

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 PRELIMINARY RESPONSE

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	BACKGROUND	4
A.	Overview of the '856 Patent.....	4
B.	History of the '856 Patent	10
1.	Prosecution History.....	10
2.	The Cisco Litigation	13
C.	Overview of Buruganahalli	16
D.	Overview of Baehr	21
E.	Level of Ordinary Skill	24
III.	THE BOARD SHOULD DENY INSTITUTION UNDER § 325(d)	24
A.	The Petition Relies on Substantially the Same Art and Arguments Considered by the Office During Prosecution	25
B.	Petitioner Has Not Shown Material Error by the Examiner	30
IV.	THE BOARD SHOULD DENY THE PETITION UNDER 35 U.S.C. § 314(a).....	34
A.	Granting the Petition Would Enable Further Harassment of Patent Owner and Encourage Additional Improper Petitions.....	34
1.	The Petition Reflects a Motivation to Harass Patent Owner.....	35
2.	Granting the Petition Would Encourage Harassment and Undermine District Court Adjudications.....	37
B.	The <i>Fintiv</i> Factors Also Weigh in Favor of Denying Institution.....	39
1.	Factors 1-3: The Trial Has Already Ended After Immense Investment by the Court and the Parties	40

2.	Factor 4: Buruganahalli is substantially the same as the Older Stealthwatch That Was Presented in the Cisco Litigation.....	40
3.	Factor 5: Petitioner and Cisco Present Substantially Similar Issues and Share a Relationship	43
4.	Factor 6: “Other Circumstances” Strongly Favor Denial	44
V.	PETITIONER FAILED TO ESTABLISH A REASONABLE LIKELIHOOD THAT IT WILL PREVAIL ON EVEN ONE CLAIM.....	45
A.	Petitioner Has Not Shown that Buruganahalli Teaches the Claimed “Filtering” Encrypted Packets	46
B.	The Petition Fails to Address Known Objective Evidence of Nonobviousness.....	53
VI.	CONCLUSION.....	57

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH</i> , No. IPR2019-01469, Paper 6 (P.T.A.B. Feb. 13, 2020).....	<i>passim</i>
<i>Amazon.com, Inc. v. Vocalife LLC</i> , No. IPR2020-00864, Paper 22 (P.T.A.B. Oct. 28, 2020)	40
<i>Apple Inc. v. Fintiv, Inc.</i> , No. IPR2020-00019, Paper 11 (P.T.A.B. Mar. 20, 2020)	<i>passim</i>
<i>Apple Inc. v. Samsung Elecs. Co.</i> , 839 F.3d 1034 (Fed. Cir. 2016) (en banc)	55
<i>Apple Inc. v. Unwired Planet Int'l Ltd.</i> , No. IPR2020-00642, Paper 15 (P.T.A.B. Sept. 9, 2020).....	40
<i>Atrium Med. Corp. v. Bard Peripheral Vascular, Inc.</i> , No. IPR2021-01200, Paper 11 (P.T.A.B. Jan. 20, 2022)	32
<i>Centripetal Networks, Inc. v. Cisco Sys., Inc.</i> , No. 2:18-cv-00094 (E.D. Va. Feb. 13, 2018)	14
<i>Coalition for Affordable Drugs V LLC v. Hoffman–LaRoche Inc.</i> , No. IPR2015-01792, Paper 14 (P.T.A.B. Mar. 11, 2016)	56
<i>Fitbit, Inc. v. Philips N. Am. LLC</i> , No. IPR2020-00828, Paper 13 (P.T.A.B. Nov. 3, 2020).....	43
<i>Gen. Plastic Indus. Co. v. Cannon Kabushiki Kaisha</i> , No. IPR2016-01357, Paper 19 (P.T.A.B. Sept. 6, 2017).....	34
<i>Ice Castles, LLC v. James Youngstrom</i> , No. IPR2021-01179, Paper 13 (P.T.A.B. Jan. 7, 2022)	36
<i>Intell. Bio-Sys., Inc. v. Illumina Cambridge Ltd.</i> , 821 F.3d 1359 (Fed. Cir. 2016)	45
<i>In re Kahn</i> , 441 F.3d 977 (Fed. Cir. 2006)	45

<i>Liqwd, Inc. v. L’Oreal USA, Inc.</i> , 941 F.3d 1133 (Fed. Cir. 2019)	53, 55
<i>Merial Ltd. v. Virbac</i> , No. IPR2014-01279, Paper 13 (P.T.A.B. Jan. 22, 2015)	56
<i>Neil Ziegman, N.P.Z., Inc. v. Carlis G. Stephens</i> , No. IPR2015-01860, Paper 11 (P.T.A.B. Feb. 24, 2016).....	2
<i>Nespresso USA, Inc. v. K-fee Sys. GmbH</i> , No. IPR2021-01222, Paper 9 (P.T.A.B. Jan. 18, 2022)	32
<i>Next Caller Inc. v. TRUSTID, Inc.</i> , No. IPR2019-00961, Paper 10 (P.T.A.B. Oct. 16, 2019)	42
<i>Omron Oilfield & Marine, Inc. v. MD/TOTCO</i> , No. IPR2013-00265, Paper 11 (P.T.A.B. Oct. 31, 2013).....	56
<i>OpenSky Industries, LLC v. VLSI Tech. LLC</i> , No. IPR2021-01064, Paper 17 (P.T.A.B. Dec. 23, 2021)	38
<i>Palo Alto Networks, Inc. v. Centripetal Networks, Inc.</i> , No. IPR2021-01156, Paper 7 (P.T.A.B. Oct. 28, 2021).....	2, 53
<i>PayPal, Inc. v. IOENGINE, LLC</i> , No. IPR2019-00885, Paper 21 (P.T.A.B. Oct. 3, 2019).....	44
<i>Robert Bosch Tool Corp. v. SD3 LLC</i> , No. IPR2016-01751, Paper 15 (P.T.A.B. Mar. 22, 2017)	56
<i>Samsung Elecs. Co. v. Clear Imaging Rsch., LLC</i> , No. IPR2020-01399, Paper 13 (P.T.A.B. Feb. 3, 2021).....	42
<i>Stryker Corp. v. KFX Med., LLC</i> , No. IPR2019-00817, Paper 10 (P.T.A.B. Sept. 16, 2019).....	36, 53, 56
Statutes	
35 U.S.C. § 314(a)	34
35 U.S.C. § 316(e)	45
35 U.S.C. § 325(d)	24

Regulations

37 C.F.R. § 42.104(b)(4).....36

37 C.F.R. § 42.108(a).....34

Other Authorities

H.R. Rep. No. 112-98, pt. 1 (2011).....37, 38

Patent Trial and Appeal Board Consolidated Trial Practice Guide,
November 2019..... 34, 36

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, available from https://web.archive.org/web/20211009155735/https://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

I. INTRODUCTION

The Board should exercise its discretion under 35 U.S.C. §§ 314(a) and 325(d) to deny Palo Alto Networks, Inc.'s ("Petitioner") petition ("Pet.") for *inter partes* review (IPR) of U.S. Patent No. 9,917,856 (Ex. 1001, "the '856 Patent"), challenging claims 1, 24, and 25.

The sole purpose of this petition is for harassment. Petitioner inappropriately seeks to exploit the IPR process and the USPTO's finite resources to gain leverage against Patent Owner Centripetal Networks, Inc. ("Centripetal" or "Patent Owner") in district court litigation that does not involve the '856 Patent or any of its family members. Petitioner has not been accused of infringing the '856 Patent but knows that it underlies a significant damages award resulting from massive willful infringement by Cisco Systems, Inc. ("Cisco") that is currently on appeal to the Federal Circuit. The Board should not endorse this tactic, particularly given the validity determination in the Cisco litigation, which Cisco is not challenging on appeal. Such harassment is exacerbated by the fact that this is Petitioner's seventeenth petition (for sixteen different patents) filed against Centripetal in less than a six-month span, including against two other patents underlying the Cisco verdict that have not been asserted against Petitioner. This petition must be denied so that Patent Owner may "avoid harassment and enjoy

quiet title to [its] rights.” *Neil Ziegman, N.P.Z., Inc. v. Carlis G. Stephens*, No. IPR2015-01860, Paper 11 at 12-13 (P.T.A.B. Feb. 24, 2016) (citation omitted).

This petition should also be discretionarily denied under Section 314(a) because the '856 Patent has already survived a thorough challenge to its validity by Cisco in district court litigation. That challenge failed, in part, because of substantial objective evidence of nonobviousness (“secondary considerations”) that Petitioner inexplicably ignores despite Patent Owner previously raising this issue.¹ Petitioner’s allegation (Pet. at 50) that it does not have access to such evidence is plainly false—one of the documents was reproduced in Petitioner’s own exhibit (Ex. 1027) twice. Petitioner’s disregard for this evidence is unconscionable given Petitioner’s familiarity with the Cisco litigation and relationship with Cisco.² The Board has warned that such repetitive attacks, even by different petitioners, constitute abusive tactics that warrant discretionary denial under Section 314(a). The unfairness to Patent Owner and the undue burden of *again* having to explain

¹ Prior to filing this petition, Patent Owner informed Petitioner that failure to address known secondary considerations is a reason for denial. *See, e.g., Palo Alto Networks, Inc. v. Centripetal Networks, Inc.*, No. IPR2021-01156, Paper 7 at 58-59 (P.T.A.B. Oct. 28, 2021).

² Both are charter members of the Cyber Threat Alliance. Ex. 2008 at 1.

why the challenged '856 Patent claims are patentable cannot be justified, particularly in light of Petitioner's other abusive conduct.

This petition should also be discretionarily denied under Section 325(d). Petitioner's art is substantially the same as that considered during original prosecution. Petitioner has also not addressed material error in the Office's prior evaluation and consideration of the art and '856 Patent claims. This alone is enough to deny institution under *Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH*, No. IPR2019-01469, Paper 6 at 8-9 (P.T.A.B. Feb. 13, 2020) (precedential) ("If . . . petitioner fails to make a showing of material error, the Director generally will exercise discretion not to institute . . .").

Even if the Board chooses not to exercise its discretion, IPR must be denied because the Petitioner failed to meet its burden of showing a reasonable likelihood that it would prevail on even one claim.

First, every challenged claim requires "filtering . . . the determined packets comprising the encrypted data." Instead of focusing on filtering encrypted packets, Petitioner points to Buruganahalli's filtering of decrypted packets. Recognizing this clear deficiency, which was shared by the art distinguished during prosecution and in the Cisco litigation, Petitioner relies on conclusory and unsupported testimony from its expert that this aspect of the challenged claims would have been

obvious. Not only can these conclusory statements not establish obviousness, however, they are flatly contradicted by Buruganahalli itself.

Second, the Board should credit the district court's finding of objective evidence of nonobviousness that led to its validity determination and an enhanced verdict of willful infringement. The objective evidence of long-felt need, industry praise, and copying are substantial. The petition's failure to address this evidence is not only a basis for denying the petition; it also demonstrates that the petition fails to establish a reasonable likelihood of prevailing. As the objective evidence of nonobviousness stands unrebutted, so too should the challenged claims.

