

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PALO ALTO NETWORKS, INC., CISCO SYSTEMS, INC.,
and KEYSIGHT TECHNOLOGIES, INC.,[†]
Petitioner

v.

CENTRIPETAL NETWORKS, INC.,
Patent Owner.

IPR2022-00182
Patent 9,917,856 B2

Before MICHELLE N. WORMMEESTER, NABEEL U. KHAN, and
AARON W. MOORE, *Administrative Patent Judges*.

MOORE, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

[†] Cisco Systems, Inc. and Keysight Technologies, Inc. filed petitions and motions for joinder in IPR2022-01151 and IPR2022-01199, respectively, and have been joined in this proceeding.

TABLE OF CONTENTS

I. SUMMARY	3
II. BACKGROUND	4
A. Background.....	4
B. Related Matters.....	5
C. The '856 Patent	6
1. Specification.....	6
a. Structure	7
b. Generate and Provision Rule s.....	10
c. Domain Name Lookup	10
d. Proxy System and Unencrypted Connection Sessions	11
e. Establish Encrypted Connection Sessions.....	13
f. Send Encrypted Packets to Proxy System	14
g. Proxy System	15
h. Send Encrypted Packets to Destination.....	16
i. Figure 7 Flowchart.....	17
2. File History	18
3. The Challenged Claims.....	23
D. Level of Ordinary Skill in The Art	25
E. Claim Construction	25
III. PATENTABILITY ANALYSIS	27
A. Overview of Buruganahalli	27
1. Architecture	31
2. Hello Message Technique	32
3. Man-in-the-Middle Technique	33
4. Security Device.....	35
5. Flowcharts.....	37

B. Claim 1 in View of Buruganahalli	37
1. “[a] method”	37
2. “receiving, by a packet-filtering system . . . configured to filter packets in accordance with a plurality of packet-filtering rules, data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprises a domain name identified as a network threat”	37
3. “identifying packets comprising unencrypted data” and “identifying packets comprising encrypted data”	39
4. “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”	40
5. “filtering . . . based on at least one of [A] a uniform resource identifier (URI) . . . , [B] data indicating a protocol version . . . , [C] data indicating a method . . . , [D] data indicating a request . . . , or [E] data indicating a command . . .”	41
6. [A] “packets comprising the portion of the unencrypted data that corresponds to one or more network-threat indicators” and [B] “the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators”	47
7. “routing . . . filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators”	47
8. Objective Indicia of Nonobviousness	49
9. Conclusion Regarding Claim 1	53
C. Claims 24 and 25 in View of Buruganahalli	53
IV. PATENTABILITY CONCLUSION	54
V. REQUESTS FOR REHEARING	54
VI. ORDER	58

I. SUMMARY

For the reasons detailed below, we find that Petitioner has shown the challenged claims of the '856 patent unpatentable. The patent describes filtering packets using “hello message” and “man-in-the-middle” techniques previously disclosed in Buruganahalli, which uses them in essentially the same way as described in the patent.

We find Patent Owner’s primary argument—that Buruganahalli does not disclose applying the claimed rule set to encrypted packets—unpersuasive because the '856 patent *also* does not describe applying the claimed rules to encrypted packets. The claims were originally drafted to cover the hello message technique used with *encrypted* packets but were rejected. To secure allowance, the applicant amended the claims to add a set of criteria that the patent describes applying to *decrypted* packets in the distinct man-in-the-middle technique. The issued claims thus seem to recite filtering encrypted packets using a set of criteria appropriate for decrypted packets, without any explanation of how that can be done.

However, one of the criteria used with the decrypted packets is a Uniform Resource Indicator (“URI”), which, we find, is a term that covers the domain name used in the hello message technique. We thus conclude that Buruganahalli discloses the claimed steps of (a) receiving network-threat indicators including a domain name; (b) identifying packets with unencrypted and encrypted data; (c) determining, based on unencrypted data corresponding to a threat indicator (i.e., a hello message domain name), packets with encrypted data that corresponds the threat indicators (identified as being in the same “flow” or “session” as the packet with the hello message domain name); (d) filtering both types of packets (the flow/session) based on a URI (the domain name); and (e) routing both types of packets to a proxy system (that then applies the man-in-the middle technique).

II. BACKGROUND

A. *Background*

Palo Alto Networks, Inc. (“Petitioner”) filed a Petition requesting an *inter partes* review of claims 1, 24, and 25 of U.S. Patent No. 9,917,856 B2 (Ex. 1001, “the ’856 patent”) under 35 U.S.C. §§ 311–319. Paper 2 (“Pet.”). Centripetal Networks, Inc. (“Patent Owner”) filed a Preliminary Response, Petitioner filed a Preliminary Reply, and Patent Owner filed a Preliminary Sur-reply. *See* Paper 6; Paper 9; Paper 10. On May 25, 2022, the Board instituted an *inter partes* review of all challenged claims. *See* Paper 11 (“Decision”), 91.

In June of 2022, Patent Owner requested rehearing of the Institution Decision, arguing that the Board misapprehended or overlooked various matters. *See* Paper 13. Patent Owner also requested that the Precedential Opinion Panel (“POP”) review the Institution Decision. *See id.* at 1.

Patent Owner then filed a Response (Paper 24, “PO Resp.”), Petitioner filed a Reply (Paper 29, “Reply”), and Patent Owner filed a Sur-Reply (Paper 36, “Sur-Reply”).

On December 6, 2022, the POP denied the request for POP review, and on January 4, 2023, as the POP process had completed, the panel denied the rehearing request. *See* Papers 31, 40.

Cisco Systems, Inc. and Keysight Technologies, Inc. filed petitions and motions for joinder in IPR2022-01151 and IPR2022-01199, respectively, and have been joined in this proceeding. *See* Papers 39, 41.

An oral hearing was held on February 15, 2023, and a transcript of the hearing is included in the record, as are the demonstratives. *See* Paper 66 (“Transcript”); Ex. 1056 (Petitioner Demonstratives); Ex. 2046 (Patent Owner Demonstratives).

We issue this Final Written Decision under 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73 and, for the reasons that follow, determine that Petitioner has shown by a preponderance of the evidence that claims 1, 24, and 25 are unpatentable.

B. Related Matters

Petitioner and Patent Owner identify the following civil action involving the '856 patent: *Centripetal Networks, Inc. v. Cisco Systems, Inc.*, No. 2:18-cv-00094 (E.D. Va.). Pet. 5; Paper 4, 1. That case went to a bench trial and the District Court found claims 24 and 25 of the '856 patent infringed and not proven invalid. *See* Ex. 1027, 57, 67. The Federal Circuit subsequently vacated the judgment because it found that the presiding judge was disqualified due to his wife's ownership of Cisco stock. *See Centripetal Networks, Inc. v. Cisco Sys., Inc.*, 38 F.4th 1025, 1027 (Fed. Cir. 2022). The District Court did not consider the prior art addressed in this decision because the validity defense presented by Cisco for the '856 patent at trial was that the accused products were in the prior art. *See* Ex. 1027, 60 ("Dr. Schmidt, in his invalidity testimony, assumed the infringement analysis by Dr. Cole and opined that all of the same functionality that Dr. Cole relies on for infringement was in the accused products prior to the priority date of the '856 Patent."). The District Court has set a new trial date of June 22, 2023. *See* Paper 61, 10.

Petitioner identifies the following civil action in which Patent Owner asserted the '856 patent against joined party Keysight Technologies: *Centripetal Networks, Inc. v. Keysight Technologies, Inc. et al.*, No. 2:17-cv-00383 (E.D. Va. filed July 20, 2017). Pet. 5.

C. The '856 Patent

1. Specification

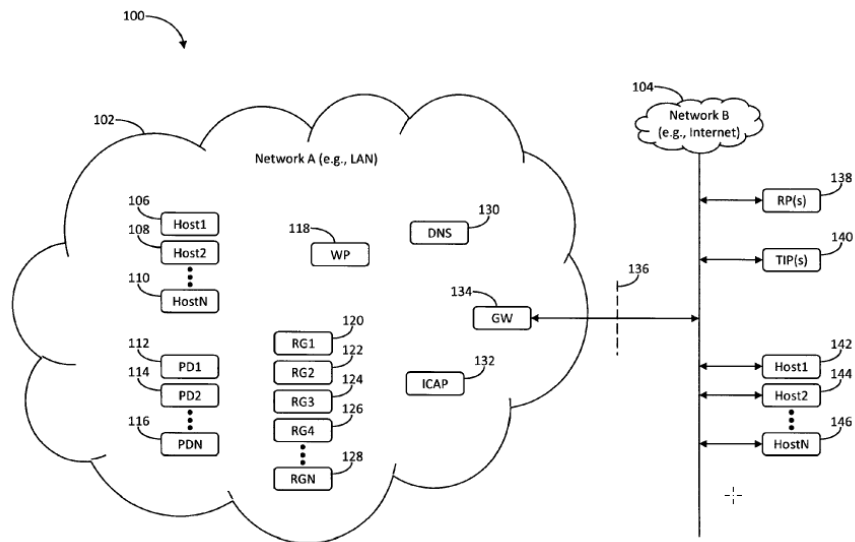
The '856 patent (Ex. 1001) is titled “Rule-Based Network-Threat Detection for Encrypted Communications” and issued on March 13, 2018, from an application filed on December 23, 2015.

According to the patent, network threats may “take a variety of forms (e.g., unauthorized requests or data transfers, viruses, malware, large volumes of traffic designed to overwhelm resources, and the like).” Ex. 1001, 1:8–11. The patent explains that network-threat services may “provide information associated with network threats, for example, reports that include listings of network-threat indicators (e.g., network addresses, domain names, uniform resource identifiers (URIs), and the like).” *Id.* at 1:11–15. The patent further explains that encrypted communications may “obfuscate data corresponding to network threats.” *Id.* at 1:17–18. The patent then identifies “a need for rule-based network-threat detection for encrypted communications.” *Id.* at 1:18–20.

To address that alleged need, the '856 patent describes “a packet-filtering system configured to filter packets in accordance with packet-filtering rules” that receives “data indicating network-threat indicators.” Ex. 1001, 1:32–36. The rules may “cause the packet-filtering system to identify packets comprising unencrypted data and packets comprising encrypted data.” *Id.* at 1:36–39. A “portion of the unencrypted data may correspond to one or more of the network-threat indicators” and the rules may “cause the packet-filtering system to determine, based on the portion of the unencrypted data, that the packets comprising encrypted data correspond to the one or more network-threat indicators.” *Id.* at 1:39–45.

a. *Structure*

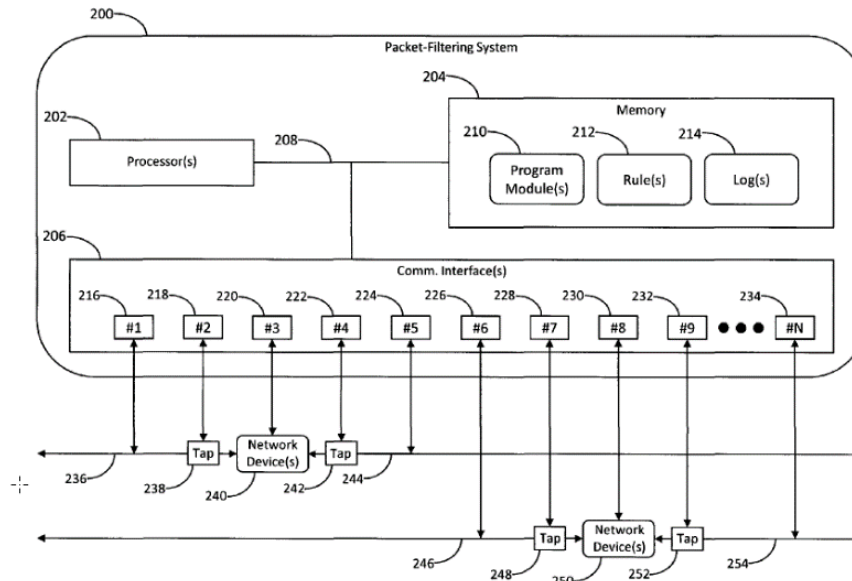
Figure 1 of the '856 patent shows an overall environment for rule-based threat detection:



“FIG. 1 depicts an illustrative environment for rule-based network-threat detection for encrypted communications.” Ex. 1001, 1:57–58.

