

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, INC.,
Patent Owner.

Case IPR2022-01151
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	11
1.	Prosecution History	11
2.	The Cisco Litigation	14
C.	Overview of Buruganahalli	17
D.	Overview of Baehr	25
E.	Level of Ordinary Skill	26
III.	THE BOARD SHOULD TERMINATE THIS CASE AND THE UNDERLYING PROCEEDING ABSENT A FINDING OF “COMPELLING MERITS” IN THE PAN PETITION	27
IV.	BURUGANAHALLI DOES NOT TEACH THE CLAIMED RULE- BASED FILTERING OF ENCRYPTED PACKETS	34
1.	Buruganahalli Filters Only Unencrypted or Decrypted Data	34
2.	Petitioner Has Not Identified a Single Instance Where Buruganahalli Teaches Filtering Encrypted Packets	41
3.	Petitioner Cannot Rewrite Buruganahalli’s Decrypt-First Approach with Conclusory Statements About a Skilled Artisan’s Understanding and Obviousness	45
V.	CONCLUSION	49

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>In re Baxter Travenol Labs.</i> , 952 F.2d 388 (Fed. Cir. 1991).....	39
<i>Centripetal Networks, Inc. v. Cisco Systems, Inc.</i> , Civil Action No. 2:18-cv-94 (E.D. Va. Feb. 18, 2018).....	2
<i>Centripetal Networks Inc. v. Keysight Technologies, Inc.</i> , Case No. 2:17-cv-00383 (E.D.Va. 2017)	32
<i>HTC Corp. v. Ancora Techs., Inc.</i> , IPR2021-00570, Paper 17 (P.T.A.B. Jun. 10, 2021).....	32
<i>Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.</i> , 821 F.3d 1359 (Fed. Cir. 2016).....	47, 49
<i>Johns Manville Corp. v. Knauf Insulation, Inc.</i> , IPR2018-00827, Paper 9 (P.T.A.B. Oct. 16, 2018)	45
<i>KSR Int’l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007).....	47
<i>In re Leithem</i> , 661 F.3d 1316 (Fed. Cir. 2011).....	33
<i>LG Elec. v. Cellular Commc’ns Equip.</i> , IPR2016- 00197	48
<i>In re Magnum Oil Tools Int’l, Ltd.</i> , 829 F.3d 1364 (Fed. Cir. 2016).....	42
<i>Metalcraft of Mayville, Inc. v. Toro Co.</i> , 848 F.3d 1358 (Fed. Cir. 2017)	48
<i>Monsanto Tech. LLC v. E.I. DuPont de Nemours & Co.</i> , 878 F.3d 1336 (Fed. Cir. 2018).....	39
<i>Nintendo Co. v. Genuine Enabling Tech. LLC</i> , IPR2018-00543, Paper 7 (P.T.A.B. Aug. 6, 2018)	46

<i>OpenSky Indus., LLC, et al. v. VLSI Tech. LLC</i> , IPR2021-01064, Paper 102 (P.T.A.B. Oct. 4, 2022).....	<i>passim</i>
---	---------------

<i>SAS Inst.</i> , 138 S. Ct. at 1357	42
---	----

Statutes

35 U.S.C. §§ 101, 112.....	12
----------------------------	----

35 U.S.C. § 315(b)	2
--------------------------	---

35 U.S.C. § 316(e)	34
--------------------------	----

Board act.....	28
----------------	----

Other Authorities

37 C.F.R. § 42.24.....	51
------------------------	----

H.R. Rep. No. 112-98, pt. 1	27, 28, 29, 31
-----------------------------------	----------------

IPR2022-00182, Centripetal’s Request for Rehearing of the Institution Decision.....	1, 33, 36
--	-----------

PAN IPR DI at 70-71	37, 42, 43, 44
---------------------------	----------------

PAN IPR ID at 69	43
------------------------	----

rules 212	6
-----------------	---

U.S. Patent No. 9,419,942.....	31
--------------------------------	----

U.S. Patent No. 9,917,856.....	<i>passim</i>
--------------------------------	---------------

U.S. Patent No. 9,967,236 (“Ashley”; Ex. 2022).....	38
---	----

EXHIBIT LIST

Exhibit	Description
2001	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)
2002	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
2003	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) – CENTRIPETAL-CSCO 087501 – 88046
2004	Minutes of Proceedings, <i>Centripetal Networks, Inc. v. Keysight Techs, Inc., and Ixia</i> , No. 2:17-cv-00383, Dkt. No. 581 (E.D. Va. Oct. 9, 2018)
2005	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)
2006	Order, <i>Centripetal Networks, Inc. v. Cisco Sys., Inc.</i> , No. 2:18-cv-00094, Dkt. No. 68 (E.D. Va. Sept. 18, 2019)
2007	Declaration of Hanna h Lee in Support of Patent Owner's Opposition to Petitioner's Motion for Joinder
2008	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)
2009	Demonstrative Exhibit DDX2 - Adam Sorini Direct Examination, <i>Centripetal Networks, Inc. v. Keysight Techs, Inc., and Ixia</i> , No. 2:17-cv-00383 (E.D. Va.)

2010	Email from S. McKeown to J. Hannah re Precedential Opinion Panel Review for IPR2022-00182, dated, June 30, 2022
2011	Statement of Jonathan Rogers (COO, Centripetal Networks, Inc.) Before the Subcommittee on Courts, Intellectual Property, and the Internet - Committee on the Judiciary United States House of Representatives (June 23, 2022) https://www.congress.gov/117/meeting/house/114937/witnesses/HHRG-117-JU03-Wstate-RogersJ-20220623.pdf
2012	RESERVED
2013	U.S. Patent Application Publication No. 2005/0138353 to Spies <i>et al.</i>
2014	U.S. Patent Application Publication No. 2012/0023576 to Sorensen <i>et al.</i>
2015	U.S. Patent Application Publication No. 2004/0199629 to Bomer <i>et al.</i>
2016	U.S. Patent Application Publication No. 2015/0207813 to Reybok <i>et al.</i>
2017	U.S. Patent Application Publication No. 2014/0317397 to Martini
2018	U.S. Patent No. 6,098,172 to Coss <i>et al.</i>
2019	U.S. Patent Application Publication No. 2004/0088542 to Daude <i>et al.</i>
2020	Opinion, <i>Centripetal Networks, Inc. v. Cisco Sys., Inc.</i> , No. 21-1888, Dkt. No. 68 (Fed. Cir. June 23, 2022)
2021	Petition for Writ of Certiorari, <i>Centripetal Networks, Inc. v. Cisco Sys., Inc.</i> , No. __ (U.S. Sept. 13, 2022)

I. INTRODUCTION

The Board should deny the Petition, and grant Centripetal's Request for Rehearing of the Board's Institution Decision in IPR2022-00182,¹ because neither party has presented a reasonable likelihood that any claim of U.S. Patent No. 9,917,856 (Ex. 1001, "the '856 Patent") is unpatentable, let alone a case that satisfies the heightened "compelling merits" standard applicable in this case. *See OpenSky Indus., LLC, et al. v. VLSI Tech. LLC*, IPR2021-01064, Paper 102 at 49 (P.T.A.B. Oct. 4, 2022) (precedential) ("[W]hen determining whether to continue an IPR initially filed for improper purposes, I must consider the public interest, which compels the USPTO to evaluate unpatentability challenges that, at the institution stage, evidence compelling merits."). Because Palo Alto Networks, Inc., ("PAN") filed its petition for many of the same "improper purposes" as the petitioner in OpenSky, and at least raises "legitimate questions about whether the petition is reasonably designed to advance the beneficial aims of the AIA," the Board should "permit[] this IPR to continue only if the panel determines that the unpatentability

¹ Centripetal's Request for Rehearing of the Institution Decision in IPR2022-00182, which this Petition seeks to join, remains pending. *See* IPR2022-00182, Paper 13.

merits were compelling as of the time of institution and on the record as it existed at that time.” *Id.* at 36, 47.

Cisco is similarly situated to joinder-petitioner Intel in *OpenSky*. Like Intel, Cisco is an otherwise time-barred petition that seeks to join an IPR proceeding initiated by a third-party having no direct interest in the patent's validity. Unlike Intel, however, whose IPR petition was filed but never adjudicated on the merits, Cisco was never denied a merits hearing before the Board because (and despite having access to the references underlying PAN's petition) Cisco consciously chose not to avail itself of this forum within the time-period specified by 35 U.S.C. § 315(b). Cisco instead proceeded to challenge the '856 Patent with its self-described “best” prior art in a highly-contested district court litigation,² which began in February 2018 and concluded with one of the largest patent verdicts in history after the judge found the '856 Patent not invalid and Cisco's infringement thereof both willful and egregious. The fact that Cisco *chose* not to avail itself of this forum in its challenge to the '856 Patent and already had its opportunity to challenge the '856 Patent in the district court, is further reason to consider this case under the “compelling merits” standard. *See OpenSky* at 48-49 (applying the “compelling

² *Centripetal Networks, Inc. v. Cisco Systems, Inc.*, Civil Action No. 2:18-cv-94 (E.D. Va. Feb. 18, 2018) (“the Cisco litigation”).

merits” standard to balance the unfairness of giving the patent challenger a second bite at the apple with the “interest of the public” and the “USPTO and AIA goals).