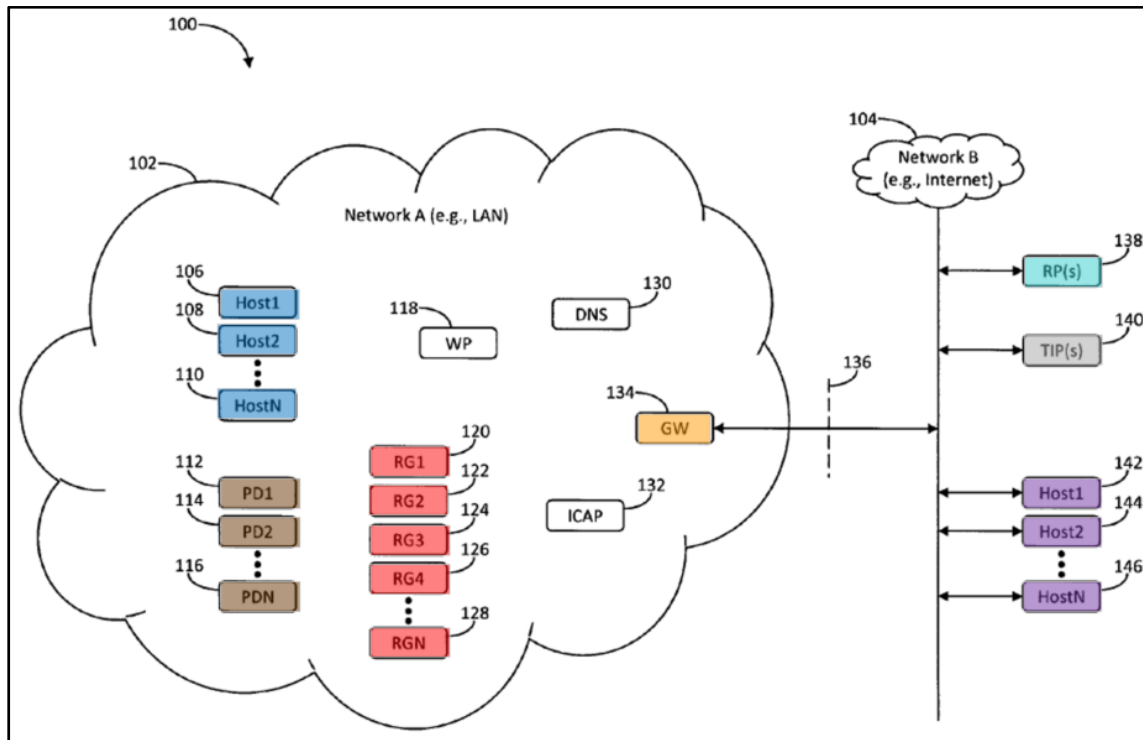
At bottom, Petitioner has not met its burden to demonstrate a reasonable likelihood that it would prevail in showing unpatentability of any challenged claim, and the Board should not countenance Petitioner's harassment of Patent Owner. The Petition should, therefore, be denied.

II. BACKGROUND

A. Overview of the '856 Patent

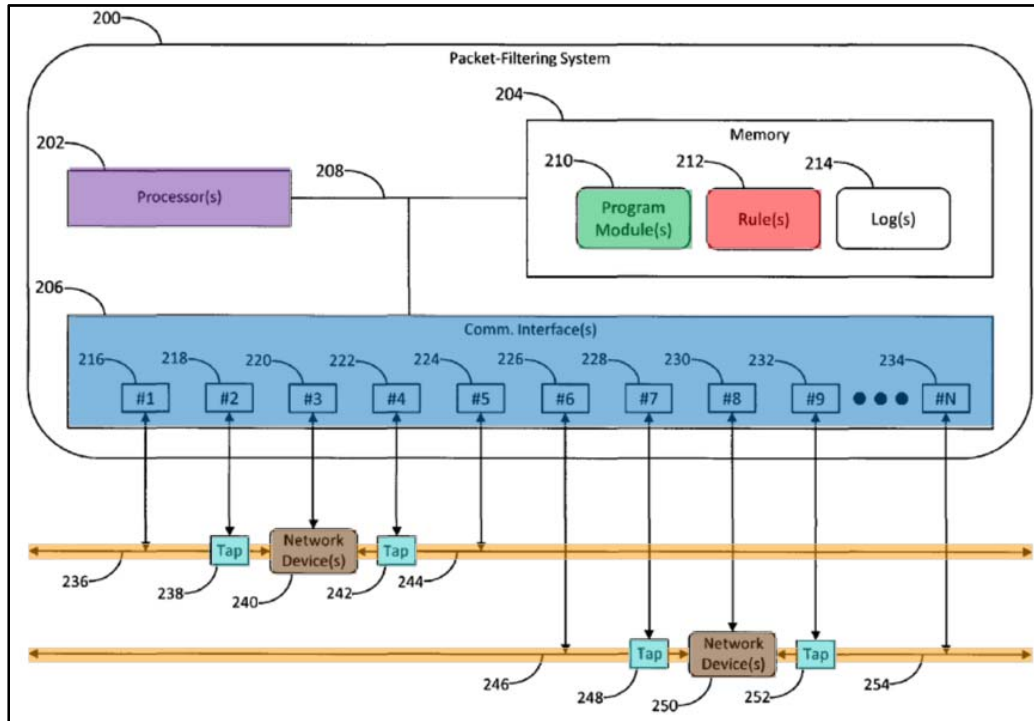
Prior to the '856 Patent, network-threat detection of encrypted packets, if done at all, was done by decrypting encrypted packets, just as in Petitioner's Buruganahalli reference. Ex. 1004 at 11:2-6. With the '856 Patent's inventive approach, network-threat detection of encrypted packets may be performed without decryption. Ex. 1001 at 9:66-10:14, 11:51-65.

Figure 1 (annotated below) of the '856 Patent depicts an illustrative environment for using an example of the disclosed approach to protect network 102 from threats in network 104 (*e.g.*, the Internet). *Id.* at 2:20-34, Fig. 1.



Ex. 1001, Fig. 1 (annotated). As shown in exemplary Figure 1, **gateway 134** is located at border 136 to interface network 102 with network 104. *Id.* at 2:50-53. The 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 2:35-53. 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 the received data, the **rule gates** configure rules to control a packet-filtering system. *Id.* at 4:16-21.

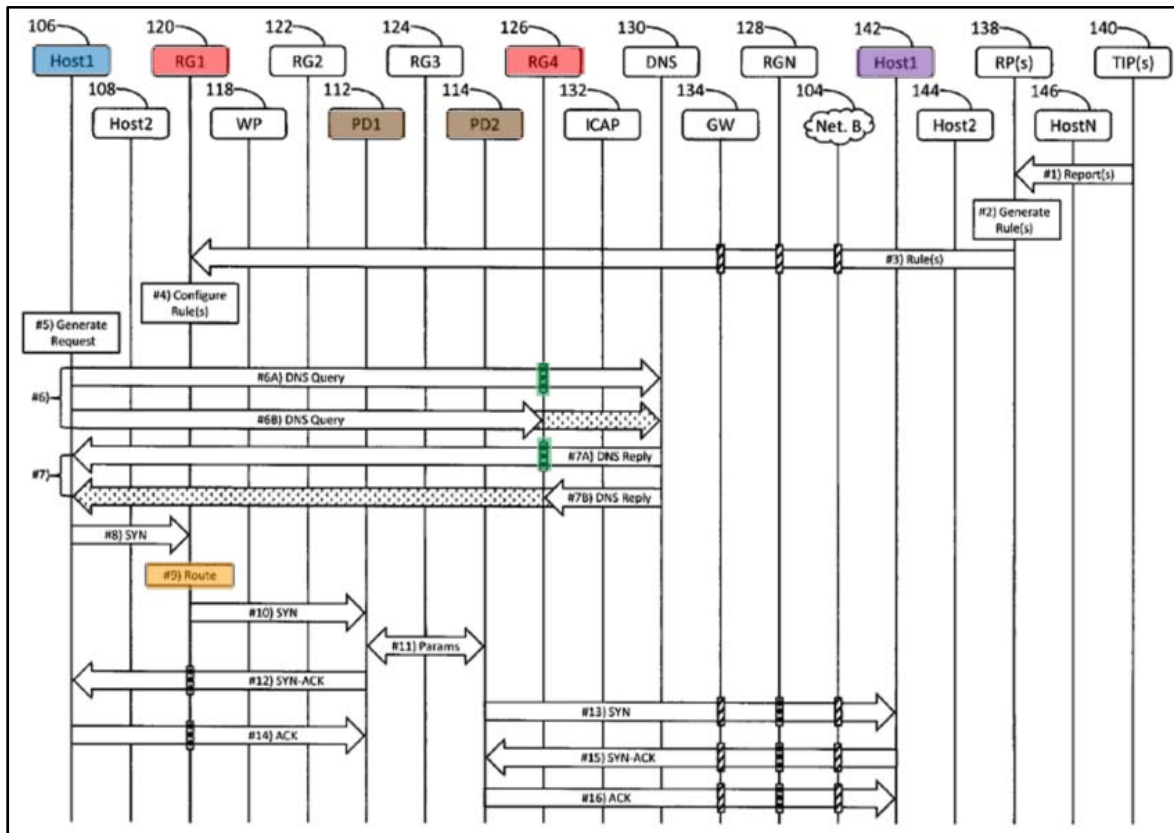
An exemplary packet-filtering system is depicted in Figure 2 (annotated below).



Ex. 1001, Fig. 2 (annotated). As shown, exemplary packet-filtering system 200 includes **one or more processors 202** for executing **one or more program modules 210** for performing rule-based network-threat detection using **rules 212**. *Id.* at 2:66-7:14. The packet-filtering system 200 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 packet-filtering system so that filtering is performed by various devices. *Id.*

Figures 3A-3C, 4A-4C, 5A-5B, and 6A-6B show different event sequences to illustrate the capabilities of the exemplary packet-filtering systems. *Id.* at 1:64-

67. With respect to Figures 3A-C, the '856 Patent discloses, in one example, **rule gate 120** of the packet-filtering system receiving data at step #3 and configuring packet-filtering rules at step #4. *Id.* at 3:65-4:21, Fig. 3A (annotated below).

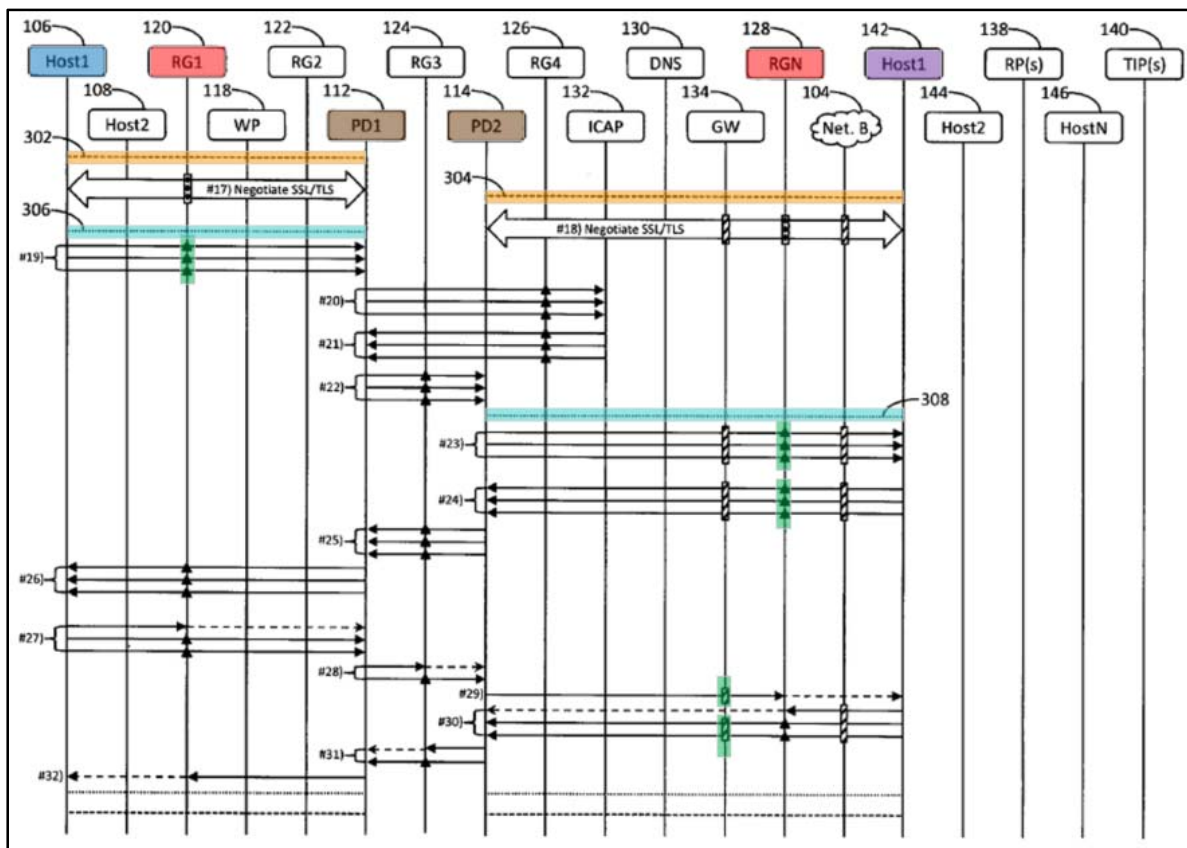


Ex. 1001, Fig. 3A (annotated).