The environment includes network 102, “associated with one or more individuals or entities,” and network 104, which is “the Internet, a similar network, or portions thereof.” Ex. 1001, 2:20–34. Network 102 includes “hosts 106, 108, and 110, proxy devices 112, 114, and 116, web proxy 118, rule gates 120, 122, 124, 126, and 128, domain name system (DNS) 130, Internet content adaptation protocol (ICAP) server 132, and gateway 134.” *Id.* at 2:39–43. Network 104 includes “one or more rule providers 138, one or more threat-intelligence providers 140, and hosts 142, 144, and 146.” *Id.* at 2:53–56. Gateway 134 serves as an interface between the networks. *See id.* at 2:50–60.

Figure 2 is a more detailed illustration of the structure of the patent's packet filtering system:

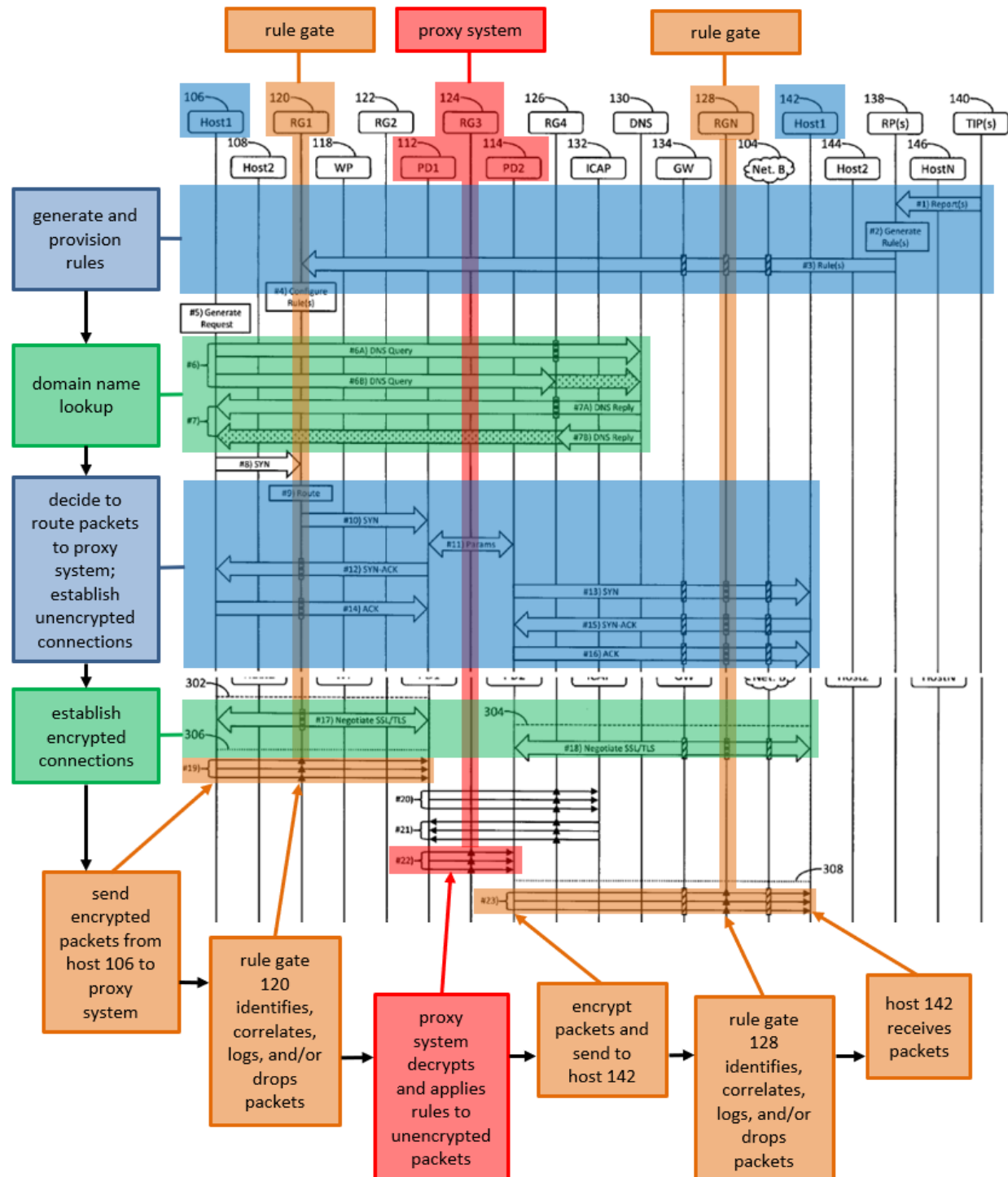


“FIG. 2 depicts an illustrative packet-filtering system for rule-based network-threat detection.” Ex. 1001, 1:60–62.

The system includes “processors 202,” “memory 204,” “communication interfaces 206,” and “data bus 208.” Ex. 1001, 2:64–3:2.

Memory 204 includes (A) “program modules 210” with instructions to cause the system to perform certain functions; (B) “rules 212,” “in accordance with which [the system] is configured to filter packets”; and (C) “logs 214” with “entries generated . . . in accordance with rules 212 for packets received” by the system. *Id.* at 3:4–14. Communication interfaces 206 may “interface” the packet-filtering system with “communication links” of networks 102 and 104, either directly, such as by links 236 and 244, or indirectly, such as by network device 240 or tap devices 238 and 242. *Id.* at 3:15–31. The system may “provision” the tap devices with rules to cause the tap devices to identify packets traversing the links that correspond to specified criteria “and route (or forward) the packets (or copies thereof)” to the taps. *Id.* at 3:31–36.

Figures 3A–C illustrate the operation of the system, and portions of Figures 3A and 3B are shown below, spliced together and annotated for reference:



Board Annotated Version of Figures 3A and 3B of the '856 Patent

b. Generate and Provision Rules

At **step 1**, “threat-intelligence providers 140 . . . communicate one or more threat-intelligence reports to rule providers 138.” Ex. 1001, 3:65–67. At **steps 2–4**, the rule provider(s) generate rules and send them to rule gate 120, which may use the “packet-filtering rules” to configure the rules to cause the system “to identify packets comprising data corresponding to at least one of the plurality of network-threat indicators.” *Id.* at 4:16–21.

c. Domain Name Lookup

At **step 5**, “host 106 may generate a request.” Ex. 1001, 4:22. For example, the host “may execute a web browser, and the web browser may generate a request in response to user input (e.g., navigation of the web browser to a URI).” *Id.* at 4:22–25.

At **step 6**, the host may generate a DNS query with the domain name from the request and send the query to domain name server 130.² If the domain name corresponds to a network-threat indicator, the rules may cause the rule gate 126 to (A) “identify one or more packets comprising the DNS query,” (B) “determine that the packets comprise the domain name corresponding to the network-threat indicator,” and/or (C) “responsive to” the identifying or determining, log and/or drop the packets. Ex. 1001, 4:29–42. The log data may include, for example, data indicating the host’s network address. *See id.* at 4:39–46. Steps 6A and 6B depict packets being sent to the domain name server or dropped, respectively.

Step 7 is a response from the domain name server, which may include a domain name corresponding to a network-threat indicator. As in step 6, the rules may cause rule gate 126 to (A) “identify” packets, (B) “determine that the packets

² “DNS” stands for Domain Name System, and a DNS query seeks an IP address for a given domain name. *See* Ex. 1007, 8–9.

comprise the domain name corresponding to the network-threat indicators,” and (C) “responsive to” the identifying or determining, log and/or drop the packets. Ex. 1001, 4:54–64. As in step 6, the rule gate may generate log data, including host’s address, and packets may be sent on or dropped. *See id.* at 4:64–5:15.

The Specification explains that the system may be configured to “correlate” packets of the unencrypted DNS query and reply, using the data that was stored in the logs. *See* Ex. 1001, 5:15–30. This may be done with network layer information, transport layer information, application layer information, other data in the packets, or environmental variables. *See id.* at 5:15–6:6.

d. Proxy System and Unencrypted Connection Sessions

At **step 8**, host 106 “may generate one or more packets destined for host 142 comprising data (e.g., a TCP:SYN handshake message) configured to establish a connection (e.g., a TCP connection or tunnel) between hosts 106 and 142” and “may communicate the packets toward host 142.” Ex. 1001, 6:17–21. The rules may cause rule gate 120 to (A) identify the packets or (B) determine that the packets include data corresponding to the network-threat indicators by correlating the packets with previous packets. *See id.* at 6:24–32.

At **step 9**, rule gate 120 may “route” the packets with the connection data to proxy device 112 and, at **step 10**, rule gate 120 may “communicate” the packets to proxy device 112. *See* Ex. 1001, 6:33–36. The rules may cause rule gate 120 to “route” the packets to proxy device 112 based on data in the packets indicating the connection between hosts 106 and 142 will be encrypted. *See id.* at 6:36–45. The rules also may cause rule gate 120 to route the packets to proxy device 112 if a host is associated with a network address for which the rules indicate that encrypted communications should be established. *Id.* at 6:45–52.

Proxy devices 112, 114, and 116 may be part of a “proxy system” used to “to filter packets comprising encrypted data based on information within the encrypted data.” Ex. 1001, 6:53–56. The rules may be configured “to cause rule gate 120 to route the packets to proxy device 112 based on a determination that host 142 is associated with a network address of a domain corresponding to the network-threat indicators.” *Id.* at 6:56–59. The network 102 may also include hosts for which the rules indicate that encrypted communication sessions should or should not use proxy devices. *Id.* at 6:60–7:11.

At **step 11**, proxy devices 112 and 114 exchange parameters determined from the configuration packets, such as network addresses in network-layer headers or ports indicated by transport-layer headers. *See* Ex. 1001, 7:33–40. Proxy device 112 uses the parameters to generate packets to establish a connection between proxy device 112 and host 106 and, at **step 12**, communicates the packets to host 106. *Id.* at 7:41–45. The rules may cause rule gate 120 to (A) identify packets, (B) “determine . . . that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets” with the earlier packets, and (C) “log [and/or] drop the packets.” *Id.* at 7:45–55.

Proxy device 114 similarly uses parameters to generate packets to establish a connection between proxy device 114 and host 142 and, at **step 13**, communicates the packets to host 142. Ex. 1001, 7:56–60. On this side of the proxy system, the rules may be configured to cause rule gate 128 to identify packets, determine that the packets include data corresponding to the network-threat indicators by correlating the packets with earlier packets, log packets, and/or drop packets. *Id.* at 7:56–8:5.

Next, host 106 may generate packets to establish a connection between proxy device 112 and host 106 and, at **step 14**, communicate the packets to proxy

device 112. Ex. 1001, 8:7–11. The rules may cause rule gate 120 to identify packets, determine that the packets include data corresponding to the network-threat indicators by correlating the packets with earlier packets, log packets, and/or drop packets. *Id.* at 8:11–21.

