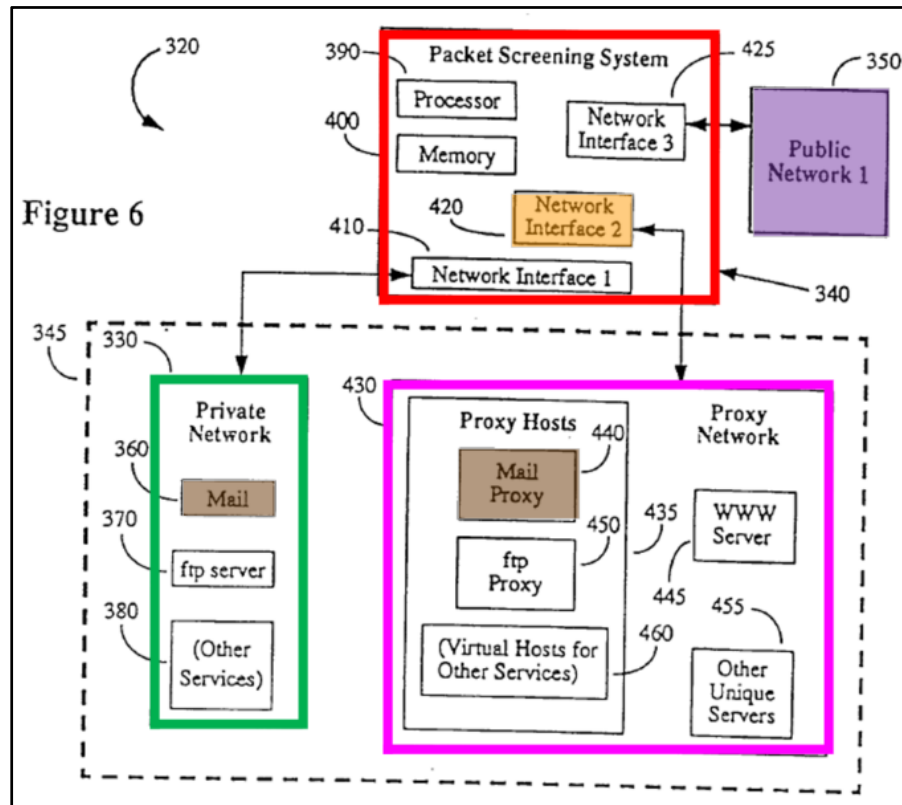


Baehr, Fig. 5 (annotated)

Packets received at the **screening system** (e.g., from the **public network**) are allowed, dropped, or sent to a host on the **proxy network**. *Id.* at Abstract, 10:46-49.

Baehr's Figure 6 provides a more detailed view of **screen 340**. *Id.* at 4:12-63, Fig. 6. A proxy host (e.g., **mail proxy 440**) of **proxy network 430** mirrors a host (e.g., **mail host 360**) on **private network 330** to perform functions as though it is

the private network host to which packets are destined. *Id.* at Abstract, 4:26-63, 8:13-17, 8:36-46; Goodrich Decl., ¶ 52.



Baehr, Fig. 6 (annotated)

There is nothing remarkable about Baehr's use of a proxy as compared to other proxy systems considered during prosecution. Goodrich Decl., ¶ 53. Baehr does not disclose the proxy performing decryption. *Id.* Baehr does not describe rule-based filtering of encrypted packets. *Id.* These deficiencies contribute to Baehr's failure to cure Buruganahalli's deficiencies and Petitioner's failure to properly combine Baehr with Buruganahalli. See §IV.C.2, *infra*.

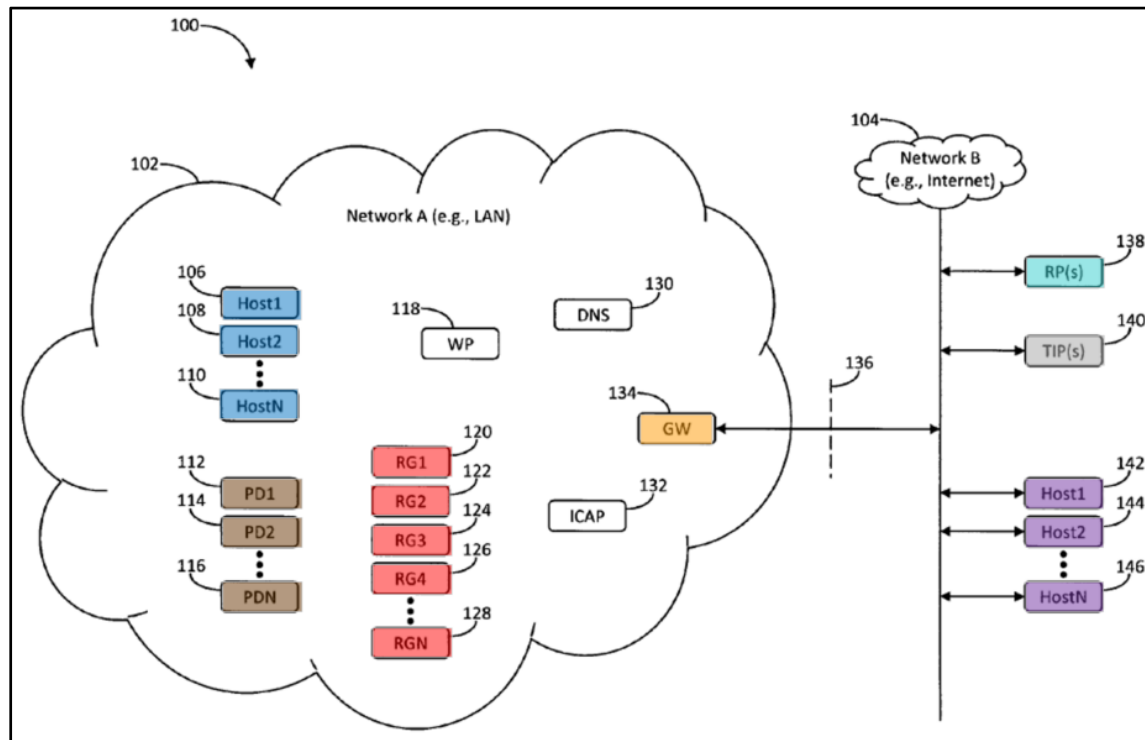
C. The '856 Patent's Contributions to the Art

Prior to the '856 Patent, firewalls either filtered unencrypted packets to block certain secure sessions before they started or decrypted encrypted packets in order to filter the decrypted data, as in Buruganahalli. Goodrich Decl., ¶ 54; Ex. 1004 at 11:2-6. With the '856 Patent's inventive approach, rule-based network-threat detection of encrypted packets is performed on encrypted traffic without decryption. Goodrich Decl., ¶ 54; Ex. 1001 at 9:66-10:14, 11:51-65.

The '856 Patent reconfigures rules based on encrypted-packet log data that otherwise would not be collected because, *e.g.*, under prior approaches, the secure session would be blocked before encrypted packets were received. Goodrich Decl., ¶ 55; Ex. 1001 at 14:4-18, 20:22-27, 22:18-19, 23:58-62, Figs. 3A-6B. The '856 Patent's approach of filtering encrypted packets accounts for possible rule updates that are received after a secure session is initiated. Ex. 1001 at 14:19-16:26 (describing use of reconfigured rules), 22:20-51 (same). This added flexibility gives firewalls and other network devices the ability to: (1) end a secure session that is later deemed to be a threat per an updated rule, or (2) allow a secure session to pass through without any further processing per an updated rule that indicates the secure session is not a threat. Goodrich Decl., ¶ 56; Ex. 1001 at 14:19-16:26, 22:20-51. means the device can prevent too much data from being extracted by bad actors if the secure session turns out to be a threat and, similarly, harm from a nascent threat

may be neutralized or reduced by blocking the flow mid-stream. Goodrich Decl., ¶ 56.

Figure 1 (annotated below) depicts an illustrative environment using the inventive approach to protect network 102 from threats in network 104. *Id.* at 2:20-34, Fig. 1.

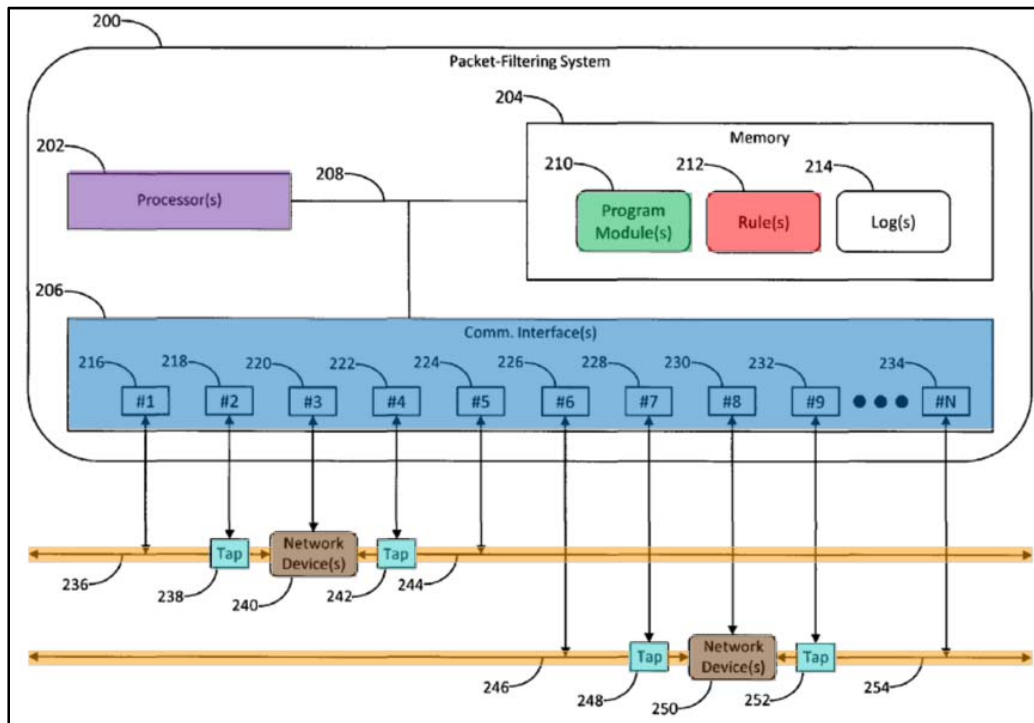


Ex. 1001, Fig. 1 (annotated)

As shown, **gateway 134** interfaces network 102 with network 104. *Id.* at 2:50-53. Network 102 includes one or more **hosts 106, 108, 110** for communicating with one or more **hosts 142, 144, 146** in network 104. *Id.* at 2:39-56. Network 102 also includes **proxy devices 112, 114, 116** and **rule gates 120 122, 124, 126, 128**. *Id.* at 2:39-43. The rule gates receive data indicating network-threat indicators (e.g.,

domain names) from **rule providers 138** based on reports from **threat-intelligence providers 140**. *Id.* at 3:65-4:9. Using this data, the **rule gates** configure rules to control a packet-filtering system. *Id.* at 4:16-21; Goodrich Decl., ¶ 57.

An illustrative packet-filtering system 200 is depicted in Figure 2 (annotated below).

