

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

KEYSIGHT TECHNOLOGIES, INC.,  
Petitioner,

v.

CENTRIPETAL NETWORKS, LLC,  
Patent Owner.

---

IPR2023-00448  
Patent 11,012,474 B2

---

Before KEVIN F. TURNER, AARON W. MOORE, and  
STEVEN M. AMUNDSON, *Administrative Patent Judges*.

AMUNDSON, *Administrative Patent Judge*.

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

## I. INTRODUCTION

Keysight Technologies, Inc. (“Petitioner”) filed a Petition requesting an *inter partes* review of claims 1–33 in U.S. Patent No. 11,012,474 B2 (Exhibit 1001, “the ’474 patent”) under 35 U.S.C. §§ 311–319. Paper 2 (“Pet.”). Centripetal Networks, LLC (“Patent Owner”) filed a Preliminary Response. Paper 6 (“Prelim. Resp.”).

In the Institution Decision, we instituted review based on all challenged claims and all challenges included in the Petition. Paper 7 (“Inst. Dec.”). We have jurisdiction under 35 U.S.C. § 6. We issue this Final Written Decision under 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73. For the reasons explained below, Petitioner has shown by a preponderance of the evidence that claims 1–5, 7–13, 15–21, 23–29, 31, and 32 are unpatentable but has not shown by a preponderance of the evidence that claims 6, 14, 22, 30, and 33 are unpatentable. *See* 35 U.S.C. § 316(e) (2018).

## II. BACKGROUND

### *A. Procedural History*

After we instituted review, Patent Owner filed a Response (Paper 12, “Resp.”), Petitioner filed a Reply (Paper 16, “Reply”), and Patent Owner filed a Sur-reply (Paper 22, “Sur-reply”). On April 22, 2024, we held an oral hearing, and the record includes the hearing transcript. Paper 24 (“Tr.”).

### *B. Real Parties in Interest*

Petitioner identifies itself as the sole real party in interest. Pet. 1. Patent Owner identifies itself as the sole real party in interest. Paper 3, 1. The parties do not raise any issue about real parties in interest.

*C. Related Matters*

Petitioner and Patent Owner identify the following civil action as a related matter involving the '474 patent: *Centripetal Networks, LLC v. Keysight Technologies, Inc.*, No. 2:22-cv-00002 (E.D. Va. filed Jan. 1, 2022). Pet. 1; Paper 3, 1.

*D. The '474 Patent (Exhibit 1001)*

The '474 patent, titled “Methods and Systems for Protecting a Secured Network,” issued on May 18, 2021, from an application filed on September 21, 2020. Ex. 1001, codes (22), (45), (54). The patent claims priority through several ancestor applications to an application filed on April 16, 2014. *Id.* at 1:7–19; *see id.* at code (60). The patent states that the disclosure relates to “protecting a secured network.” *Id.* at 1:57–58.

The '474 patent explains that the “TCP/IP network protocols (e.g., the Transmission Control Protocol (TCP) and the Internet Protocol (IP)) were designed to build large, resilient, reliable, and robust networks” but “were not originally designed with security in mind.” Ex. 1001, 1:25–29. Although subsequent developments “have extended such protocols to provide for secure communication between peers,” the “networks themselves remain vulnerable to attack.” *Id.* at 1:29–33.

The '474 patent endeavors to improve network security by providing “one or more packet security gateways” associated with a “security policy management server.” Ex. 1001, 1:58–60, code (57). Each packet security gateway may receive a “dynamic security policy” from the security policy management server. *Id.* at 1:60–62, code (57). Each packet security gateway may perform “at least one of multiple packet transformation functions specified by the dynamic security policy” on “packets associated

with a network protected by the packet security gateway.” *Id.* at 1:60–66, code (57). “Performing the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets may include performing at least one packet transformation function” other than “forwarding (accepting or allowing) or dropping (denying) a packet,” such as routing a packet to a monitoring device. *Id.* at 1:66–2:3, 8:23–33.