Nevertheless, in view of the Board’s mistaken understanding of the Buruganahalli reference, neither this Petition nor PAN’s demonstrates even a reasonable likelihood that any claim of the ’856 Patent is invalid. In instituting trial in the underlying case, the panel misapprehended Buruganahalli’s teachings—wrongly concluding that Buruganahalli discloses rule-based of filtering encrypted packets without decryption. Although the Board’s Institution Decision pointed to Buruganahalli’s disclosure of actions that can be taken without having to decrypt encrypted traffic, not one of those disclosures is, involves, or suggests applying the claimed packet filtering rules to encrypted packets. To the contrary, Buruganahalli is explicit that when applying rules/policies to blacklisted packets that those packets *must* be decrypted. Evidence that Cisco copied Centripetal’s technology and then bragged that its stolen technology solved a “network security challenge previously thought to be unsolvable” only reinforces the fact that Buruganahalli does not teach or suggest the claimed solution to this identified problem. Ex. 1027 at 63-64.

Centripetal respectfully requests, therefore, that the Board consider the arguments and evidence presented in this case and determine that Cisco has not raised a reasonable likelihood that any of the Challenged Claims is unpatentable. The Board should also deny this Petition as a result of granting Centripetal’s pending

Request for Rehearing because PAN's nearly identical petition failed to demonstrate a reasonable likelihood that the Challenged Claims are obvious, let alone "compelling merits" that could justify instituting trial in this case.

II. BACKGROUND

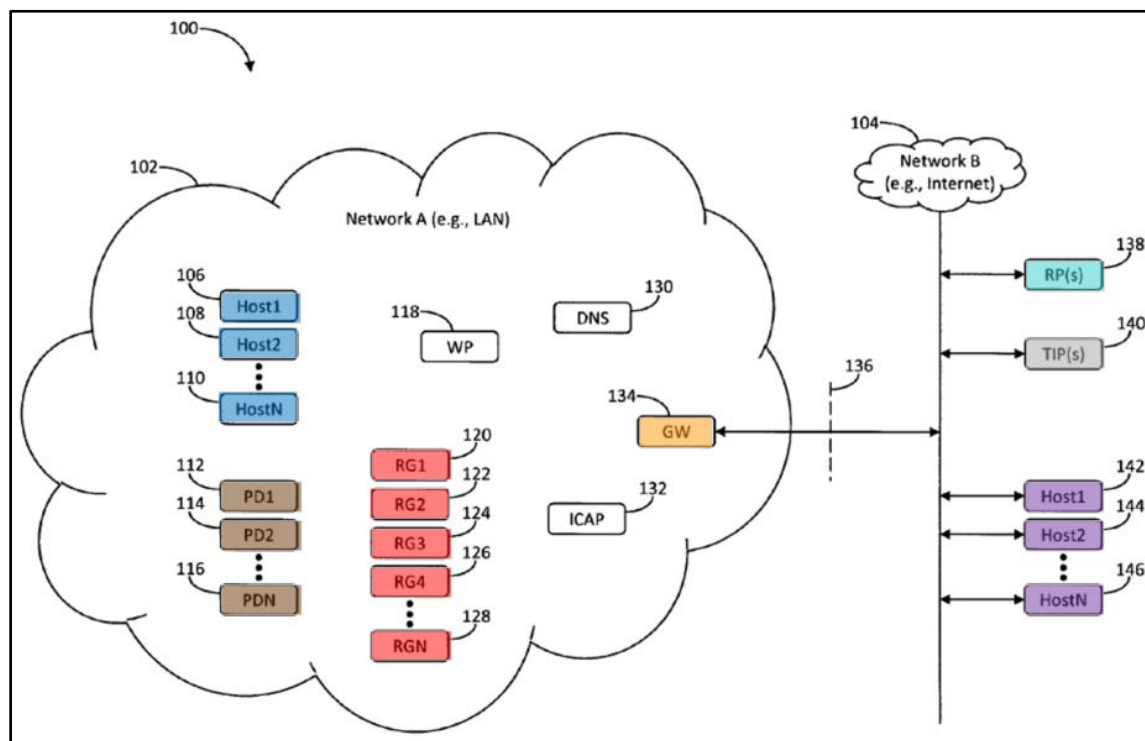
A. Overview of the '856 Patent

Prior to the '856 Patent, firewalls either filtered unencrypted packets to stop certain secure sessions of encrypted packets before they started, or attempted to decrypt encrypted packets and filter the decrypted data, as in Buruganahalli. Ex. 1004 ("Buruganahalli") at 11:2-6. With the '856 Patent's inventive approach, network-threat detection of encrypted packets is performed on encrypted traffic without decryption. 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. 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 the ability to: (i) end a secure session that is later deemed to be a threat per an updated rule, or (ii) allow a secure session to pass through the firewall without any further processing per an

updated rule that indicates the secure session is not a threat. Ex. 1001 at 14:19-16:26, 22:20-51. Another advantage of a firewall implementing the '856 Patent's technology to perform rule-based filtering of encrypted packets is that it can allow a secure session initially and end it after a time or data limit is exceeded because such firewall continues to log encrypted packets. See generally Ex. 1001 at 9:33-46, 11:28-35. This means the firewall can prevent too much data from being extracted by bad actors if the secure session turns out to be a threat.

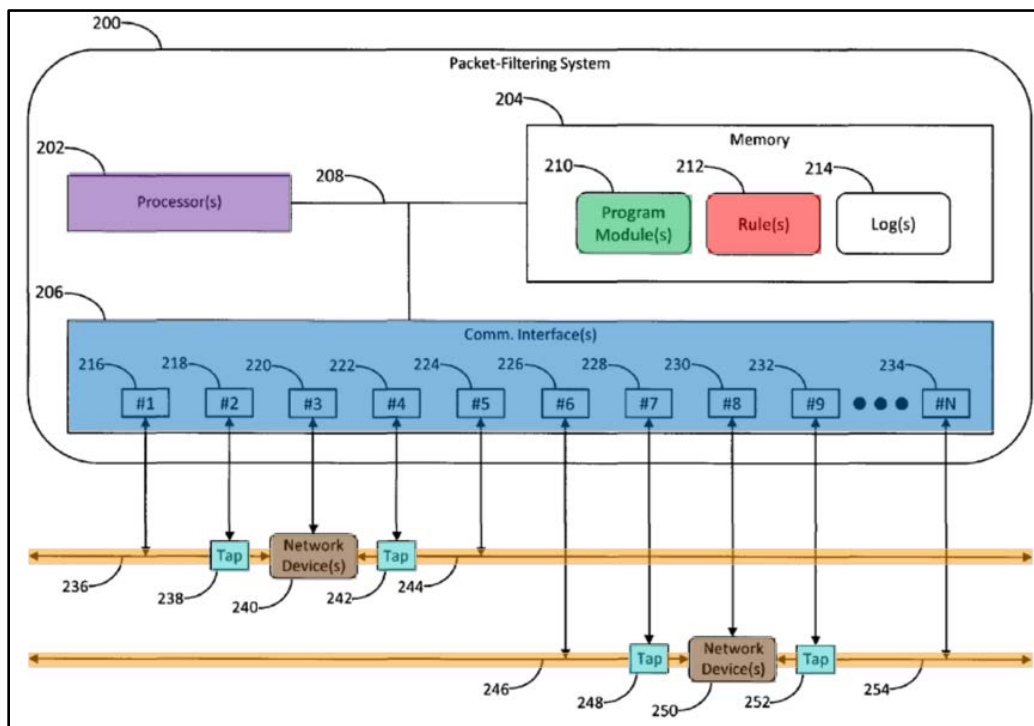
Figure 1 (annotated below) depicts an illustrative environment using the inventive approach to protect network 102 from threats in network 104. *Id.* at 2:20-34, Fig. 1.



Ex. 1001, Fig. 1 (annotated)

Gateway 134 interfaces network 102 with network 104. *Id.* at 2:50-53. Network 102 includes **hosts 106, 108, 110** for communicating with **hosts 142, 144, 146**. *Id.* at 2:35-53. Network 102 also includes **proxy devices 112, 114, 116** and **rule gates 120 122, 124, 126, 128**. *Id.* at 2:35-43. 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.