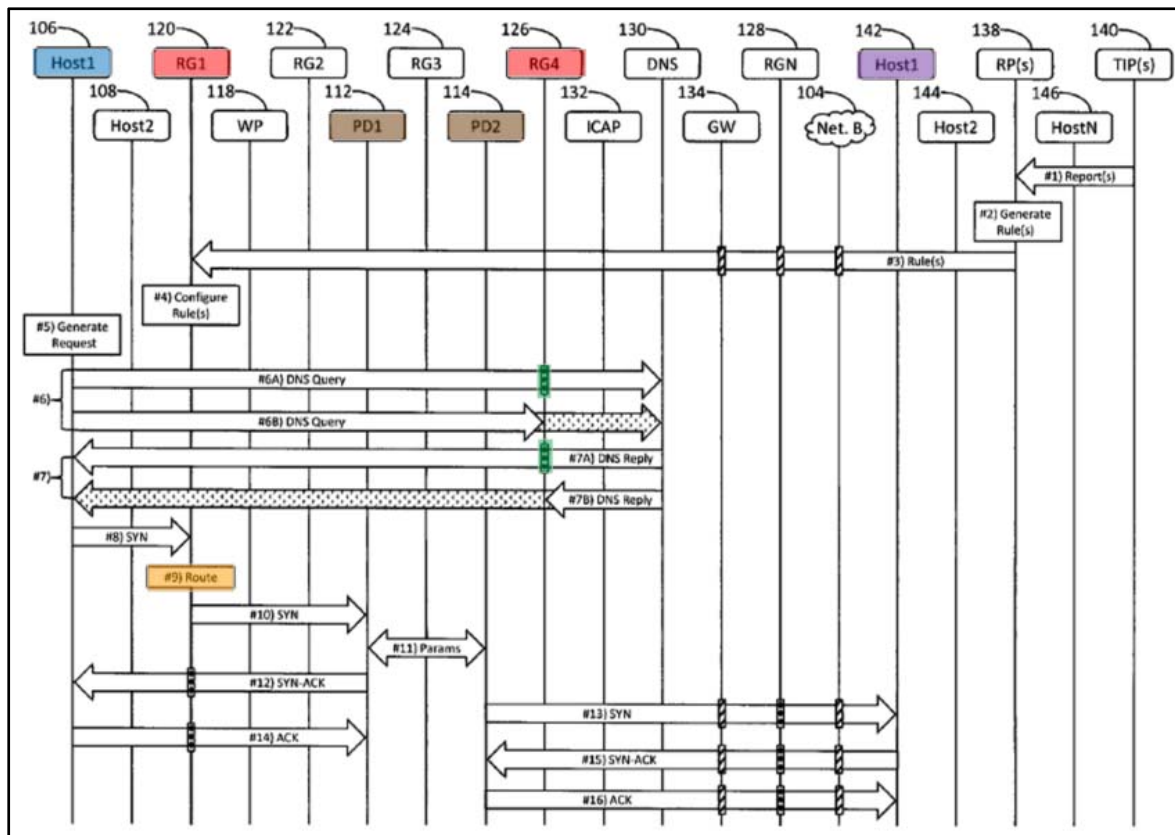


Ex. 1001, Fig. 2 (annotated)

Packet-filtering system 200 includes **processor(s) 202** for executing **program module(s) 210** for performing rule-based network-threat detection using **rules 212**. Ex. 1001 at 2:66-3:14. It also includes a **communication interface 206** for interfacing with **communication links 236, 244, 246, 254** directly or indirectly through **tap devices 238, 242, 248, 252** or **network devices 240, 250**. *Id.* at 3:15-

56. The **rules 212** are deployed throughout the system so that filtering is performed by various devices (e.g., tap device 238). *Id.*; Goodrich Decl., ¶¶ 58-59.

Figures 3A-3C, 4A-4C, 5A-5B, and 6A-6B show different event sequences to illustrate exemplary capabilities of the system. Ex. 1001 at 1:64-67. Regarding Figures 3A-C, the '856 Patent teaches **rule gate 120** receiving data (step #3) and configuring packet-filtering rules (step #4). *Id.* at 3:65-4:21, Fig. 3A (annotated below).

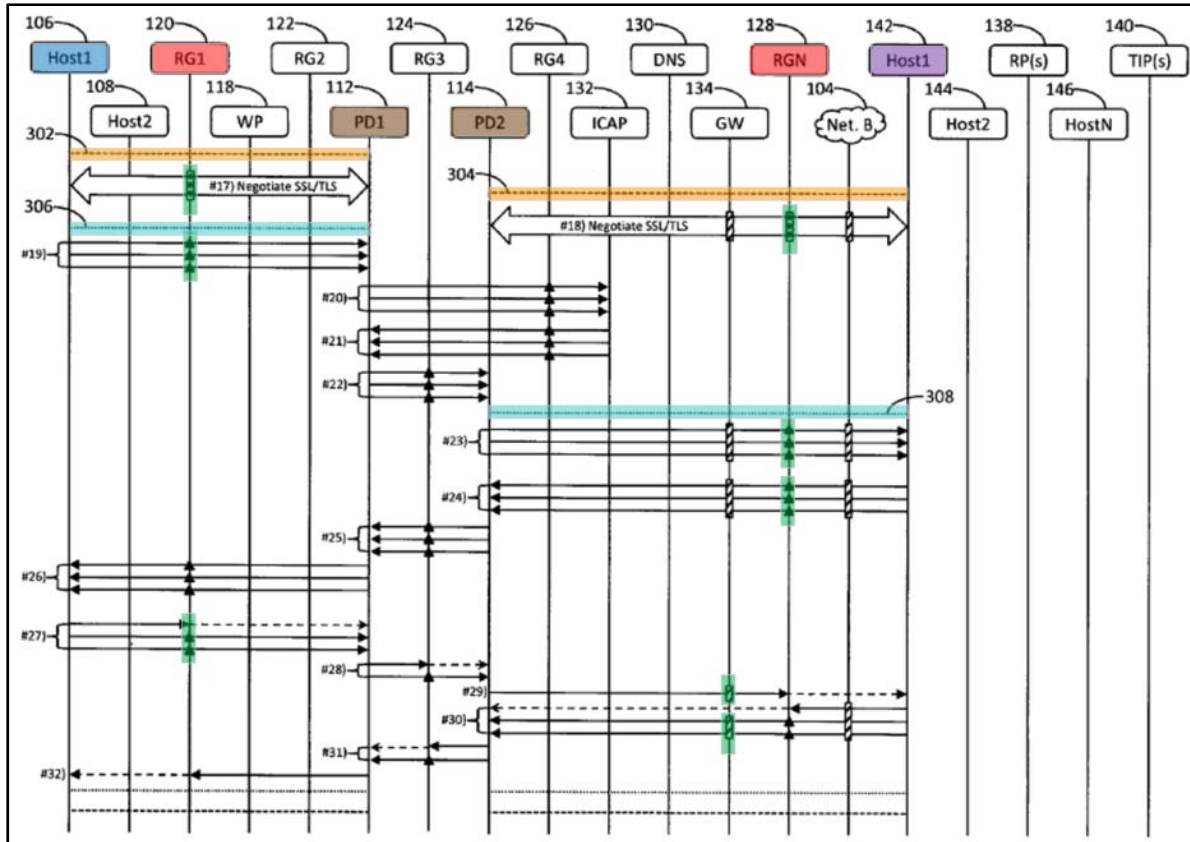


Ex. 1001, Fig. 3A (annotated)

When a user of **host 106** (e.g., personal computer) requests a webpage associated with a domain name (step #5), a DNS query including the domain name

is transmitted to a domain name system (DNS) (step #6) which responds with a DNS reply (step #7) providing a network address (*e.g.*, for **host 142**) associated with the domain name. *Id.* at 4:22-5:9. The packet-filtering system, specifically **rule gate 126** in this example, **filters** the DNS query or DNS reply. *Id.* at 4:28-6:16. Assuming the DNS reply is received, **host 106** sends (step #8) a SYN message (a Transmission Control Protocol (TCP) handshake message). *Id.* at 6:17-21. The packet-filtering system, specifically **rule gate 126**, **routes** (steps #9-10) the SYN message to **proxy device 112** based on the packet-filtering rules. *Id.* at 6:33-7:32.

After receiving the SYN message, **proxy device 112**, in conjunction with **proxy device 114**, sets up two separate connections (steps #11-16): **connection 302** (*e.g.*, a TCP connection) between **the proxy system** and **host 106** and **connection 304** (*e.g.*, another TCP connection) between **the proxy system** and **host 142**. *Id.* at 7:33-8:64, Figs. 3A, 3B (annotated below).



Ex. 1001, Fig. 3B (annotated)

Handshake messages are exchanged over both connections 302 and 304 to establish two separate encrypted communication sessions (steps #17-18): **encrypted communication session 306** (e.g., SSL/TLS session) between the **proxy system** and **host 106** and **encrypted communication session 308** (e.g., another SSL/TLS session) between the **proxy system** and **host 142**. *Id.* at 8:65-9:65, Fig. 3B. These handshake messages include, e.g., a client hello message having unencrypted data, such as a domain name. *Id.* at 9:16-33. **Rule gate 120** using rules may **filter** the handshake messages based on the domain name. *Id.* at 9:16-33. Similarly, **rule gate**

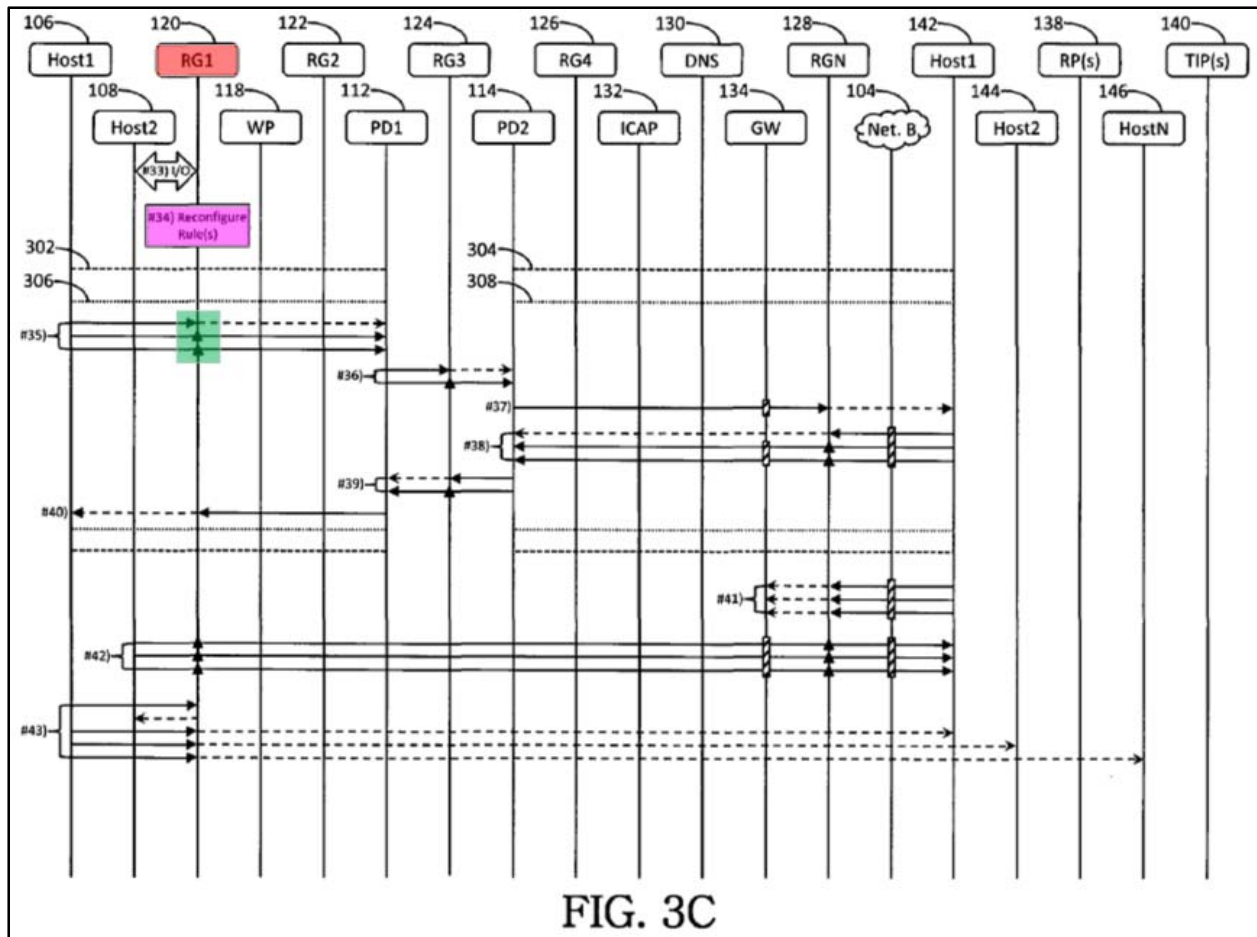
128 using rules may **filter** the handshake messages for establishing encrypted communication session 308. *Id.* at 9:47-65; Goodrich Decl., ¶¶ 61-63.