The ’474 patent’s Figure 1 (reproduced below) depicts an exemplary network environment with a security policy management (SPM) server and packet security gateways (PSGs) situated between networks:

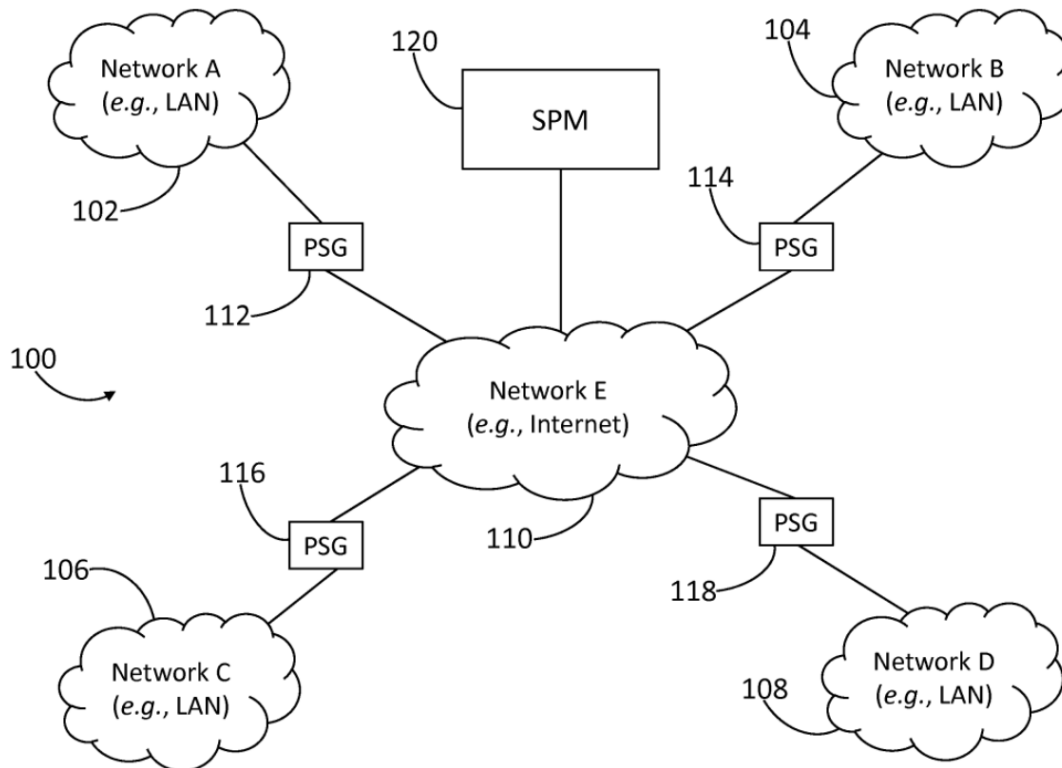


FIG. 1

Figure 1 illustrates network environment 100 including the following:

- (1) network A 102, network B 104, network C 106, network D 108, and network E 110, such as “a Local Area Network (LAN) or a Wide Area Network (WAN)” associated with “an organization (e.g., a company, university, enterprise, or government agency)”;

- (2) packet security gateways 112, 114, 116, and 118 “configured to perform a packet transformation function,” e.g., accept or deny, on packets associated with network A 102, network B 104, network C 106, and network D 108; and
- (3) security policy management server 120 “configured to communicate one or more dynamic security policies to one or more packet security gateways within network environment 100.”

See Ex. 1001, 4:47–55, 5:54–60, 14:25–28, Fig. 1; see *id.* at 4:1–3.

The ’474 patent’s Figure 3 (reproduced below) depicts an exemplary dynamic security policy:

five-tuple

300

| Rule #     | Protocol | Source Address | Source Port | Destination Address | Destination Port | Action                                       |
|------------|----------|----------------|-------------|---------------------|------------------|----------------------------------------------|
| 1<br>(302) | TCP      | 140.*          | *           | 130.*               | 20               | Accept                                       |
| 2<br>(304) | TCP      | 140.*          | *           | *                   | 80               | Accept                                       |
| 3<br>(306) | TCP      | 150.*          | *           | 120.*               | 90               | Accept &<br>Route to<br>Monitoring<br>Device |
| 4<br>(308) | UDP      | 150.*          | *           | *                   | 3030             | Accept                                       |
| 5<br>(310) | *        | *              | *           | *                   | *                | Deny                                         |