Following this example, 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) 130 (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. *Id.* at 6:17-21.

After receiving the routed SYN message, the packet filtering system, sets up two separate connections (steps #11-16): **connection 302** (e.g., a TCP connection) and **connection 304** (e.g., another TCP connection). *Id.* at 7:33-8:64, Figs. 3A, 3B (annotated below).



Ex. 1001, Fig. 3B (annotated).

Handshake messages are exchanged over each of connections 302 and 304 to establish two separate encrypted communication sessions (steps #17-18). *Id.* at 8:65-9:65, Fig. 3B. These handshake messages include, for example, a client hello

message having unencrypted data, such as a domain name. *Id.* at 9:16-33. **Rule gate 120** using rules 212 may **filter** the handshake messages based on the domain name. *Id.* at 9:2-46. Similarly, **rule gate 128** using rules 212 may **filter** the handshake messages for establishing encrypted communication session 308. *Id.* at 9:47-65.

Once the **encrypted communication sessions 306, 308** are established, encrypted packets may be communicated in those sessions. For example, encrypted packets are sent from **host 106** and **filtered** by **rule gate 120**. *Id.* 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 without decrypting the packets. *Id.* at 10:2-14. 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 Petitioner's prior art as it was during prosecution and the Cisco litigation.

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) (emphasis added).

B. History of the '856 Patent

1. Prosecution History

Application No. 14/757,638 was filed on December 23, 2015, and issued as the '856 Patent on March 13, 2018. Ex. 1002 ('856 File History) at 1-64, 1453; Ex. 1001.

The first non-final Office Action rejected all 25 pending claims. The Office Action included rejections under 35 U.S.C. §§ 101, 112 (second paragraph), and § 103. Ex. 1002 at 1061-1084. The then-pending independent claims and most dependent claims were rejected based on a combination of Spies (Ex. 2001) and

Sorenson (Ex. 2002). Ex. 1002 at 1070-81. Then-pending claims 14 and 15 were rejected on Spies, Sorenson, and Bomer (Ex. 2003). Ex. 1002 at 1081-83.

On October 11, 2017, Patent Owner filed a response. *Id.* at 1351-67. The response included amending representative independent claim 1, in part, as follows:

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

filtering, by the packet-filtering system:

packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators; and

the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators.

Id. at 1352.

In response to the § 103 rejection, Patent Owner explained that “antispam filtering and other content-based filtering of Spies is applied to a scanned and **unencrypted** version of a message.” *Id.* at 1365 (emphasis added) (citation omitted). Patent Owner also explained that “Spies discusses additional processing operations such as virus scanning, spam filtering, notifications, archiving, or security policy enforcement may be performed on the **decrypted** message and the

resulting **decrypted** and processed version of the message may be provided to the recipient.” *Id.* (emphasis added). The response also included additional arguments to distinguish the claimed “network-threat indicators” from Spies’ disclosure of a domain name. *Id.* Finally, the response explained that Sorensen and Bomer fail to remedy the deficiencies of Spies and Sorensen. *Id.* at 1366.

A Notice of Allowance was mailed on December 20, 2017, and included an Examiner’s Amendment based on a prior interview. *Id.* at 1374-1400. With respect to claim 1, the Examiner’s Amendment added: (i) “wherein at least one of the one or more network-threat indicators comprise a domain name identified as a network threat” to the “receiving” step, (ii) “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[.]” to the “filtering” step, and (iii) the entire “routing” step. *Id.* at 1380-81. Similar amendments were made to the other independent claims and other amendments were made to some dependent claims. *See id.* at 1381-86.

In the statement of reasons for allowance, the Examiner stated that the “instant application is directed towards packet-filtering rules with threat indicators

to identify packets comprising unencrypted data, and packets comprising encrypted data.” *Id.* at 1388. The reasons for allowance also recited portions of the “filtering” and “routing” steps. *Id.* The Examiner also stated that: “Examiner performed updated search and additional search does not yield other specific references that reasonably, either singularly or in combination with cited references, would result [in] a proper rejection that would have anticipated or made obvious all the steps disclosed in the independent claims 1, 24 and 25 with proper motivation at or before the time it was effectively filed.” *Id.* at 1389. As evidence of this further search and consideration, the Examiner specifically discussed one of the references, Reybok (*id.* at 1389-90), which also describes performing decryption before filtering. Ex. 2004 at ¶¶ 0068-0069, Fig. 6B.

An amendment after allowance was filed on January 23, 2018 to make minor amendments to place the application in better form. Ex. 1002 at 1413-24. That amendment as well as a separate paper included brief comments on the statement of reasons for allowance. *Id.* at 1423-24, 1448. The amendment after allowance was entered and the ’856 Patent issued. *Id.* at 1450-53.

2. The Cisco Litigation

On February 13, 2018, Patent Owner filed a complaint against Cisco alleging infringement of several of Patent Owner’s patents, including the ’856

Patent. Ex. 1027 at 1-3. After a twenty-two day bench trial in that case,³ the district court concluded that Cisco willfully infringed four of Centripetal's patents, including the '856 Patent. Cisco's massive infringement amounted to approximately \$21.4 billion of revenue; the district court awarded approximately \$1.9 billion in past damages and interest, plus royalties for future sales. *Id.* at 3, 147, 166.

In its findings of fact for the '856 Patent, the court noted that “[t]he process at the core of this technology involves using unencrypted information located in a packet to determine if there is a threat embedded in the encrypted portion.” *Id.* at 32. The court rebuked Cisco's multifaceted validity challenge. Cisco asserted multiple documents describing Cisco's earlier Stealthwatch system⁴ using Cisco's proprietary logging framework, Netflow. *Id.* at 33-35, 56-58. 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 and believed this was the strongest

³ *Centripetal Networks, Inc. v. Cisco Sys., Inc.*, No. 2:18-cv-00094 (E.D. Va. Feb. 13, 2018) (“the Cisco litigation”).

⁴ Stealthwatch refers to Cisco's code for analyzing network traffic based on information received from Cisco's Netflow operating on Cisco's switches and routers. Ex. 1027 at 33-35, 57.

prior art to the '856 Patent. Cisco also sought to support its invalidity challenge with expert testimony. Cisco's expert, Dr. Schmidt, attempted to use Centripetal's infringement contentions against it and argued that all of the functionality relied upon was in the prior art. *See id.* at 61. The court concluded—consistent with the prosecution history—that Cisco's prior art lacked “the functionality to identify threats in encrypted traffic **without** the use of decryption.” *Id.* (emphasis in original).

The court continued its validity analysis by discussing various evidence of nonobviousness, including publications after the '856 patent's 2015 filing date. Specifically, the court discussed a technical guide that described the 2017 version of Stealthwatch (identified as PTX-383) as the ““first and only solution in the industry that can detect malware in encrypted traffic without decryption using Encrypted Traffic Analytics.”” *Id.* at 62. The court also discussed, and even reproduced, a 2017 Cisco press release describing Cisco's system as “solving a ‘network security challenge previously thought to be unsolvable.’” *Id.* at 63 (citation omitted); *see also id.* at 64. 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.

The court's infringement analysis is also telling of the '856 Patent's validity. In finding infringement of the '856 Patent, the court explained that the '856 Patent does not require decryption and that Cisco performed filtering (*e.g.*, an encrypted flow is blocked or quarantined) based on unencrypted portions of encrypted packets. *Id.* at 55-57. As the court acknowledged, Cisco copied the claimed inventions of the four infringed patents, including the '856 Patent, and further found Cisco's infringement to be willful. *Id.* at 160 (finding that Cisco "embedded . . . copied software functionality from [Centripetal's] patents in its [products]" and that this "new functionality" was "copied from Centripetal during and after [a] Nondisclosure Agreement.") (citation omitted); *see also id.* at 157 (concluding that "damages should be enhanced for copying.") (citation omitted). As acknowledged by Petitioner, Cisco has not challenged the district court's validity determination in its pending appeal. Pet. 9; Ex. 1028 at 20-21.

C. Overview of Buruganahalli

Buruganahalli (Ex. 1004) relates to "[t]echniques for destination domain extraction for secure protocols." Ex. 1004 at Abstract. In particular, Buruganahalli discloses applying policies to decrypted packets rather than filtering encrypted packets. *Id.* at 4:45-5:10.

With respect to Figure 3A, if a destination domain is on the whitelist, the firewall would allow a secure connection (*e.g.*, TLS connection) to be established

between the client and server. *Id.* at 7:52-59, 6:1-11, 5:43-51, 10:54-11:6, 16:35-41, Fig. 3A. In this first scenario, no filtering takes place as the subsequent traffic is simply forwarded without being analyzed. *Id.*

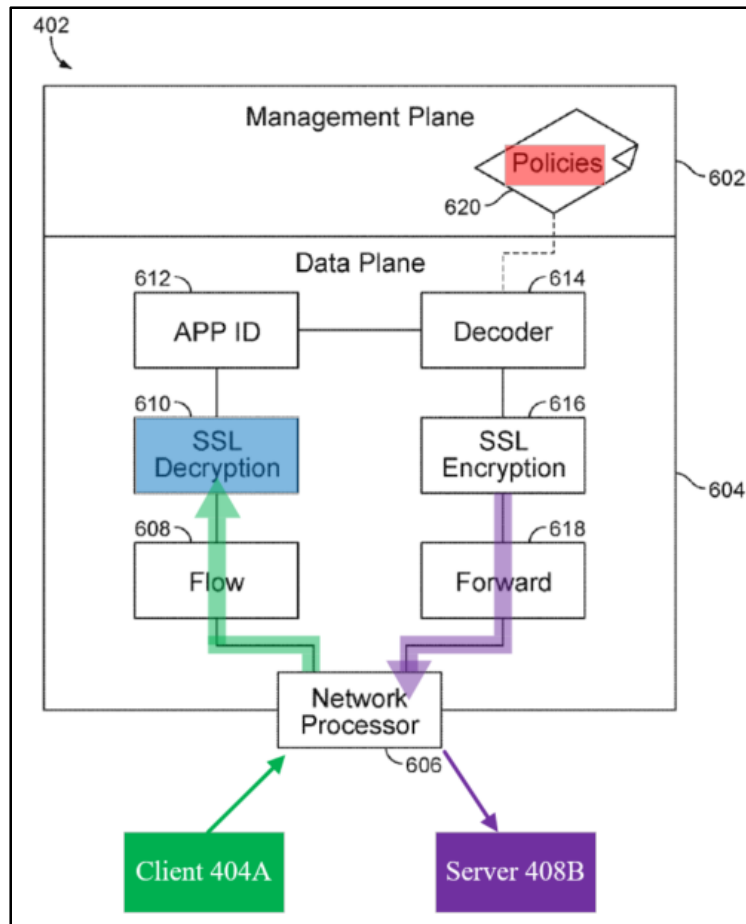
On the other hand, if the destination domain is on the blacklist, the firewall may block the session. *Id.* at 5:64-6:1, 10:54-11:19, 4:31-44, Fig. 3A. In this second scenario, the secure connection is not established and thus no encrypted packets are received by the firewall or filtered, as depicted in annotated Figure 3A. *See id.* Buruganahalli states that the firewall can apply a policy “without having to decrypt,” but that is simply a product of preventing all packets from the outset. *Id.* at 11:7-19; *see also id.* at 4:31-44. Buruganahalli explains that because firewall 304 does not perform decryption of encrypted packets, it “cannot detect such firewall policy/rule violation(s)” thereby confirming that policies cannot be applied to encrypted packets. *Id.* at 11:2-6.