Once **encrypted communication sessions 306, 308** are established, encrypted packets may be communicated in those sessions. Goodrich Decl., ¶ 64. For example, encrypted packets are sent from **host 106**, **filtered** by **rule gate 120** using rules, and delivered to **proxy device 112** (step #19). Ex. 1001 at 9:66-10:14. This filtering includes correlating the encrypted packets with previous packets (*e.g.*, previous unencrypted packets) determined to comprise data corresponding to network threat indicators and then logging or dropping the encrypted packets. *Id.* at 10:2-14. Even though an encrypted packet may be passed by **rule gate 120** at the beginning of a secure session (step #19), **rule gate 120** continues to **filter** encrypted packets and may later drop another encrypted packet of that session (step #27). *Id.* at 12:28-42. Similar **filtering** is performed by **rule gate 128** on encrypted packets during encrypted communication session 308 (steps #23, 24, 29, 30). *Id.* at 11:36-65, 12:58-13:22. Notably, these filtering steps use rules to filter encrypted packets without decryption—an important difference over Buruganahalli as it was during prosecution and the Cisco litigation. Goodrich Decl., ¶ 65.

This difference is captured by each independent claim. For example, representative claim 1 recites “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;**” and “**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**: ...**the determined packets comprising the encrypted data** that corresponds to the one or more network-threat indicators.” *Id.* at 25:24-45 (claim 1). This rule-based filtering of encrypted packets marks a significant advancement over the prior art. Goodrich Decl., ¶ 66.

The data logged from filtering encrypted packets (as shown above in Figure 3B) can be used to **reconfigure rules** (step #34), as shown in Figure 3C (annotated below). Ex. 1001 at 14:4-18, Figs. 3B, 3C (annotated below).



Ex. 1001, Fig. 3C (annotated)

This improves cyberthreat analysis by enabling **rule gate 120** to act on updated rules. Goodrich Decl., ¶ 67. Indeed, Figure 3C shows **rule gate 120** **filtering** based on the reconfigured rules to drop an encrypted packet after the secure session is established (step #35). Ex. 1001 at 14:19-34.

The rule-based filtering of encrypted packets is not the only claimed difference, though. As discussed below (IV.B-C, *infra*), the prior art also fails to disclose or teach “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.” *Id.* at 25:46-49 (claim 1).

D. The Claims of the '856 Patent Have Repeatedly Been Held Valid Over Prior Art that Does Not Filter Encrypted Packets and Multiple Prior Challengers Passed on Raising Buruganahalli

Two highly resourced, sophisticated parties have passed over Buruganahalli when defending against their infringement of the '856 Patent. Centripetal served its complaint asserting the '856 Patent on Keysight Technologies, Inc. on June 13, 2018. Ex. 2019 at 60, 82. Keysight elected Buruganahalli as one of its 24 prior art references and served invalidity contentions, mapping disclosures from Buruganahalli against the challenged claims.² Ex. 2020; Ex. 2021 at 2. Keysight's expert also considered Buruganahalli in his expert report. Ex. 2022 at 9. Yet, in tacit recognition of the significant flaws with Buruganahalli (*see* §IV, *infra*), Keysight and its expert dropped Buruganahalli entirely and proceeded to trial with other art. Ex. 2022 at 3, 284-351.

² Keysight cited U.S. Patent No. 9,419,942, Buruganahalli's (Ex. 1004) parent application with a nearly identical disclosure. The reference to U.S. Patent No. 7,185,356 in Ex. 2020 appears to be a typographical error.

After Cisco brazenly copied Centripetal's patented technology following private disclosure meetings with Centripetal (Ex. 1027 at 150-151), Centripetal was forced to initiate an action to enforce its patents, including the '856 Patent. Ex. 2023. Cisco opted to try validity of the '856 Patent in district court instead of an IPR. Ex. 2024. Cisco was provided with Keysight's invalidity contentions and expert reports, including their analysis of Buruganahalli. Ex. 2025³. Like Keysight, Cisco passed over Buruganahalli and the chance to file any IPR, instead opting to pursue its self-characterized "best" system-based prior art (IPR2022-01151, Paper 2 (Pet.) at 25) through trial. Ex. 1027 at 57-67. Cisco lost its "best" possible invalidity case after an extensive trial, where the '856 Patent was found both not invalid and willfully infringed by Cisco. *Id.* at 166. Cisco never challenged the judge's validity findings with respect to the '856 Patent on appeal. *Centripetal Networks, Inc., v. Cisco Sys., Inc.*, 38 F.4th 1025, 1028, 1040 (Fed. Cir. 2022).

Cisco's "best" prior art was Cisco's earlier Stealthwatch product. Cisco, a multi-billion dollar company and one of the largest players in the network security space, had access to an abundance of relevant prior art—including Buruganahalli—

³ Keysight's invalidity chart for the '856 Patent and the Expert Report of Adam Sorini regarding invalidity are filed concurrently in this proceeding as Exhibits 2020 and 2022, respectively.

and believed this was the strongest prior art to the '856 Patent. The court found—consistent with the prosecution history—that Cisco's prior art lacked “the functionality to identify threats in encrypted traffic **without** the use of decryption.” Ex. 1027 at 61. The court ultimately concluded that “Cisco has failed to present clear and convincing evidence that the '856 Patent is invalid for anticipation and obviousness” because “[t]he prior art does not disclose the functionality to identify encrypted packets and then make determinations based on unencrypted information within those packet headers and flows.” *Id.* at 65. Indeed, Cisco recognized the groundbreaking nature of Centripetal's solution as it characterized its 2017 version of Stealthwatch—which post-dates its meetings with Centripetal—as solving the “unsolvable” problem with the “first and only solution in the industry that can detect malware in encrypted traffic without any decryption using Encrypted Traffic Analytics.” *Id.* at 62-64.

The prosecution history tells a similar story. During prosecution, Patent Owner distinguished prior art (Spies) for only filtering unencrypted data: “antispam filtering and other content-based filtering of Spies is applied to a scanned and unencrypted version of a message” with additional processing (*e.g.*, spam filtering and security policy enforcement) “performed on the decrypted message.” Ex. 1002 at 1365. In allowing the claims, the examiner specifically considered another reference, Reybok (*id.* at 1389-90), which also describes performing decryption

before filtering. Ex. 2004 at ¶¶ 0068-0069, Fig. 6B. The examiner also considered U.S. Patent Application Publication 2014/0317397 (“Martini”) (Ex. 2005) and the International Search Report and Written Opinion from related international application PCT/US2016/067111. Ex. 1002 at 1340, 1346-47, 1395, 1398. As the Board recognized in the Institution Decision (*see* ID at 42-43), Martini does not teach the claimed “filtering...the determined packets comprising the encrypted data” because it decrypts encrypted messages before inspection. This is the same defect in Buruganahalli. *See* §IV.A, *infra*.

E. Level of Ordinary Skill

The field of art is computer network security. Ex. 1001 at 1:7-20, 2:20-64. A person of ordinary skill in the art (“POSITA” or “skilled artisan”) at the time of the invention would have had a bachelor’s degree in computer science or a related field, and either 2 or more years of industry experience and/or an advanced degree in computer science or a related field. Goodrich Decl., ¶¶ 26-30.

III. CLAIM CONSTRUCTION

Petitioner has not met its burden to address multiple district court claim constructions of “network-threat indicators” and “proxy system.” Nor did Petitioner attempt to apply its own claim construction of the term “network-threat indicator” to its analysis of Buruganahalli’s blacklisted domains, which do not represent “identity of a resource associated with a network threat.”

A petition must identify “[h]ow the challenged claim is to be construed” and “[h]ow the construed claim is unpatentable” and “specify where each element of the claim is found in the prior art.” 37 C.F.R. §§ 42.104(b)(3)-(4). By failing to apply Petitioner’s own claim construction or address two district court claim constructions, the Petition violates 37 C.F.R. §§ 42.104(b)(3) and 42.104(b)(4); *see Infinera Corp. v. Core Optical Techs. LLC*, IPR2018-01259, Paper 9 at 9-14 (P.T.A.B. Jan. 14, 2019) (failure to comply with §§ 42.104(b)(3)-(4) are “reason enough to deny the petition”); *Hologic, Inc. v. Enzo Life Sciences, Inc.*, IPR2018-00019, Paper 17 at 6-10 (P.T.A.B. Apr. 18, 2018) (failure to explain how challenged claims are unpatentable under Petitioner’s construction “does not satisfy 37 C.F.R. § 42.104(b)”); *3Shape A/S v. Align Tech., Inc.*, IPR2020-00222, Paper 12 at 12-16 (P.T.A.B. May 26, 2020) (impossible to “discern from the Petition how Petitioner is applying its proposed constructions and those of the [ITC] ALJ” in violation of the rules); *Kingston Tech. Co., Inc. v. Imation Corp.*, IPR2015-00066, Paper 19 at 31-33 (P.T.A.B. Mar. 24, 2016) (final written decision finding that Petitioner has not met its burden to prove claims unpatentable for violation of §§ 42.104(b)(3)-(4)). The Board cannot cure this failure of compliance post-institution. *SAS Inst., Inc. v. Iancu*, 138 S. Ct. 1348, 1357 (2018) (“[P]etitioner’s contentions . . . define the scope of the litigation all the way from institution through to conclusion.”).

A. Petitioner Fails to Apply its Own Claim Construction or the District Court's Construction of "Network-Threat Indicators"

Petitioner asserts that only one term—"network-threat indicators"—"needs to be construed" and that "[a]ll other terms should be accorded their plain and ordinary meaning." Pet. 17. Petitioner urges the Board to adopt a construction for this term from another IPR proceeding involving U.S. Patent No. 9,413,722. *Id.* (citing Ex. 1026 at 8-10). Petitioner ignores that the '722 Patent does not have the same specification as the '856 Patent and that the term was construed in that case under the broadest reasonable interpretation standard rather than the *Phillips* standard applied in district courts and before the P.T.A.B. (for petitions filed after November 13, 2018).⁴ Moreover, the construction urged by Petitioner is not the same as that used in the Cisco litigation—another fact Petitioner ignores:

District Court's Construction	Petitioner's Construction
Indicators of packets associated with network threats, such as network addresses, ports, domain names, uniform resource locators (URLs), or the like.	Indicators that represent the identity of a resource associated with a network threat.

Compare Pet. 17 with Ex. 1027 at 39. Petitioner offers no explanation for diverging from the district court's construction, which followed a *Markman* hearing specific to the '856 Patent, in favor of another construction for a different patent entirely.

⁴ The '856 Patent incorporates by reference the parent of the '722 Patent.

Petitioner does not address the district court's or its own proposed construction when applying the prior art to the term. *See, e.g.*, Pet. 29-30. This is a fatal flaw, and the Board does not even need to reach a construction of this term to reject Petitioner's challenge. Whether the Board adopts the district court's construction or Petitioner's new construction, however, the Petition still fails to show that destination domains on Buruganahalli's blacklist are "network-threat indicators" under any construction of that term. *See* §IV.B, *infra*.

**B. Petitioner Fails to Address the District Court Claim
Constructions of "Proxy System"**

Petitioner ignores that the term "proxy system" was previously construed twice, offers no construction of its own, and fails to explain how the prior art discloses a proxy system under any reasonable construction of the term. Once again, Petitioner's failure to explain how the cited references disclose a proxy system as the term is properly construed provides sufficient basis for the Board to reject Petitioner's challenge.

The district courts in the Cisco and Keysight litigations (*Centripetal Networks, Inc. v. Keysight Technologies, Inc.*, Civil Action No. 2:17-cv-383 (E.D. Va. Jul. 20, 2017)) construed "proxy system" to mean "a proxy system which intervenes to prevent threats in communications between devices." Ex. 1027 at 39; Ex. 1030 at 33-34, 36. Despite this construction being in two of its own exhibits (Exhibits 1027 and 1030), Petitioner has not addressed this known construction in

violation of 37 C.F.R. §§ 42.104(b)(3)-(4). Simply put, the prior art does not teach the claimed “routing, by the packet-filtering system, filtered packets to a proxy system...” Indeed, Petitioner fails to explain how Buruganahalli allegedly teaches such a proxy system.