FIG. 3

Figure 3 illustrates dynamic security policy 300 including rule 1 (302), rule 2 (304), rule 3 (306), rule 4 (308), and rule 5 (310). Ex. 1001, 7:27–30, Fig. 3; see *id.* at 4:5. “Each rule may specify criteria and one or more packet transformation functions that should be performed for packets associated

with the specified criteria.” *Id.* at 7:30–33. The “specified criteria may take the form of a five-tuple of values selected from packet header information,” such as the following five values:

- (1) “a protocol type of the data section of the IP packet (e.g., TCP, UDP, ICMP, or any other protocol)”;<sup>1</sup>
- (2) “one or more source IP addresses”;
- (3) “one or more source port[s]”;
- (4) “one or more destination IP addresses”; and
- (5) “one or more destination ports.”

*Id.* at 7:33–39.

As an example, rule 1 (302) may “specify that IP packets containing TCP packets, originating from a source IP address that begins with 140, having any source port, destined for an IP address that begins with 130, and destined for port 20 should have an accept packet transformation function (e.g., the identity function) performed on them.” Ex. 1001, 7:39–45. As another example, rule 2 (304) may “specify that IP packets containing TCP packets, originating from a source IP address that begins with 140, having any source port, destined for any IP address, and destined for port 80 should have an accept packet transformation function performed on them.” *Id.* at 7:45–50.

A combination of rules may “effectuate an implementation of an informational service for performing a network communications awareness service, a network security awareness service, and/or a network threat

---

<sup>1</sup> The acronym “TCP” stands for “Transmission Control Protocol.” The acronym “UDP” stands for “User Datagram Protocol.” The acronym “ICMP” stands for “Internet Control Message Protocol.”

awareness service.” Ex. 1001, 11:52–57. The rules may “specify a packet transformation function” that produces a packet log (or digest) containing “selected packet information and/or system information (e.g., associated network addresses, ports, protocol types, URIs, arrival times, packet sizes, directions, interface names, media access control (MAC) addresses, matching rule IDs, metadata associated with matching rules, enforced policy names, or the like).” *Id.* at 11:63–12:5.

The ’474 patent’s Figure 5 (reproduced below) depicts an exemplary security policy management server:

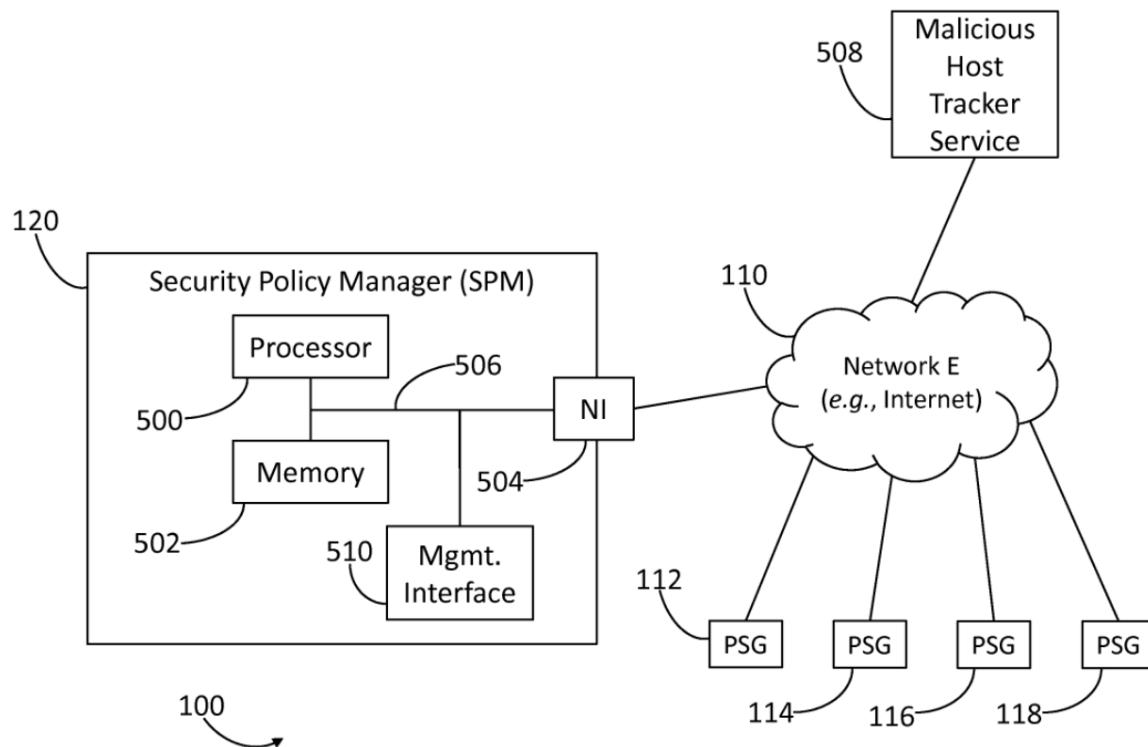


FIG. 5

Figure 5 illustrates security policy management server 120 including “processor 500, memory 502, and network interface 504” interconnected “via data bus 506.” Ex. 1001, 14:8–12, Fig. 5; *see id.* at 4:8–9. Figure 5 also illustrates malicious host tracker service 508 communicating with

security policy management server 120 via network E 110, e.g., the Internet. *Id.* at 15:10–13, Fig. 5.

Malicious host tracker service 508 may “aggregate information associated with malicious network traffic.” Ex. 1001, 15:13–15. Malicious host tracker service 508 may also provide updates to security policy management server 120 that include “one or more network addresses that have been determined to be associated with malicious network traffic.” *Id.* at 15:15–18.

Security policy management server 120 may “create or alter one or more rules included within a dynamic security policy associated with malicious host tracker service 508 to block traffic associated with the network addresses received from malicious host tracker service 508.” Ex. 1001, 15:18–23. Security policy management server 120 may also “add, remove, and/or alter one or more dynamic security policies stored in memory 502 based on information received from two or more devices within network environment 100.” *Id.* at 15:30–34. For instance, security policy management server 120 may “receive updates (e.g., as part of a subscription) from malicious host tracker service 508 and/or one or more other services.” *Id.* at 15:34–37. The “updates from the two or more services may be correlated” by security policy management server 120. *Id.* at 15:37–39.

For example, security policy management server 120 may “combine the rules associated with these correlated updates from two or more services within one or more dynamic security policies.” Ex. 1001, 15:44–47. Additionally, “duplicate network addresses may be removed, and/or overlapping ranges of network addresses may be combined into one or more new network address ranges.” *Id.* at 15:52–55. By reducing the size of one

or more dynamic security policies, security policy management server 120 may improve a packet security gateway's performance because its performance may depend on "the size of and/or correlations within [the] dynamic security policies." *Id.* at 15:48–52.

### *E. The Challenged Claims*

Petitioner challenges the following claims:

- (1) independent claim 1 for a method of filtering packets at a packet security gateway;
- (2) claims 2–8 that depend directly or indirectly from claim 1;
- (3) independent claim 9 for a packet security gateway;
- (4) claims 10–16 that depend directly or indirectly from claim 9;
- (5) independent claim 17 for one or more non-transitory computer-readable media;
- (6) claims 18–24 that depend directly or indirectly from claim 17;
- (7) independent claim 25 for a system; and
- (8) claims 26–33 that depend directly or indirectly from claim 25.

Pet. 2–3, 11–73.

Claim 1 exemplifies the challenged claims and reads as follows (with formatting added for clarity and with bracketed numbers added for reference purposes):<sup>2</sup>

1. [1.0] A method of filtering packets at a packet security gateway configured for protection of a network, wherein the

---

<sup>2</sup> We use the same numbers that Petitioner uses to identify the claim language. *See* Pet. 19–45; Ex. 1012 (Listing of Claims), 1.

packet security gateway is capable of receiving a plurality of dynamic security policies and is associated with a security policy management server external from the network, the method comprising:

[1.1] receiving, by the packet security gateway and from the security policy management server, a dynamic security policy comprising packet filtering rules,

[1.2] wherein one or both of the dynamic security policy or one or more of the packet filtering rules of the dynamic security policy were automatically created or altered, by the security policy management server, based on malicious traffic information received from a plurality of malicious host tracker services,

[1.3] wherein at least two of the plurality of malicious host tracker services are managed by different organizations,

[1.4] wherein one or more of the packet filtering rules were added, removed, or altered by the security policy management server based on a correlation between portions of the malicious traffic information, and

[1.5] wherein a first packet matching rule of the packet filtering rules comprises: at least one packet matching criterion, a corresponding packet transformation function, and an indication of a feed managed by at least one of the plurality of malicious host tracker services; and

[1.6] performing, based on the packet filtering rules, packet filtering on individual packets of a plurality of packets associated with the network protected by the packet security gateway,

[1.7] wherein the packet filtering comprises: inspecting individual packets; and

[1.8] filtering each packet based on content determined from the inspection of that individual packet.