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

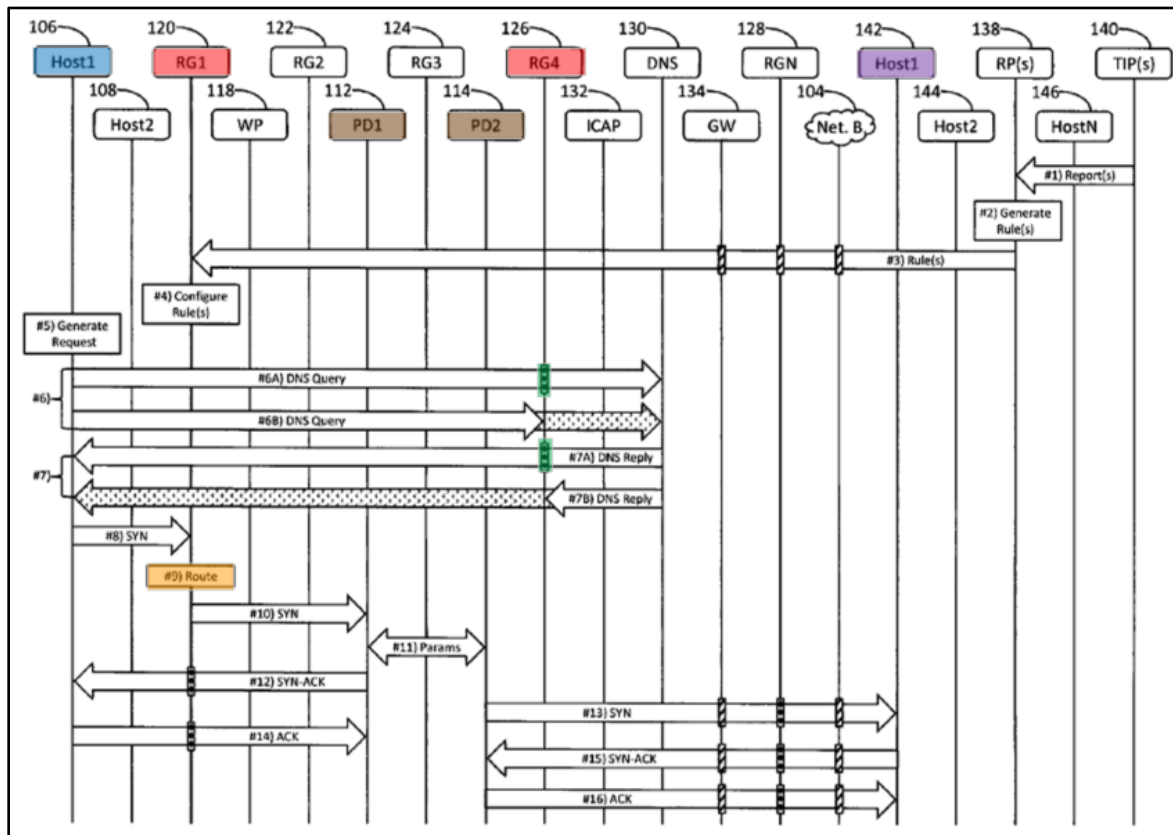


Ex. 1001, Fig. 2 (annotated)

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 2:66-7:14. It also includes a **communication interface 206** for

interfacing with **communication links 236, 244, 246, 254** through **tap devices 238, 242, 248, 252** or **network devices 240, 250**. *Id.* at 3:15-56.

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).

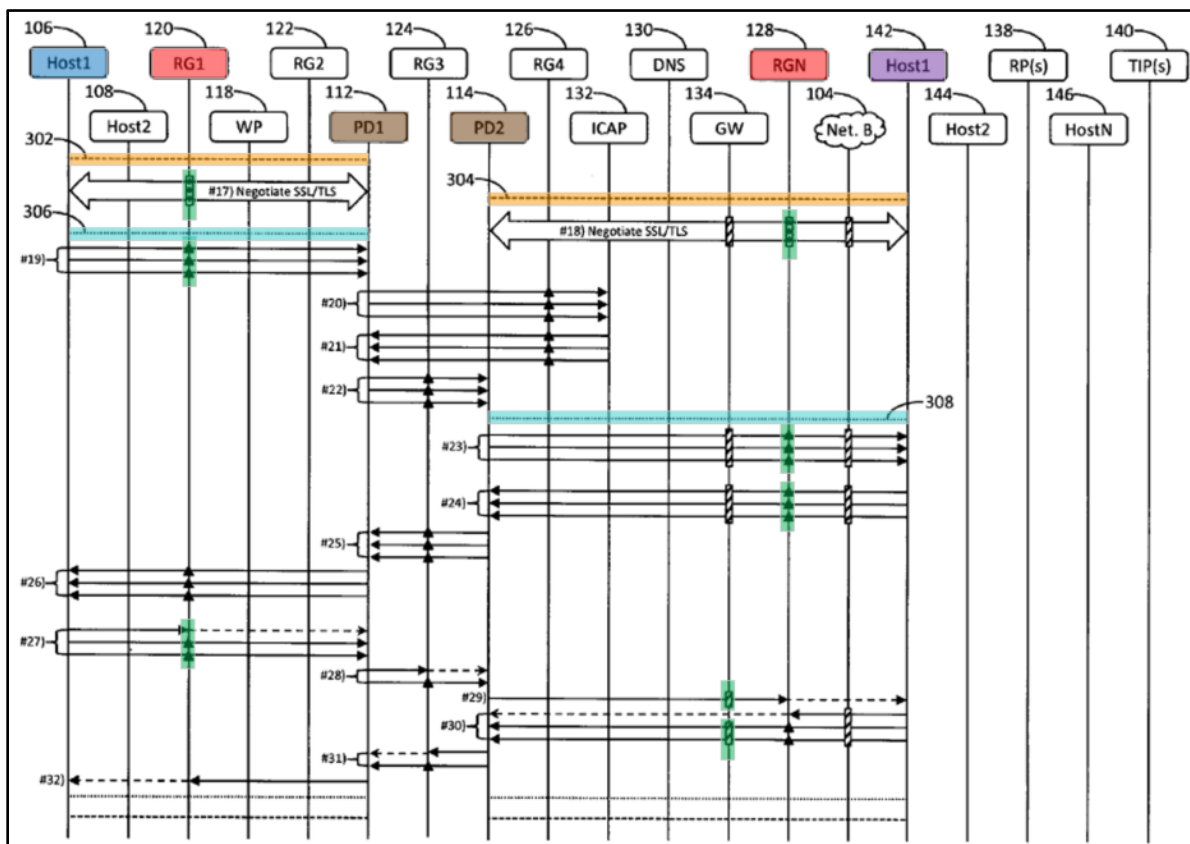


Ex. 1001, Fig. 3A (annotated)

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. **Rule gate 126 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. **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.

Proxy devices 112, 114 set up two separate connections (steps #11-16): **connection 302** between **the proxy system** and **host 106** and **connection 304** between **the proxy system** and **host 142**. *Id.* at 7:33-8:64, Figs. 3A, 3B (annotated below).



Ex. 1001, Fig. 3B (annotated)

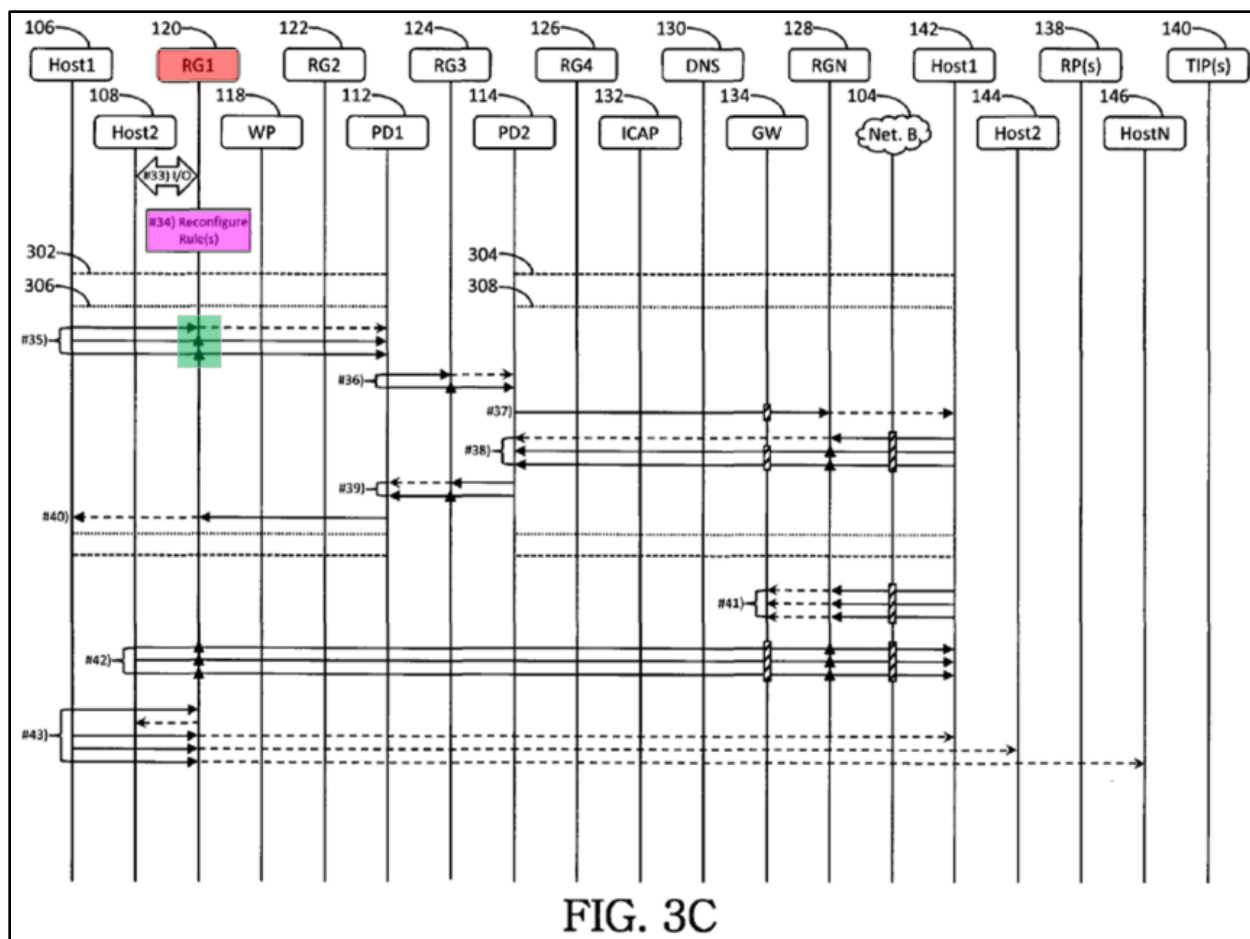
Handshake messages are exchanged to establish two separate encrypted communication sessions (steps #17-18): **encrypted communication sessions 306 and 308**. *Id.* at 8:65-9:65, Fig. 3B. These handshake messages include, *e.g.*, a client hello message having unencrypted data. *Id.* at 9:16-33. **Rule gate 120** using rules may **filter** the handshake messages. *Id.* at 9:2-46. Similarly, **rule gate 128** using rules may **filter** the handshake messages for establishing encrypted communication session 308. *Id.* at 9:47-65.