Tellingly, Petitioner cites to Baehr for its disclosure of a traditional proxy system, but Baehr's description of proxy network 430 including proxy hosts 435 “acting as a proxy for” hosts on private network 330 does not cure Buruganahalli's defect with respect to the “proxy system” and Petitioner's combination has other flaws, including that there is no motivation to combine Baehr's proxy network with Buruganahalli. See Goodrich Decl., ¶¶ 117-34; Ex. 2006 at 1:43-48; §IV.C.2, *infra*. Regardless whether the Board adopts the district courts' construction or applies the plain and ordinary meaning, Buruganahalli, alone or in combination with Baehr, fails to teach “routing, by the packet-filtering system, filtered packets to a proxy system” as claimed. See §IV.C, *infra*.

IV. THE PRIOR ART DOES NOT RENDER THE CHALLENGED CLAIMS UNPATENTABLE

Only independent claims 1, 24, and 25 are challenged and each challenged claim has similar limitations including: (1) “filtering” based on information specified by packet-filtering rules “the determined packets comprising the encrypted data;” (2) “network-threat indicators;” and (3) “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.” See, e.g., Ex. 1001, Claim 1. Petitioner has not shown that any of these limitations were taught by the prior art—Buruganahalli and Baehr—or would have otherwise been obvious to a skilled artisan. Goodrich Decl., ¶ 77.

A. Buruganahalli Does Not Teach Rule-Based Filtering of Encrypted Packets

Buruganahalli does not teach rule-based filtering of encrypted packets, as recited in each of the Challenged Claims. ’856 Patent, Claim 1 (“filtering... the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators”). Just like the art considered during prosecution of the ’856 Patent and during the Cisco and Keysight litigations, Buruganahalli expressly requires that encrypted packets be decrypted prior to applying its firewall policies/rules. See Ex. 1004 at 7:39-51 (disclosing a whitelist/blacklist embodiment in which “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”), *id.* at 7:60-67 (same).

In response to Patent Owner’s Preliminary Response, which pointed out this fatal flaw, Petitioner *altered its unpatentability theory*. See Paper 9 (“PPR Reply”) at 5 (“Stated simply, the Challenged Claims do not rely on use of decryption to detect threats in encrypted traffic; nor does the Petition’s mapping to Buruganahalli. That is, filtering **based on the handshake processing** of

Buruganahalli—not decryption—is mapped to the claimed filtering limitations.”). This theory was not presented in the Petition. Pet. at 38 (arguing that “the firewall filters encrypted data communications after a determination that the handshake traffic corresponds to a network-threat indicator”).

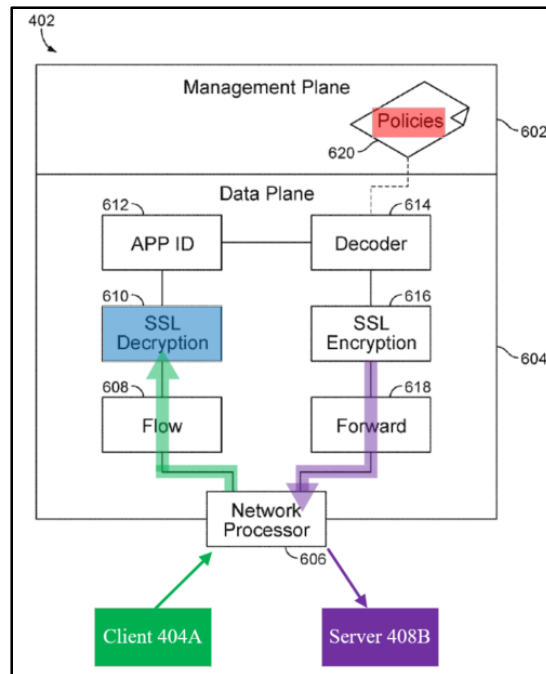
As discussed below, each citation in support of this statement refers to the firewall policies/rules that are applied to encrypted packets only after those packets have been decrypted. See §IV.A.3, *infra*. More importantly, Petitioner’s new theory fails because encrypted packets are not filtered utilizing packet-filtering rules at any point during the handshake processing. See §IV.A.3, *infra*. Indeed, Petitioner’s expert acknowledged that the alleged “rule” Petitioner now relies on to meet the claimed filtering of encrypted packets involves matching an IP address and port number to a flow table rather than any of the criteria that must be in the packet filtering rule to meet the challenged claims.⁵ Weissman Tr., at 28:18-22, 35:4-25. Buruganahalli does not teach this limitation under Petitioner’s original theory, the unrelated ground relied upon in the ID (regarding Buruganahalli’s Fig.

⁵ Those criteria from the rules are: “at least one of a uniform resource identifier (URI)”; “data indicating a protocol version”; “data indicating a method specified”; “data indicating a request”; or “data indicating a command.” Ex. 1001, Claim 1.

3A), or Petitioner's new flow analysis theory, first presented in Petitioner's Reply to Patent Owner's Preliminary Response.

1. Buruganahalli Only Applies its Firewall Rules/Policies to Unencrypted or Decrypted Data

Petitioner exclusively relies on Buruganahalli for the claimed "filtering" of encrypted data. Specifically, Petitioner equates Buruganahalli's firewall policies/rules, including the blacklist policy, to the claimed "plurality of packet-filtering rules." See Pet. 29-30. Petitioner specifically cites to policies 620 in Buruganahalli's Figure 6. *Id.* at 29 (citing Ex. 1004 at 14:58-60, Fig. 6). But **policies 620** (annotated in **red** below) are used by decoder 614 after decryption is performed by **SSL decryption engine 610**. Ex. 1004 at 14:8-15:3, Fig. 6. These policies are also never applied to encrypted packets during the "handshake processing" that Petitioner now argues corresponds to the claimed "filtering." PPR Reply at 5; see §IV.A.4, *infra*.

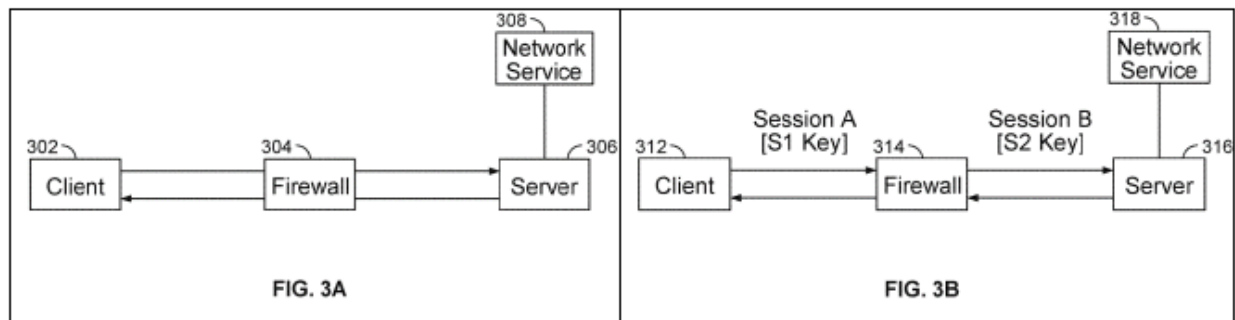


Ex. 1004, Fig. 6 (annotated)

When encrypted packets are received by Buruganahalli's security device 402 (*e.g.*, a firewall), security device 402 performs decryption before using these policies for filtering. *Id.*; *see id.* at 12:29-32 (explaining that, in Fig. 3B, after setting up Sessions A and B, "any data that is communicated from the client 312 to the firewall 314 is decrypted using a session key S1 and is then inspected by the firewall 314"). Buruganahalli's policy-based filtering is performed on **decrypted** data, not "packets comprising encrypted data" as claimed.⁶ Goodrich Decl., ¶¶ 79-82.

⁶ If the received packet is unencrypted, then decryption would not be necessary and **SSL decryption engine 610** would not be used. Ex. 1004 at 14:37-38. Either way, only unencrypted/decrypted packets are filtered. Goodrich Decl., ¶ 82, n.5.

Buruganahalli never describes rule-based filtering of encrypted packets. *Id.* Instead, Buruganahalli illustrates two separate embodiments, neither of which uses rules to filter encrypted packets: (1) using policies to filter unencrypted packets (*i.e.*, hello messages) without needing decryption (Fig. 3A); and (2) using policies to filter data only after decrypting encrypted packets (Fig. 3B):



Ex. 1004, Figs. 3A (left) and 3B (right)

Id. at 10:54-13:4, Figs. 3A, 3B; Goodrich Decl., ¶ 83. Indeed, the Board correctly acknowledges that “Figure 3B’s embodiment differs from Figure 3A’s embodiment.” ID at 70. These figures cover the three scenarios of whitelisting based on an unencrypted packet (Fig. 3A), blacklisting and blocking a session before it starts (Fig. 3A), and blacklisting based on an unencrypted packet but allowing and decrypting the subsequent encrypted session (Fig. 3B). *See* §II.B.1, *supra*.

Instead of performing policy-based filtering of encrypted packets, Buruganahalli discloses splitting the secure session and performing man-in-the-middle decryption to apply its policies to **decrypted** data. Goodrich Decl., ¶ 84; Ex. 1004 at 8:45-54, 9:61-10:9, 11:59-12:61, 15:22-45, Figs. 3B, 8. This is because

firewall 304 “typically cannot decrypt the encrypted secure tunnel session traffic and, thus, cannot detect such firewall policy/rule violation(s)” (Ex. 1004 at 11:4-6) without this approach. *Id.* at 11:2-6, Fig. 3A; Goodrich Decl., ¶ 85. This decrypt-first approach is consistent with other portions of Buruganahalli describing this same process. Ex. 1004 at 5:62-6:1 (“if a new flow . . . violate[s] a policy prior to the set-up of the encrypted data communication . . . , then the flow can be blocked and decryption is not required”), 5:24-51 (early application of policy to the SNI extension of an unencrypted hello message so “the rest of the stream can be forwarded without any decryption”), 7:1-9 (no decryption required because the firewall uses “the SNI field [of unencrypted hello message] for applying a policy”), 7:45-47 (communications “are not decrypted if the destination domain is included in the whitelist”); Goodrich Decl., ¶ 85.

Buruganahalli repeatedly and universally states that decryption is needed to monitor encrypted packets. For example, Buruganahalli describes that “techniques for decrypting such secure communications are needed in order to monitor such encrypted data communications and to apply filtering based on a policy.” Ex. 1004 at 4:19-22; *see id.* at 4:51-55 (destination domain information in encrypted data determined by “waiting until application data associated with the flow is decrypted”). There are numerous similar statements of decryption occurring before filtering based on policies throughout Buruganahalli. *Id.* at 6:17-22, 7:7:39-51, 8:1-

54, 9:61-10:9, 11:66-12, 12:29-32, 12:52-55, 12:59-61, 14:33-36, 14:60-15:3, 15:30-37, cl. 1 (communications “are decrypted” to verify that the destination domain extracted from the unencrypted client hello matches another domain), cl. 7 (“decrypt a monitored encrypted network communications”), cl. 8 (“decrypt encrypted traffic”); Goodrich Decl., ¶¶ 86-87.

There is no dispute that Figure 3B only involves applying policies to decrypted packets. Ex. 1004 at 11:59-12:64, Fig. 3B. The Board rightly acknowledges this fact. ID at 70-71 (“Buruganahalli explains that ‘any data that is communicated from the client 312 to the firewall 314 is decrypted [. . .] and is then inspected by the firewall 314,’ e.g., ‘to monitor the session traffic for firewall policy/rule compliance.’”) (citing Ex. 1004 at 12:29–32, 12:42–44).

2. The Figure 3A Embodiment Does Not Involve Applying Packet-Filtering Rules to Encrypted Packets

In view of the Petition failing to show that Buruganahalli’s firewall policies/rules are applied to encrypted packets, the panel turned to Figure 3A’s embodiment,⁷ relying on a statement that policies are applied “without ‘having to decrypt’” encrypted communications. ID at 71 (discussing applying rules to “hello message[s]”) (citing Ex. 1004 at 11:7-19); *see id.* at 22, 41, 53. Respectfully, the

⁷ Petitioner never maps any disclosures related to Figure 3A to filtering encrypted packets. *See* Pet. at 38-39 (citing no disclosures from Ex. 1004 at 10:54-12:3).

Board misunderstood this embodiment, which was not cited by the Petitioner and was not supported by any of its expert's testimony.