Ex. 1001, 25:31–64.

*F. The Asserted References*

For its challenges, Petitioner relies on the following references:

| Name    | Reference                                                                                                                                                                                                | Exhibit |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| Law     | US 2011/0072506 A1, published March 24, 2011<br>(based on an application filed September 23, 2010)                                                                                                       | 1005    |
| Wood    | US 2007/0097976 A1, published May 3, 2007<br>(based on an application filed May 19, 2006)                                                                                                                | 1006    |
| Jungck  | US 2009/0262741 A1, published October 22, 2009<br>(based on an application filed June 29, 2009)                                                                                                          | 1008    |
| Golnabi | Korosh Golnabi et al., <i>Analysis of Firewall Policy Rules Using Data Mining Techniques</i> , 2006<br>IEEE/IFIP Network Operations and Management Symposium NOMS 2006, 305–15 (April 2006) <sup>3</sup> | 1009    |
| Ke      | US 7,095,716 B1, issued August 22, 2006<br>(based on an application filed March 28, 2002)                                                                                                                | 1010    |
| Johnson | US 2004/0123220 A1, published June 24, 2004<br>(based on an application filed December 18, 2002)                                                                                                         | 1011    |

Pet. 2–3, 11–73. Petitioner asserts that “each of these references is prior art under 35 U.S.C. § 102(a)(1).” *Id.* at 3.<sup>4</sup>

---

<sup>3</sup> The acronym “IEEE” stands for “Institute of Electrical and Electronics Engineers.” The acronym “IFIP” stands for “International Federation for Information Processing.”

<sup>4</sup> The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284 (2011), amended 35 U.S.C. § 102 and § 103 effective March 16, 2013. Patent Owner bears the burden of establishing the benefit of priority based on an earlier filed application. *See, e.g., In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1376 (Fed. Cir. 2016). The analysis for the benefit of priority proceeds on a claim-by-claim basis. *See Lucent Techs., Inc. v. Gateway, Inc.*, 543 F.3d 710, 718 (Fed. Cir. 2008); *Waldemar Link, GmbH v. Osteonics Corp.*, 32 F.3d 556, 558 (Fed. Cir. 1994). Because the ’474 patent claims priority through several ancestor applications to an

Patent Owner does not dispute that each reference qualifies as prior art. *See, e.g.*, Resp. 8–34.

*G. The Asserted Challenges to Patentability*

Petitioner asserts the following challenges to patentability:

| <b>Claim(s) Challenged</b>                                  | <b>35 U.S.C. §</b> | <b>Reference(s)/Basis</b> |
|-------------------------------------------------------------|--------------------|---------------------------|
| 1–3, 5–7, 9–11,<br>13–15, 17–19, 21–23,<br>25–27, 29–31, 33 | 103                | Law, Golnabi              |
| 2, 10, 18, 26                                               | 103                | Law, Golnabi, Wood        |
| 4, 12, 20, 28                                               | 103                | Law, Golnabi, Ke          |
| 5, 13, 21, 29                                               | 103                | Law, Golnabi, Jungck      |
| 7, 8, 15, 16, 23,<br>24, 31, 32                             | 103                | Law, Golnabi, Johnson     |

Pet. 2–3, 11–73.

*H. Testimonial Evidence*

To support its challenges, Petitioner relies on the Declaration of Doug W. Jacobson, Ph.D. (Exhibit 1003) and the Reply Declaration of Doug W. Jacobson, Ph.D. (Exhibit 1017). Dr. Jacobson states, “I am a University Professor in the Department of Electrical and Computer Engineering at Iowa State University,” “currently hold the Sunil & Sujata Gaitonde Professorship in Cybersecurity,” and “joined the faculty in 1985 after receiving a PhD degree in Computer Engineering from Iowa State University in 1985.”