Alternatively, 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 secure connection. *Id.* at 6:12-38, 7:60-67, 8:25-44, 11:59-12:64, Fig. 3B. In this third scenario, the secure connection is established, but is split into two sessions so that the packets may be decrypted and inspected. *See id.* This allows the firewall to **decrypt** encrypted packets for further analysis. *Id.* at 12:4-61 (explaining that “[a]fter the session set-up handshaking is completed for each of Session A and

Session 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” and “[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”) (emphasis added).

Importantly, Buruganahalli does not disclose filtering encrypted packets because communications sessions are either allowed uninspected, terminated before a session is established, or (if the domain name is on the blacklist) decrypted prior to filtering. *See id.* at 6:12-38, 7:60-67, 8:25-44, 11:59-12:64, Fig. 3B. Indeed, Buruganahalli emphasizes the importance of decryption: “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 4:19-22.

Buruganahalli reinforces this in its description of other drawings. For example, in Figure 6 (annotated below), Buruganahalli depicts a security device 402 (*e.g.*, firewall) having a management plane storing **policies 620** and a data plane for handling packets. *Id.* at 14:8-20, 14:58-60, Fig. 6.



Ex. 1004, Fig. 6 (annotated).

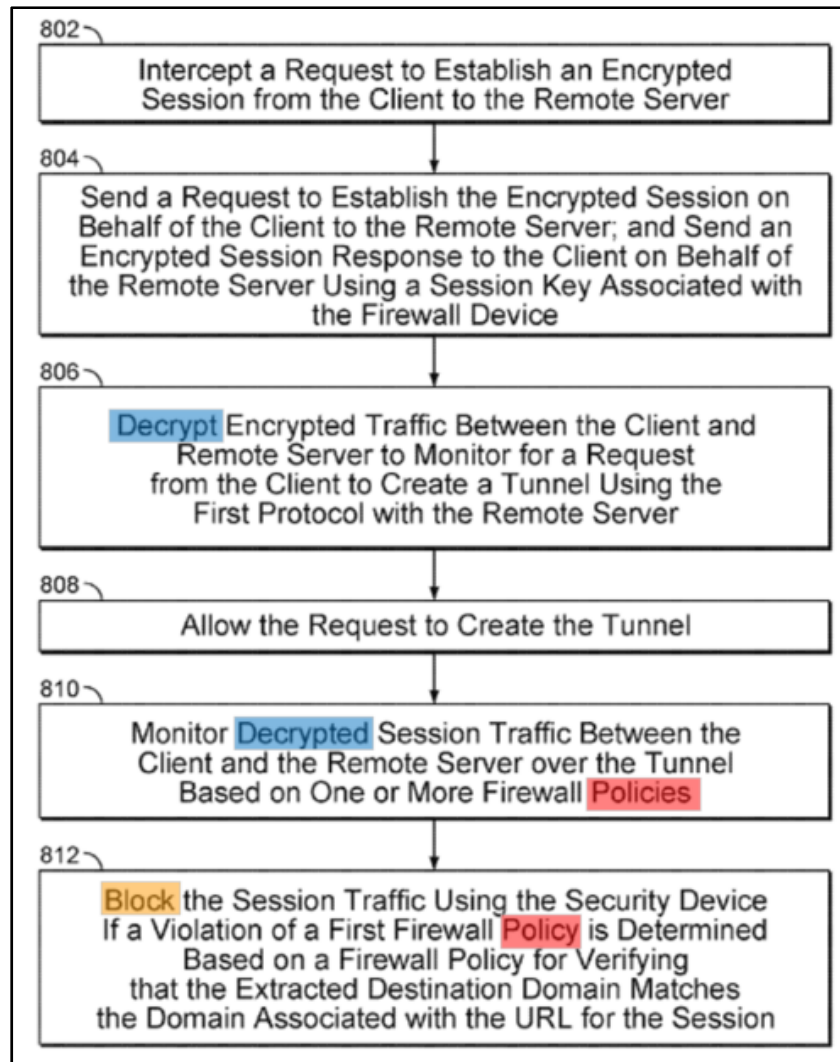
As shown, network processor 606 receives a packet from **client 404A** intended for **server 408B**. *Id.* at 14:21-22. The encrypted packet is then decrypted by **SSL decryption engine 610**. *Id.* at 14:33-38. The **policies 620** are not applied to an encrypted packet until the decrypted data is decoded by an appropriate

decoder 614, as evidenced by the dashed line in Figure 6. *Id.* at 14:50-57, Fig. 6.⁵

Assuming the policy does not require blocking the decrypted and decoded data, that data is encrypted by SSL encryption engine 616 and forwarded on to the server 408B. *Id.* at 14:57-58, 14:21-22, Fig. 6.

Finally, with respect to Figure 8 (annotated below), Buruganahalli provides a flow diagram showing that encrypted traffic is **decrypted** and the **decrypted** traffic is monitored based on **policies**, which may result in **blocking** the traffic. *Id.* at 15:22-45, Fig. 8.

⁵ Likewise, regarding its Figure 1 embodiment, Buruganahalli describes report and enforce policy engine 120 applying policies after receiving results from decrypting and decoding encrypted traffic. Ex. 1004 at 9:44-10:28, Fig. 1.

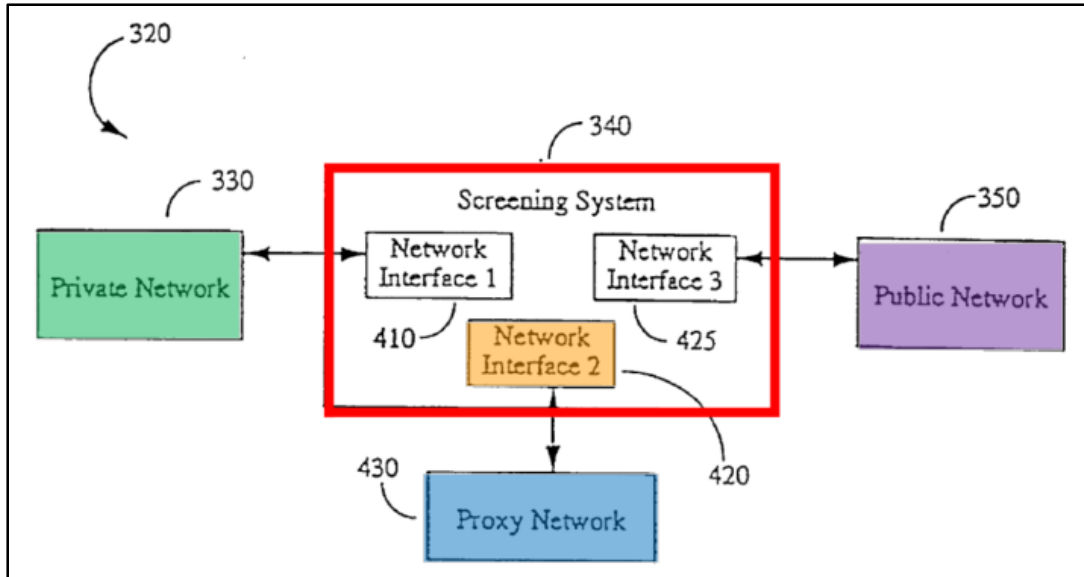


Ex. 1004, Fig. 8 (annotated).

D. Overview of Baehr

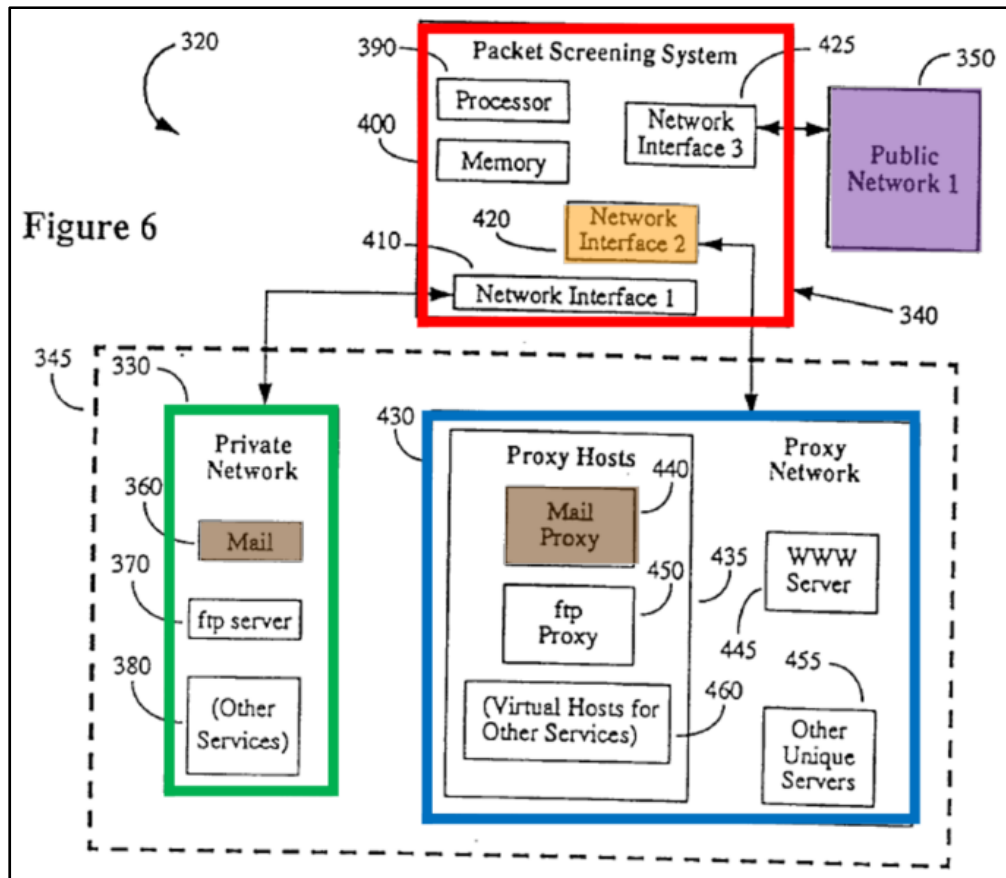
Baehr (Ex. 1005) relates to a system for screening data packets transmitted between a protected network (e.g., **private network**) and a **public network**. Ex. 1005 at Abstract, 1:9-17, 2:10-17, Fig. 5 (annotated below). Baehr does not describe filtering encrypted packets based on rules.

Baehr describes adding **network interface 420** to **screening system (or “screen”) 340** for coupling it to **proxy network 430**. *Id.* at 3:51-64.



Ex. 1005, Fig. 5 (annotated).

Packets received at the **screen** (e.g., packets transmitted from the **public network** to the **private network**) may be allowed, dropped, or sent to the **proxy network**. *Id.* at Abstract, 2:41-47. Baehr's Figure 6 (annotated below) provides a more detailed view of **screen 340** from Figure 5. *Id.* at 4:12-63, Fig. 6.



Ex. 1005, Fig. 6 (annotated).

A proxy host (e.g., **mail proxy 440**) of **proxy network 430** may mirror a host (e.g., **mail host 360**) on **private network 330** so as to perform functions as though it is the private network host to which the packet(s) is destined. *See id.* at Abstract, 4:26-63, 8:13-17, 8:36-46.