Host 142 may then generate packets to establish a connection between proxy device 114 and host 142 and, **at step 15**, may communicate the packets to proxy device 114. Ex. 1001, 8:22–27. In response, proxy device 114 may generate packets comprising data configured to establish the connection between proxy device 114 and host 142 and, **at step 16**, communicates the packets to host 142. For each of those communications, the rules may cause rule gate 128 to identify packets, determine that the packets include data corresponding to the network-threat indicators by correlating the packets with earlier packets, log packets, and/or drop packets. *See id.* at 8:38–53.

e. Establish Encrypted Connection Sessions

At **step 17** and **step 18**, the proxy devices and hosts for each connection exchange data to establish encrypted communication sessions 306 and 308 corresponding to the unencrypted connection sessions 302 and 304. *See* Ex. 1001, 8:65–9:65.

At **step 17**, the rules may be configured to (A) identify the packets, (B) “determine . . . that the packets comprise data corresponding to the network-threat indicators, for example, *by correlating the packets*” with previous packets, and (C) log and/or drop the packets. Ex. 1001, 9:2–12 (emphasis added).

The rules also may cause rule gate 120 to (A) identify the packets or (B) “determine that the packets comprise data corresponding to the network-threat indicators *based on data included in the packets.*” Ex. 1001, 9:14–16 (emphasis added). Specifically, the patent explains that the packets may include handshake

messages with “unencrypted data including a domain name corresponding to the network-threat indicators, for example, a hello message generated by the client . . . or a certificate message generated by the server.” *Id.* at 9:21–25. The rules may cause rule gate 120 to (A) identify the packets and/or (B) “determine that the packets comprise data corresponding to the network-threat indicators based on data included in the one or more handshake messages.” *Id.* at 9:29–32. Unencrypted information from the certificate message may also be used in the same way. *See id.* at 9:33–46.

The use of the rules at **step 18** includes (A) identifying the packets, (B) determining that the packets comprise data corresponding to the network-threat indicators, for example, *by correlating*, and (C) logging and/or dropping the packets. *See* Ex. 1001, 9:47–65. However, the correlating in this step uses either “one or more packets previously determined . . . to comprise data corresponding to the network-threat indicators” or “the packets comprising [the] handshake messages configured to establish session 308 that comprise unencrypted data (e.g., including the domain name) corresponding to the network-threat indicators.” *Id.* at 9:56–65.

f. Send Encrypted Packets to Proxy System

At **step 19**, the two encrypted communication sessions have been established and “host 106 may generate packets comprising data encrypted in accordance with one or more parameters of session 306” and “communicate the packets to proxy device 112 via session 306.” Ex. 1001, 9:66–10:2. The rules may cause rule gate 120 to (A) identify the packets,” (B) “determine . . . that the packets comprise data corresponding to the network-threat indicators, for example, *by correlating the*

packets” with previous packets, and/or (C) “log and/or drop the packets.” *Id.* at 10:3–14 (emphasis added).³

This step is illustrated in orange in the Board’s annotated version of Figures 3A and 3B (page 9, *supra*), with rule gate 120 (RG1) acting on *encrypted* packets between host 106 (Host1) and proxy device 112 (PD1).

g. Proxy System

At **step 22**, “[p]roxy device 112 may generate packets” and communicate [them] to proxy device 114.” Ex. 1001, 10:56–58. Rule gate 124 may access “a communication link internal to the proxy system comprising proxy devices 112 and 114,” and, thus, “packets traversing the communication link may comprise unencrypted data,” such that “rule gate 124 may be ‘the man in the middle’ of proxy devices 112 and 114.” *Id.* at 10:59–63.

The rules may cause rule gate 124 to (A) identify the packets, (B) “determine . . . that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets” with previous packets, and/or (C) log and/or drop the packets. Ex. 1001, 10:65–11:7.

In addition, the rules may cause rule gate 124 to (A) identify the packets or (B) “determine that the packets comprise data corresponding to the network-threat indicators *based on data included in the packets*, for example, *unencrypted data* in the packets corresponding to one or more of the network-threat indicators.” Ex. 1001, 11:9–13 (emphasis added). In particular, the rules may cause rule gate 124 to “determine that the packets comprise data corresponding to the network-threat indicators based on the packets including [1] a URI . . . , [2] data indicating a

³ Steps 20 and 21 involve communications between proxy device 112 and an “Internet content adaptation protocol (ICAP) server.” *See* Ex. 1001, 2:42–43, 10:15–55.

protocol version . . . , [3] data indicating a method . . . , [4] data indicating a request . . . , [5] or data indicating a command” *Id.* at 11:19–28. This is the set of rules recited in the independent claims.

This step shown in red in the Board’s annotated version of Figures 3A and 3B (page 9, *supra*), with rule gate 124 (RG3) acting on unencrypted packets between proxy device 112 (PD1) and proxy device 114 (PD2).

h. Send Encrypted Packets to Destination

Proxy device 114 receives the packets and generates corresponding packets with data that is encrypted according to the parameters of session 308 and, at **step 23**, communicates the packets to host 142. *See* Ex. 1001, 11:36–40.

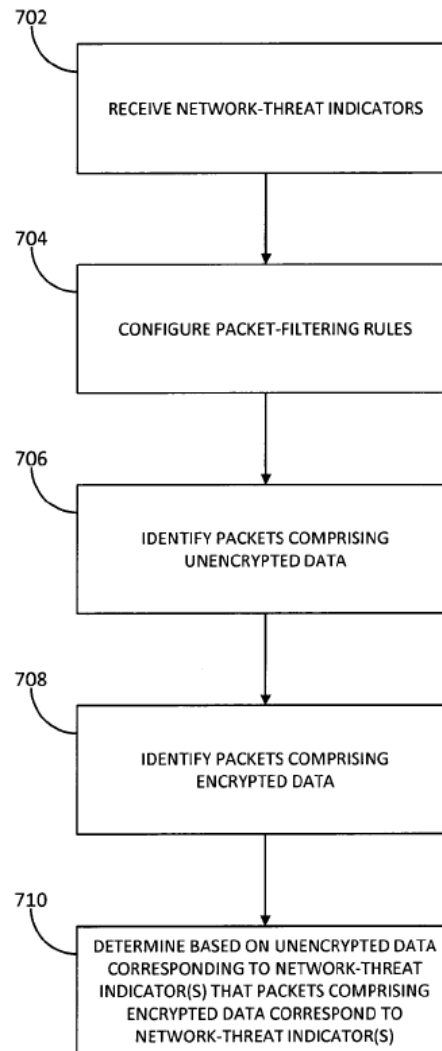
The rules cause rule gate 128 to (A) identify the packets, (B) “determine . . . that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets” with previous packets, and/or (C) log and/or drop the packets. Ex. 1001, 11:41–50.

This step is illustrated in orange in the Board’s annotated version of Figures 3A and 3B, with rule gate 128 (RGN) acting on encrypted packets between proxy device 114 (PD2) and host 142 (Host1).

The process then continues with similar communications between host 142 and host 106, and rules applied in a similar fashion by rule gates 120, 124, and 128. *See* Ex. 1001, 11:51–12:27.

i. *Figure 7 Flowchart*

Figure 7, reproduced below, is a flowchart for a “method for rule-based network-threat detection for encrypted communications.” Ex. 1001, 23:63–65.



In **step 702**, “a packet-filtering system may receive data indicating network-threat indicators,” for example, rules generated by rule providers 138 based on “network-threat indicators provided by threat-intelligence providers 140.” Ex. 1001, 23:66–24:4. In **step 704**, “the packet-filtering system may configure packet-filtering rules in accordance with which it is configured to filter packets.” *Id.* at 24:4–6.

In **step 706**, “the packet-filtering system may identify packets comprising unencrypted data,” such as “a DNS query, a reply to a DNS query, or a handshake message configured to establish an encrypted communication session.” Ex. 1001, 24:8–12. In **step 708**, “the packet-filtering system may identify packets comprising encrypted data.” *Id.* at 24:13–17.

In **step 710**, “the packet-filtering system may determine based on a portion of the unencrypted data corresponding to the network-threat indicators that the packets comprising encrypted data correspond to the network-threat indicators.” Ex. 1001, 24:18–21. For example, the system “may determine that a domain name included in the DNS query, the reply to the DNS query, or the handshake message corresponds to the network-threat indicators, and packet-filtering system 200 may determine that one or more of the packets” encrypted according to an SSL/TLS protocol “correlate to one or more packets comprising the DNS query, the reply to the DNS query, or the one or more handshake messages.” *Id.* at 24:22–30.

Figure 7 thus describes looking for packets with network threat indicators in unencrypted information (e.g., a domain name in a hello message) and then determining that other, encrypted packets correlate to those packets.

2. *File History*

We discuss the prosecution history of the ’856 patent in detail below because it bears on Patent Owner’s arguments.

The application that issued as the ’856 patent was filed with independent method claim 1, and corresponding independent system and computer readable media claims 24 and claim 25. *See* Ex. 1002, 43–49. Our discussion focuses on claim 1, but the same considerations apply to claims 24 and 25.

Original claim 1 read as follows:

1. A method comprising:

receiving, by a packet-filtering system configured to filter packets in accordance with a plurality of packet-filtering rules, data indicating a plurality of network-threat indicators; and

configuring, by the packet-filtering system, the plurality of packet-filtering rules to cause the packet-filtering system to:

identify packets comprising unencrypted data;

identify packets comprising encrypted data; 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 correspond to the one or more network-threat indicators.

Ex. 1002, 43.

Claim 1 thus originally recited (1) receiving data indicating a plurality of network-threat indicators, (2) configuring rules to identify packets with unencrypted data and identify packets with encrypted data, and (3) determining, based on a portion of the *unencrypted* data corresponding to a network-threat indicator, that the packets with *encrypted* data correspond to the network-threat indicator.

This is consistent with the Figure 7 flowchart and the operation of rule gates 120 and 128 in Figure 3B, as described above, where the packets with the unencrypted data would be the handshake packets with a domain name in the hello message, and the packets with the encrypted data would be encrypted packets that are correlated to the handshake packet.

The Examiner rejected the claims under § 103 as unpatentable over Spies and Sorensen,⁴ citing Spies for most of the claimed subject matter and Sorensen for network-threat indicators. *See* Ex. 1002, 1070–72.

In an effort to overcome the rejection, the applicant amended claim 1 as follows:

1. A method comprising:

receiving, by a packet-filtering system comprising a hardware processor and a memory and configured to filter packets in accordance with a plurality of packet-filtering rules, data indicating a plurality of network-threat indicators; ~~and~~

~~configuring, by the packet-filtering system, the plurality of packet filtering rules to cause the packet filtering system to:~~

~~identify~~ identifying packets comprising unencrypted data;

~~identify~~ identifying packets comprising encrypted data; ~~and~~

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.

See Ex. 1002, 1352.

⁴ “Spies” is U.S. Patent App. Pub. No. 2005/0138353 A1 and “Sorensen” is U.S. Patent App. Pub. No. 2012/0023576 A1. The Examiner also rejected claims 1, 24, and 25 under § 101, and under § 112(b) due to an “antecedent basis error.” *See* Ex. 1002, 1064–69. Those rejections were overcome, but are not discussed further because they are not pertinent to our analysis.

This amendment addressed the Section 101 rejection and added that, in addition to determining that packets with encrypted data correspond to the indicators, the method would “filter” both the unencrypted and encrypted packets.

The applicant’s attorney and the Examiner then conducted an interview, during which the Examiner “confirmed authorization from Attorney of record . . . to implement Examiner’s Amendment based on Applicant’s proposed examiner’s amendment submitted by email on 12/06/2017.” Ex. 1002, 1391.

The Examiner subsequently entered an amendment, presumably as submitted by the applicant.⁵ Claim 1 was amended as follows:

1. A method comprising:

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

identifying packets comprising unencrypted data;

identifying packets comprising encrypted data;

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

⁵ The email with the proposed amendment does not appear to have been made of record in the prosecution.

packets comprising the portion of the unencrypted data that corresponds ~~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; and

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

Ex. 1002, 1380–81.