Ex. 1003 ¶ 5. Dr. Jacobson also states, “I have been retained by counsel for Petitioner” and “have been asked to provide my opinions about the state of

---

application filed on April 16, 2014, this decision refers to the post-AIA versions of § 102 and § 103. *See* Ex. 1001, 1:7–19. But our analysis would not change under the pre-AIA versions of § 102 and § 103.

the art of the technology described” in the ’474 patent and the patentability of claim 1–33 “in view of prior art, obviousness considerations, and the understanding of a person of ordinary skill in the art.” *Id.* ¶ 1.

Petitioner also relies on the declaration of Nathaniel E. Frank-White (Exhibit 1007). Mr. Frank-White states, “I am a Records Request Processor at the Internet Archive” that “provides access to a digital library of Internet sites and other cultural artifacts in digital form.” Ex. 1007 ¶¶ 1–2.

Mr. Frank-White provides a copy of an Internet site for Assurent Secure Technologies having the following address:<sup>5</sup> <https://web.archive.org/web/20070202094127/http://www.assurent.com:80/index.php?id=58>. *Id.* at Ex. A.

To support its positions, Patent Owner relies on the Declaration of Dr. Michael T. Goodrich (Exhibit 2002). Dr. Goodrich states, “I received a Bachelor of Arts degree in Mathematics and Computer Science from Calvin University, in Grand Rapids, Michigan, in 1983, a Master of Science (M.S.) degree in Computer Science from Purdue University, in West Lafayette, Indiana, in 1985, and a Ph.D. in Computer Science from Purdue University in 1987.” Ex. 2002 ¶ 6. Dr. Goodrich also states, “I have been asked to provide my technical opinions relating to arguments raised by [Petitioner] in its Petition,” i.e., whether claims 1–33 in the ’474 patent are “valid over the obviousness challenges brought by [Petitioner].” *Id.* ¶ 3.

Additionally, Petitioner submits Dr. Goodrich’s deposition testimony, and Patent Owner submits Dr. Jacobson’s deposition testimony. *See*

---

<sup>5</sup> Law describes Assurent Secure Technologies as a source for threat data, such as “firewall ruleset data.” Ex. 1005 ¶ 92.

Ex. 1018 (Jan. 16, 2024, Goodrich Dep. Tr.); Ex. 2006 (Oct. 2, 2023, Jacobson Dep. Tr.); Ex. 2007 (Mar. 27, 2024, Jacobson Dep. Tr.).

### *I. Burden*

In an *inter partes* review, a petitioner bears the burden of persuasion to prove “unpatentability by a preponderance of the evidence.” *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015) (quoting 35 U.S.C. § 316(e)); *see* 37 C.F.R. § 42.1(d) (2023).

## III. PATENTABILITY ANALYSIS

### *A. Legal Principles: Obviousness*

A patent may not be obtained “if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains.” 35 U.S.C. § 103. An obviousness analysis involves underlying factual inquiries including (1) the scope and content of the prior art; (2) differences between the claimed invention and the prior art; (3) the level of ordinary skill in the art; and (4) where in evidence, objective indicia of nonobviousness, such as commercial success, long-felt but unsolved needs, and failure of others.<sup>6</sup> *Graham v. John Deere Co.*, 383 U.S. 1, 17–18, 35–36 (1966); *Apple Inc. v. Samsung Elecs. Co.*, 839 F.3d 1034, 1047–48 (Fed. Cir. 2016) (en banc). When evaluating a combination of references, an obviousness analysis should address “whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007).

---

<sup>6</sup> The record does not include evidence or argument regarding objective indicia of nonobviousness.

We analyze the obviousness issues according to these principles.

*B. Level of Ordinary Skill in the Art*

Factors pertinent to determining the level of ordinary skill in the art include (1) the educational level of the inventor; (2) the type of problems encountered in the art; (3) prior-art solutions to those problems; (4) the rapidity with which innovations are made; (5) the sophistication of the technology; and (6) the educational level of workers active in the field. *Envtl. Designs, Ltd. v. Union Oil Co.*, 713 F.2d 693, 696–97 (Fed. Cir. 1983). Not all factors may exist in every case, and one or more of these or other factors may predominate in a particular case. *Id.* These factors are not exhaustive, but merely a guide to determining the level of ordinary skill in the art. *Daiichi Sankyo Co. v. Apotex, Inc.*, 501 F.3d 1254, 1256 (Fed. Cir. 2007). Moreover, the prior art itself may reflect an appropriate skill level. *Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001).