Once **encrypted communication sessions 306, 308** are established, encrypted packets are communicated in those sessions. 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. Even though an encrypted packet may be passed by **rule gate 120** (step #19), **rule gate 120** continues to **filter** encrypted packets and may later drop another encrypted packet (step #27). *Id.* at 12:28-42. Similar **filtering** is performed by **rule gate 128** (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).

This difference is captured by each independent claim. 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). This rule-based filtering of encrypted packets marks a significant advancement over the prior art.

The data logged from filtering encrypted packets can be used to **reconfigure rules** (step #34). 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. 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.

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 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. Most claims were rejected based on a combination of Spies (Ex. 2013) and Sorenson (Ex. 2014). Ex. 1002 at 1070-81. Then-pending claims 14 and 15 were rejected on Spies, Sorenson, and Bomer (Ex. 2015). *Id.* at 1081-83.

Patent Owner's response included amending representative independent claim 1 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 1351-67.

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). 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.*

The Notice of Allowance included an examiner’s amendment based on a prior interview. *Id.* at 1374-1400. For 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. *Id.* at 1381-86.

The examiner’s reasons for allowance stated that the “instant application is directed toward 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, and stated: “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.* As evidence of this further search and consideration, the examiner specifically discussed one of the references, Reybok (*Id.* at 1389-90), which, like Cisco’s Buruganahalli reference, also describes performing decryption before filtering. Ex. 2016 at ¶¶ 0068-0069, Fig. 6B.

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 1-2. After a twenty-two day bench trial, the district court concluded that Cisco willfully infringed four of Centripetal’s patents, including the ’856 Patent. Cisco’s 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 factual findings 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 system³ using Cisco’s proprietary logging framework, Netflow. *Id.* at 34, 57. 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—and believed this was the strongest prior art to the '856 Patent. Indeed, Cisco believes the Stealthwatch system was its “best” prior art to the '856 Patent. Pet. 25. Cisco’s trial 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. Ex. 1027 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.*

³ 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 34, 57.

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 63-64. 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[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 55-56. 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"), 157 (concluding that "damages should be enhanced for copying").

Cisco appealed the district court's judgment, but never challenged the judge's validity findings with respect to the '856 Patent on appeal. Ex. 2020 at 7. Instead, Cisco challenged the district court judgment on the basis that the district court judge was allegedly biased because his wife owned Cisco stock. *Id.* at 5-14. Cisco argued that the judge should have recused himself and that his placing the stock into a blind trust was insufficient. *Id.* Although the district court judge did not learn of his wife's stock until after he prepared a full draft of his opinion in favor of Centripetal (a decision that adversely affects any interest he may have in Cisco's stock), the Federal Circuit vacated the district court's judgment finding that placement of the stock in a blind trust was insufficient and not harmless error. *Id.* at 2-4, 25-27. Centripetal has recently filed a Petition for Writ of Certiorari with the U.S. Supreme Court to reconsider the Federal Circuit's vacatur. Ex. 2021.

C. Overview of Buruganahalli

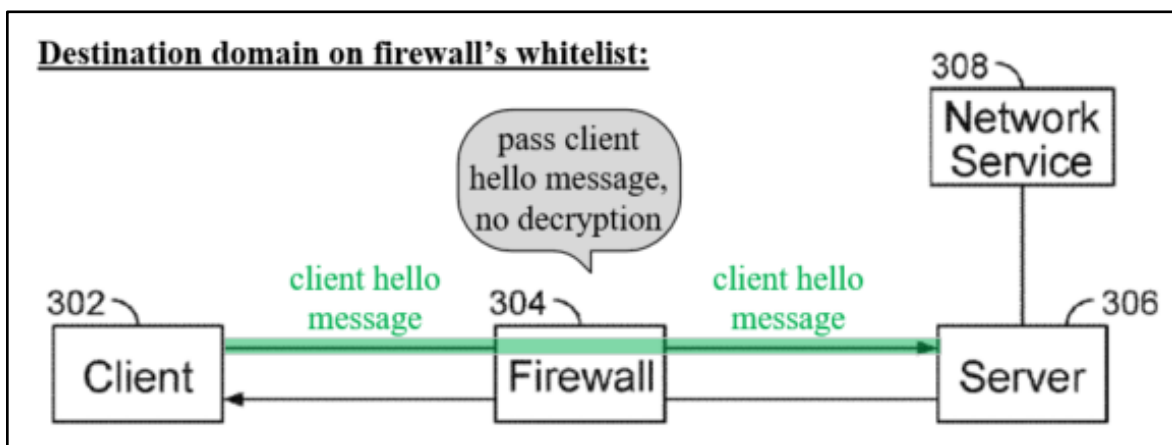
Like the old Stealthwatch and each of the references considered during prosecution of the '856 Patent, Buruganahalli lacks "the functionality to identify threats in encrypted traffic **without** the use of decryption." Ex. 1027 at 61. Buruganahalli is explicit: "[A] session associated with the network communications

between the client and the remote server are decrypted if the destination domain is included in the blacklist),⁴ and/or a uniform resource locator (URL)/category filtering policy.” Ex. 1004 at 7:47-51; *see id.* at 7:63-67 (“[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.”).

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 4:45-67. 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. Buruganahalli describes three scenarios for utilizing this SNI field, none of which involve applying packet-filtering rules to encrypted packets without decrypting them first.

⁴ Notably, Petitioner relies on the blacklist embodiments in Buruganahalli because only blacklisted domains allegedly correspond to the claimed “network-threat indicators.” *See* Pet. at 31.

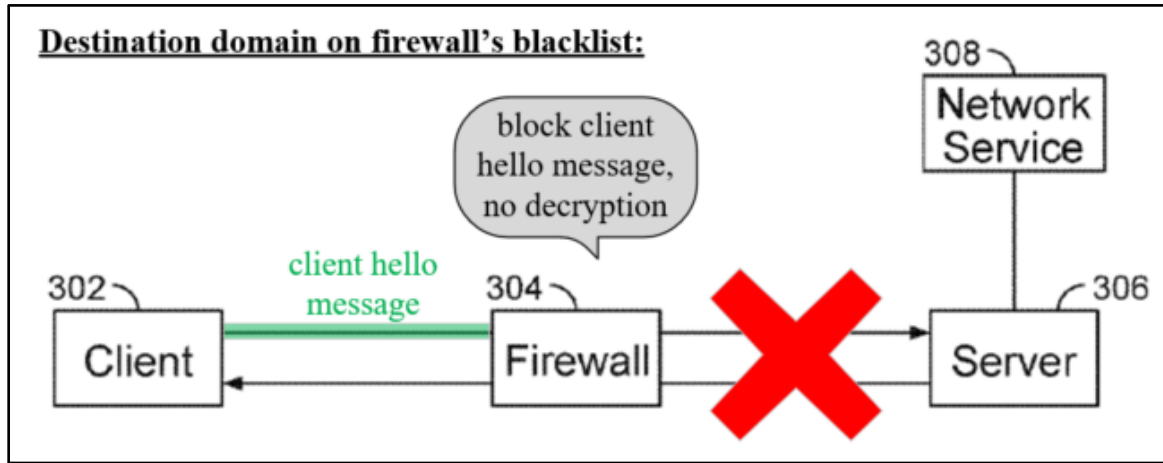
First, regarding Figure 3A (annotated below), if a destination domain is on the *whitelist*, the firewall allows the **client hello message** to pass through to the server and allows a secure connection to be established between the client and server. Ex. 1004 at 5:43-51, 6:1-11, 7:52-59, 10:54-11:6,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



Buruganahalli, Fig. 3A (annotated)

Second, if the destination domain is on the blacklist, the firewall can block the unencrypted **client hello message** from passing through to the server. *Id.* at 5:64-6:11, 10:54-11:19, 4:31-44. In this scenario, no encrypted packets are ever received because no secure connection is established in the first place. Ex. 1004 at 5:64-6:11, 10:54-11:19, 4:31-44. Buruganahalli thus unsurprisingly states that, in this scenario, the firewall can apply a policy “without having to decrypt,” because no secure, encrypted session is ever started and no encrypted packets are received. Ex. 1004 at 11:7-19, 4:31-44. Because firewall 304 does not perform decryption of encrypted

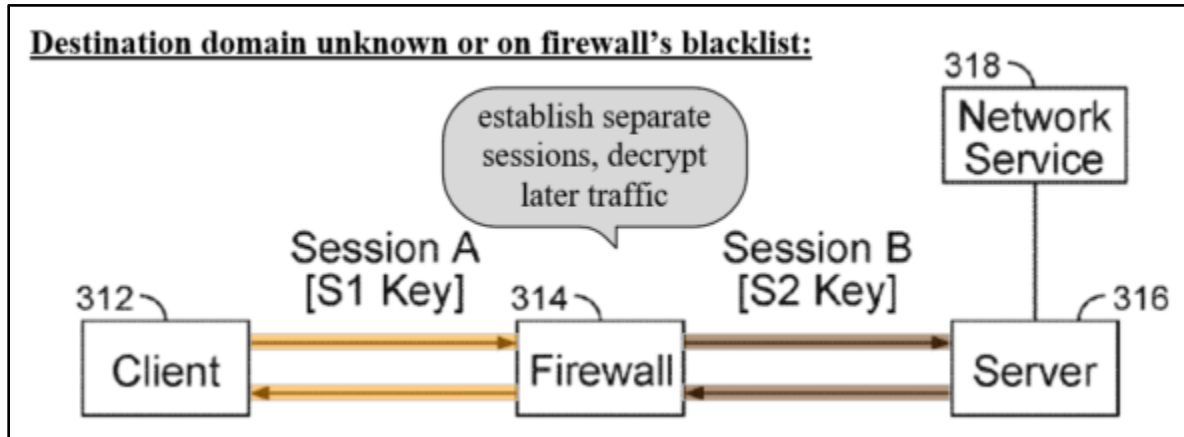
packets, it also “cannot detect such firewall policy/rule violation(s)” in the encrypted packets. Ex. 1004 at 11:2-6.