There is nothing remarkable about Baehr's use of a proxy as compared to other proxy systems considered during prosecution of the '856 Patent. Baehr does not describe the proxy host communicating via an SSL or TLS connection. Baehr does not describe the proxy host communicating with the private network host, and thus a packet (or information therein) that is sent to a proxy host never reaches the

private network host to which it was directed. Baehr does not disclose the proxy host performing decryption. Baehr does not describe any functionality with regard to encrypted packets.

E. Level of Ordinary Skill

At this preliminary stage and without conceding it is correct, Patent Owner has applied Petitioner's proposed definition for a person of ordinary skill in the art ("POSITA" or "skilled artisan"). See Pet. at 16.

III. THE BOARD SHOULD DENY INSTITUTION UNDER § 325(d)

During prosecution, the Examiner considered substantially the same art and arguments that Petitioner repeats here. The Board should therefore deny institution under 35 U.S.C. § 325(d) ("[T]he Director may take into account whether, and reject the petition or request because, the same or substantially the same prior art or arguments previously were presented to the Office."). Allowing this proceeding to continue would be contrary to the Board's "commitment to defer to previous Office evaluations of the evidence of record unless material error is shown."

Advanced Bionics, Paper 6 at 7.

Under the two-part framework established in *Advanced Bionics*, the Board first considers "whether the same or substantially the same art previously was presented to the Office or whether the same or substantially the same arguments previously were presented to the Office." *Id.* at 8. If either condition of the first

part is satisfied, the Board then determines “whether the petitioner has demonstrated that the Office erred in a manner material to the patentability of challenged claims.” *Id.*

A. The Petition Relies on Substantially the Same Art and Arguments Considered by the Office During Prosecution

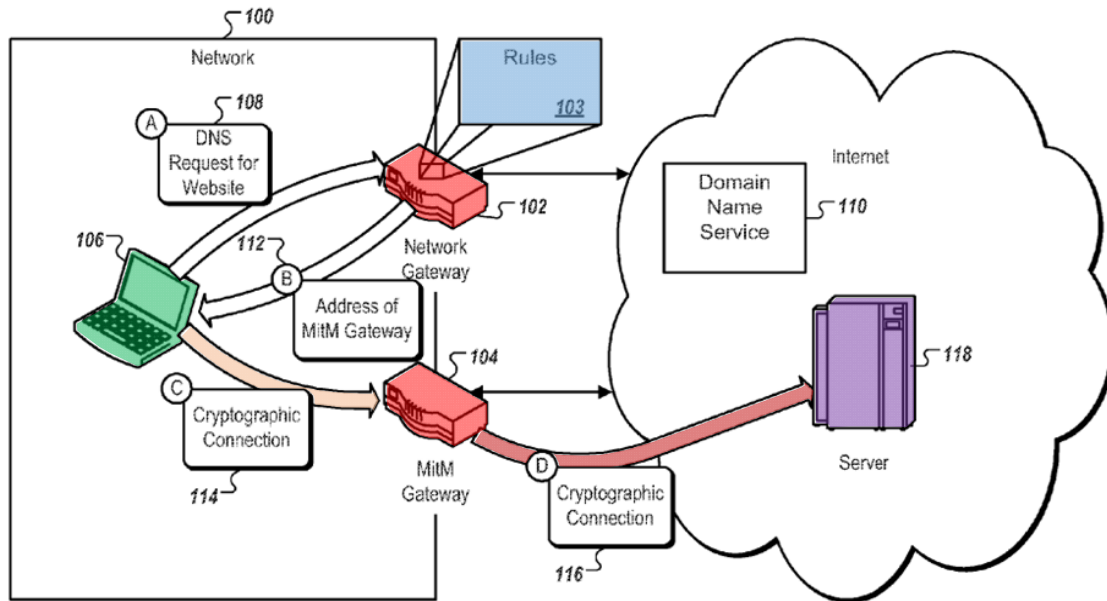
When evaluating art in a petition, the Board considers similarity of that art to art considered during prosecution, as well as the cumulative nature of the art urged in the petition. *Id.* at 9-10 & n.10 (citation omitted). By either measure, Buruganahalli and Baehr are substantially the same as art considered by the Examiner during prosecution of the application that became the '856 Patent.

Buruganahalli is, in all relevant aspects and as explained below, the same as U.S. Patent Application Publication 2014/0317397 (Martini) (Ex. 2005). Martini was cited in International Search Report and Written Opinion from related international application PCT/US2016/067111. Ex. 1002 at 1398. The search report characterized Martini as an “X” reference (a “document of particular relevance”), which is the PCT equivalent of an anticipation or single-reference obviousness rejection. *Id.* at 1340. The written opinion included a detailed application of Martini to original independent claim 1, which was identical to original claim 1 of the '638 application that became the '856 Patent. *Id.* at 1343, 1346-47. The Examiner considered Martini, the International Search Report, and the Written Opinion during prosecution of the '856 Patent and allowed the claims

after entering an Examiner Amendment. *Id.* at 1379-81. Accordingly, the Examiner determined that the '856 Patent was patentable over substantially the same art ***and arguments*** that Petitioner retreads here with respect to Buruganahalli. *See id.* at 1395.

Buruganahalli describes a firewall has the ability to create a secure connection. Ex. 1004 at 5:24-35, 15:11-13. A firewall is implemented as a “gateway.” *Id.* at 1:28-31, 2:55-60, 10:39-46. If a destination domain is on a “whitelist,” a session associated with communications between a client and remote server is permitted with no filtering. *Id.* at 7:52-59. If the destination domain is on a “blacklist,” a session associated with communications between a client and remote server is decrypted, and the decrypted communications are monitored further. *Id.* at 6:22-39, 7:52-59, 8:36-38, 15:35-37. The firewall uses “man-in-the-middle decryption techniques” to monitor the encrypted communications. *Id.* at 8:48-50. “[U]sing these techniques the firewall 314 is between the client 312 and the server 316 and can present itself as server of the session to the client and can present itself as the client of the session to the server.” *Id.* at 12:56-59. “In this manner, the firewall 314 can inspect decrypted traffic and re-encrypt it before forwarding it to the other party.” *Id.* at 12:59-61.

Martini, which is titled “Selectively Performing Man in the Middle Decryption,” describes the same thing. Ex. 2005, title. Martini’s Figure 1 is reproduced below with color annotations.



Ex. 2005, Martini, Fig. 1 (annotated).

Like Buruganahalli, Martini describes a **gateway** that has the ability to create a secure connection. *Id.*, ¶¶ 0020 (DNS request is plaintext traffic), 0024 (“the network gateway may intercept and examine a DNS request 108 from the **browser device** 106”; request 108 includes “URL or URI”). Martini describes comparing the extracted domain name to a policy and/or list of domain names. *Id.*, ¶¶ 0024 (“[b]ased on, for example, the URL or URI in the DNS request 108 and **rules** 103 indicating which destination should be decrypted and which should be passed directly to the Internet destination”), 0038 (“These **rules** 103 may include, for example, a list of domain names and IP address mapped to security policies,

content classifications, or directions for handling of network traffic (e.g., specifying that the traffic should be decrypted and inspected).”).

Martini describes determining whether to decrypt and monitor based on whether a domain name is specified for decryption and inspection. *Id.* Martini further describes “man in the middle” decryption that is just like the “man-in-the-middle decryption techniques” of Buruganahalli. *Id.*, ¶ 0025 (“The browser device 106 . . . can initialize **a cryptographic connection** 114 with the **MitM gateway** 104 . . . The MitM [man in the middle] gateway 104 may then initialize another **cryptographic connection** 116 with a **server** 118 that hosts the resource identified by the URL or URI of the DNS request 108.”). And like Buruganahalli, Martini describes that the MitM gateway may “receive an encrypted message from the browser device 106, decrypt the message, inspect the message, optionally alter or drop the message, encrypt the possibly altered message into a second encrypted form, and pass the message to the server 118.” *Id.*, ¶ 0026.

There are numerous other similarities between Martini and Buruganahalli. For example, both references propose man-in-the-middle decryption as a solution to the same problem. *Compare* Ex. 1004 at 4:16-18 (“secure protocols can be used to evade detection by security devices, such as firewalls, by encrypting data communications between a client and a remote server”) *with* Ex. 2005, ¶ 0018 (“When data on a network is encrypted (e.g., by SSL or TLS) the data can pose

challenges to network security appliances and routines in that it makes it difficult to inspect the data as it is transferred between the end users and servers on the Internet.”). Given its identity to Martini on all relevant points, Buruganahalli is substantially similar to art already presented to the Office.

Buruganahalli is also cumulative of Spies (U.S. Patent Application Publication 2005/0138353) (Ex. 2001), which the Examiner applied to reject claims during prosecution. *See* Ex. 1002 at 1069-81. Like Buruganahalli, Spies describes a firewall that filters IP packets based on port and destination address information, communications that include encrypted data, decryption of the encrypted data from those communications, and inspection of that data **after** it has been decrypted. Ex. 2001, ¶¶ 0084, 0094, 0130, 0131, 0147, 0160, 0161.

The other reference asserted in the petition is Baehr. But in all relevant aspects, Baehr is substantially the same as numerous references considered by the Examiner during prosecution. Petitioner relies on Baehr for allegedly disclosing “a packet filtering system sending packets aside to a proxy network.” Pet. at 43. Yet Petitioner’s own expert argues that art cited during prosecution “discloses routing packets to a proxy for security reasons.” Ex. 1003 (“Weissman Decl.”), ¶ 74 (citing Ex. 1033, which is a publication of a continuation of U.S. Patent 7,299,353 (Le Pennecc)); Ex. 1002 at 1093 (indicating Examiner consideration of Le Pennecc). The Examiner also considered multiple other references that describe similar

sending of packets to a proxy network. U.S. Patent 6,098,172 (Coss), the first reference listed on page 1 of the '856 Patent, describes “proxy reflection” that “involves redirecting a network session to another, ‘remote’ proxy server for processing, and then later passing it back via the firewall to the intended destination.” Ex. 2006 at 9:35-38; Ex. 1002 at 1093 (showing Examiner consideration of Coss). As but another example, U.S. Patent Application Publication 2004/0088542 (Daude) describes a firewall and forwarding engine functional block of a gateway sending data packets to a proxy server. Ex. 2007, ¶¶ 0132, 0133; Ex. 1002 at 1098 (showing Examiner consideration of Daude).

Because the Petition asserts art that is substantially the same as art that was considered during prosecution and over which the '856 Patent claims were found to be patentable, the first part of the *Advanced Bionics* framework is satisfied.

B. Petitioner Has Not Shown Material Error by the Examiner

“If a condition in the first part of the framework is satisfied and the petitioner fails to make a showing of material error, the Director generally will exercise discretion not to institute” *Advanced Bionics*, Paper 6 at 8-9.

Petitioner has failed to demonstrate any error—much less a material error—by the Office when it determined the challenged claims to be patentable over art that is substantially the same as Buruganahalli and Baehr. The petition does not even

acknowledge consideration of those references or attempt to show any error—much less any ***material*** error—by the Examiner.

Nor could Petitioner have made that showing under the three factors considered by the Board: (1) the extent of evaluation of the art, including whether the prior art was the basis for rejection; (2) whether Petitioner has sufficiently alleged error; and (3) any additional evidence and facts in the petition that warrant reconsideration. *Id.* at 9-11 & n.10; *see also id.* at 21 (“Petitioner must demonstrate that the Examiner erred in the evaluation of the prior art, for example, by showing that the Examiner misapprehended or overlooked specific teachings in the relevant prior art such that the error by the Office was material to the patentability of the challenged claims.”). All three factors weigh strongly in favor of denial.