Essentially, the examiner’s amendment added that (a) the network threat indicators include a domain name, (b) the filtering is based on a URI or one of four other types of data in the packets, and (c) the filtered packets are routed to a “proxy system” based on the determination that they include data corresponding to a threat indicator. The Examiner then allowed the claims. *See* Ex. 1002, 1386–1389.⁶

There appears to be a problem with the examiner’s amendment, which complicates the patentability analysis, at least as argued by Patent Owner, because the rules that were added to the claim by the amendment are those that the patent describes applying in *step 22*, by rule gate 124, which is operating on *decrypted* packets. The patent does not describe filtering *encrypted* packets using that set of rules and, indeed, it does not appear possible to apply some of those rules to encrypted packets because at least some of the data (i.e., the protocol version, method, request, or command) would be encrypted. There is nothing in the patent that explains how to apply those rules to a packet without decrypting it first.

In addition, the patent does not appear to describe routing packets filtered using the claimed rules to a proxy system, because those rules are applied *within the proxy system*, not prior to routing to the proxy system, and the rules are only

⁶ Patent Owner amended claims 1, 24, and 25 after allowance to make minor changes. *See* Ex. 1002, 1414, 1420–22.

described as being used to “identify the packets or determine that the packets comprise data corresponding to the network-threat indicators,” not as a basis for further routing. *See* Ex. 1001, 11:8–35.⁷

These issues are material to our analysis because Patent Owner’s primary argument is that “Buruganahalli does not teach rule-based filtering of encrypted packets, as recited in each of the Challenged Claims.” PO Resp. 31; *see id.* at 20 (asserting that the patent’s steps 19 and 23 “use rules to filter encrypted packets without decryption—an important difference over Buruganahalli as it was during prosecution and the Cisco litigation”).

To be clear, to the extent the ’856 patent describes filtering encrypted packets, it does so (a) by *correlation* at steps 19 and 23, for example, not by applying rules directly to encrypted packets, or (b) by *decrypting* the packets in the proxy system and applying the rules recited in the claims after the packets are decrypted.⁸

3. *The Challenged Claims*

Petitioner challenges independent claims 1, 24, and 25. *See* Pet. 8. Claim 1 recites a method for filtering and routing packets comprising several steps. Claim 24 recites a system with a processor and a memory storing instructions for

⁷ We do not consider whether these issues might give rise to a problem under 35 U.S.C. § 112 because this proceeding is limited to grounds “that could be raised under section 102 or 103.” *See* 35 U.S.C. § 311(b).

⁸ Notably, original dependent claim 14 recited applying the claimed rules to packets “generated by the proxy system,” presumably referring packets that were generated by the proxy system’s decryption of encrypted packets. *See* Ex. 1002, 47 (emphasis added).

performing steps similar to those of claim 1, and claim 25 recites a computer-readable medium with instructions for performing steps similar to those of claim 1.

Claim 1, which thus exemplifies the subject matter of the challenged claims, reads as follows (with some formatting added for clarity):

1. A method comprising:

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

[1.b] identifying packets comprising unencrypted data; [1.c] identifying packets comprising encrypted data; [1.d] determining, by the packet-filtering system and based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;

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

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

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

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

Ex. 1001, 25:14–49.

D. Level of Ordinary Skill in The Art

The level of skill in the art is a factual determination that provides a primary guarantee of objectivity in an obviousness analysis. *See Al-Site Corp. v. VSI Int'l Inc.*, 174 F.3d 1308, 1323 (Fed. Cir. 1999) (citing *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966)). The level of skill in the art also informs the claim construction analysis. *See Teva Pharms. USA, Inc. v. Sandoz, Inc.*, 574 U.S. 318, 332 (2015) (explaining that claim construction seeks the meaning “a skilled artisan would ascribe” to the claim term “in the context of the specific patent claim”).

Petitioner asserts that a person of ordinary skill in the art “would have had a bachelor’s degree in computer science, computer engineering, or an equivalent, and four years of professional experience” and that “[l]ack of work experience could be remedied by additional education, and vice versa.” Pet. 16 (citing Ex. 1003 ¶¶ 29–30).

Patent Owner argues that a person of ordinary skill in the art at the time of the invention “would have had a bachelor’s degree in computer science or a related field, and either 2 or more years of industry experience and/or an advanced degree in computer science or a related field.” PO Resp. 26 (citing Ex. 2026 ¶¶ 26–30).

Neither side argues there is a difference in the competing proposals that would affect the patentability analysis or otherwise change the outcome. As we did at institution, we will apply Petitioner’s description of an ordinarily skilled artisan, as we find it consistent with the ’856 patent and the asserted prior art.

E. Claim Construction

Petitioner contends that the term “network-threat indicators” should be construed to mean “indicators that represent the identity of a resource associated with a network threat,” a construction Petitioner argues is consistent with the ’856 patent’s specification and was adopted in IPRs filed against other of Patent

Owner’s patents in which this same claim term appears. *See* Pet. 17 (citing Ex. 1001, 1:11–15, 3:65–4:4; Ex. 1003 ¶¶ 20–23, 85–87). Petitioner contends that “[a]ll other terms should be accorded their plain and ordinary meaning.” *Id.* (citing Ex. 1003 ¶¶ 83–84).

Patent Owner argues that “Petitioner has not met its burden to address multiple district court claim constructions of ‘network-threat indicators’ and ‘proxy system.’” PO Resp. 26. According to Patent Owner, “the Petition violates 37 C.F.R. §§ 42.104(b)(3) and 42.104(b)(4)” and “[t]he Board cannot cure this failure of compliance post-institution.” *Id.* at 27. However, Patent Owner does not offer its own constructions for these terms or assert that Petitioner’s construction of “network-threat indicators” is incorrect.

The Petition does not violate our rules. Rule 42.104(b)(3) simply requires that the Petition set forth “[h]ow the challenged claim is to be construed,” which Petitioner has done by asserting that the language of the claims is entitled to its ordinary meaning, except for “network-threat indicators,” for which Petitioner proposes a construction. Rule 42.104(b)(3) requires that the Petitioner set forth “[h]ow the construed claim is unpatentable under the statutory grounds identified” and “specify where each element of the claim is found in the prior art patents or printed publications relied upon,” which Petitioner has also done. *See* Pet. 18–50. A petition must be complete and sufficient as presented, but we are aware of nothing that would require a Petitioner to base its unpatentability arguments in a petition on any particular claim construction.

Moreover, while it is true that the District Court’s construction of “network-threat indicators” uses different words than the construction offered for that term in the Petition, it appears to be very similar substantively, and Patent Owner does not identify any difference that would have a material impact on our analysis.

Because we find Patent Owner’s arguments unpersuasive, and because we find that Petitioner’s proposed construction of “network-threat indicators” is consistent with how the term is used in the ’856 patent, we apply Petitioner’s proposed construction in this decision.

III. PATENTABILITY ANALYSIS

The Petition asserts that independent claims 1, 24, and 25 would have been obvious in view of Buruganahalli.⁹ The Petition then asserts that those same claims would have been obvious in view of Buruganahalli and Baehr.¹⁰

However, because Petitioner cites Baehr in the event the “proxy system” needs to be a separate system,¹¹ and no party requests a claim construction requiring that, or otherwise argues that the proxy system must be separate, we find that we need not address Baehr, and thus consider only the ground based on Buruganahalli alone.

A. *Overview of Buruganahalli*

Buruganahalli is a U.S. patent titled “Destination Domain Extraction for Secure Protocols,” that discloses “techniques for destination domain extraction for secure protocols.” Ex. 1001, 4:47–50. It was a continuation of U.S. Patent Application No. 13/951,320, which was filed on July 25, 2013, and issued on June 13, 2017 as U.S. Pat. No. 9,419,942. The 2013 priority date makes Buruganahalli prior art to the ’856 patent under §102(a)(2). Palo Alto Networks was the applicant and original assignee.

⁹ US 9,680,795 B2, issued June 13, 2017 (Ex. 1004).

¹⁰ US 5,878,231, issued March 2, 1999 (Ex. 1005).

¹¹ See Transcript 11–12 (“[Q:] Is the Baehr reference in the case -- in case a proxy needs to be a separate system? . . . [Petitioner’s counsel:] Right.”).

Buruganahalli explains that “[f]irewalls typically deny or permit network transmission based on a set of rules,” which are “often referred to as policies (e.g., network policies or network security policies)” and that, “[f]or example, a firewall can filter inbound traffic by applying a set of rules or policies to prevent unwanted outside traffic from reaching protected devices.” Ex. 1004, 2:61–66.

Buruganahalli describes “stateless packet filtering firewalls” that “inspect the individual packets themselves and apply rules based on the inspected packets (e.g., using a combination of a packet’s source and destination address information, protocol information, and a port number).” Ex. 1004, 3:2–24. It also describes “stateful firewalls” in which “each packet is examined within the context of a series of packets associated with that network transmission’s flow of packets/packet flow.” *Id.* at 3:40–44. Such firewalls “maintain[] records of all connections passing through the firewall and [are] able to determine whether a packet is the start of a new connection, a part of an existing connection, or is an invalid packet,” and “the state of a connection can itself be one of the criteria that triggers a rule within a policy.” *Id.* at 3:44–50.

One problem, however, was that “secure protocols [could] be used to evade detection by security devices, such as firewalls, by encrypting data communications between a client and a remote server.” Ex. 1004, 4:16–19. Buruganahalli thus explains that “techniques for decrypting . . . 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 further explains that “it would be desirable and efficient to further facilitate policy-based filtering on . . . data communication flows (e.g., sessions) prior to the set-up of the encrypted data communication for such flows (e.g., to monitor the initial unencrypted/clear text data communications exchanged

as part of an initial handshake to setup a secure connection for a new session between a client and a remote server, which is prior to the establishment of the secure communication channel/tunnel after which any data communications intercepted between the client and the remote server would be encrypted).” Ex. 1004, 4:33–44.

The reference explains that “as part of a TLS protocol exchange, a client hello is generally the first message sent by a client to a remote server,” but that an IP address in such a message is “often not accurate, because it is possible that a single IP address in the cloud can be hosting multiple virtual domains” such that “there is no easy way for the client to indicate to the server as to which domain” is the actual target. Ex. 1004, 4:59–64. However, Buruganahalli further explains that “a Server Name Indication (SNI) was added as part of the TLS protocol standard extension to the client hello message in order to allow the remote server to overcome this ambiguity.” *Id.* at 4:64–5:1. The SNI “indicates what hostname (e.g., destination domain) that the client is attempting to connect to at the start of the hand shaking process for setting a secure TLS communication channel/session between a client and a remote server.” *Id.* at 5:6–10.

Buruganahalli describes how the SNI extension can be used “as a mechanism to facilitate destination domain extraction for secure protocols without requiring decryption.” Ex. 1004, 5:25–27. In particular, a firewall can “extract the hostname data from the SNI field (e.g., server name field of the SNI extension), which is sent as an unencrypted data communication from the client” to the server “at the start of the handshaking process for setting up a secure TLS communication channel/session between a client and a remote server).” *Id.* at 5:29–35. The “extracted hostname data (e.g., destination domain) can then be used by the firewall to perform an action(s) based on a firewall policy.” *Id.* at 5:35–37.

The reference explains that “if a new flow is determined to violate a policy prior to the set-up of the encrypted data communication for that flow between a client and a remote server, then the flow can be blocked and decryption is not required.” Ex. 1004, 5:65–6:1.

Alternately, the system may “determine whether a new session using a secure protocol should be initially allowed based on a policy (e.g., security policy, such as a firewall policy), and then to further monitor encrypted data communications associated with the session.” Ex. 1004, 6:13–16. For example, “if a flow is initially determined to be permissible based on a policy prior to the set-up of the encrypted data communication for that flow between a client and a remote server, then the flow can be allowed, and a policy may require that the session be decrypted for further analysis and further potential filtering based on the policy.” *Id.* at 6:17–23.