Buruganahalli, Fig. 3A (annotated)

Third, 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 of any further encrypted traffic associated with that session. *Id.* 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 12:4-61 (“[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”; “[s]imilarly, traffic coming from the server is **decrypted** with the session key S2, inspected by the firewall 314, and

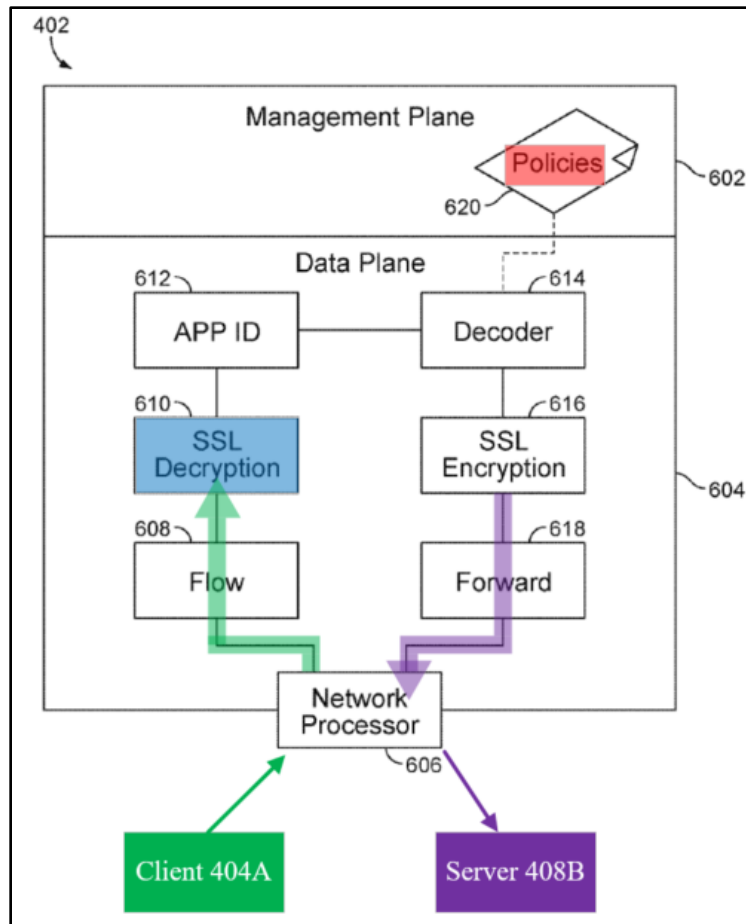
then encrypted using the session key S1 and forwarded to the client 312”) (emphasis added).



Buruganahalli, Fig. 3B (annotated)

None of these three scenarios involves rule-based filtering of encrypted packets. In every scenario, Buruganahalli processes *only* unencrypted packets or decrypts encrypted packets. 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 4:20-22.

Buruganahalli reinforces this when describing 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.

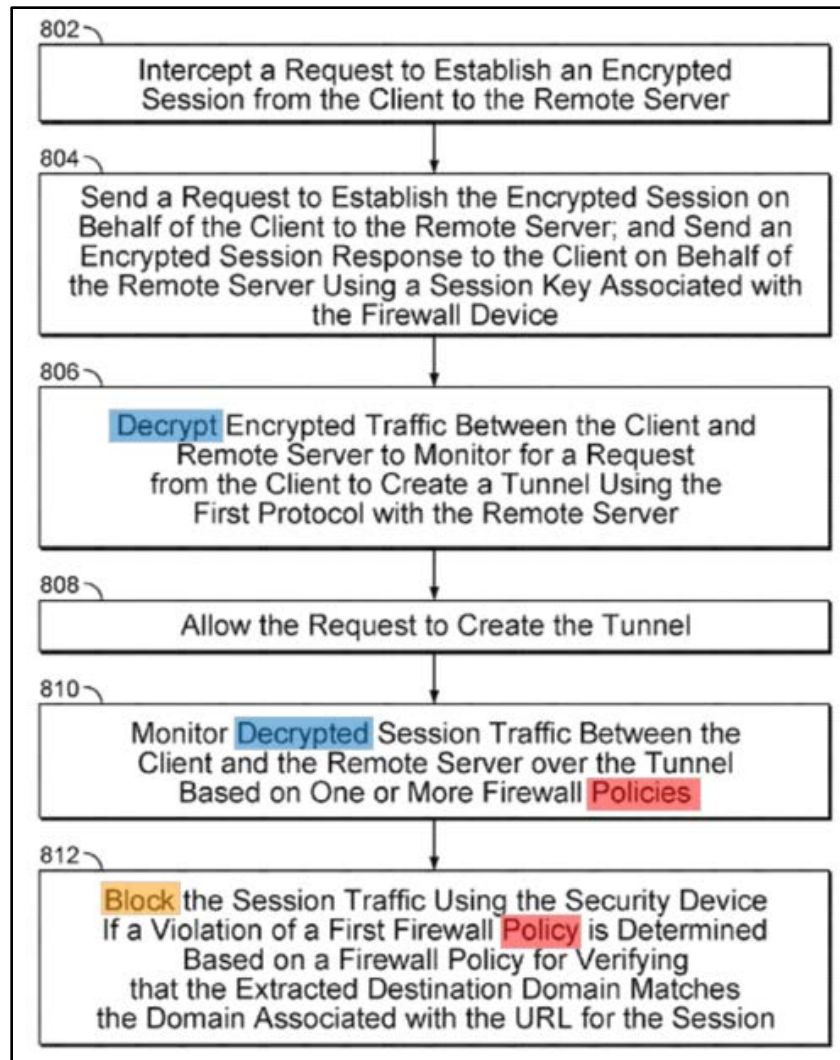


Buruganahalli, Fig. 6 (annotated)

Network processor 606 receives a packet from **client 404A** intended for **server 408B**. *Id.* 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, 9:25-30 (describing use of IP address). If an encrypted packet does not belong to a whitelisted flow/session, it is decrypted by an internal **SSL decryption engine 610**—not routed to a proxy system external to the firewall. *Id.* 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. *Id.* at 14:50-58, 14:21-22, Fig. 6; *see also id.* at 9:44-10:28, Fig. 1 (describing policy engine 120 applying policies after receiving results from decrypting and decoding encrypted traffic).

Finally, regarding Figure 8 (annotated below), 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. *Id.* at 15:22-45, Fig. 8.

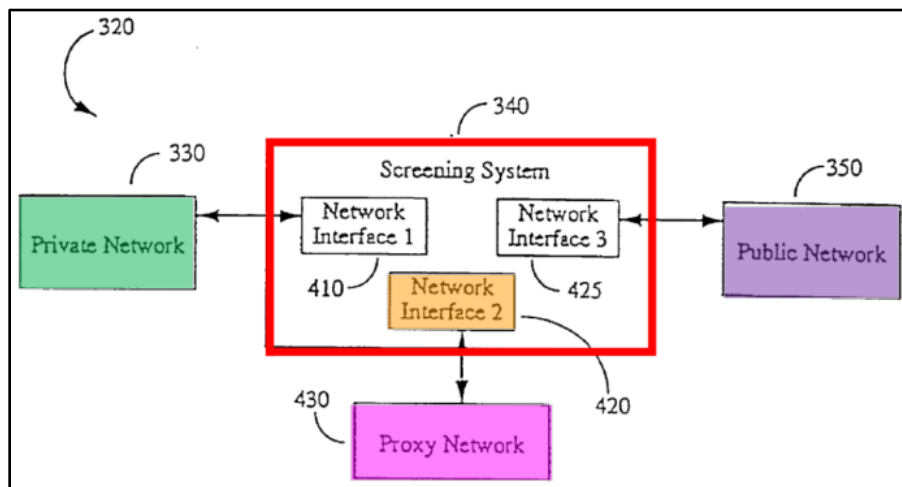


Buruganahalli, Fig. 8 (annotated)

Accordingly, in every instance Buruganahalli only applies policies to unencrypted packets or decrypted data—never to encrypted packets. Indeed, 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. *Id.* at 4:16-22, 11:59-13:4, claims 1, 6-10. Because the firewall itself is the man-in-the-middle, it never routes filtered packets to a separate proxy system.