Spies was expressly considered, discussed, and distinguished during prosecution. And while Petitioner makes a half-hearted attempt to draw a distinction between Spies and Buruganahalli, it ignores the limitations added in the Examiner Amendment that led to allowance. *See* Pet. at 9-10 (failing to address the “filtering” limitations that led to allowance). In particular, Petitioner fails to explain how Buruganahalli’s technique of applying a security policy to decrypted data is any different than Spies’ approach. *Id.* It is not.

There is also no question that the Examiner also carefully considered Martini, Le Pennec, Coss, and Daude. The Examiner initialed all of those references on information disclosure statements and expressly stated that “all references considered except where lined through.” Ex. 1002 at 1087-1110, 1118-1124, 1393-1399. That some of these references were not applied in a rejection is not determinative. *See Nespresso USA, Inc. v. K-fee Sys. GmbH*, No. IPR2021-01222, Paper 9 at 11 (P.T.A.B. Jan. 18, 2022). Because Patent Owner shows that the Office previously considered art that is substantially the same as art asserted in the petition, the burden shifts to Petitioner to show material error, regardless of whether an examiner applied a reference in rejection. *Advanced Bionics*, No. IPR2019-01469, Paper 6 at 8; *Nespresso USA*, Paper 9 at 25-26. This applies not only when the same art was previously considered, but also when the previously considered art and arguments are substantially the same as those asserted in a petition. *Atrium Med. Corp. v. Bard Peripheral Vascular, Inc.*, No. IPR2021-01200, Paper 11 at 23-24 (P.T.A.B. Jan. 20, 2022).

In any event, it is not surprising that Martini, Le Pennec, Coss, and Daude were not discussed by the Examiner in a rejection. Those references, like Buruganahalli, fail to teach “filtering . . . based on [information specified by the plurality of packet-filtering rules]: . . . the determined packets comprising the encrypted data.” *See* § V.A, *infra*. Portions of these features were added by

Examiner's Amendment after an interview, including an amendment to claim 1 to add: "based on at least one of a uniform resource identifier (URI) . . . or data indicating a command specified by the plurality of packet-filtering rules" to the "filtering" step. Ex. 1002 at 1379-81.

That interview and amendment occurred after the office action and response addressing and amending the claims in light of Spies and after the submission of the information disclosure statement that identified Martini, the PCT written opinion discussing Martini, Le Pennec, Coss, and Daude. *See id.* at 1127-33, 1061-85, 1351-67, 1378-81, 1389-91. After considering these references, including an ISR and Written Opinion applying Martini to the same claim, the Examiner proposed an amendment that distinguished them. Because the Applicant agreed to that amendment, there was no occasion for a further rejection.

As noted above, Petitioner does not acknowledge the Examiner's consideration of Martini and other references. Indeed, the petition does not reflect Petitioner having made any effort to review any of the cited art to assess similarity to Buruganahalli or Baehr. The Petition thus has not shown material error by the Examiner. No "additional evidence and facts presented in the Petition warrant reconsideration of the prior art or arguments." *Advanced Bionics*, Paper 6, 9 n.10 (citation omitted). Because Petitioner has not demonstrated any material error in

the Office's prior consideration of Martini and other references, the Board should exercise its discretion under Section 325(d) and deny institution.⁶

IV. THE BOARD SHOULD DENY THE PETITION UNDER 35 U.S.C. § 314(a)

A. Granting the Petition Would Enable Further Harassment of Patent Owner and Encourage Additional Improper Petitions

The Board has broad discretion under 35 U.S.C. § 314(a) and 37 C.F.R. § 42.108(a) to deny institution. *Gen. Plastic Indus. Co. v. Cannon Kabushiki Kaisha*, No. IPR2016-01357, Paper 19 at 18-19 (P.T.A.B. Sept. 6, 2017) (precedential) (recognizing the importance of addressing “the potential impacts on both the efficiency of the inter partes review process and the fundamental fairness of the process for all parties”). A petitioner's bad faith or misconduct is a relevant consideration. The non-exhaustive factors applied by the Board under *General Plastic* and *Fintiv* Section 314(a) are merely examples of how the Board can take “undue inequities and prejudices to Patent Owner into account.” *Id.* at 17; *see also* Consolidated Trial Practice Guide at 58 (Nov. 2019) (“CTPG”); *Apple Inc. v. Fintiv, Inc.*, No. IPR2020-00019, Paper 11 at 16 (P.T.A.B. Mar. 20, 2020) (precedential) (noting that “[o]ther facts and circumstances may also impact the

⁶ Both Buruganahalli and Martini have been applied in continuations of the '856 Patent.

Board's discretion to deny institution" including "factors unrelated to parallel proceedings").

1. The Petition Reflects a Motivation to Harass Patent Owner

Petitioner has no reasonable basis to maintain this challenge other than harassment, particularly in view of Cisco's own decision to drop its invalidity challenge on appeal to the Federal Circuit. Petitioner has no stake in the outcome of this proceeding. The '856 Patent has never been asserted, or threatened to be asserted, against Petitioner. Petitioner seeks to leverage this IPR against Patent Owner in unrelated litigation because the '856 Patent underlies a significant damages award based on Cisco's massive and willful infringement.

Petitioner's haphazard claim chart, in which it relies on piecemeal disclosures from the references and conclusory allegations of what a POSITA would have known for Ground 1, along with its failure to address how Ground 2 meets any claim element, further evidence that Petitioner's sole purpose for filing this petition is harassment and leverage. Had Petitioner truly been motivated by some other reason (e.g., a sense of public duty to uphold the integrity of the U.S. patent system), **Petitioner would have challenged more than only the claims underlying the Cisco verdict.** But it did not. It attacked only the willfully infringed claims. Even if Petitioner were to prevail here, 22 claims would still exist.

The lack of effort put into the Petition is highlighted by the short shrift given to the validity finding and known evidence of objective indicia of nonobviousness (secondary considerations) from the Cisco litigation. *See* Pet. at 8-9, 50. Failing to address the validity finding and evidence of nonobviousness weighs in favor of denial. *See Stryker Corp. v. KFX Med., LLC*, No. IPR2019-00817, Paper 10 at 27-29 (P.T.A.B. Sept. 16, 2019) (“Petitioner’s failure to address the known evidence of secondary considerations further weighs in favor of denying institution.”); *see also* § V, *supra*.

The Petition also never attempts to specify where each claim element is found in the combination relied upon for Ground 2, as required under the rules. 37 C.F.R. § 42.104(b)(4); *see also* CTPG at 42. This is yet another basis for denial. *See Ice Castles, LLC v. James Youngstrom*, No. IPR2021-01179, Paper 13 at 28-29 (P.T.A.B. Jan. 7, 2022) (denying institution under 37 C.F.R. § 42.104(b)(4) because Petitioner fails to specify where limitations are found in a proposed combination and “ostensibly relies on the arguments for the asserted ground of unpatentability” previously discussed in the petition).

With this seventeenth petition within six months—including two additional petitions challenging patents underlying the Cisco damages award but not asserted against Petitioner, Petitioner has wasted the Board’s and Patent Owner’s limited resources. There is no reason to further expend those finite resources.

2. Granting the Petition Would Encourage Harassment and Undermine District Court Adjudications

Congress did not seek to place bounties on Article III court judgments. The Office must not be used as a tool by opportunistic petitioners who have no direct interest in the patent at issue to collaterally attack judgments from Article III courts through administrative proceedings. Congress granted the Office discretion to deny institution in order to prevent such gamesmanship. Allowing Petitioner's gamesmanship here will only encourage bad actors to harass patent owners by filing IPRs any time a meaningful judgment is entered against third-party defendants, in hopes of extracting some form of advantage (monetary or otherwise). Such behavior should not be rewarded or encouraged; this is not what IPRs are for.

The '856 Patent has already withstood a validity challenge in the Cisco litigation. See H.R. Rep. No. 112-98, pt. 1, at 48 (2011) (recognizing "the importance of quiet title to patent owners to ensure continued investment resources"). Congress recognized the serious concerns that IPRs "not to be used as tools for harassment or a means to prevent market entry through repeated litigation and administrative attacks on the validity of a patent." *Id.* ("Doing so would frustrate the purpose of the section as providing quick and cost effective alternatives to litigation" and "divert resources from the research and development of inventions."). Indeed, Congress intended the USPTO "to address potential

abuses and current inefficiencies under its expanded procedural authority.” *Id.*
Congress thus directed the Board to deny petitions in the event of harassment as
IPRs “are not to be used as tools for harassment.” *See id.*

While a recent non-precedential Board decision did institute IPR after a
district court verdict against an unrelated defendant, *OpenSky Industries, LLC v.*
VLSI Tech. LLC, No. IPR2021-01064, Paper 17 (P.T.A.B. Dec. 23, 2021), that case
involved vastly different facts. In *OpenSky*, the Board emphasized that “because
the [prior] Intel litigation did not resolve issues presented by this proceeding, there
is no chance of an inconsistent outcome” and “Patent Owner has not argued that
resolving a dispute in this proceeding would conflict with an aspect of the Intel
litigation.” *Id.* at 8-9. But here, there is a chance of an inconsistent outcome that
could conflict with the prior Cisco litigation. In the Cisco litigation, the court
already found the ’856 Patent valid over asserted prior art that taught filtering
decrypted data—not filtering encrypted packets—and the court found that a wealth
of objective indicia supported its determination of nonobviousness. *See* § II.B.2,
supra.

Further, in *OpenSky*, the petitioner (OpenSky) was not sued by the patent
owner, so the IPR there was not a settlement leverage play like it is here. Nor did
OpenSky assert sixteen other petitions against VLSI in an effort to strain VLSI’s
resources the way Palo Alto Networks has done so with this seventeenth petition.

Finally, unlike in *OpenSky* where the petitioner was a newly formed company and submitted a declaration attesting to its unfamiliarity with the prior Intel litigation at issue until after the verdict, Petitioner Palo Alto Networks has been around for years, has a relationship with Cisco, and has not made any similar attestation.

The facts here illustrate why instituting review would pose a grave threat to the integrity of the patent system. Permitting Petitioner—who has not been accused of infringing this patent—to harass Patent Owner would not promote any desirable public policy. This is not a situation in which Petitioner requires its “own day in court,” as Petitioner has nothing at risk. And to the extent the public has an interest in the validity of the ’856 Patent, the claims have already withstood thorough examination and an extensive district court bench trial. Granting institution here would effectively declare open season on similarly situated patent owners and district court judgments, inviting administrative challenges by opportunistic parties for reasons that have nothing to do with patent quality.

B. The *Fintiv* Factors Also Weigh in Favor of Denying Institution

The Petition should also be denied under the factors articulated in *Fintiv*, Paper 11 at 6. As in the district court litigation and during prosecution, Petitioner’s obviousness case is similarly based on art that requires decrypting encrypted packets to detect threats. See § III.A, *supra*, § IV.B.2, *infra*. And because “the Board takes a holistic view of whether efficiency and integrity of the system are

best served by denying or instituting review,” *Fintiv*, Paper 6 at 6, the abusive nature of this Petition, combined with suspect tactics motivating Petitioner, further support a denial under § 314(a).