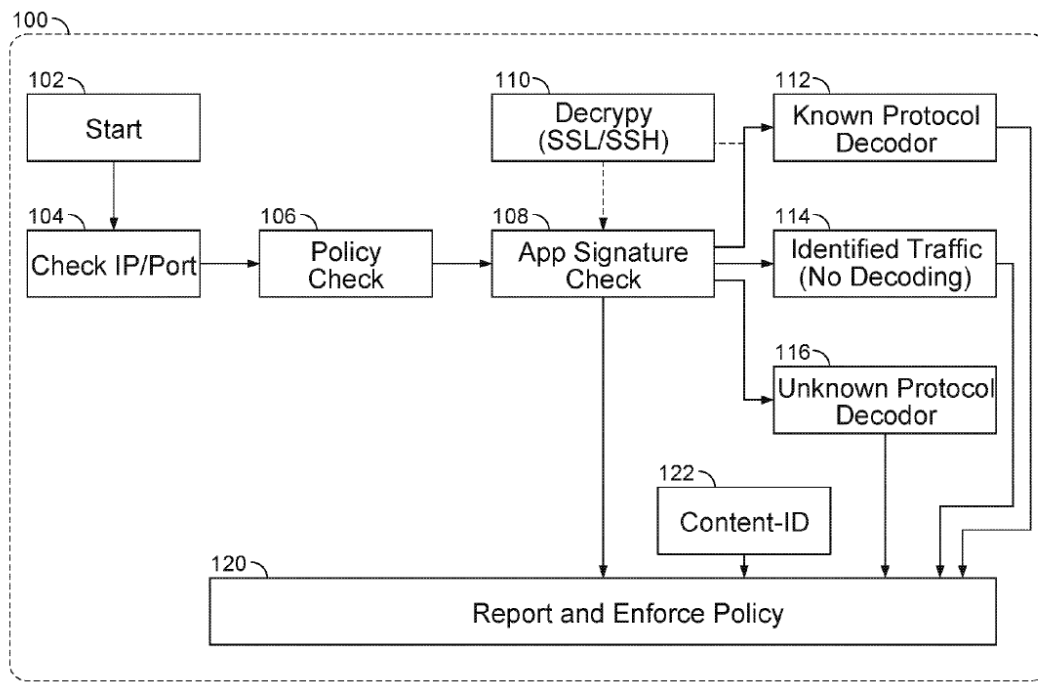
Buruganahalli also explains that the destination domain extraction can include “applying a security policy based on the destination domain to filter traffic at the security device.” Ex. 1004, 7:39–42. The security policy can include a “malware detection policy,” a “whitelist/blacklist policy,” “and/or a uniform resource locator (URL)/category filtering policy.” *Id.* at 7:43–51. The “whitelist/blacklist policy” involves not decrypting a session if the destination domain is on the whitelist, and decrypting a session if the destination domain is on the blacklist. *See id.* at 7:52–67.

The reference also explains that the “destination domain extraction may include monitoring encrypted network communications between a client and a remote server,” such as with “man-in-the-middle decryption techniques” in which the “network communications are encrypted,” and “performing an action based on

the decrypted network communications between the client and the remote server.”
Ex. 1004, 8:45–54.

1. Architecture

Buruganahalli’s Figure 1 shows the overall architecture:



“FIG. 1 is a functional diagram of an architecture of a security device that can be used for destination domain extraction for secure protocols in accordance with some embodiments.” Ex. 1004, 1:46–49.

IP address and port engine 104 “determines an IP address and port number for a monitored traffic flow (e.g., a session) based on packet analysis,” and “policy check engine 106 determines whether any policies can be applied based on the IP address and port number.” Ex. 1004, 9:26–32. Application signature check engine 108 then “identifies an application,” for example, determining what type of traffic the session involves (HTTP, SSL/TLS, etc.)” to allow an “appropriate decoder, such as decoders 112, 114, and 116, to decode the classified traffic for each monitored session’s traffic flow.” *Id.* at 9:33–43.

The known protocol decoder engine 112 decodes and analyzes flows that use known protocols and reports the analysis to report and enforce policy engine 120. Ex. 1004, 9:45–48. For example, it can decode certain secure protocols, such as SSL/TLS, to provide domain extraction using various techniques, including “parsing a client hello message to extract a hostname that identifies the destination domain being requested by the client to the remote server.” *Id.* at 9:55–57.

If the monitored traffic is encrypted, “the security device can be configured (e.g., based on a firewall policy) to decrypt the monitored traffic using a decrypt engine 110 (e.g., applying trusted man-in-the-middle techniques using a self-signed certificate).” Ex. 1004, 9:63–67. For example, “if the extracted destination domain is not trusted . . . then the firewall can be configured to decrypt the monitored traffic for further traffic monitoring and inspection based on a policy (e.g., a firewall policy).” *Id.* at 9:67–10:4.

Firewall 100 may also include content-ID engine 122, with content that can be used to provide, for example, URL/category filtering to enforce various security/firewall policies/rules. *See* Ex. 1004, 10:21–28.

2. Hello Message Technique

Buruganahalli’s FIG. 3A is a block diagram illustrating an SSL/TLS session passing through a firewall:

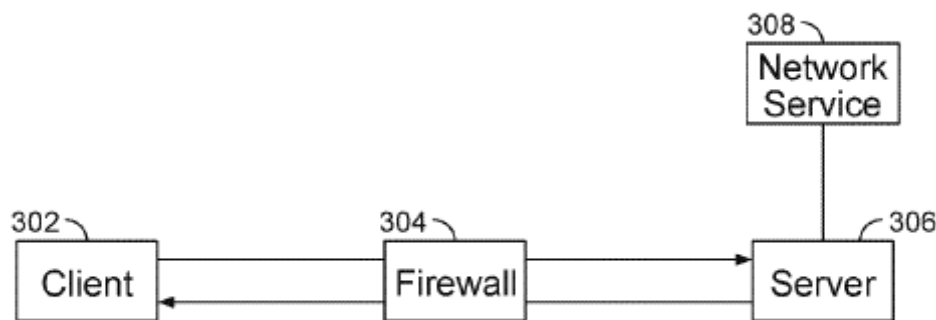


FIG. 3A depicts an illustrative event sequence for rule-based network-threat detection.

In such a session, the firewall can only inspect the handshake traffic, “as all the application data is encrypted.” Ex. 1004, 10:60–61. Client 302 “establishes a secure tunnel session . . . with a remote server 306” and then “can use the secure tunnel to access a network service 308, which can be a network service activity that is in violation of one or more firewall policies/rules implemented by the firewall device 304.” *Id.* at 10:61–67. Because “the firewall 304 typically cannot decrypt the encrypted secure tunnel session traffic” it “cannot detect such firewall policy/rule violation(s).” *Id.* at 11:4–6.

However, Buruganahalli explains that by using its destination domain extraction techniques, the firewall can apply its policies “prior to and/or without having to decrypt the encrypted secure tunnel session traffic.” Ex. 1004, 11:17–19.

Specifically, the client identifies, in the hello message, which hostname it wants to setup the secure connection with so that the server knows which public certificate to send back to the client. Ex. 1004, 11:25–28. The firewall can intercept and decode this handshake exchange to extract the hostname from the client hello message in order to apply policies based on the destination domain. *Id.* at 11:47–51.

Buruganahalli’s hello message technique is essentially identical to the ’856 patent’s description of using unencrypted data in handshaking packets, including data in a hello message, as a basis for applying a policy to a session.

3. *Man-in-the-Middle Technique*

Buruganahalli also describes “techniques for intercepting and decoding encrypted tunneling communications from a client to a remote server,” including “a trusted man-in-the-middle technique that can be used for intercepting and decoding encrypted tunneling communications to further monitor such traffic in clear text (e.g., unencrypted).” Ex. 1004, 11:59–65. Buruganahalli explains that

“[t]hese decryption techniques can be used in addition to and/or in combination with the . . . destination domain extraction for secure protocols to further enhance the various security and firewall related techniques disclosed herein.” *Id.* at 11:66–12:3.

Buruganahalli’s man-in-the-middle technique is described in connection with Figure 3B:

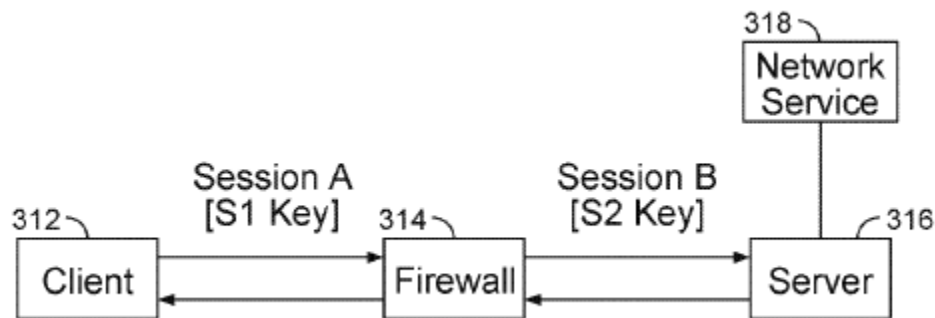


FIG. 3B depicts an illustrative event sequence for rule-based network-threat detection.

In this method, client 312 attempts to establish an SSL session with a remote server 316 and “the SSL session request is intercepted and detected by the firewall 314,” which “performs a trusted man-in-the-middle technique by effectively splitting the SSL session between the client 312 and the remote server 316 into two half sessions, shown as Session A and Session B.” Ex. 1004, 12:7–18.

In Session A, “the firewall 314 acts as the remote server 316 such that it is transparent to the client 312 that it is not communicating directly with the remote server 316” and “traffic is encrypted using the session key S1.” Ex. 1004, 12:18–21. In Session B, “the firewall 314 acts as the client 312 such that it is transparent to the remote server 316 that it is not communicating directly with the client 312” and “traffic is encrypted using the session key S2.” *Id.* at 12:22–26.

After the handshaking is completed for 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.” Ex. 1004, 12:30–32. Firewall 314 is thus “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” allowing it to “inspect decrypted traffic and re-encrypt it before forwarding it to the other party.” *Id.* at 12:56–61.

Buruganahalli’s man-in-the-middle technique is essentially identical to the ’856 patent’s description—at step 22—of using a proxy system to decrypt packets so they can be filtered based on their contents.

4. *Security Device*

Buruganahalli’s Figure 4 is “a block diagram illustrating another network architecture that can be used for destination domain extraction for secure protocols in accordance with some embodiments.” Ex. 1004, 13:5–8.

“[C]lient devices 404A, 404B, and 404C are in communication with the Internet 406 via a security device 402,” which may include a firewall that performs “some or all of the functions described . . . with respect to FIGS. 1 and 3B.” Ex. 1004, 13:8–10, 13:21–22. In this embodiment, “detection of security policy violations and/or vulnerabilities based on destination domain extraction for secure protocols can be reported to the security cloud service 410 by the security device 402,” and “the security device 402 can extract destination domain information” and provide it to the “security cloud service 410 [to] facilitate identification of new, zero-day threats, new vulnerabilities, prevent false positives, and/or provide a feedback loop for any of such activities or trends aggregated and correlated using the security cloud service.” *Id.* at 13:40–51.

Figure 6, shown below, “is a representation of logical components that can be included in security device 402,” including a management plane 602 and a data plane 604. Ex. 1004, 14:13–14.