D. Overview of Baehr

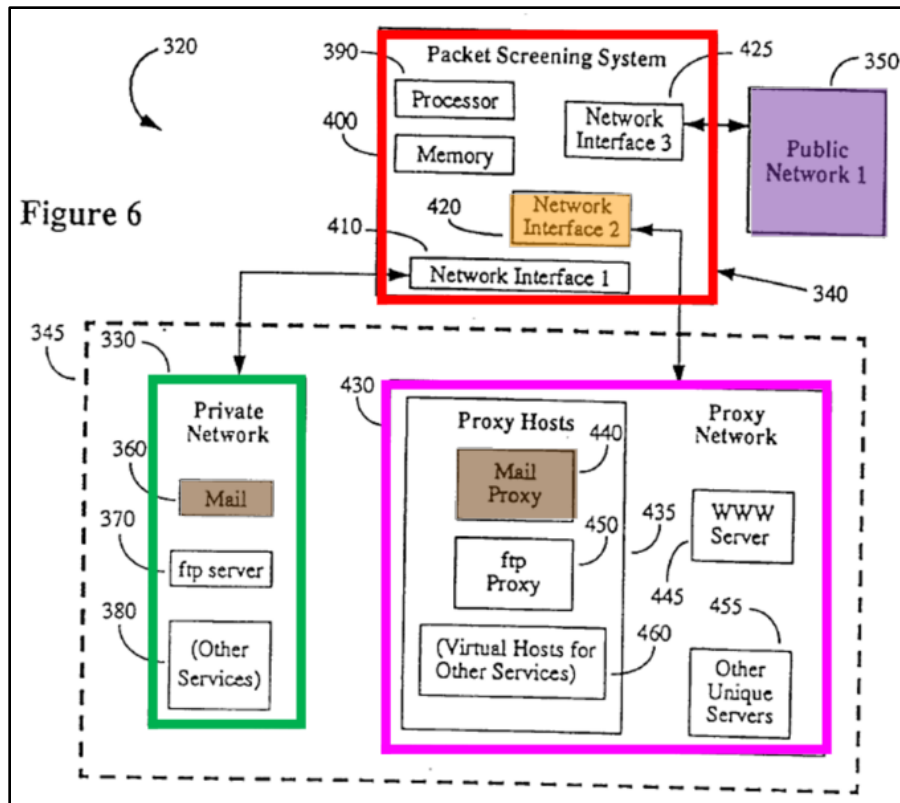
Baehr (Ex. 1005) describes a system for screening packets transmitted between a **private network** and a **public network**. Ex. 1005, Abstract, 1:9-17, 2:10-17, Fig. 5 (annotated below). Baehr adds **network interface 420** to **screen 340** for coupling it to **proxy network 430**. *Id.* at 3:51-64.



Baehr, Fig. 5 (annotated)

Packets received at the **screen** (e.g., from the **public network**) are allowed, dropped, or sent to a host on the **proxy network**. Ex. 1006 at Abstract, 10:46-49.

Baehr's Figure 6 (annotated below) 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.



Baehr, Fig. 6 (annotated)

There is nothing remarkable about Baehr's use of a proxy as compared to other proxy systems considered during prosecution. And, Baehr is not even relied on for curing the deficiency of Buruganahalli (*see* Section VI, *infra*) to teach the claimed rule-based filtering of 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. 32-33.

III. The Board Should Terminate this Case and the Underlying Proceeding Absent a Finding of “Compelling Merits” in the PAN Petition

The Director recently issued a precedential opinion in *OpenSky*. That case shares many of the procedural anomalies at issue here. Just like in *OpenSky*, a party not accused of infringement challenged a patent underlying a recent, significant damages award. See *OpenSky* at 34-44. As a result of concerns about the Director determined that “[a]lthough it is not *per se* improper for a person not charged with infringement to file an IPR petition, the posture of a petitioner, in conjunction with surrounding circumstances, could raise legitimate questions about whether the petition is reasonably designed to advance the beneficial aims of the AIA or this Office and whether, in addition, the filing amounts to an abuse of process.” *OpenSky* at 36. And although there is no evidence to suggest that PAN committed some of the more egregious abuses at issue in *OpenSky*, including formation of the entity directly following the district court verdict and attempting to extract cash payments from both parties in return for a promise to alter its litigation strategy, the “surrounding circumstances” here warrant a conclusion that the underlying Petition that Cisco seeks to join does not “advance the beneficial aims of the AIA or this Office.” *Id.*

In passing the AIA, Congress did not seek to place bounties on Article III. To the contrary, Congress expressly stated its intention that the PTAB provide a “quick and cost effective alternative[] to litigation.” H.R. Rep. No. 112-98, pt. 1, at 48. A

system where every Article III judgment is open to collateral attacks by parties with no stake in the outcome fully undermines this goal because such attacks allow defendants to have their cake and eat it too. And although the Director stated that the circumstances of the *OpenSky* case “are unusual and are not likely to reoccur,” a permissive attitude towards the type of collateral attack filed in *this* case only will undoubtedly encourage more opportunistic behavior that deprives patent owners of any hope of quiet title. *OpenSky* at 48; H.R. Rep. No. 112-98, pt. 1, at 48 (recognizing “the importance of quiet title to patent owners to ensure continued investment resources”).

Any decision that encourages petitioners like PAN, who has not been accused of infringing the '856 Patent, also encourages similarly situated petitioners to request that the Board act as a *de facto* appellate body to review Article III judgments. Nothing in the AIA or its legislative history indicates that Congress sought to undermine the courts, and as the Director correctly notes, “AIA proceedings were not... intended to replace patent litigation, which remains a vital forum for determining patent validity.” *OpenSky* at 28-29. But when the validity of a patent that has been fully litigated in district court is subject to cancellation in a

subsequently-initiated AIA proceeding,⁵ the result is one which, for all intents and purposes, replaces patent litigation.

That the Board applies a more lenient standard of proof the district court and third-party petitioners have access to arguments, evidence, and judicial opinions stemming from district court challenges only make the filing of such post-judgment challenges more pernicious. Rather than ensuring that IPRs are “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,” such challenges promise to put a cloud over every patent judgment and harass patent owners who in many cases have already had to withstand one or more validity challenges. H.R. Rep. No. 112-98, pt. 1, at 48 (“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.*

⁵ Centripetal does not suggest that parties with a concrete interest in the validity of a patent cannot raise their own validity challenges in the venue of their choice, subject to

The “surrounding circumstances” here illustrate why instituting review would pose a grave threat to the integrity of the patent system, or at least should require consideration of PAN’s Petition (for which a Request for Rehearing remains pending) the application of the “compelling-merits” standard. *OpenSky* at 36, 48-49. Absent “compelling merits,” of which there are none, the “public interest in cancelling invalid patents” has already been vindicated here. The claims have already withstood a thorough vetting process through 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.

The status of the parties involved here (*i.e.* PAN, Cisco, and a second joinder Petitioner, Keysight Technologies, Inc.), as practicing entities rather than non-practicing entities, like *OpenSky*, also raises issues not addressed in the *OpenSky* decision. Any decision in this case not to apply the “compelling merits” standard to the underlying Petition in this case will only encourage *more* instances of industry members collaterally attacking Article III judgments decided against their competitors and reopening the door to otherwise time-barred parties to a second (or third) bite at the invalidity apple. So long as the parties cooperate to check each other’s Article III verdicts openly and without express coordination with a time-

barred party (which would implicate real-party-in-interest bars to such petitions), AIA proceedings will no longer serve their intended purpose as alternatives to district court litigation promise to supplant that venue entirely. Such a result fully undermines the AIA's goal to provide an alternative to district court litigation and allows entrenched incumbents "prevent market entry through repeated litigation and administrative attacks on the validity of a patent." H.R. Rep. No. 112-98, pt. 1, at 48.

Other "surrounding circumstances" also "raise legitimate concerns about whether the petition is reasonably designed to advance the beneficial aims of the AIA." *OpenSky* at 36. As Cisco readily admits, it consciously chose to proceed with its validity challenge to the '856 Patent in district court because its "best" art (Pet. 25) was system art that could not be raised in an IPR, which only permits challenged based on patents and printed publications. Pet. 25; Ex. 1027 at 57. Cisco proceeded to trial with the old Stealthwatch system art despite being well aware of Buruganahalli at least as of November 2019, when Patent Owner produced invalidity contentions and expert reports from a prior litigation to Cisco. Ex. 2002; Ex. 2003. Those documents produced included U.S. Patent No. 9,419,942 ("Buruganahalli 942"), which is the parent of the Buruganahalli reference used in this petition. *See* Ex. 2007.

Further, Buruganahalli was readily available to the public long before Cisco's one year time bar (*i.e.*, March 29, 2019) and easily discoverable, as demonstrated by Keysight in a previous litigation (*Centripetal Networks Inc. v. Keysight Technologies, Inc.*, Case No. 2:17-cv-00383 (E.D.Va. 2017)). Indeed, the parent of Buruganahalli was included in Keysight's identification of the prior art on July 5, 2018, and entered into the public record of the prior Keysight litigation on September 27, 2018. Ex. 2008. That the Buruganahalli reference public knowledge long before Cisco's 315(b) bar date and the filing of PAN's petition asserting the reference, raises significant concerns when coupled with the timing of the petitions asserting Buruganahalli. That is, although each of the parties had access to Buruganahalli, not one of the parties initiated an AIA proceeding asserting obviousness over Buruganahalli until the '856 Patent district court reached its verdict finding the '856 Patent valid and willfully and egregiously infringed. Long delays in asserting AIA challenges based on known art *alone* weigh in favor of the Board dismissing such challenges. *See HTC Corp. v. Ancora Techs., Inc.*, IPR2021-00570, Paper 17 at 9-10 (P.T.A.B. Jun. 10, 2021) (finding *General Plastic* factors 1 and 2 favor denial where petitioner delayed in filing an IPR petition on prior art publicly disclosed in third-party litigations). Such long delays coupled with the fact that PAN's petition was filed on the heels of an Article III verdict only reinforces the problematic "surrounding circumstances" here. *OpenSky* at 36.