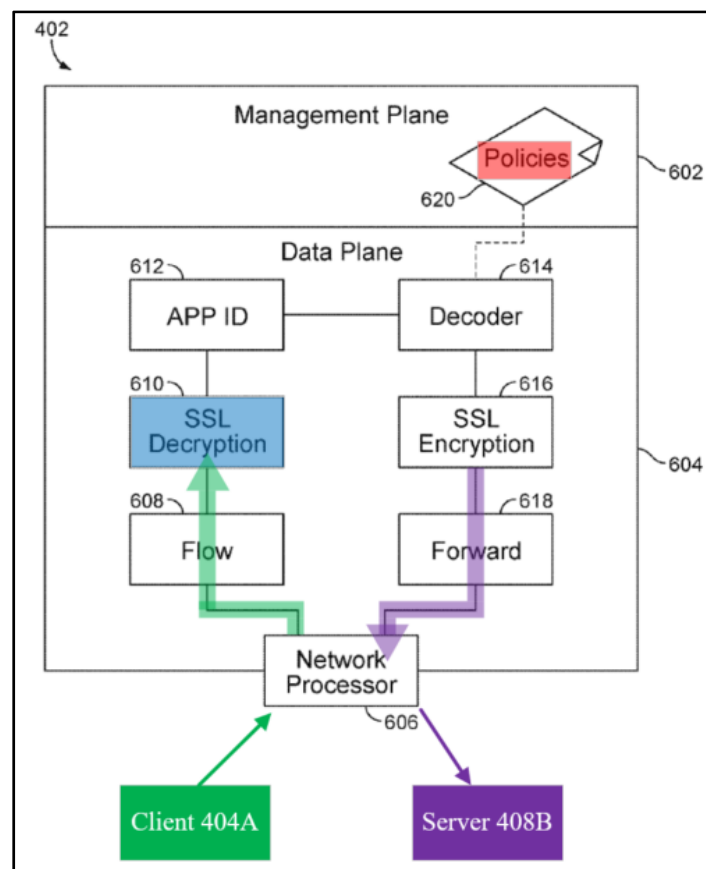
1. Factors 1-3: The Trial Has Already Ended After Immense Investment by the Court and the Parties

The district court, Cisco, and Patent Owner have invested enormous resources in resolving contentions that the old version of Stealthwatch invalidates the '856 Patent. These years-long efforts culminated in a 22-day bench trial and a final judgment upholding the validity of Claims 24 and 25 of the '856 Patent that Cisco has not challenged on appeal. *See* Ex. 1027 at 59-67; *see also* Ex. 1028 at 20-21. Thus, there can be no debate that no stay is possible (Factor 1), that the trial has already completed long before the Board's statutory deadline (Factor 2), and that there have been massive investments in that parallel proceeding (Factor 3). Factors 1-3 strongly favor denial. *See, e.g., Apple Inc. v. Unwired Planet Int'l Ltd.*, No. IPR2020-00642, Paper 15 at 6-7 (P.T.A.B. Sept. 9, 2020) (prior trial “strongly favors” denial); *Amazon.com, Inc. v. Vocalife LLC*, No. IPR2020-00864, Paper 22 at 9-11 (P.T.A.B. Oct. 28, 2020) (same).

2. Factor 4: Buruganahalli is substantially the same as the Older Stealthwatch That Was Presented in the Cisco Litigation

Factor 4, “overlap between issues raised in the petition and in the parallel proceeding,” favors denial “if the petition includes the same or substantially the

same claims, grounds, arguments, and evidence as presented in the parallel proceeding.” *Fintiv*, Paper 11 at 6, 12. Here, Buruganahalli is substantially similar to Cisco’s older Stealthwatch product, which Cisco asserted in the district court litigation to challenge the validity of the ’856 Patent because both require the use of decryption hardware in the middle of encryption flows to detect threats. See Ex. 1027 at 57-59, 61; see also Ex. 1004, Fig. 6 (reproduced below with annotations).



Ex. 1004, Fig. 6 (annotated).

The district court rejected Cisco’s invalidity challenge, finding that because the older Stealthwatch product requires the use of decryption it fails to “detect malware in encrypted traffic without any decryption,” which Claims 24 and 25

require. Ex. 1027 at 62 (citation omitted) (quotation omitted); *see also id.* at 61 (“The Court, in order to find invalidity, would be required to find that Cisco’s prior art disclosed the functionality to identify threats in encrypted traffic **without** the use of decryption. It is evident to the Court that Cisco lacked this functionality prior to 2017”) (emphasis in original).

Petitioner also challenges Claim 1 that was not at issue in the Cisco trial. However, Claim 1 is directed to the same subject matter of Claims 24 and 25. Indeed, Petitioner confirms that “Claim 1 is a method claim, ***the substance of which is representative of system Claim 24 and non-transitory media Claim 25.***” Pet. at 28 (emphasis added). Because the claims are all directed to the same subject matter, and Petitioner does not contend that they differ in some significant way or that it would be harmed if institution of the non-overlapping Claim 1 is denied, Factor 4 strongly favors denial. *See Next Caller Inc. v. TRUSTID, Inc.*, No. IPR2019-00961, Paper 10 at 14 (P.T.A.B. Oct. 16, 2019) (denying institution where the claims are all directed to the same subject matter and petitioner did not assert that the non-overlapping claims significantly differ or that it would be harmed if institution is denied); *Samsung Elecs. Co. v. Clear Imaging Rsch., LLC*, No. IPR2020-01399, Paper 13 at 21 (P.T.A.B. Feb. 3, 2021) (denying institution where the non-overlapping claims do not differ in any significant way).

3. Factor 5: Petitioner and Cisco Present Substantially Similar Issues and Share a Relationship

Petitioner was not a party to the Cisco trial, but that does not mean that the litigation is “irrelevant.” Pet. at 8. “Even when a petitioner is unrelated to a defendant, . . . if the issues are the same as, or substantially similar to, those already or about to be litigated, or other circumstances weigh against redoing the work of another tribunal, the Board may, nonetheless, exercise the authority to deny institution.” *Fintiv*, Paper 11 at 14 (warning that “[a]n unrelated petitioner should, . . . address any other district court or Federal Circuit proceedings involving the challenged patent . . .”). Indeed, the Board has found this factor to favor denial in such circumstances. *See, e.g., Fitbit, Inc. v. Philips N. Am. LLC*, No. IPR2020-00828, Paper 13 at 13-16 (P.T.A.B. Nov. 3, 2020) (weighing Factors 4 and 5 in favor of denying institution in view of substantially similar issues pending in a litigation with a different party).

The relationship between Petitioner and Cisco further weights Factor 5 in favor of discretionary denial. Petitioner partners with Cisco to help their customers keep their “competitive edge in today’s business environment.” Ex. 2008 at 1; Ex. 2009 at 1. This collaboration involves deploying Petitioner’s Next-Generation Firewall with Cisco’s “Application Centric Infrastructure (ACI)” in order to “protect traffic flow at the application level” utilizing “a device package . . . that allows Cisco’s Application Policy Infrastructure Controller (APIC) to configure

[Petitioner's] physical and virtualized firewalls.” Ex. 2009 at 1; *see also PayPal, Inc. v. IOENGINE, LLC*, No. IPR2019-00885, Paper 21 at 11 (P.T.A.B. Oct. 3, 2019) (finding a relationship where petitioners had a customer-supplier relationship). Petitioner and Cisco are also “Charter Members” of the Cyber Threat Alliance (CTA), which is a membership organization for cybersecurity providers. Ex. 2008 at 1.

As described in connection with Factor 4, substantially similar issues were already litigated because Buruganahalli is substantially similar to the older version of Stealthwatch, which Cisco unsuccessfully asserted in challenging the validity of the '856 Patent. Factor 5, therefore, favors denial.

4. Factor 6: “Other Circumstances” Strongly Favor Denial

Factor 6, “other circumstances that impact the Board’s exercise of discretion, including the merits,” *Fintiv*, Paper 11 at 14, also strongly favors denial. As discussed in Section III, *supra*, the Petition presents art that is duplicative and cumulative to art previously considered by the Office and Petitioner has not identified any error in the Office’s evaluation. *See Fintiv*, Paper 11 at 16 (“The parties should explain whether these or other facts and circumstances [including “considerations implicated by 35 U.S.C. § 325(d)”] exist,” as well as their impact on the “efficiency and integrity of the patent system”). The Petition is also unlikely to succeed on the merits for the reasons explained in Section V, *infra*.

Moreover, as explained above, Petitioner's duplicative challenge is a transparent and harassing attempt to gain leverage against Patent Owner in unrelated litigation.

See § IV.A, *supra*.

**V. PETITIONER FAILED TO ESTABLISH A REASONABLE
LIKELIHOOD THAT IT WILL PREVAIL ON EVEN ONE CLAIM**

A petitioner in an IPR has “the burden of proving . . . unpatentability by a preponderance of the evidence.” 35 U.S.C. § 316(e). If a petitioner asserts unpatentability based on obviousness, it has the further “burden to demonstrate both ‘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.’” *Intell. Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1367-68 (Fed. Cir. 2016) (citations omitted). Obviousness cannot be established by bald conclusions. *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006).

As explained in more detail below, the petition does not show any of the challenged claims to be obvious over Buruganahalli or the alleged combination of Buruganahalli and Baehr. Only independent claims 1, 24, and 25 are challenged and each challenged claim includes similar limitations directed to filtering encrypted data: “determining, . . . based on a portion of the unencrypted data corresponding to one or more network-threat indicators . . . packets comprising encrypted data that corresponds to the one or more network-threat indicators” and

“filtering” based on information specified by packet-filtering rules: “the determined packets comprising the encrypted data.” *See, e.g.*, Ex. 1001, claim 1. Petitioner has not shown that the limitation was taught in the prior art or would have otherwise been obvious to a skilled artisan.

A. Petitioner Has Not Shown that Buruganahalli Teaches the Claimed “Filtering” Encrypted Packets

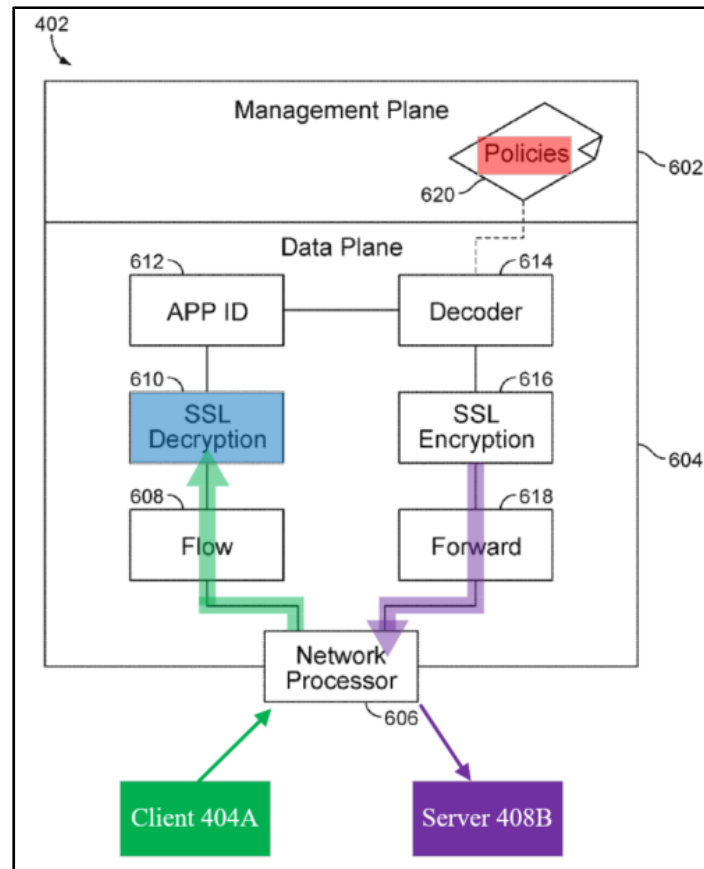
Buruganahalli⁷ does not disclose filtering determined encrypted packets because all encrypted packets that are subject to filtering must be decrypted before that filtering occurs. This technique is no different than the approach disclosed in Spies and Martini, which were distinguished during prosecution, and old Stealthwatch, which was distinguished in a concluded district court litigation. Notably, the claimed “filtering” is not met by just any filtering of any packet; it must be “based on” criteria⁸ “specified by the plurality of packet-filtering rules, and it must be performed on encrypted packets. *See* Ex. 1001, claim 1 (reciting

⁷ Petitioner only cites Buruganahalli for this claim element, so Patent Owner’s arguments apply equally to Grounds 1 and 2 of the Petition.