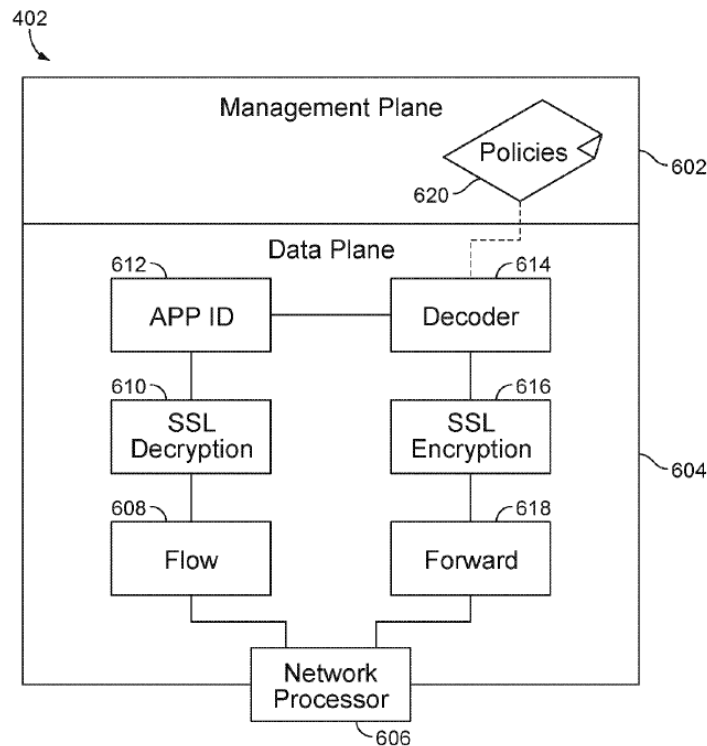


FIG. 6 is a functional diagram of logical components of a security device. Ex. 1004, 2:1–2.

The “management plane is responsible for managing user interactions, such as by providing a user interface for configuring policies and viewing log data” and the “data plane is responsible for managing data, such as by performing packet processing and session handling.” *Id.* at 14:15–20.

If a client 404A attempts to access a server 408B using an encrypted session protocol, network processor 606 is “configured to receive packets from client 404A, and provide the packets to data plane 604 for processing,” flow 608 “identifies the packets as being part of a new session and creates a new session

flow,” and “[s]ubsequent packets will be identified as belonging to the session based on a flow lookup.” Ex. 1004, 14:23–28.

“[A]n initial TLS handshake exchange of that flow can be parsed to extract a hostname” to “apply one or more policies if applicable based on the extracted destination domain” and “[i]f applicable (e.g., using one or more policies based on the extracted destination domain), SSL decryption is applied by SSL decryption engine 610.” Ex. 1004, 14:28–36.

5. *Flowcharts*

Buruganahalli’s Figures 7 and 8 are flowcharts corresponding to the hello message and man-in-the-middle techniques, respectively.

B. *Claim 1 in View of Buruganahalli*

1. *“[a] method”*

Petitioner contends that Buruganahalli discloses the preamble because it describes “a method for filtering packets in communications between a client and a remote server.” Pet. 28 (citing Ex. 1004, 4:31–40).

Patent Owner does not argue that Buruganahalli does not disclose “a method,” and we find that it does.

2. *“receiving, by a packet-filtering system . . . configured to filter packets in accordance with a plurality of packet-filtering rules, data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprises a domain name identified as a network threat”*

Petitioner asserts that Buruganahalli discloses “a packet-filtering system . . . configured to filter packets in accordance with a plurality of packet-filtering rules” because it describes a “packet-filtering firewall” that filters packets in accordance with a “set of rules . . . referred to as policies.” Pet. 29 (citing Ex. 1004, 2:55–60,

5:35–43; 7:27–29, 7:42–67, 8:1–44, 14:58–67, 10:66–11:2, 15:37–45, Fig. 6; Ex. 1003 ¶ 107).

Petitioner argues that the system “receiv[es] . . . data indicating a plurality of network-threat indicators,” because it receives a “blacklist” or data that identifies “threats” or “vulnerabilities.” Pet. 30 (citing Ex. 1004, 7:42–67; 13:43–52; Ex. 1003 ¶¶ 59–63, 109). Specifically, Petitioner cites a passage of Buruganahalli describing how the blacklist “comprises network-threat indicators (e.g., whether a destination domain presents security risk)” using data “based on ‘identification of new, zero-day threats, new vulnerabilities, prevent false positives, and/or provide a feedback loop for any of such activities or trends aggregated and correlated using the security cloud service.’” *Id.* at 30 (citing Ex. 1004, 13:43–52; Ex. 1003 ¶¶ 59–63, 109). Petitioner asserts that at least one of the threat indicators received in Buruganahalli is a “domain name.” *Id.* at 29–30 (citing Ex. 1004, 5:35–43, 7:27–29, 8:1–44, 10:66–11:2, 14:60–67, 15:37–45; Ex. 1003 ¶ 108).

Patent Owner argues that Petitioner has not shown “network-threat indicators” in Buruganahalli because it “does not teach that the destination domains on its blacklist indicate network threats.” PO Resp. 49 (citing Ex. 2026 Decl. ¶ 105). Patent Owner argues that Buruganahalli “never characterizes the blacklist as being associated with network threats,” “is silent as to how the blacklist is formed,” and “merely describes that the destination domains on the blacklist are used to decide whether to block or decrypt packets.” *Id.* at 49–50. According to Patent Owner, “Buruganahalli’s blacklist is simply a list of domains that a network administrator has identified for monitoring or blocking.” *Id.* at 50 (citing Ex. 2026 ¶ 107; Ex. 1004, 5:64–6:38; Ex. 2006, 1:25–36). Patent Owner also argues that “Petitioner’s expert characterized Buruganahalli’s blacklist as a list of domains that represent *potential* threats.” *Id.*

We agree with Petitioner that one of ordinary skill in the art would have understood that Buruganahalli's blacklist would include "data indicating a plurality of network-threat indicators," including "a domain name identified as a network threat." They are identified for monitoring or blocking precisely because they may represent a threat to the network. *See* Ex. 1004, 9:67–10:4 (explaining that "if the extracted destination domain is not trusted . . . then the firewall can be configured to decrypt the monitored traffic for further traffic monitoring and inspection based on a policy (e.g., a firewall policy)"). We find it sufficient that the threat be "potential" because, in practice, any such system would have no way of knowing for certain that a given domain was an actual threat, as, for example, the content existing at the domain could have changed or disappeared since the threat was identified.

Patent Owner also argues that the passage regarding the security device 402 shows that it is "the security service cloud 410—not Buruganahalli's firewall having the blacklist—that identifies threats, vulnerabilities, etc." PO Resp. 51.

This argument is not persuasive because the claim does not require that the system *identifies* the threat, only that it "receiv[e] . . . data indicating a plurality of network-threat indicators." Figure 4 of Buruganahalli shows cloud security service 410 that "aggregate[s] and correlate[s]," among other things, "new, zero-day threats" and "new vulnerabilities" and sends them to the local security device 402.

We conclude that Petitioner has shown this limitation to be met in Buruganahalli.

3. *"identifying packets comprising unencrypted data" and "identifying packets comprising encrypted data"*

Petitioner contends that Buruganahalli discloses identifying packets with *unencrypted* data, namely packets with the "unencrypted/clear text data

communications exchanged as part of an initial handshake” and in the “hello message.” *See* Pet. 30–31 (citing Ex. 1004, 4:37–43, 10:54–61, 11:7–42, 12:32–36, 14:25–29). Petitioner further contends that Buruganahalli discloses identifying packets with *encrypted* data because it describes “Flow 608” that “identifies the packets as being part of a new session and creates a new session flow,” such that “[s]ubsequent packets will be identified as belonging to the session based on a flow lookup.” *Id.* at 32 (citing Ex. 1004, 4:31–44, 5:43–52, 5:62–6:22, 12:33–48).

Patent Owner does not argue that Buruganahalli does not disclose identifying packets with unencrypted data and packets with encrypted data, and we find that it does.

4. *“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”*

Petitioner asserts that Buruganahalli describes determining, based on a portion of the unencrypted data (e.g., data in the unencrypted handshake traffic) that corresponds to a network-threat indicator (a destination domain on the blacklist), encrypted packets that correspond to a network-threat indicator.

Specifically, Petitioner contends that Buruganahalli extracts a domain name from handshake data and determines whether the destination domain is on the blacklist, and that one of ordinary skill in the art “would have understood that Buruganahalli teaches determining that encrypted packets correlate to a session initiated by a hello message in TLS handshake traffic.” Pet. 33–34 (citing Ex. 1004, 9:25–28, 13:62–14:1; Ex. 1003 ¶¶ 119–120).

Petitioner further asserts that one of ordinary skill in the art “would have understood that Buruganahalli teaches determining encrypted packets comprising data corresponding to one or more network-threat indicators”—i.e., “a blacklisted

destination domain”—that is “based on data included in the hello message”—i.e., the “destination domain and associated IP address”—used to establish the encrypted session, because “both the encrypted session and the hello message would be associated with the same destination IP address of the remote server.” Pet. 33–34 (citing Ex. 1003 ¶ 120).

Patent Owner does not argue that Buruganahalli does not meet this limitation,¹² and we find that Petitioner’s showing is sufficient. Buruganahalli describes using unencrypted handshake data corresponding to network-threat indicators (domains on the blacklist) and identifies packets comprising encrypted data that correlate to those packets. This is essentially the same as the disclosure of the ’856 patent, which describes “correlating the packets with one or more packets previously determined by packet-filtering system . . . to comprise data corresponding to the network-threat indicators based on data stored in [the] logs.” Ex. 1001, 9:7–10.

5. *“filtering . . . based on at least one of [A] a uniform resource identifier (URI) . . . , [B] data indicating a protocol version . . . , [C] data indicating a method . . . , [D] data indicating a request . . . , or [E] data indicating a command”*

Petitioner contends that “Buruganahalli discloses parsing a client’s SSL/TLS request (e.g., packets in handshake traffic, a hello message) to create a secure connection with a remote server to determine whether the destination domain extracted from the request corresponds to data on a blacklist” and that “[t]he system applies a security rule based on the destination domain extracted from the

¹² As noted above, Patent Owner does dispute that there are “network-threat indicators” in Buruganahalli.

request to ‘filter traffic’ from the request. Pet. 35 (citing Ex. 1004, Abstract, 5:24–52, 7:12–29, 7:39–51, 7:60–67; 8:25–44, 15:4–21; Ex. 1003 ¶¶ 122–124).

Petitioner further contends that “Buruganahalli discloses a firewall that filters packets based on identifiers for a ‘domain’ (e.g., ‘uniform resource locator (URL)’ specified in the firewall security policies or rules” and that it “discloses performing ‘application layer filtering’ and ‘content scanning.’” Pet. 35 (citing Ex. 1004, 3:25–39, 4:1–3, 7:39–7:51, 9:16–24, 9:28–43, 10:15–28, 15:37–45).

Petitioner asserts that one of ordinary skill in the art “would have understood, as was well-known and conventional, that URLs are examples of uniform resource identifiers.” *Id.* (citing Ex. 1037, 12:25–27).

Patent Owner’s primary argument is that “Buruganahalli does not teach rule-based filtering of encrypted packets, as recited in each of the Challenged Claims” because “Buruganahalli expressly requires that encrypted packets be decrypted prior to applying its firewall policies/rules. PO Resp. 31; *see* Transcript 35, 35 ([Patent Owner’s Counsel]: “[in Buruganahalli] there’s simply no application of any type of rules or any policy to that traffic before it’s decrypted”; “[in Buruganahalli] there is not a single instance where it teaches this filtering of the . . . encrypted packets based on the claimed packet filtering rules with the criteria”).

This argument is unpersuasive because Buruganahalli uses rules/policies to filter encrypted packets by correlating them with handshaking packets that have unencrypted data, in the same way that is done in the ’856 patent. The only “filtering step” in the patent that “use[s] rules to filter encrypted packets without

decryption” (PO Resp. 20), is the hello message approach used, for example, at steps 19 and 23 (*see id.*), which is clearly disclosed in Buruganahalli.¹³

As explained above, the ’856 patent does not describe applying rules to encrypted packets. Instead, it describes (a) filtering encrypted packets by correlating them with unencrypted data in other packets and (b) decrypting packets and applying the rules that are recited in the claims to unencrypted data.