In the Figure 3A embodiment, packet-filtering rules are never applied to encrypted packets, *with or without* decryption. Goodrich Decl., ¶¶ 88-89. In particular, Buruganahalli discloses that the “typical firewall” of Figure 3A “typically cannot decrypt the encrypted secure tunnel session traffic and, thus, cannot detect such firewall policy/rule violation(s).” Ex. 1004 at 11:4-6; *see id.* at 10:57-61. 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.” *Id.* at 11:17-19. This technique, which is explained more fulsomely earlier in Buruganahalli, refers to the firewall's ability to determine whether a new flow “violate[s] a policy *prior to the set-up* of the encrypted data communication” (Ex. 1004 at 5:65-66) so that “the flow can be blocked and decryption is not required” (*id.* at 5:67-6:1), whereas the session is allowed without any filtering of encrypted packets if the domain is trusted. *See id.* at 7:52-59 (“a session associated with the network communications between the client and the remote server are not decrypted if the destination domain is included in a whitelist of the whitelist/blacklist policy.”).

Thus, Buruganahalli's disclosure of a typical firewall applying policies to secure protocol communications "prior to and/or without having to decrypt the encrypted secure tunnel session traffic" does not mean that any packet-filtering rules satisfying the "filtering" limitations are applied to encrypted packets. Goodrich Decl., ¶ 90 (quoting Ex. 1004 at 11:17-19). Instead, the policies are applied to **unencrypted** packets before an encrypted session ever begins (*i.e.* prior to beginning the encrypted session), making decryption entirely because the session is either allowed without subjecting the encrypted packets to any filtering or blocked before any encrypted packets are received unnecessary (*i.e.* without having to decrypt encrypted packets). Goodrich Decl., ¶ 90. Specifically, the firewall applies a policy to an unencrypted hello message⁸ and then decides whether to prevent the entire encrypted session before it ever begins, and if the session is allowed, encrypted packets are passed without decryption or filtering. Ex. 1004 at 10:57-61 ("In that session, a typical firewall can initially just inspect the handshake traffic (e.g., the initial negotiation to setup a secure communication channel/tunnel between a client and a remote server), as all the application data is encrypted."); *see also id.* at 4:16-44, 5:24-6:1, 10:54-11:58; Goodrich Decl., ¶ 90.

⁸ Petitioner admits a hello message is unencrypted. Pet. 30 (relying on hello message as "unencrypted data"); Ex. 1004 at 5:27-35.

The policies in Figure 3A are thus applied “prior to and/or without having to decrypt” any encrypted traffic, but also without applying packet-filtering rules to encrypted packets. Ex. 1004 at 11:17-19 (“prior to and/or without having to decrypt” encrypted packets”), 4:34-47 (policy-based filtering is “prior to the set-up of the encrypted data communication”); Goodrich Decl., ¶ 91 (discussing Ex. 1004 at 11:7-19). Because Buruganahalli only applies policies to unencrypted packets to block a secure session before encrypted packets are received or to decrypted data, Buruganahalli does not teach the claimed rule-based filtering of encrypted packets.

3. Petitioner's Has Not Identified a Single Instance Where Buruganahalli Teaches Filtering Encrypted Packets

Petitioner does not cite a single instance in Buruganahalli that involves “filtering” encrypted packets with packet-filtering rules. To illustrate, Petitioner relies on a short passage in Buruganahalli as allegedly disclosing the claimed filtering of encrypted data communications. Pet. 38 (citing Ex. 1004 at 4:16-22). But even that portion of Buruganahalli states that “encrypt[ed] data communications” (Ex. 1004 at 4:17-18) in secure protocols must be decrypted before filtering: “techniques for decrypting such secure communications are needed in order to monitor such encrypted data communications and to apply filtering based on a policy.” *Id.* at 4:20-22.

Petitioner next represents that Buruganahalli discloses filtering “encrypted data communications after a determination that the handshake traffic corresponds to

a network-threat indicator” and furthering monitoring “encrypted data communications . . . for filtering based on a firewall policy.” Pet. 38 (citing Ex. 1004 at 6:12-39). But, again, the 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.” Ex. 1004 at 6:21-22.

In its institution decision, the panel turned to other portions of Buruganahalli for allegedly reaching the filtering of encrypted packets. See ID at 69 (citing Ex. 1004 at 8:55-60, 11:47-51, 14:21-33, 14:50-55). As an initial matter, the Board cannot attempt to cure the Petition in this manner. *SAS Inst.*, 138 S. Ct. at 1357 (“[P]etitioner’s contentions . . . define the scope of the litigation all the way from institution through to conclusion.”); *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1381 (Fed. Cir. 2016). (“[W]hile the PTO has broad authority to establish procedures for revisiting earlier-granted patents in IPRs, that authority is not so broad that it allows the PTO to raise, address, and decide unpatentability theories never presented by the petitioner and not supported by record evidence.”).

Nevertheless, not one of these four portions of Buruganahalli discloses filtering encrypted packets based on any rule criteria. Ex. 1004 at 8:57-60 (“inspection of the session traffic” can include “possibly encrypted data communications” but this says nothing about filtering using rules or whether packets

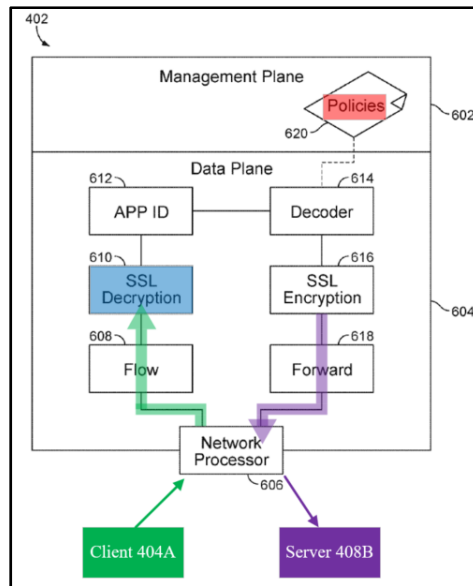
are decrypted first), *id.* at 11:47-51 (discussing unencrypted hello messages), *id.* at 14:21-33 (discussing an unencrypted TLS handshake (*i.e.*, client hello message)), *id.* at 14:50-55 (discussing decoder 614 and the TLS handshake). As explained above, the claimed “filtering” must be “based on” criteria “specified by the plurality of packet-filtering rules.” The institution decision repeatedly uses ellipses to omit the “based on” rule criteria and thus overlooks this limitation when evaluating these disclosures. ID at 68-69; *see id.* at 21-22, 40-41, 43.

Although Petitioner never asserts a combination of Buruganahalli's Figures 3A and 3B, the institution decision ostensibly combines them, alleging: “Buruganahalli discloses using techniques according to Figure 3A's embodiment separately or together with techniques according to Figure 3B's embodiment.” ID at 71 (citing Ex. 1004 at 11:7-12:3). But Buruganahalli merely suggests that firewall 304 may switch from operating as shown in Figure 3A's embodiment (filtering unencrypted packets or just passing encrypted packets if whitelisted) to operating as shown in Figure 3B's embodiment (splitting the secure session to perform man-in-the-middle decryption). Ex. 1004, 6:12-38, 7:39-67, 8:25-54, 9:61-10:4, 11:59-12:64; Goodrich Decl., ¶¶ 92-93. This still does not fix the issue though, as neither Figure 3A or 3B filter encrypted packets using policies. *Id.* at ¶ 93.

The panel also incorrectly relied on Buruganahalli's flow lookup related to the TLS handshake and operation of decoder 614 in Figure 6. ID at 69 (citing Ex.

1004 at 14:21-33, 14:50-55). As an initial matter, the Petition and Board's institution decision both point to Buruganahalli's flow lookup for limitations [1.b] and [1.c] of "identifying" unencrypted and encrypted packets, respectively. Pet. 30-32; ID at 60-62. It is inconsistent and contrary to the doctrine of attributing different meaning to different claim terms to rely on Buruganahalli's flow lookup for the separate step of "filtering." See *Becton, Dickenson, and Co. v. Tyco Healthcare Grp., LP*, 616 F.3d 1249 (Fed. Cir. 2010) ("Where a claim lists elements separately, "the clear implication of the claim language" is that those elements are "distinct component[s]" of the patented invention"). If it was truly Petitioner's position that the flow lookup satisfied the claimed "filtering" step, it was incumbent on Petitioner to explain how its position overcame this "clear implication" and demonstrate that Buruganahalli's flow lookup satisfied the claims as properly construed. 37 C.F.R. §§ 42.104(b)(3)-4). Petitioner did neither. Indeed, this theory makes no sense in the context of the Challenged claims because there is an intermediate "determining" step that must occur for the identified packets prior to the "filtering the determined encrypted packets" with the claimed packet-filtering rules. See Ex. 1001 at Claim 1, 24, and 25; Goodrich Decl., ¶ 94.

As shown in Figure 6, Buruganahalli's flow lookup 608 is performed on encrypted packets without applying **policies**, **decryption engine 610** decrypts the encrypted packets, and then decoder 614 applies **policies** to the decrypted data:



Ex. 1004, Fig. 6 (annotated)

Id. at 14:8-15:3, Fig. 6. Buruganahalli never discloses (and the Petition never asserts) that flow lookup uses policies to filter encrypted packets. *See, e.g.,* Ex. 1004 at 14:25-33.

In no instance does Buruganahalli apply its policies to encrypted packets. And neither the Petition nor the institution decision identify any contrary disclosure. Goodrich Decl., ¶ 95. Buruganahalli always decrypts encrypted packets before applying its policies. *Id.*

4. Petitioner Cannot Rewrite Buruganahalli's Decrypt-First Approach with Conclusory Statements About a Skilled Artisan's Understanding and Obviousness

In tacit recognition that Buruganahalli does not disclose filtering encrypted data, Petitioner tries twice to fill this gap: by first making conclusory statements about a skilled artisan's understanding and second alleging a motivation to rewrite

Buruganahalli. *See* Pet. 38-39. But Petitioner cites no supporting evidence beyond similar conclusory statements in its expert declaration. Ex. 1003, ¶¶ 134-135. Conclusory assertions are legally insufficient. *Johns Manville Corp. v. Knauf Insulation, Inc.*, IPR2018-00827, Paper 9 at 13-14 (P.T.A.B. Oct. 16, 2018) (informative).

Petitioner first attempts to turn to a skilled artisan's understanding to gap-fill Buruganahalli. Petitioner states that “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).” Pet. 38. This conclusory statement ignores that the claims require filtering encrypted data based on specific rules and that Buruganahalli's “packets communicated as part of a secure session” are decrypted before any policy-based filtering. *See* Ex. 1004 at 11:2-6, 12:29-32, 12:59-61, 15:35-45.

Petitioner also makes another unsupported statement that the destination domain in the handshake message and encrypted data are correlated: “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.” Pet. 38; *Nintendo Co. v. Genuine Enabling Tech. LLC*, IPR2018-00543, Paper 7 at 24 (P.T.A.B. Aug. 6, 2018)

("[Petitioner's] only support is a conclusory statement without any evidentiary support, which has no weight."). Buruganahalli itself dispels Petitioner's unsupported, hindsight-driven correlation argument via its disclosure 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. 1004 at 8:20-22; Goodrich Decl., ¶¶ 96-100.

Petitioner next falls back to obviousness. Obviousness requires "a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007). Petitioner bears the burden to demonstrate "that a skilled artisan would have been motivated to combine the teachings of the prior art references to achieve the claimed invention, and that the skilled artisan would have had a reasonable expectation of success in doing so." *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1367-68 (Fed. Cir. 2016) (citation omitted). Petitioner does not meet this burden.

Petitioner contends that "a POSITA would have been motivated and found it obvious in view of 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.” Pet. 38-39. There are four problems with this rationale. Goodrich Decl., ¶ 101.