⁸ 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.

“filtering . . . the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators.”).

The petition equates Buruganahalli's firewall policies/rules including the blacklist policy to the claimed “plurality of packet-filtering rules.” *See* Pet. at 29-30. The petition specifically cites to the policies 620 in Buruganahalli's Figure 6. *See 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. That is, when encrypted packets are received by Buruganahalli's security device 402 (*e.g.*, a firewall), the security device 402 performs decryption before filtering any traffic with those policies. *See id.*; *see also id.* at 12:29-32 (with respect to Fig. 3B, explaining that after setting up Sessions A and B, “[A]ny 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.”). Thus, Buruganahalli's policy-based filtering approach is performed on decrypted data, not “packets comprising encrypted data” as claimed. In this respect, Buruganahalli is no different than the prior art distinguished during original prosecution and in the Cisco litigation. *See* §§ II.B.1, II.B.2, *supra* (citing Ex. 1002 at 1365 and Ex. 1027 at 61).



Ex. 1004, Fig. 6 (annotated).

If the received packet (e.g., packet from **client 404A** in the described example) is not encrypted, then decryption would not be applicable and **SSL decryption engine 610** would not be used. Ex. 1004 at 14:37-38. Accordingly, that situation deals only with unencrypted packets, not encrypted packets.

Petitioner cites no instance in which Buruganahalli teaches “filtering . . . based on” criteria “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,” as claimed. *See, e.g.*, Ex. 1001, claim 1. Nor could it. Buruganahalli explains that if its firewall cannot decrypt the encrypted

data, it “cannot detect such firewall policy/rule violation(s).” Ex. 1004 at 11:2-6.

This is why Buruganahalli describes creating two half sessions in Figure 3B—so it can perform decryption and “inspect decrypted traffic.” *Id.* at 12:4-64, Fig. 3B. In other words, if encrypted packets are to be monitored, they are always decrypted, and the decrypted data is filtered based on policies.

Petitioner relies on a short passage in Buruganahalli as allegedly disclosing the claimed filtering of encrypted data communications. Pet. at 38 (citing Ex. 1004 at 4:16-22). But that portion of Buruganahalli explicitly states that “encrypt[ed] data communications” 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.” Ex. 1004 at 4:16-22.

Petitioner next represents that, in Buruganahalli, “the firewall filters encrypted data communications after a determination that the handshake traffic corresponds to a network-threat indicator (*e.g.*, whether the extracted destination domain is on a blacklist)” and that Buruganahalli discloses “encrypted data communications associated with a secure session monitored for filtering based on a firewall policy.” Pet. at 38 (citing Ex. 1004 at 6:12-39). But, again, the cited portion of Buruganahalli explains the firewall may initially allow a session/flow

but then “require[s] that the session be **decrypted** for further analysis and further potential filtering based on the policy.” Ex. 1004 at 6:17-22 (emphasis added).

In stark contrast to Buruganahalli's decrypt-first approach is the '856 Patent's approach, which describes a packet-filtering system that filters packets comprising encrypted data time-and-time again. *See, e.g., id.* at 9:66-10:15 (step 19 in Fig. 3B), 11:36-51 (step 23 in Fig. 3B), 11:51-65 (step 24 in Fig. 3B). This concept is captured in the claims through the “determining” step and filtering “the determined packets comprising the encrypted data.” *See, e.g.,* Ex. 1001, claim 1. The '856 Patent's only reference to decryption describes decrypting data *after* (and separate from) the filtering. Ex. 1001 at 10:15-16.

In tacit recognition that Buruganahalli does not disclose filtering encrypted data, Petitioner makes conclusory statements about a skilled artisan's understanding and motivation. Pet. at 38. But Petitioner cites no supporting evidence beyond similarly conclusory statements in its expert declaration. Ex. 1003, ¶¶ 134-135. For example, 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. at 38. But, again, this assertion does not address the claimed filtering of encrypted packets based on specific rules because, in Buruganahalli, the

“packets communicated as part of a secure session” must be decrypted before filtering based on the policies. See Ex. 1004 at 11:2-6; *id.* at 7:64-67 (“[A] session associated with the 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.”); see also *id.*, at 12:29-32, 12:59-61, 15:35-45.

Next, Petitioner switches to obviousness, contending 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. at 38-39. This conclusory argument again ignores that Buruganahalli teaches decrypting the encrypted data and **then** filtering decrypted data and ignores the rest of the claimed filtering step, which requires the filtering to be “based on” information specified by the claimed rules. This argument also ignores the substantial objective indicia of nonobviousness with a direct nexus to this claim element. See § V.B, *infra*.

Petitioner's obviousness rationale, that “because the handshake message comprises data (*e.g.*, destination domain) that also applies to the encrypted data of the session, such that the security risks associated with the handshake message and encrypted data are correlated,” ignores the express teachings of Buruganahalli.

Pet. at 38. First, Buruganahalli teaches that when a new flow is determined to be undesirable, the entire flow is blocked before the encrypted session is even established. Ex. 1004 at 5:62-6:1. Accordingly, in circumstances where Buruganahalli would block a communications session based on data located in a handshake packet, it blocks those sessions before any encrypted data is even received and does not, therefore, filter encrypted packets. *Id.*

Second, Buruganahalli teaches that one cannot assume “that the security risks associated with the handshake message and encrypted data are correlated,” as Petitioner conclusory suggests. To the contrary, Buruganahalli discloses that encrypted packets must be decrypted in order to determine whether the extracted destination domain name matches the domain associated with the session’s URL “in order to detect malware that attempts to fool a hosting site by including false destination domain information.” *Id.* at 8:11-24.

As all three challenged independent claims require “[filter/filtering] . . . based on” criteria “specified by the plurality of packet-filtering rules,” “the determined packets comprising the encrypted data,” Petitioner has failed to establish a reasonable likelihood that it will prevail on any claim, and institution should be denied.

B. The Petition Fails to Address Known Objective Evidence of Nonobviousness

The petition should be denied for failure to address known objective evidence of nonobviousness. *See Stryker*, Paper 10 at 27-29 (discretionarily denying institution for “failure to address the known evidence of secondary considerations”). This failure is egregious given that Petitioner was on notice of such evidence from the Cisco litigation⁹ and that Petitioner’s counsel is keenly aware of Petitioner’s burden to address such evidence. Aside from this procedural failure, the evidence itself establishes that there is no reasonable likelihood Petitioner will prevail.

As discussed in Section V.A, *supra*, the petition fails to demonstrate that any claim is obvious, much less “overwhelmingly” so. Pet. at 50. 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).

⁹ Patent Owner previously argued that Petitioner failed to address these known secondary considerations. *See, e.g.*, IPR2021-01156, Paper 7 at 58-59.

Objective indicia of nonobviousness were integral to the court's validity determination and enhanced verdict of willful infringement in the Cisco litigation. *See* Ex. 1027 at 57-58, 61-65. Petitioner correctly states that "the trial transcript in the Cisco suit references purported secondary considerations for the '856 patent (Ex. 1029 at 3215:4-3240:4)," but falsely states "the underlying evidence is not publicly available and Petitioner does not have access to such evidence." Pet. at 50. In fact, a portion of the underlying evidence appears in Petitioner's own exhibit—twice. Petitioner's Exhibit 1027 (the Cisco litigation Opinion) twice reproduces a Cisco press release from 2017 called PTX-1135, 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. 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 (citation omitted). Indeed, Cisco's engineers touted that the very technology it copied from Centripetal, detecting network attacks in encrypted traffic "solv[ed] a network security challenge previously thought to be unsolvable." *Id.* at 63 (citation omitted) (quotation omitted); *see also id.* at 60-63. 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 established by way of the court’s finding that the ’856 Patent was infringed by, in part, Cisco’s Encrypted Traffic Analytics. *See* Ex. 1027 at 30-57.

Additionally, the district court found that Cisco copied the ’856 Patent. *Id.* at 57, 160-161. “It is well established that copying by a competitor is a relevant consideration in the objective indicia analysis.” *Liqwd*, 941 F.3d at 1137 (citations omitted). 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. Yet, Petitioner ignores that the court in the Cisco litigation also found compelling evidence of copying.

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, 155-157. 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.*

Petitioner cannot hide from this objective evidence of nonobviousness. The Board has repeatedly “cautioned petitioners in prior proceedings that petitions may be denied if they do not address known evidence of secondary considerations.” *See Stryker*, Paper 10 at 27-29 (discretionarily denying institution) (referencing *Robert Bosch Tool Corp. v. SD3 LLC*, No. IPR2016-01751, Paper 15 at 22-33 (P.T.A.B. Mar. 22, 2017) (denying institution on the merits for failure to address objective indicia presented during an ITC proceeding); *Coalition for Affordable Drugs V LLC v. Hoffman–LaRoche Inc.*, No. IPR2015-01792, Paper 14 at 17-18 (P.T.A.B. Mar. 11, 2016) (same but during prosecution); *Merial Ltd. v. Virbac*, No. IPR2014-01279, Paper 13 at 26-27 (P.T.A.B. Jan. 22, 2015) (same); *Omron Oilfield & Marine, Inc. v. MD/TOTCO*, No. IPR2013-00265, Paper 11 at 12-16 (P.T.A.B. Oct. 31, 2013) (same but during reexamination)).

As now recognized among practitioners before the Board: “the failure to address previously established indicia could prove fatal to [a] petition,” and “Petitioners would be wise to address previously argued objective indicia in order

to complete a proper *Graham factor* analysis.” Ex. 2010 at 1, Scott McKeown, *PTAB Denies Petition Overlooking Objective Indicia of Non-Obviousness*, Ropes & Gray - Patents Post-Grant (Sept. 18, 2019).¹⁰ Petitioner has not heeded its own counsel's warning, ignoring the significant record of objective indicia of nonobviousness. For this reason, the petition should be denied.

VI. CONCLUSION

Because the petition's only purpose is harassment, because the prior art is substantially similar to that overcome during prosecution and in district court, and because the petition fails to show a reasonable likelihood of prevailing on any challenged claim, Patent Owner requests the Board deny institution.

¹⁰ Ex. 2010, available at

<https://web.archive.org/web/20210303015939/https://www.patentspostgrant.com/pat-tab-denies-petition-overlooking-objective-indicia-of-non-obviousness/>.

Patent Owner's Preliminary Response
IPR2022-00182 (U.S. Patent No. 9,917,856)

Respectfully submitted,

Dated: February 28, 2022

/James Hannah/

James Hannah (Reg. No. 56,369)
Jenna Fuller (Reg. No. 74,212)
Kramer Levin Naftalis & Frankel LLP
990 Marsh Road
Menlo Park, CA 94025
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)
Blair A. Silver (Reg. No. 68,003)
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 COMPLIANCE

The undersigned hereby certifies that the portions of the above-captioned PATENT OWNER'S PRELIMINARY RESPONSE specified in 37 C.F.R. § 42.24 has 11,234 words in compliance with the 14,000-word limit set forth in C.F.R. § 42.24(b)(1)(i). This word count was prepared using the Microsoft Word word-processing system used to prepare this paper.

Respectfully submitted,

Dated: February 28, 2022

/James Hannah/
James Hannah (Reg. No. 56,369)
Jenna Fuller (Reg. No. 74,212)
Kramer Levin Naftalis & Frankel LLP
990 Marsh Road
Menlo Park, CA 94025
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)
Blair A. Silver (Reg. No. 68,003)
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, service was made on Petitioner as detailed below.

<i>Date of service</i>	February 28, 2022
<i>Manner of service</i>	Electronic Filing with the Board
<i>Documents served</i>	PATENT OWNER'S PRELIMINARY RESPONSE
<i>Persons served</i>	ROPES & GRAY LLP Scott A. McKeown James Batchelder Mark D. Rowland Andrew Radsch Keyna Chow

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