As also explained above, the second amendment added the rules of step 22, which are applied to decrypted data, to a claim that was drafted to cover filtering of encrypted packets. *However*, among the criteria used in the filtering performed at step 22 is a “uniform resource identifier (URI),” which, we conclude, covers Buruganahalli’s “domain name.” Thus, despite the error made during prosecution, the claims that issued cover Buruganahalli’s method of determining that a session should be filtered based on a domain name in unencrypted handshake data.

At the hearing, Patent Owner argued there is no URI (or URL) in Buruganahalli’s handshake message. *See* Transcript 61. We find that argument waived, because it was not raised earlier. *See* Paper 12, 8 (warning that “any patentability arguments not raised in the response may be deemed waived”). But we also find that it would be unpersuasive even if it had been raised earlier. No party has sought a construction of “URI” or “Uniform Resource Identifier,” and we conclude that the plain language would encompass domain names, which are a “uniform” way of “identifying” a “resource.”

¹³ Notably, Patent Owner’s description of the patent focuses on the filtering of *encrypted* packets at steps 19 and 23, but then skips to a description of the criteria recited in the claim, without acknowledging that those criteria are actually used at distinct step 22, on *decrypted* packets. *See* PO Resp. 20–21.

Patent Owner argues that the Petition relies on Buruganahalli's man-in-the-middle technique for the claimed filtering. *See* PO Resp. 31–37. That is not correct. As explained above, the Petition contends that “Buruganahalli discloses parsing a client's SSL/TLS request (e.g., packets in handshake traffic, a hello message) to create a secure connection with a remote server to determine whether the destination domain extracted from the request corresponds to data on a blacklist” and then “applies a security rule based on the destination domain extracted from the request to ‘filter traffic’ from the request.” Pet. 35. That is referring to Buruganahalli's hello message technique, not the man-in-the-middle technique.

Regarding Buruganahalli's hello message technique, Patent Owner argues that “packet-filtering rules are never applied to encrypted packets, *with or without* decryption.” PO Resp. 38 (citing Ex. 2026 ¶¶ 88–89). Patent Owner claims that “[t]his technique . . . refers to the firewall's ability to determine whether a new flow ‘violate[s] a policy prior to the set-up of the encrypted data communication’ . . . so that ‘the flow can be blocked and decryption is not required’ . . . whereas the session is allowed without any filtering of encrypted packets if the domain is trusted.” *Id.* Patent Owner contends that “the policies are applied to unencrypted packets before an encrypted session ever begins (i.e. prior to beginning the encrypted session), making decryption entirely because the session is either allowed without subjecting the encrypted packets to any filtering or blocked before any encrypted packets are received unnecessary (i.e. without having to decrypt encrypted packets).” *Id.* at 39 (citing Ex. 2026 ¶ 90). Patent Owner concludes that “[b]ecause 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.” *Id.* at 40.

This argument is not persuasive because, in addition to describing how the hello message technique can be used to allow or completely block a flow, Buruganahalli describes how its methods “can also be used to determine whether a new session using a secure protocol should be initially allowed based on a policy (e.g., security policy, such as a firewall policy), and then to further monitor encrypted data communications associated with the session.” Ex. 1004, 6:12–16. The reference explains how the system “extract[s] . . . the destination domain by parsing the handshake traffic (e.g., parsing a client hello message to extract a hostname that identifies the destination domain being requested by the client to the remote server)” and then “can apply one or more firewall policies/rules implemented by the firewall device 304 (e.g., a policy that includes requirements or rules related to destination domains that may be used for secure protocol communications) prior to and/or without having to decrypt the encrypted secure tunnel session traffic.” *Id.* at 11:9–19. Buruganahalli then explains that “a trusted man-in-the-middle technique . . . can be used for intercepting and decoding encrypted tunneling communications to *further monitor* such traffic in clear text (e.g., unencrypted).” *Id.* at 11:61–65 (emphasis added). This technique “can be used *in addition to and/or in combination with*” the hello message technique. *Id.* at 11:66–67 (emphasis added). Buruganahalli thus describes filtering encrypted packets for further analysis because they are in the same flow as packets that have exposed handshaking data that corresponds to a threat indicator.

Patent Owner argues that “the Petition and Board’s institution decision both point to Buruganahalli’s flow lookup for limitations [1.b] and [1.c] of ‘identifying’ unencrypted and encrypted packets, respectively” and that “[i]t is inconsistent and

contrary to the doctrine of attributing different meaning to different claim terms to rely on Buruganahalli's flow lookup for the separate step of "filtering." PO Resp. 43 (citing Pet. 30–32; Decision 60–62). There is no inconsistency. The "identifying" is determining that the two types of packets are in a given flow; the "filtering" is taking an appropriate action because the unencrypted data in the handshaking data for that flow corresponds to a threat indicator.

Patent Owner also cites Figure 6 of Buruganahalli to argue that "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." PO Resp. 43. Patent Owner concludes that "Buruganahalli never discloses (and the Petition never asserts) that flow lookup uses policies to filter encrypted packets." *Id.* at 44 (citing Ex. 1004, 14:25–33). We do not agree.

Figure 6 describes a client attempting to access a server using an encrypted session protocol. *See* Ex. 1004, 14:21–22. Network processor 606 receives packets from client 404A and "[f]low 608 identifies the packets as being part of a new session and creates a new session flow." *Id.* at 14:25–26. Subsequent packets are identified as belonging to the session based on a flow lookup, which corresponds to the claimed "identifying" step. Then, the "handshake exchange of that flow can be parsed to extract a hostname to facilitate destination domain extraction for secure protocols," such as "apply[ing] one or more policies if applicable based on the extracted destination domain," which corresponds to the claimed "filtering" step. *Id.* at 14:29–33. Thus, contrary to Patent Owner's argument, Buruganahalli uses policies in conjunction with the flow lookup to filter encrypted packets.

Patent Owner also disputes Petitioner's contention that one of ordinary skill in the art would have 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.” PO Resp. 46–47 (citing Pet. 38–39). However, Petitioner only made that argument “[t]o the extent it is argued that Buruganahalli does not explicitly disclose filtering the packets with encrypted data that corresponds to a network-threat indicator.” Pet. 38. Because, for the reasons described above, we find that Buruganahalli does explicitly disclose “filtering the packets with encrypted data that corresponds to a network-threat indicator,” this argument is moot.

We conclude that Petitioner has shown this limitation to be met in Buruganahalli.

6. *[A] “packets comprising the portion of the unencrypted data that corresponds to one or more network-threat indicators” and [B] “the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators”*

As described above, Buruganahalli filters (A) the packets with the unencrypted data, for example those with the hello message, and (B) the encrypted packets that are part of the same flow/session. We, accordingly, find that Petitioner has shown this limitation to be met in Buruganahalli.

7. *“routing . . . filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators”*

Petitioner contends that Buruganahalli teaches this limitation because it describes sending “the encrypted data communications” to a firewall with a decrypt engine that “applies ‘trusted man-in-the-middle techniques using a self-signed certificate.’” Pet. 39–40 (quoting Ex. 1004, 9:66–67). Petitioner asserts that the firewall includes “functionality acting as a proxy for both the remote server

and the client by standing in line of their communications in a ‘transparent’ manner, as was known in the art.” *Id.* at 40–41 (citing Ex. 1005, 4:50–63, 8:36–47, 8:65–9:7; Ex. 1034, 8:12–19; Ex. 1036, 14).

Patent Owner argues that “Buruganahalli’s firewall does not route filtered packets to a proxy system.” PO Resp. 51. Specifically, Patent Owner argues that “no filtering of encrypted packets occurs until after they have been decrypted, so the decrypt engine cannot receive filtered packets—it decrypts traffic so that the firewall can monitor and filter decrypted packets.” *Id.* at 52.

This argument is unpersuasive because, as described above, Buruganahalli describes “filtering” packets based on their status as part of a flow, and then sending packets of the flow to a proxy system for decryption and further analysis. This, again, is essentially the same as how the system of the ’856 patent works.

Patent Owner next contends that “Petitioner equates Buruganahalli’s ‘decrypt engine’ with the claimed ‘proxy system’ and that “Buruganahalli’s decrypt engines 110, 610 are not a proxy, and Petitioner never even attempted to demonstrate that it satisfies the proper construction of the term, which is ‘a proxy system which intervenes to prevent threats in communications between devices.’” PO Resp. 53. This too is unpersuasive because the Petition actually relies on the firewall 314 shown in Buruganahalli’s Figure 3B, which operates as a proxy between client 312 and server 316, decrypting the packets so that they can be inspected by the firewall. *See* Pet. 39–41 (reproducing and describing Figure 3B); Ex. 1004, 12:4–32; 9:67–10:4 (“if the extracted destination domain is not trusted . . . then the firewall can be configured to decrypt the monitored traffic for further traffic monitoring and inspection based on a policy (e.g., a firewall policy)”). Again, this is essentially the same as how the proxy system of the ’856 patent operates. The patent’s Host 106 corresponds to Buruganahalli’s Client 312, the

patent's PD1, RG3, and PD2 correspond to Buruganahalli's Firewall 314, and the patent's Host 128 corresponds to Buruganahalli's Server 316.

We conclude that Petitioner has shown this limitation to be met in Buruganahalli.

8. *Objective Indicia of Nonobviousness*

Patent Owner argues that objective indicia of nonobviousness overcome Petitioner's obviousness showing. Specifically, Patent Owner points to evidence of a "long-felt need in the industry" and "substantial industry praise," as well as copying of the '856 patent by Cisco. *See* PO Resp. 68–70. We find the secondary considerations arguments unpersuasive.

As an initial matter, we observe that a strong showing of obviousness may stand "even in the face of considerable evidence of secondary considerations." *ZUP, LLC v. Nash Mfg., Inc.*, 896 F.3d 1365, 1374–75 (Fed. Cir. 2018) (quoting *Rothman v. Target Corp.*, 556 F.3d 1310, 1322 (Fed. Cir. 2009)); *see also Wyers v. Master Lock Co.*, 616 F.3d 1231, 1246 (Fed. Cir. 2010) ("secondary considerations of nonobviousness . . . simply cannot overcome a strong prima facie case of obviousness").

For the reasons described above, we find that Buruganahalli presents a strong case of obviousness and, in fact, is essentially anticipatory, describing both the hello message technique that the '856 patent uses for filtering packets in a flow and the man-in-the-middle technique that the '856 patent uses for filtering decrypted packets. Thus, even if Patent Owner's objective evidence was strong, we would find it insufficient to establish nonobviousness. We also find, however, that the evidence offered would be insufficient to overcome even a weak case of obviousness.

Long Felt Need and Industry Praise

Patent Owner argues that “the Cisco press release is evidence of long-felt need and industry recognition for the technology claimed in the ’856 Patent because it describes the problem of detecting threats in encrypted traffic as ‘unsolvable.’” PO Resp. 68 (citing Ex. 1027, 64). Given that this is a press release by a company announcing that company’s new commercial product, however, we are reluctant to give the “unsolvable” characterization much weight, as it may amount to puffery. *See Bayer Healthcare v. Watson Pharms.*, 713 F.3d 1369, 1377 (Fed. Cir. 2013) (explaining that bare journal citations and self-referential commendation fall short of demonstrating industry praise). But beyond that, it appears that the problem identified as “unsolvable” in the press release—“detect[ing] known attack signatures even in encrypted traffic”—had, in fact, already been solved in Buruganahalli, using the very same hello message, correlation, and man-in-the-middle techniques described in the ’856 patent. We thus cannot say that the press release identifies a long-felt need that was actually unsolved. *See ZUP*, 896 F.3d at 1374 (explaining that “[w]here the differences between the prior art and the claimed invention are . . . minimal . . . it cannot be said that any long-felt need was unsolved”) (quoting *Geo. M. Martin Co. v. All. Mach. Sys. Int’l LLC*, 618 F.3d 1294, 1304–05 (Fed. Cir. 2010)).