Additionally, the Board's institution of the underlying petition in this case has encouraged Cisco, an otherwise time-barred petitioner to raise new issues responding to arguments raised in Centripetal's POPR and findings in the Board's Institution Decision in the underlying case. *In re Leithem*, 661 F.3d 1316, 1319-1320 (Fed. Cir. 2011) (new ground does not require new prior art, but can be based on "new facts and rationales not previously raised"). In particular, Cisco presented new arguments purporting to shore up PAN's failure to address evidence of objective indicia of non-obviousness. Pet. 67-75 (addressing POPR in PAN IPR (IPR2022-00182, Paper 6 at 53)). Applying the "compelling merits" standard to PAN's petition, based only on the record existing at the time the PAN case was instituted (and Centripetal's Request for Rehearing, which presents no new arguments or evidence), would adequately address Cisco's improper attempts to fix the deficiencies in the underlying petition.

For at least these reasons, the Board should apply the "compelling merits" standard to its reconsideration of the Institution Decision, deny that Petition on the record before it at institution, and, therefore, deny this joinder petition because the underlying proceeding will have been terminated. In the alternative, the Board should consider the arguments and evidence presented herein and determine that neither this Petition nor the PAN Petition presents a reasonable likelihood than any claim of the '856 Patent is unpatentable.

IV. BURUGANAHALLI DOES NOT TEACH THE CLAIMED RULE-BASED FILTERING OF ENCRYPTED PACKETS

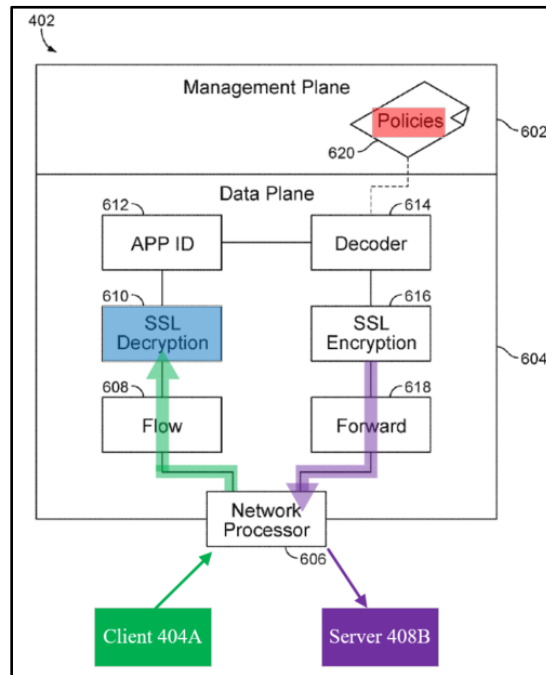
A petitioner in an IPR has “the burden of proving ... unpatentability by a preponderance of the evidence.” 35 U.S.C. § 316(e). Cisco asserts the same grounds as PAN. Thus, Cisco has failed to carry its burden, just as PAN failed. Although the panel in the PAN IPR initially held otherwise and instituted the PAN IPR, that decision suffers from material errors. In particular, the panel misapprehended Buruganahalli as supposedly disclosing filtering without decryption and overlooked that the claims require *rule-based* filtering of encrypted packets. The Challenged Claims require “filtering” of encrypted packets based on a number of criteria⁶ “specified by the plurality of packet-filtering rules.” *See, e.g.*, Ex. 1001, cl. 1. Buruganahalli does not teach this limitation.

1. Buruganahalli Filters Only Unencrypted or Decrypted Data

Like PAN, Cisco exclusively relies on Buruganahalli for the claimed “filtering” of encrypted data. First, Cisco equates Buruganahalli’s firewall policies/rules, including the blacklist policy, to the claimed “plurality of packet-filtering rules.” *See* Pet. 45-46. Cisco specifically cites to policies 620 in

⁶ 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, cl. 1.

Buruganahalli's Figure 6. Pet. 46 (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.

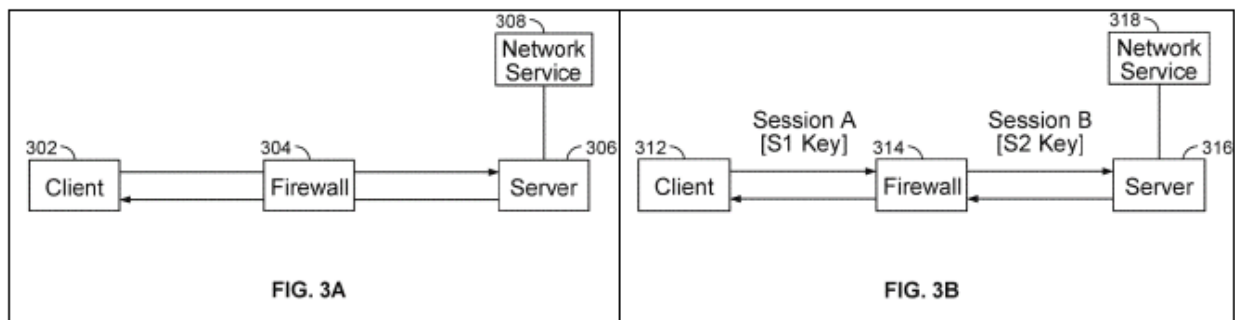


Buruganahalli, Fig. 6 (annotated)

That is, when encrypted packets are received by Buruganahalli's security device 402 (*e.g.*, a firewall), security device 402 performs decryption before using 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.⁷

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):



Buruganahalli, Figs. 3A (left) and 3B (right)

Ex. 1004, 10:54-13:4, Figs. 3A, 3B.

Indeed, in the institution decision of the PAN IPR, the Board correctly acknowledges that "Figure 3B's embodiment differs from Figure 3A's embodiment." IPR2022-00182, Paper 11 ("PAN IPR DI") at 70. These figures

⁷ 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.

cover the three scenarios of whitelisting based on an unencrypted packet (Fig. 3A), blacklisting and blocking an encrypted session based on an unencrypted packet (Fig. 3A), and blacklisting based on an unencrypted packet but allowing and decrypting the subsequent encrypted session (Fig. 3B). *See* Section II.C, *supra*.

As Cisco's petition copies the merits arguments of PAN's petition, it remains that 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, in the PAN IPR's institution decision, rightly acknowledges this. PAN IPR DI 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). So, the Board's institution decision turned to Figure 3A's embodiment, relying on a statement that policies are applied "without 'having to decrypt'" encrypted communications. PAN IPR DI at 71 (discussing applying rules to "hello message[s]") (citing Ex. 1004 at 11:7-19); *see* PAN IPR DI at 22, 41, 53. But the Board misunderstood this embodiment.

The Board should not make the same mistake in this IPR, particularly given the more-developed record in this IPR on this point. In Buruganahalli's Figure 3A whitelist-blacklist embodiment, policies are not applied to encrypted packets without decryption. The only reason Buruganahalli says "without having to decrypt"

in connection with Figure 3A is because the policies are being applied to an unencrypted packet before an encrypted session ever begins, making decryption entirely unnecessary. The firewall applies a policy to an unencrypted hello message⁸ and then decides whether to prevent the entire encrypted session before it ever begins. Ex. 1004 at 10:54-11:58; *see id.* at 4:16-44, 5:24-6:1. The policies in Figure 3A are thus applied “prior to” any encrypted session and never to an encrypted packet. Ex. 1004 at 11:7-19 (“prior to and/or without having to decrypt” encrypted packets”), 4:31-44 (policy-based filtering is “prior to the set-up of the encrypted data communication.”).

This is corroborated by U.S. Patent No. 9,967,236 (“Ashley”; Ex. 2022) that, like Buruganahalli, is assigned to PAN. Ashley has stock Figures 1-6 that are nearly identical to Buruganahalli’s Figures 1-6 and was filed after Buruganahalli’s parent but before Buruganahalli. Ex. 2022, Figs. 1-6. In describing Figure 3A, Ashley explains the secure session through firewall 304 may be in violation of a policy, but “because the secure tunnel session traffic is encrypted and passes through a firewall 304, the firewall 304 cannot decrypt the encrypted secure tunnel session traffic and, thus, cannot detect such firewall policy/rule violation(s).” Ex. 2022 at 12:25-41, Fig.

⁸ Petitioner admits a hello message is unencrypted. Pet. 47 (relying on hello message as “unencrypted data”); Ex. 1004 at 5:27-35.

3A. Notably, Ashley removes Buruganahalli's "without having to decrypt" language (Ex. 1004 at 11:7-19). Such extrinsic evidence demonstrates that Buruganahalli, in describing nearly identical figures, does not teach policy-based filtering encrypted packets without decryption. *See In re Baxter Travenol Labs.*, 952 F.2d 388, 390 (Fed. Cir. 1991) ("extrinsic evidence may be considered when it is used to explain, but not expand, the meaning of a reference"); *Monsanto Tech. LLC v. E.I. DuPont de Nemours & Co.*, 878 F.3d 1336, 1345 (Fed. Cir. 2018) (extrinsic evidence may be used to shed light on what a reference means).

Instead of performing policy-based filtering of encrypted packets, Buruganahalli's solution is to simply split the secure session and perform man-in-the-middle decryption to apply its policies to the decrypted data. 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)" without this approach. Ex. 1004 at 11:2-6, Fig. 3A.

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”), 7:39-51 (communications “are not decrypted if the destination domain is included in the whitelist”).

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”).