First, Petitioner’s contention that a skilled artisan would be motivated “to monitor transmission, into or out of a protected network, of data that potentially presents a security risk” does not point in the direction of the Challenged Claims. Buruganahalli *already* monitors encrypted traffic into and out of a protected network via the old method of decrypting encrypted traffic when the destination domain indicates that the traffic is a potential threat. This argument is not, therefore, a motivation or reason for “how and why” a skilled artisan would modify Buruganahalli to apply the claimed packet-filtering rules to encrypted packets. *See Metalcraft of Mayville, Inc. v. Toro Co.*, 848 F.3d 1358, 1367 (Fed. Cir. 2017) (grounds must explain “how or why the references would be combined to arrive at the claimed invention” or “we are left with only hindsight bias that KSR warns against.”)(citation omitted). Petitioner provides no reason for how or why a skilled artisan would deviate from that solution. *LG Elec. v. Cellular Commc’ns Equip.*, IPR2016-00197, Paper 7 at 7-9 (P.T.A.B. Apr. 29, 2016) (obviousness lacked sufficient reasons for “why a person of ordinary skill would turn to [the secondary reference] for the teaching of an element that, according to Petitioner, is already taught by [the primary reference].”).

Second, Petitioner's purported motivation ignores the key limitation in the filtering step, which requires the filtering of encrypted packets to be "based on" information specified by the claimed rules. Petitioner's argument does not mention this criteria at all, soeven if Petitioner's stated rationale is adopted—and it should not be—Petitioner's obviousness theory does not address "policy" based filtering of data in encrypted packets. In other words, Petitioner has provided no reason for why or how a skilled artisan would apply the claimed packet-filtering rules to filter encrypted packets without first decrypting the packets, as Buruganahalli teaches.

Third, and telling of its failure to explain why or how a skilled artisan would modify Buruganahalli to arrive at the claimed rule-based filtering of encrypted packets, Petitioner does not provide any assertion that a skilled artisan would have reasonably expected success in making its vague modification to Buruganahalli. As discussed below, objective indicia of nonobviousness demonstrates that the problem of detecting threats in encrypted communications session was an considered an "unsolvable" problem, right up to the moment that Cisco copied and incorporated Centripetal's technology into its Stealthwatch product. *See* § V.B, *infra*. All of the prior art asserted against the '856 Patent to date, Buruganahalli included, discloses the same approach: decrypt the encrypted communications to determine whether the communications pose a threat. *See* §§II.D and IV.A, *supra*. Buruganahalli admits

that as of its filing date, such threats could not be detected without decryption. Ex. 1004 at 11:2-6; Goodrich Decl., ¶¶ 102-04.

This lack of a proper motivation or rationale to modify Buruganahalli and failure to allege a reasonable expectation of success is fatal to Petitioner's obviousness ground. *Intelligent Bio-Sys.*, 821 F.3d at 1367-68. Buruganahalli does not disclose applying filtering rules to encrypted packets, as recited in the Challenged Claims. Petitioner also has not shown that it would have been obvious to modify Buruganahalli to practice the Challenged Claims.

B. Petitioner Has Not Shown that Buruganahalli Teaches the Claimed “Network-Threat Indicators”

All three challenged claims also recite “network-threat indicators” multiple times. Ex. 1001, Claims 1, 24, 25. Petitioner has not applied the district court's or even own construction of this term. Regardless, Petitioner has not shown the prior art discloses “network-threat indicators” because Buruganahalli does not teach that the destination domains on its blacklist indicate network threats. Goodrich Decl., ¶ 105.

Petitioner relies on the destination domains on Buruganahalli's blacklist for the “network-threat indicators.” Pet. 29-30, 32-34. Buruganahalli, however, never characterizes the blacklist as being associated with network threats and is silent as to how the blacklist is formed. See Goodrich Decl., ¶ 106. Buruganahalli merely describes that the destination domains on the blacklist are used to decide whether to

block or decrypt packets. Ex. 1004 at 5:64-6:38, 7:39-67, 10:54-11:19, cl. 6. Buruganahalli does not teach that the blacklisted destination domains indicate network threats. Goodrich Decl., ¶ 106.

Rather than representing the “identity of a resource associated with a network threat” (per Petitioner’s construction) or “packets associated with network threats, such as network addresses, ports, domain names, uniform resource locators (URLs), or the like” (per the district court’s construction). Buruganahalli’s blacklist is simply a list of domains that a network administrator has identified for monitoring or blocking. Goodrich Decl., ¶ 107; Ex. 1004 at 5:64-6:38; Ex. 2006 at 1:25-36; Ex. 2007, ¶ 0007 (an access control lists (ACL) “is a list of entries that grant or deny specific access rights to individuals or groups”). In fact, Petitioner’s expert characterized Buruganahalli’s blacklist as a list of domains that represent ***potential*** threats:

I think if -- in the full scope of Buru, because one of the potential actions to take on encrypted packets that might relate to HTTP sessions or SSL sessions is to decrypt and look for concerning patterns. To me, then, the domain name, URI, is -- Buru is -- the blacklists in question here are **potential** network threats. Because it's not necessarily blocking every blacklist. Handshake, all right, some are going through and then we do deeper analysis, there is deeper analysis in some cases.

Weissman Tr. at 60:12-22; *id.* at 59:14-22 (testifying that Buruganahalli does not disclose that blacklisted domains are a threat).

Unable to located invalidating prior art, Petitioner once again attempts to fill Buruganahalli's gap with a conclusory statement about a skilled artisan's supposed knowledge:

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 a 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.'

Pet. 30 (citing Ex. 1004 at 13:43-52). But the relied upon portion of Buruganahalli merely describes using security device 402 (which includes the firewall) to report destination domains to a security service cloud 410 remote from the firewall. Goodrich Decl., ¶¶ 108-09. It is the security service cloud 410—not Buruganahalli's firewall having the blacklist—that identifies threats, vulnerabilities, etc. *Id.* Buruganahalli does not teach or disclose security service cloud 410 providing the destination domains that it identifies as network threats to Buruganahalli's firewall for inclusion on the blacklist. *Id.*

As Petitioner has failed to show that Buruganahalli teaches the claimed “network-threat indicators,” none of the challenged claims should be canceled.

C. The Prior Art Does Not Teach the Claimed Routing Filtered Packets to a Proxy System

Each challenged claim recites “[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” (the “routing step”). Ex. 1001, Claims 1, 24, 25. But Buruganahalli’s firewall does not route filtered packets to a proxy system.

In its first ground, Petitioner wrongly attempts to use a decryption engine within Buruganahalli’s firewall as the claimed “proxy system.” Goodrich Decl., ¶¶ 110-11. Recognizing the futility of this argument, Petitioner turns to Baehr for teaching a proxy network in its second ground. But, like its single-reference obviousness ground based on Buruganahalli (*see* §IV.A.3, *supra*), Petitioner’s Baehr ground does not describe what the proposed combination of Buruganahalli and Baehr would be, how it meets the challenged claims, or why a skilled artisan would have combined Baehr and Buruganahalli in the claimed manner. Instead, the alleged motivations are general and superficial. And, once again, Petitioner does not demonstrate a reasonable expectation of success in making whatever its vague combination is.

Without a proper rationale showing motivation and expectation of success, Petitioner’s combination is clearly based on improper hindsight.

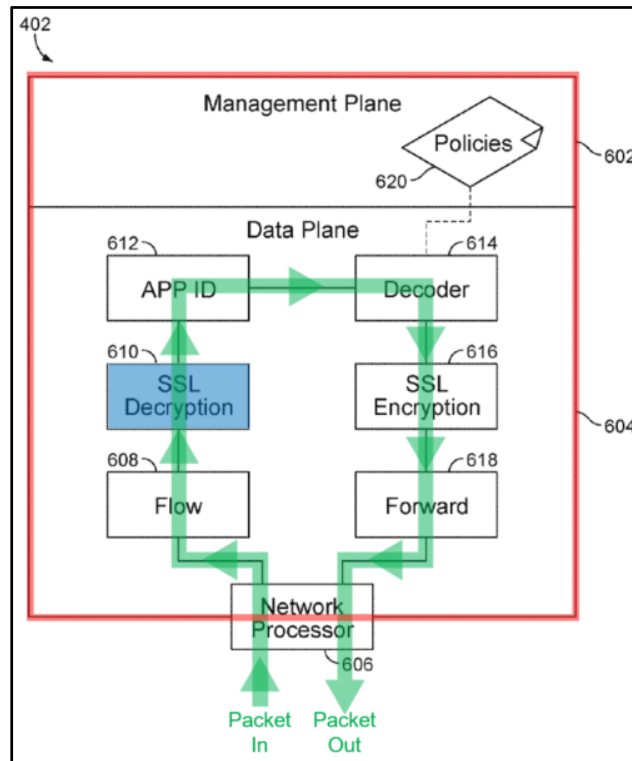
1. Buruganahalli Does Not Disclose the Claimed Routing Filtered Packets to a Proxy System

Petitioner's argument that "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'" is meritless. Pet. 39 (citing Ex. 1004 at 7:39-51, 7:60-67, 9:61-67). As discussed in detail above, no filtering of encrypted packets occurs until *after* they have been decrypted, so the decrypt engine cannot receive filtered packets—it decrypts traffic so that the firewall can monitor and filter decrypted packets. See §IV.A.1, *supra*.

Petitioner equates Buruganahalli's "decrypt engine" with the claimed "proxy system." Pet. 39. However, Buruganahalli's decrypt engines 110, 610 are not a proxy, and Petitioner never even attempted to demonstrate that it satisfies the proper construction of the term, which is "a proxy system which intervenes to prevent threats in communications between devices." Ex. 1027 at 39; Ex. 1030 at 33-34, 36. Goodrich Decl., ¶¶ 112-13.

To the contrary, Buruganahalli's decrypt engines 110, 610 perform one step (*i.e.*, decryption) of the firewall's own filtering process without "interven[ing] to prevent threats in communications between devices." See Ex. 1004 at 14:21-60; Goodrich Decl., ¶¶ 114-15. This technique is illustrated in the following drawing

showing the **packet flow** through Buruganahalli's **firewall** in which **decrypt engine 610** performs decryption in the middle of the process:



Ex. 1004, Fig. 6 (annotated)

Goodrich Decl., ¶ 115; Ex. 1004 at 14:21-60, Fig. 6. Thus, Buruganahalli's decrypt engines 110, 610 do not meet the proper construction of the term "proxy system." Goodrich Decl., ¶ 116. Notably, on cross-examination Petitioner's expert could not articulate any reason why the firewall's decrypt engine would be considered a proxy system while other functional blocks within the firewall would not be, stating that he had not "really given it a ton of thought" (Weissman Tr. at 50:4-5) and finally settling on the idea that the proxy has "to carry out certain special functions" (*id.* at 51:20-21) that "the normal network . . . implementation would do." *Id.* at 52:2-4.

But Buruganahalli's use of decryption to filter encrypted network traffic was the common solution at the time of Buruganahalli, so its use in this instance does not represent any "certain special functions." *Id.*; Goodrich Decl., ¶¶ 116-18.

Petitioner next turns to Buruganahalli's Figure 3B as allegedly disclosing proxy-like functionality. *See* Pet. 39-40. Petitioner's theory fails for the same reason set forth above (*i.e.*, the decrypt engine merely functions to carry out the firewall's own decryption process). This argument is also meritless because the Board recognized that the embodiment of Figure 3B does not satisfy the Challenged Claims. *See* §IV.A.1, *supra* (panel recognizing that the Figure 3B embodiment cannot satisfy the Challenged Claims because it decrypts encrypted packets before applying any firewall policies/rules). Thus, although Petitioner relies on Buruganahalli's decrypt engines 110, 610, those engines do not "interven[e] to prevent threats in communications between devices." *See* §III, *supra*.

For at least these reasons, Buruganahalli does not teach the claimed "routing" step.

2. The Petition Provides No Reason for Why a Skilled Artisan Would Have Been Motivated to or Would Reasonably Expect Success Modifying Buruganahalli in View of Baehr

Recognizing that its argument for using Buruganahalli's internal decrypt engine inside the firewall as the claimed proxy system is untenable, Petitioner proposes a second ground (Ground 2) combining Buruganahalli with Baehr. *See* Pet.

42-50. Petitioner discusses each of Buruganahalli and Baehr individually, but then never explains how these references are combined or what supposedly results from the combination. *Oracle Corp. v. Crossroads Sys., Inc.*, IPR2014-01207, Paper 78 at 33-35 (P.T.A.B. Jan. 29, 2016) (Petitioner “fail[s] to account for the prior art as a whole and improperly pick and choose from the references”). Without providing the actual combination, Petitioner’s alleged motivations for modifying Buruganahalli and conclusory statement that a skilled artisan would have reasonably expected success lack the necessary specificity to avoid hindsight. *See Metalcraft of Mayville*, 848 F.3d at 1367 (grounds must explain “how or why the references would be combined to arrive at the claimed invention”) (citation omitted).