Patent Owner also argues that the Cisco press release provides “compelling evidence of nonobviousness” because “[i]ndustry participants, especially competitors, are not likely to praise an obvious advance over the known art.” PO Resp. 69 (quoting *Apple Inc. v. Samsung Elecs. Co.*, 839 F.3d 1034, 1053 (Fed. Cir. 2016) (en banc)). We find this unpersuasive because Cisco promoting its *own* new product does not appear to be an example of “the industry” or “a competitor” praising the claimed invention. This is quite different than the evidence in *Apple v.*

Samsung, which showed *competitors of Apple* praising *Apple's* patented “slide to unlock” feature. *See* 839 F.3d at 1053–1054.

Nexus

Patent Owner argues that “[t]he nexus between this evidence and the ’856 Patent claims was . . . established by way of the court’s finding that . . . Cisco’s Encrypted Traffic Analytics [(“ETA”)] technology . . . infringed the ’856 Patent.” PO Resp. 69 (citing Ex. 1027, 30–57). Although the District Court’s infringement finding has been vacated, the decision does describe the factual basis for the infringement conclusion.

In particular, Patent Owner’s expert explained that Cisco’s “accused routers and switches will make a determination if the packets are encrypted or unencrypted” and then send “representations of information from the unencrypted portion of encrypted packets” to “Stealthwatch,” “which is running both ETA and Cognitive Threat Analytics (“CTA”)” using “Cisco’s proprietary logging framework known as NetFlow.” Ex. 1027, 34 (¶¶ 14–17).

Stealthwatch, which “analyzes the NetFlow from the packets and identifies malware threats in encrypted traffic without running any form of standard decryption,” receives “real-time threat intelligence indicators” that contain “known malicious IP addresses, domain names, protocol versions and other indicators of malicious traffic.” Ex. 1027, 34 (¶ 17) Stealthwatch then “determines if any encrypted traffic in the network matches any known malicious signatures *based on unencrypted information provided in NetFlow such as the IDP, Server Name Indicator (“SNI”) or Transport Layer Security (“TLS”).*” *Id.* at 35 (¶¶ 18–20)

(emphasis added).¹⁴ Notably, SNI is the TLS extension from which Buruganahalli extracts its unencrypted hostname data. *See* Ex. 1004, 5:6–51.

Stealthwatch next “sends the results of its analysis to the Identity Services Engine, which “will provision rules or change of authorizations . . . to the switches and routers.” Ex. 1027, 35–36 (¶¶ 21–22). The switches and routers “operate inline and are able to drop incoming packets from the malicious source and outgoing packets containing sensitive data attempting to be exfiltrated by embedded malware” and “[b]locked packets are routed to a proxy system, known as a null interface, that is used to drop packet traffic.” *Id.* at 36 (¶¶ 22–23).

The District Court did not provide an element-by-element analysis of how the claims of the ’856 patent cover the accused products. *See* Ex. 1027, 41. However, from the description, we understand the Court to have concluded that the Cisco system receives rules, identifies a set of packets as part of a flow using the NetFlow logs, “determines” that *encrypted* packets in the flow match known malicious signatures based on *unencrypted* data in other packets (e.g., data in the SNI), and then filters the flow based in a URI (e.g., that from the SNI), routing it to the null interface. The Court does not describe *how* the system “determines” that encrypted packets match known malicious signatures based on information in unencrypted packets, but we assume that is done as in the ’856 patent, by correlation, i.e., an encrypted packet is “determined” to match a threat indicator if it is in the same flow as a packet with unencrypted information that matches the threat indicator.

With that understanding, we conclude that the allegedly infringing system operates, as least at the level described in the court’s decision, in the same way

¹⁴ “IDP” is the “Initial Data Packet,” which includes “data such as an HTTP URL, DNS hostname and address, and other data elements.” Ex. 1027, 33 (¶ 12).

Buruganahalli's system operates, filtering encrypted packets due to their presence in a flow that includes packets with unencrypted data, such as in a handshaking packet. It follows that Patent Owner is unable to establish a nexus, because "[w]here the offered secondary consideration actually results from something other than what is both claimed *and novel* in the claim, there is no nexus to the merits of the claimed invention." *Novartis AG v. Torrent Pharms. Ltd.*, 853 F.3d 1316, 1330 (Fed. Cir. 2017) (quoting *In re Kao*, 639 F.3d 1057, 1068 (Fed. Cir. 2011)).

Copying

Patent Owner also argues that the District Court "found compelling evidence of copying" by Cisco. *See* PO Resp. 69–70. As Petitioner observes, however, the District Court's decision has been vacated, so the Court's ultimate factual finding of copying by Cisco is not evidence upon which we can rely. And, although some of the underlying evidence on that issue may be available, we certainly are not in a position to evaluate the entirety of the litigation record, weigh witness testimony, and make a factual finding about copying by Cisco.

9. Conclusion Regarding Claim 1

Petitioner's analysis establishes that Buruganahalli teaches every limitation of claim 1, Patent Owner's arguments regarding the prior art are unpersuasive, and Patent Owner's evidence of objective indicia of nonobviousness is insufficient. We thus conclude that Petitioner has proven claim 1 unpatentable under § 103 as obvious over Buruganahalli.

C. Claims 24 and 25 in View of Buruganahalli

Petitioner contends that claims 24 and 25 are unpatentable under § 103 as obvious over Buruganahalli for essentially the same reasons as claim 1. *See* Pet. 28–42; Ex. 1003 ¶¶ 101–146.

Claim 1 is directed to a method with steps that are performed by a packet-filtering system, and claim 24 is directed to a packet filtering system with a processor and memory storing instructions that, when executed, perform the steps recited in claim 1.

Claim 25 is directed to computer readable media with instructions for performing a method similar to that of claims 1 and 24, but also requires that the URI specified by the packet-filtering rules “indicat[e] one or more of the plurality of network-threat indicators.” Ex. 1001, 25:14–49, 28:59–30:31. Petitioner contends that Buruganahalli “discloses packet-filtering rules that indicate network-threat indicators” and “[f]or example, the rules are implemented for security purposes to protect the network.” Pet. 35–36 (citing Ex. 1004, 1:32–36, 2:61–66, 7:27–29, 7:42–67, 8:1–44, 10:66–11:2, 13:43–52).

Patent Owner argues that claims 24 and 25 are patentable over Buruganahalli for the same reasons as claim 1. *See* PO Resp. 30–52 (arguing the independent claims together).

For the reasons discussed above for claim 1, we conclude that Petitioner has proven claims 24 and 25 unpatentable under § 103 as obvious over Buruganahalli.

D. Patentability Conclusion

Claims 1, 24, and 25 of the ’856 patent are unpatentable because they would have been obvious under 35 U.S.C. § 103 in view of Buruganahalli.

IV. REQUESTS FOR REHEARING

As noted above, we granted and joined petitions filed by Cisco Systems, Inc. and Keysight Technologies, Inc. in IPR2022-01151 and IPR2022-01199. *See* Papers 39, 41. Patent Owner filed Requests for Rehearing (Papers 48 and 49), arguing that the Cisco and Keysight institution decisions should be vacated (a) due to a conflict and (b) because the panel adopted an argument that Petitioner did not

raise. *See, e.g.*, Paper 48 (“Rh’g Req.”), 1–2. Prior to the hearing, we addressed the conflict arguments and determined that there was no conflict that warranted vacatur. *See* Paper 55. We now turn to the second argument raised in the rehearing requests.

Patent Owner contends that the Board raised unpatentability theories never presented by the petitioner and also that those theories are incorrect. *See* Rh’g Req. 6–12. The gist of the argument is that “Buruganahalli discloses . . . that the decision to decrypt an encrypted communications flow is made at the policy check engine/flow processing engine based on the IP address and port number associated with the encrypted packet, not any of the criteria recited in the claimed packet-filtering rules,” and that “the Board departed from the record and invented a new argument on behalf of Petitioners, namely that Buruganahalli discloses an embodiment in which policies are applied without first sending encrypted traffic for decryption.” *Id.* at 8. Neither of those allegations is correct.

First, as explained above, Buruganahalli describes determining “whether a new session using a secure protocol should be initially allowed based on a policy” and “further monitor[ing] encrypted data communications associated with the session.” Ex. 1004, 6:12–16. The system “extract[s] . . . the destination domain by parsing the handshake traffic” and then “can apply one or more firewall policies/rules implemented by the firewall device 304 (e.g., a policy that includes requirements or rules related to destination domains that may be used for secure protocol communications) prior to and/or without having to decrypt the encrypted secure tunnel session traffic.” *Id.* at 11:9–19. “[I]n addition to and/or in combination with” the handshake traffic (hello message) technique, “a trusted man-in-the-middle technique . . . can be used for intercepting and decoding encrypted tunneling communications to further monitor such traffic in clear text

(e.g., unencrypted).” *Id.* at 11:61–67. Buruganahalli thus describes filtering flows based on the presence of the domain name, and forwarding those filtered flows to a proxy system for decryption and further analysis. Patent Owner’s argument that the filtering in Buruganahalli is “based on the IP address and port number associated with the encrypted packet” is unpersuasive because it does not address the filtering of flows based on the hello message domains.

Second, the Petitions clearly identify the hello message theory of filtering, stating, for example, that “Buruganahalli discloses parsing a client’s SSL/TLS request (e.g., packets in handshake traffic, a hello message) to create a secure connection with a remote server to determine whether the destination domain extracted from the request corresponds to data on a blacklist” and that “[t]he system applies a security rule based on the destination domain extracted from the request to ‘filter traffic’ from the request.” *See* IPR2022-01151, Paper 2, 51; IPR2022-1199, Paper 1, 37. The Board did not raise this theory on its own.

Because we find Patent Owner’s rehearing arguments unpersuasive, the Requests for Rehearing are denied.

V. CONCLUSION

Petitioner has met its burden in showing claims 1, 24, and 25 are unpatentable.¹⁵

Claim(s)	35 U.S.C. §	Reference(s)	Claim(s) Shown Unpatentable	Claim(s) Not Shown Unpatentable
1, 24, 25	103	Buruganahalli	1, 24, 25	
1, 24, 25	103 ¹⁶	Buruganahalli, Baehr		
Overall Outcome			1, 24, 25	

¹⁵ Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner's attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. See 84 Fed. Reg. 16654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. See 37 C.F.R. § 42.8(a)(3), (b)(2).

¹⁶ We do not reach this ground because we determine that the challenged claims are unpatentable based on Buruganahalli alone.

VI. ORDER

For the reasons given, it is:

ORDERED that claims 1, 24, and 25 of U.S. Patent 9,917,856 B2 have been shown to be unpatentable;

ORDERED that Patent Owner's Motions for Reconsideration (Papers 48 and 49) are denied; and

FURTHER ORDERED that, because this is a Final Written Decision, the parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

IPR2022-00182
Patent 9,917,856 B2

FOR PETITIONER:

James Hannah
Jeffrey Price
Jenna Fuller
KRAMER LEVIN NAFTALIS & FRANKEL LLP
jhannah@kramerlevin.com
jprice@kramerlevin.com
jfuller@kramerlevin.com

FOR PATENT OWNER:

Bradley Wright
Scott Kelly
Blair Silver
BANNER & WITCOFF, LTD.
bwright@bannerwitcoff.com
skelly@bannerwitcoff.com
bsilver@bannerwitcoff.com