In stark contrast to Buruganahalli’s decrypt-first policy, the ’856 Patent’s only reference to decryption describes the proxy device 112—not the packet-filtering system—decrypting data after (and separate from) the filtering. Ex. 1001 at 10:15-

16. Time-and-time again, the '856 Patent describes rule gates of the packet-filtering system performing filtering on packets comprising encrypted data. *See e.g., id.* at 9:66-10:14 (step 19 in Fig. 3B), 11:36-50 (step 23 in Fig. 3B), 11:51-65 (step 24 in Fig. 3B).

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.

2. Petitioner Has Not Identified a Single Instance Where Buruganahalli Teaches Filtering Encrypted Packets

In sharp contrast to Buruganahalli's many disclosures of decrypting, Cisco (like PAN) cannot muster a single instance where Buruganahalli teaches "filtering" encrypted packets. To illustrate, Cisco relies on a short passage in Buruganahalli as allegedly disclosing the claimed filtering of encrypted data communications. Pet. 55 (citing Ex. 1004 at 4:16-22). That cited portion of Buruganahalli merely 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 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. 55 (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 6:17-22 (emphasis added).

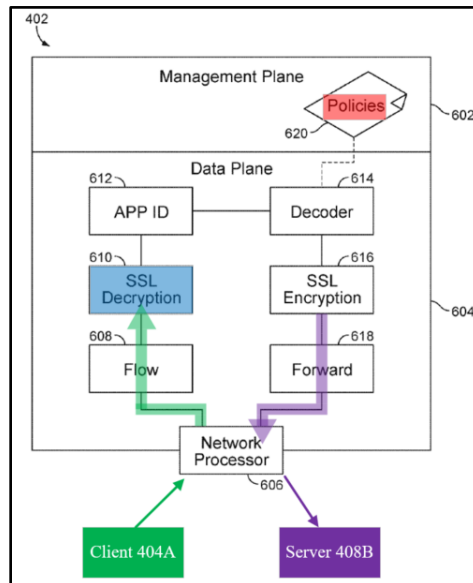
Attempting to shore up PAN’s petition in the PAN IPR, the institution decision there turned to four other portions of Buruganahalli for allegedly reaching the filtering of encrypted packets. See PAN IPR DI at 69 (citing Ex. 1004 at 8:55-60, 11:47-51, 14:21-33, 14:50-55). Despite filing its petition after that institution decision, Cisco does not rely on those other portions. The Board should not attempt to cure Cisco’s petition. *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). (The PTO’s “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.”).

Even so, like Cisco’s evidence, none of those four portions of Buruganahalli discloses filtering encrypted packets based on any rule criteria. Ex. 1004 at 8:55-60 (“inspection of session traffic” can include “possibly encrypted data communications” but this says nothing about filtering using rules or whether packets

are decrypted first), 11:47-51 (discussing unencrypted hello messages), 14:21-33 (discussing an unencrypted TLS handshake (*i.e.*, client hello message)), 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 in the PAN IPR repeatedly uses ellipses to omit the “based on” rule criteria and thus overlooks this limitation when evaluating these disclosures. PAN IPR DI at 68-69; *see id.* at 21-22, 40, 41, 43.

The PAN IPR's institution decision also incorrectly relies on Buruganahalli's flow lookup related to the TLS handshake and operation of decoder 614 in Figure 6. PAN IPR ID at 69 (citing Ex. 1004 at 14:21-33, 14:50-55). As an initial matter, Cisco's petition and the Board's prior institution decision both point to Buruganahalli's flow lookup for limitations [1.b] and [1.c] of “identifying” unencrypted and encrypted packets, respectively. Pet. 47-49; PAN IPR DI at 60-62. It is inconsistent and contrary to the doctrine of attributing different meaning to different claim terms to rely on the same flow lookup for the separate step of “filtering.” This is particularly troublesome here where there is yet another separate intermediate step (*i.e.*, the “determining” step) and the claimed “filtering” clearly entails more than mere flow look-up. 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:



Buruganahalli, Fig. 6 (annotated)

Ex. 1004 at 14:8-15:3, Fig. 6; *see* Ex. 2022 at 16:50-17:40. Buruganahalli never discloses (and Cisco never asserts) that flow lookup uses policies to filter encrypted packets. Ex. 1004 at 14:25-33. To the contrary, as Cisco's expert admits, flow lookup simply compares 5-tuple information in packet headers. *See* Ex. 1003, ¶ 64.

Notably, Cisco, like PAN, never asserts a combination of Buruganahalli's Figures 3A and 3B. Thus, the Board should not, as it ostensibly did in the PAN IPR institution decision, combine them. There, the Board alleged: "Buruganahalli discloses using techniques according to Figure 3A's embodiment separately or together with techniques according to Figure 3B's embodiment." PAN IPR DI 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 at 6:12-38, 7:39-67, 8:25-54, 9:61-10:4, 11:59-12:64. This still does not fix the issue though, as neither Figure 3A or 3B filter encrypted packets using policies.

In no instance does Buruganahalli apply its policies to encrypted packets. And neither Cisco's petition nor the Board's institution decision in the PAN IPR identify any contrary disclosure. Buruganahalli always decrypts encrypted packets before applying its policies. *Id.*

3. 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, Cisco tries twice to fill this gap: first by making conclusory statements about a skilled artisan's understanding, and second by alleging a motivation to rewrite Buruganahalli. Pet. 55. But Cisco cites no supporting evidence beyond similar conclusory statements in its expert declaration. Ex. 1003, ¶¶ 134-135. Conclusory assertions are legally insufficient. *See, e.g., Johns Manville Corp. v. Knauf Insulation, Inc.*, IPR2018-00827, Paper 9 at 13-14 (P.T.A.B. Oct. 16, 2018) (informative).

Cisco first attempts to turn to a skilled artisan's understanding to gap-fill Buruganahalli. Cisco 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. 55. 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.

Cisco 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. 55. *See 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.”). But Cisco again only tells half the story and does not explain how that correlation occurs. Buruganahalli discloses that encrypted packets still 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 8:11-24.

Cisco 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, 1367–1368 (Fed. Cir. 2016) (internal citations omitted). Cisco does not come close to meeting its burden.

Cisco 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. 55. There are four problems with this conclusion.

First, Cisco’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” is merely a statement of the purported functional result of this

supposed modification to Buruganahalli. This is not a motivation or reason for “how and why” a skilled artisan would modify Buruganahalli. *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.”).

Second, Buruganahalli already describes how to monitor transmissions into or out of a protected network: by decrypting the encrypted data and then filtering decrypted data. Ex. 1004 at 12:4-61. Cisco readily admits this throughout its petition. *E.g.*, Pet. 12, 36, 38-41, 56-59. Cisco provides no reason for how or why a skilled artisan would deviate from that solution.⁹ *LG Elec. v. Cellular Commc'ns Equip.*, IPR2016- 00197, Paper 7 at 8 (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].”).

Third, Cisco'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. Cisco does not mention policies at all. So, even if Cisco's stated rationale is adopted—and it should not be—Cisco's obviousness

⁹ Petitioner has not alleged substitution.

theory does not address “policy”-based filtering of data in encrypted packets. In other words, Cisco has provided no reason for why or how a skilled artisan would apply policies to filter encrypted packets without first decrypting the packets, as Buruganahalli teaches.

Fourth, 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, Cisco does not provide any assertion that a skilled artisan would have reasonably expected success in making its vague modification to Buruganahalli.

This lack of a proper motivation or rationale to modify Buruganahalli and failure to allege a reasonable expectation of success is fatal to Cisco's obviousness ground. *Intelligent Bio-Sys.*, 821 F.3d at 1367–1368.

V. CONCLUSION

Because the petition is harassment from a time-barred petitioner, the prior art is substantially similar to that overcome during prosecution and in district court, the petition violates the rules requiring petitioners to construe the claims and particularly specify how the construed claim is met, and the petition fails to show a reasonable likelihood of prevailing on any challenged claim, Patent Owner requests the Board deny institution.

Respectfully submitted,

Dated: October 7, 2022

/ James Hannah /
James Hannah (Reg. No. 56,369)

Patent Owner's Preliminary Response
IPR2022-01151 (U.S. Patent No. 9,917,856)

Kramer Levin Naftalis & Frankel LLP333
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 WORD COUNT

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 9,223 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 and by hand-counting added words in annotated figures.

Dated: October 7, 2022

By: /James Hannah/
James Hannah (Reg. No. 56,369)
Jeffrey H. Price (Reg. No. 69,141)
KRAMER LEVIN NAFTALIS & FRANKEL LLP
333 Twin Dolphin Drive, Suite 700
Redwood Shores, CA 94065
Tel: (650) 752-1700
Email: jhannah@kramerlevin.com
Email: jprice@kramerlevin.com

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
Email: skelly@bannerwitcoff.com
Email: bsilver@bannerwitcoff.com
Email: bwright@bannerwitcoff.com

*Attorneys for Patent Owner
Centripetal Networks, Inc.*

CERTIFICATE OF SERVICE

The undersigned certifies, in accordance with 37 C.F.R. § 42.6(e), that service was made on Petitioner as detailed below.

Date of service October 7, 2022

Manner of service E-MAIL

Documents served PATENT OWNER'S PRELIMINARY RESPONSE

Persons Served HAYNES AND BOONE, LLP
Theodore M. Foster
ipr.theo.foster@haynesboone.com

David L. McCombs
david.mccombs.ipr@haynesboone.com

Gregory P. Huh
gregory.huh.ipr@haynesboone.com

By: /James Hannah/
James Hannah (Reg. No. 56,369)
Jeffrey H. Price (Reg. No. 69,141)

Attorney for Patent Owner
Centripetal Networks, Inc.