(a) Petitioner Never Explains How the Proposed Combination Meets the Claim Elements

Petitioner never explains how the combination in Ground 2 meets any specific claim element. The petition merely states that “[a]lternatively, 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.” Pet. 42-43. But, the petition never maps this alternative combination to the claim language. This violates 37 C.F.R. § 42.104(b)(4) (“[t]he petition must specify where each element of the claim is found in the prior art”) and fails to provide the necessary *Graham* factor requiring explaining the differences between the claims and prior art. *See Graham*

v. *John Deere Co.*, 383 U.S. 1, 17 (1966). Petitioner was required to show how all of the limitations are met by the proposed combination, but it did not.

For example, the petition does not identify any deficiency in *Buruganahalli* with respect to the claims that it seeks to cure with *Baehr*. *Medtronic, Inc. v. Teleflex Innovations S.A.R.L.*, IPR 2020-01341, Paper 93 at 53 (P.T.A.B. Feb. 7, 2022) (“Petitioner neglects to address the differences between the Challenged Claims and the asserted combination of [two references], as required by *Graham*”)(citation omitted). *Progenity Inc. v. Natera, Inc.*, IPR2021-00280, Paper 10 at 11-15 (P.T.A.B. Jun. 25, 2021) (denying IPR because Petition failed to identify any difference between references and claims). To illustrate, the claims require “routing ... 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.” Petitioner does not explain how the claimed “routing” in *Baehr*’s “sending packets aside to a proxy network” (Pet. 42-43) would be based “based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators” as required by the claims or whether it is relying on *Baehr* or *Buruganahalli* for this limitation in Ground 2.

The closest Petitioner gets to any specificity is a statement that “*Buruganahalli*’s techniques characterizing a transparent proxy function would have been implemented in a proxy system separate from and external to the firewall.” Pet.

47. Petitioner never identifies what is meant by “transparent proxy function[s].” And, even then, this vague assertion is not a reason why a skilled artisan would do anything and thus is not an actual motivation to combine.⁹ Petitioner never states what in Buruganahalli would be implemented in Baehr’s proxy system and thus it is not clear whether the packets routed to Baehr’s proxy would have been filtered first without decryption, particularly because Buruganahalli does not filter before decrypting. Goodrich Decl., ¶¶ 119-21.

As for Baehr’s proxy in general, Petitioner cannot even decide whether the purported proxy would be implemented as a physically separate device or merely a logically separate device somewhere in the combination. *Compare* Pet. 44 (handing off filtered traffic “to dedicated proxy servers as an alternative [to] performing the proxy functions internally”) *with id.* at 47 (proxy network can merely be a “separate logical entity” internal to the filtering system). Indeed, the latter “separate logical entity” combination is no different from Buruganahalli’s components. *See* Ex. 1004 at 14:8-11, Fig. 6. That makes this ground the same as its flawed Ground 1 relying on Buruganahalli alone for the proxy and renders the combination unnecessary. *LG*

⁹ If Petitioner is referring to decryption, its logic is faulty. Decrypted packets still need inspection. Ex. 1004 at 12:59-61 (firewall “inspect[s] decrypted traffic and re-encrypt[s] it before forwarding”); *id.* at 4:19-22, 8:45-54, 9:61-10:4.

Elec., IPR2016-00197, Paper 7 at 7-9 (obviousness lacking when element “according to Petitioner, is already taught by [the primary reference].”); *Becton, Dickinson & Co. v. B. Braun Melsungen AG*, IPR2017-01588, Paper 75 at 52, 60-62 (P.T.A.B. Dec. 12, 2018) (rejecting stated advantage for modifying reference when advantage was already present in the primary reference).

As for a physically separate proxy, Petitioner has identified no benefit to using a physically separate proxy for encrypting and forwarding packets over Buruganahalli's use of logical components for encryption engine 616 and forwarding module 618 that Petitioner seems to acknowledge already exist in Buruganahalli. Goodrich Decl., ¶ 122; Ex. 1004 at 2:24-31, 14:8-12, 14:57-58, Fig. 6. Adding a physically separate proxy increases costs due to additional interfaces needed between the firewall and new proxy, increased power consumption from a separate device, and transmission delay in processing. Ex. 1005 at 3:59-64, Fig. 5 (adding interface 420). Any benefit asserted for an obviousness argument must be weighed against the downsides. *Winner Int'l Royalty Corp. v. Wang*, 202 F.3d 1340, 1349 & n.8 (Fed. Cir. 2000) (“benefits, both lost and gained, should be weighed against one another”). Petitioner has not done so.

(b) Petitioner Does Not Provide Any Persuasive Reason for Why a Skilled Artisan Would Implement its Vague Combination Using Baehr

In addition to not explaining the “how,” Petitioner also does not provide a cogent reason “why” a skilled artisan would combine Buruganahalli with Baehr in the claimed manner. Obviousness requires “a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does.” *KSR Int’l*, 550 U.S. at 418. Conclusory “assertion[s] that it would have been so” and “unsupported statement[s]” that the combinations are “within the skill” of a skilled artisan and “‘well-known and predictable’ does not meet Petitioner’s burden.” *Johns Manville*, IPR2018-00827, Paper 9 at 13-14 (informative) (citation omitted). Even assuming Petitioner’s proposed Ground 2 combination is properly presented, Petitioner has not shown why a skilled artisan would have been motivated to make the asserted combination to meet the claims—whatever it is. *Goodrich Decl.*, ¶ 123.

As previously explained, Buruganahalli does not disclose the routing element. *See* §IV.C.1, *supra*. Buruganahalli does not disclose a proxy system and the only action left for its firewall after the firewall inspects the decrypted data is to re-encrypt the data and forward it to the client or server. *See* Ex. 1004 at 12:56-61. Baehr’s proxy network 430—cited by Petitioner—does not fill this gap. Pet. 45-46. Baehr’s proxy network 430 is for mirroring host devices in a private network, not for

performing packet-forwarding and encryption. Ex. 1005, Abstract, 4:26-63, 8:13-17, 8:36-46, Fig. 6. For example, Baehr teaches redirecting packets to a mail proxy 440 that can provide the email functionality of the mail host 360 in the private network. *Id.* at 4:33-40. Baehr describes screen 340 itself performing actions such as encryption, and does not provide a reason for offloading encryption from a firewall to a proxy. *Id.* at 7:8-10, 7:45-54; Goodrich Decl., ¶¶ 124-25. Thus, Baehr does not fix the issues with Buruganahalli.

As for specific motivations, Petitioner alleges that Baehr teaches the proxy network as “advantageous for various reasons.” Pet. 46. The first reason given is to isolate the private network. *Id.*; *see also id.* at 47-48 (regurgitating this same reason as though it provides “added advantages”). Buruganahalli’s firewall, however, already isolates the client from the server by creating split sessions. Ex. 1004 at 12:4-55, Fig. 3B. There’s no isolation advantage over Buruganahalli. Goodrich Decl., ¶ 126. The second reason given (which is related to the first) is to provide seamless communication with outsiders. Pet. 46. Again, this is not an advantage over Buruganahalli’s firewall which also provides seamless communication with the server as if the server was communicating with the client. Ex. 1004 at 12:4-55, Fig. 3B; Goodrich Decl., ¶¶ 126-27. Without an actual advantage, there is no rationale to support Petitioner’s proposed combination. *See Becton, Dickinson*, IPR2017-01588, Paper 75 at 52, 60-62 (rejecting Petitioner’s combination because stated advantage

for modifying the primary reference was already present in the primary reference); *LG Elec.*, IPR2016-00197, Paper 7 at 7-9 (obviousness lacked sufficient reasoning when element “according to Petitioner, is already taught by [the primary reference].”).

Petitioner also contends its vague combination would “reduce load on a firewall” by “hand[ing] off” filtered traffic to dedicated proxy servers as an alternative [to] performing the proxy functions internally.” Pet. 44. Petitioner once again does not indicate what it means by internal “proxy functions.” Petitioner does not identify any portion of Buruganahalli as teaching a reason to hand off whatever is intended by these internal proxy functions. *See id.* Likewise, Petitioner does not identify any portion of Baehr that teaches, for example, its screen 340 handing off functions to its proxy network. Instead, Baehr’s proxy network has proxy hosts 435 that perform the functions of the hosts in the private network—not the functions of the screen 340. Ex. 1005 at 4:20-63. Indeed, there is no rationale for modifying Buruganahalli to perform a hand-off that meets the claims. The only alleged support for this hand-off argument is “NIST, 14” and “Weissman, ¶150.” Pet. 44. But, NIST describes a firewall handing off traffic to a proxy server to “perform filtering or logging” (Ex. 1036 at 25) and therefore does not teach the routing element, and Petitioner’s expert only parrots the petition. Ex. 1003, ¶ 150.

Moreover, any reduced load achieved by somehow adding a proxy to Buruganahalli would be entirely minimal. The claims require routing “filtered” packets to the proxy system. After Buruganahalli filters packets, the only task left is to encrypt (if necessary) and forward them to the client or server. Goodrich Decl., ¶¶ 128-29. Whether the forwarding and possible encryption is done by the firewall or a proxy device, the overall workload of the system is the same, and Petitioner has not alleged otherwise. *Id.* And if Baehr’s proxy is implemented as an internal logical entity as Petitioner suggests at one point (Pet. 47), the lack of load reduction is even more apparent as the internal work load would not change at all. Goodrich Decl., ¶¶ 128-29.

Petitioner next asserts motivations of “preserving computing resources, achieving load balancing, and maximizing performance” also fail. Pet. 47. But, each of these attributes—computing resources, load balancing, and performance—would be unchanged under Petitioner’s theory (*id.* at 47) of implementing Baehr’s proxy as an internal logical entity. The computing resources, load balancing, and performance would be the same. Goodrich Decl., ¶¶ 130-31. Even so, these alleged motivations are also flawed regardless of Petitioner’s theory for combining Buruganahalli with Baehr.

First, the petition offers no support for “preserving computing resources.” See *id.* Petitioner cites Exhibit 1036 (“NIST”), but that exhibit does not explain that

computing resources are preserved. Ex. 1036 at 14; Goodrich Decl., ¶ 132. The overall system would use the same amount of computing resources whether or not a separate proxy system is used—the only difference would be the distribution of those resources. See Ex. 1036 at 14 (describing that dedicated proxy servers are used in addition to firewalls); Goodrich Decl., ¶ 132.

Second, it is unclear how the proposed combination achieving load balancing. Load balancing in the context of network traffic typically refers to balancing the traffic across multiple similar devices. Goodrich Decl., ¶ 133; Ex. 1036 at 17 (“load balancing” is when “two or more firewalls are employed”), 58 (load balancing involving shifting traffic to “backup firewall”). That would not lead a skilled artisan to modify Buruganahalli to add a proxy system for receiving filtered packets, but rather to add one or more additional firewalls to share the load with Buruganahalli’s single firewall. Goodrich Decl., ¶ 133.

Alternatively, if by “load balancing,” Petitioner is referring to handing off the load to a proxy system, that alleged motivation was addressed above. It also incorrectly assumes Buruganahalli is limited to using the same component (*e.g.*, same processor) for performing the filtering and proxy functions. But, there is no need for load balancing where the filtering and proxy functions (*e.g.*, decryption and encryption) are implemented with dedicated logical components, as in Buruganahalli’s firewall. Ex. 1004 at 14:8-12, 14:57-58; Goodrich Decl., ¶ 134. In

that case, the load is already balanced among the different logical components. Goodrich Decl., ¶ 134. Moreover, Petitioner's Exhibit 1036 does not describe load balancing that involves relocating decryption functionality from a firewall to proxy servers. See Ex. 1036 at 14-16; Goodrich Decl., ¶ 134.

Third, Petitioner also provides no support for "maximizing performance." The Petition makes no mention of inadequate performance in Buruganahalli. And, the Petition does not explain how adding a proxy maximizes performance or what metric is used for measuring performance here. Goodrich Decl., ¶ 135.

Considering that Petitioner's alleged motivations all fail, a skilled artisan would not have incurred the additional cost of adding a proxy system to Buruganahalli. Goodrich Decl., ¶ 136. Likewise, the added complexity of incorporating a proxy system into Buruganahalli would have discouraged a skilled artisan from such modification. *Id.*; Ex. 1005 at 3:59-64, Fig. 5 (adding interface 420). The increased cost and complexity far outweigh any benefit—and Petitioner has not identified an actual one—from adding a proxy system to Buruganahalli. Without knowing how Petitioner proposes to combine Buruganahalli with Baehr, Patent Owner and the Board cannot assess whether there are additional factors that weigh against the combination.

**(c) Petitioner's Vague Allegation of Expected Success
Should be Rejected**

Petitioner's conclusion that the result of its vague combination would "yield the claimed limitations" and "would predictably work and provide the expected functionality" is not supported. Pet. 49. The Board should not accept this leap of faith. *Precision Planting LLC v. Deere & Co.*, IPR2019-01052, Paper 91 at 43 (P.T.A.B. Dec. 31, 2020) (Petitioner did not carry its "burden to establish that a person of ordinary skill would have been motivated to combine the references in the proposed manner and would have reasonably expect success in doing so.")(citation omitted); *Samsung Elects. Co. v. Elm 3DS Innovations, LLC*, 925 F.3d 1373, 1383 (Fed. Cir. 2019) (affirming Board's finding of a lack of reasonable expectation of success and that the issue is dispositive). Because Petitioner has never articulated how its vague proposed combination meets the claims or a persuasive reason to modify Buruganahalli, it is implausible to conclude a skilled artisan would have had a reasonable expected success, as Petitioner does and its expert merely parrots.¹⁰ See

¹⁰ The allegation is followed by an improper attempt to incorporate Petitioner's expert declaration by reference. 37 C.F.R. § 42.6(a)(3); see also *Cisco Sys., Inc. v. C-Cation Techs., LLC*, IPR2014-00454, Paper 12 at 9 (P.T.A.B. Aug. 29, 2014). Still, there is no additional analysis in the declaration.

Pet. 49. There simply is no showing that a skilled artisan would have been motivated to or reasonably expected the proposed combination to include the “routing” step.

V. OBJECTIVE EVIDENCE OF NONOBVIOUSNESS ALSO DEMONSTRATES THAT THE CLAIMS ARE VALID

“Objective indicia ‘can be the most probative evidence of nonobviousness in the record, and enables the court to avert the trap of hindsight.’” *Leo Pharm. Prods., Ltd. v. Rea*, 726 F.3d 1346, 1358 (Fed. Cir. 2013) (quoting *Crocs, Inc. v. Int’l Trade Comm’n*, 598 F.3d 1294, 1310 (Fed. Cir. 2010)). Such evidence “cannot be overlooked” and can “serve to resist the temptation to read into the prior art teachings of the invention in issue.” *Plantronics, Inc. v. Aliph, Inc.*, 724 F.3d 1343, 1355 (Fed. Cir. 2013) (quoting *In re Cyclobenzaprine Hydrochloride Extended–Release Capsule Pat. Litig.*, 676 F.3d 1063, 1079 (Fed. Cir. 2012)) ; *see also Rambus Inc. v. Rea*, 731 F.3d 1248, 1257 (Fed. Cir. 2013) (overturning Board for failing to properly consider objective indicia of nonobviousness).

As discussed above (§IV, *supra*), the petition fails to demonstrate that any claim is obvious, much less “overwhelmingly” so. Regardless, Petitioner cites no support for its assertion that objective indicia cannot overcome its purported showing of obviousness. This is flatly contradicted by precedent: “[O]bjective indicia ‘may often be the most probative and cogent evidence’ of nonobviousness,” and must be considered by the Board. *Liqwd, Inc. v. L’Oreal USA, Inc.*, 941 F.3d 1133, 1136-37 (Fed. Cir. 2019)(citation omitted); *Plantronics*, 724 F.3d at 1354-55.

A. The '856 Patent Satisfied a Long-Felt Need in the Industry and Received Substantial Industry Praise

Objective 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. *See* Ex. 1027 at 58, 61-65. Petitioner correctly states that "the trial transcript in the Cisco suit references purported secondary considerations for the '856 patent (EX1029, 3215:4-3240:4)," but falsely states "the underlying evidence is not publicly available and Petitioner does not have access to such evidence." Pet. 50. In fact, a portion of the underlying evidence appears in Petitioner's own exhibit—twice. Petitioner's Exhibit 1027 twice reproduces a Cisco press release from 2017 called PTX-1135 (Ex. 2013), which is the very same document described in the trial transcript. *Compare* Ex. 1027 at 63-64, 138 *with* Ex. 1029 at 3216:8-12.

As the court appreciated, the Cisco press release is evidence of long-felt need and industry recognition for the technology claimed in the '856 Patent because it describes the problem of detecting threats in encrypted traffic as "unsolvable" and the '856 Patent solves that problem with its steps of "determining" and "filtering," based on rule criteria, "the determined packets comprising the encrypted data." Ex. 1027 at 64; Ex. 1001, Claim 1; Goodrich Decl., ¶¶ 137-39.

Regarding the Cisco press release, the district court noted "Cisco's technical and marketing documents which contribute the addition of the infringing

functionality as a ‘breakthrough’ in building ‘an intelligent platform with unmatched security.’” Ex. 1027 at 137. This is compelling evidence of nonobviousness, as “[i]ndustry participants, especially competitors, are not likely to praise an obvious advance over the known art.” *Apple Inc. v. Samsung Elecs. Co.*, 839 F.3d 1034, 1053 (Fed. Cir. 2016) (*en banc*). The nexus between this evidence and the ’856 Patent claims was also established by way of the court’s finding that the Cisco’s Encrypted Traffic Analytics technology, which claimed to solved the unsolvable problem, infringed the ’856 Patent. Ex. 1027 at 30-57.

B. Cisco Copied the ’856 Patent

Additionally, the district court found that the ’856 Patent had been copied by Cisco. Ex. 1027 at 157, 160. “It is well established that copying by a competitor is a relevant consideration in the objective indicia analysis.” *Liqwd*, 941 F.3d at 1137. In *Liqwd*, the Federal Circuit held that the Board erred by disregarding evidence of copying that established a competitor had copied a patented method based on access to the patentee’s non-public information. *Id.* at 1138-39. Petitioner ignores that the court in the Cisco litigation also found compelling evidence of copying and that the evidence of copying was public at the time it filed the Petition. *See, e.g.*, Ex. 1029 at 31:7-32:3; *see also* Ex. 2016 at 258:21-25, 260:2-18; Ex. 2017 at 1128:8-1129:5; Ex. 2018 at 1220:1-1222:25.

The Cisco litigation opinion provides a lengthy discussion and findings of fact that show how Cisco obtained confidential Centripetal information and then released products incorporating Centripetal's patented technology. Ex. 1027 at 149-152, 155-156. As the court explained, "Cisco was provided with demonstrations of the product and confidential information regarding Centripetal's proprietary algorithms," and "[w]ithin a year of these meetings, Cisco released the 'network of the future,' involving the release of older products embedded with new software functionality that was outlined and detailed to them by disclosure of the patents and multiple technical discussions and demonstrations." *Id.* at 157. As the court also recognized, "[t]he fact that Cisco released products with Centripetal's functionality within a year of these meetings goes beyond mere coincidence." *Id.*

C. The Board Should Find the Challenged Claims Patentable Because Petitioner did not Address the *Graham* Factors

Finally, Petitioner's failure to address the objective evidence of non-obviousness is a failure of the Graham analysis. *See Graham v. John Deere Co.*, 383 U.S. 1, 17-18 (1966). "Factual inquiries for an obviousness determination include secondary considerations based on objective evidence of nonobviousness." *Lectrosonics, Inc. v. Zaxcom, Inc.*, IPR2018-01129, Paper 33, at 72 (P.T.A.B. Jan. 24, 2020) (citing *Graham*) (precedential).

Petitioner's expert stated during cross-examination that he never examined Exhibit 1029 (a portion of the Cisco trial transcript discussed above), which was

filed by PAN and which was cited as part of the list of materials considered attached to Dr. Weissman's declaration. Weissman Tr. at 62:17-63:7; *see also* §§ V.A-B, *supra*. Thus, despite testifying that "the underlying evidence" of secondary considerations "is not publicly available," Dr. Weissman was in no position to make that statement given that he did not review Ex. 1029 and "[knew] nothing about the Cisco matter." Weissman Tr. at 63:14-25. Most worryingly, Dr. Weissman stated that he was not "provided any public information," suggesting that Petitioner never actually provided Ex. 1029 to Dr. Weissman before he testified that there was no public information regarding secondary considerations emanating from the Cisco litigation. *Id.* at 63:21-25. In fact, Petitioner failed to file or apprise Dr. Weissman of several other public trial transcripts with information concerning Cisco's copying of the '856 Patent. *See* Exs. 2016-2018; *see also* § V.B, *supra*.

Because Petitioner failed to perform a proper obviousness determination, and appears to have withheld key information from its own expert, Petitioner failed to carry its burden to show that any of the challenged claims are obvious. Indeed, Petitioner's own counsel acknowledges this. Ex. 2010 at 1.

VI. CONCLUSION

For these reasons, no claims should be canceled.

Respectfully submitted,

Dated: August 26, 2022

/James Hannah/
James Hannah (Reg. No. 56,369)
Jenna Fuller (Reg. No. 74,212)
Kramer Levin Naftalis & Frankel LLP
333 Twin Dolphin Drive, Suite 700
Redwood Shores, CA 94065
Tel: (650) 752-1700 Fax: (650)752-1800

Jeffrey H. Price (Reg. No. 69,141)
Kramer Levin Naftalis & Frankel LLP
1177 Avenue of the Americas
New York, NY 10036
Tel: (212) 715-7502 Fax: (212)715-8302

Scott M. Kelly (Reg. No. 65,121)
Bradley C. Wright (Reg. No. 38,061)
BANNER & WITCOFF, LTD.
1100 13th Street, NW, Suite 1200
Washington, DC 20005
Tel: (202) 824-3000 Fax: (202) 824-3001

(Case No. IPR2022-00182)

Attorneys for Patent Owner

CERTIFICATE OF COMPLIANCE

The undersigned hereby certifies that the portions of the above-captioned PATENT OWNER'S RESPONSE specified in 37 C.F.R. § 42.24 has 13,992 words in compliance with the 14,000-word limit set forth in 37 C.F.R. § 42.24(b)(2). This word count was prepared using the Microsoft Word word-processing system used to prepare this paper.

Dated: August 26, 2022

By: /James Hannah/
James Hannah (Reg. No. 56,369)
Jenna Fuller (Reg. No. 74,212)
Kramer Levin Naftalis & Frankel LLP
333 Twin Dolphin Drive, Suite 700
Redwood Shores, CA 94065
Tel: (650) 752-1700 Fax: (650) 752-1800

Jeffrey H. Price (Reg. No. 69,141)
Kramer Levin Naftalis & Frankel LLP
1177 Avenue of the Americas
New York, NY 10036
Tel: (212) 715-7502 Fax: (212) 715-8302

Scott M. Kelly (Reg. No. 65,121)
Bradley C. Wright (Reg. No. 38,061)
BANNER & WITCOFF, LTD.
1100 13th Street, NW, Suite 1200
Washington, DC 20005
Tel: (202) 824-3000 Fax: (202) 824-3001

Attorneys for Patent Owner

CERTIFICATE OF SERVICE

The undersigned certifies, in accordance with 37 C.F.R. § 42.6(e), and pursuant to agreement by the parties that filing with the Board through the PTAB End 2 End system constitutes electronic service, that service was made on Petitioner as detailed below.

<i>Date of service</i>	August 26, 2022
<i>Manner of service</i>	Electronic Filing with the Board
<i>Documents served</i>	PATENT OWNER'S RESPONSE
<i>Persons served</i>	ROPES & GRAY LLP Scott A. McKeown Mark D. Rowland James Batchelder Andrew Radsch Keyna Chow

/James Hannah/
James Hannah
Registration No. 56,369
Lead Counsel for Patent Owner