Petitioner asserts that a person of ordinary skill in the art at the '474 patent's effective filing date "would have had a bachelor's degree in computer science, computer engineering, or an equivalent, four years of professional experience, and a working knowledge of packet-switched networking, firewalls, security policies, communication protocols and layers, and the use of customized rules to address cyber-attack." Pet. 8 (quoting *Cisco Sys., Inc. v. Centripetal Networks, Inc.*, IPR2018-01443, Paper 7 at 6 (PTAB Feb. 12, 2019)). Dr. Jacobson's testimony supports Petitioner's assertion. *See* Ex. 1003 ¶ 33.

Patent Owner asserts that a person of ordinary skill in the art at the '474 patent's effective filing date "would have had a bachelor's degree in computer science, computer engineering, or an equivalent, four years of

professional experience, and a working knowledge of packet-switched networking, firewalls, security policies, communication protocols and layers, and the use of customized rules to address cyber-attack.” Resp. 6–7 (citing Ex. 2002 ¶¶ 25–30; Ex. 2004, 6). Dr. Goodrich’s testimony supports Patent Owner’s assertion. *See* Ex. 2002 ¶ 28.

The parties provide the same description of a person of ordinary skill in the art. Pet. 8; Resp. 6–7; *see* Ex. 1003 ¶ 33; Ex. 2002 ¶ 28. We adopt that description because it comports with the technology and claims of the ’474 patent as well as the asserted references. *See, e.g.*, Ex. 1001, 1:50–2:54, 25:31–30:51; Ex. 1003 ¶ 33; Ex. 2002 ¶ 28.

### *C. Claim Construction*

We construe claim terms “using the same claim construction standard” that district courts use to construe claim terms in civil actions under 35 U.S.C. § 282(b). *See* 37 C.F.R. § 42.100(b). Under that standard, claim terms “are given their ordinary and customary meaning, which is the meaning the term would have to a person of ordinary skill in the art at the time of the invention.” *Power Integrations, Inc. v. Fairchild Semiconductor Int’l, Inc.*, 904 F.3d 965, 971 (Fed. Cir. 2018) (citing *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (en banc)). The meaning of claim terms may be determined by “look[ing] principally to the intrinsic evidence of record, examining the claim language itself, the written description, and the prosecution history, if in evidence.” *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 469 F.3d 1005, 1014 (Fed. Cir. 2006) (citing *Phillips*, 415 F.3d at 1312–17).

Petitioner notes that the Board has construed the following claim terms in various proceedings involving patents related to the ’474 patent:

- (1) packet security gateway;
- (2) packet transformation function;
- (3) rule(s);
- (4) dynamic security policy; and
- (5) security policy management server.

Pet. 8–10. To “the extent necessary to resolve any controversy,” Petitioner “requests that the Board adopt those same constructions here.” *Id.* at 8.

Patent Owner contends that the disputes in this proceeding do not “turn on” the constructions of the above-identified claim terms. Resp. 8. Nevertheless, Patent Owner “applies the Board’s previously adopted constructions” for “the purpose of this proceeding.” *Id.*

“[O]nly those terms need be construed that are in controversy, and only to the extent necessary to resolve the controversy.” *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999); *see Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017). We determine that no claim term requires an explicit construction to decide whether Petitioner satisfies the “preponderance of the evidence” standard for proving unpatentability.

*D. Alleged Obviousness over Law and Golnabi:*  
*Claims 1–3, 5–7, 9–11, 13–15, 17–19, 21–23, 25–27, 29–31, and 33*

Petitioner contends that claims 1–3, 5–7, 9–11, 13–15, 17–19, 21–23, 25–27, 29–31, and 33 are unpatentable under § 103 as obvious over Law and Golnabi. *See, e.g.*, Pet. 2–3, 11–58; Reply 2–22. Patent Owner disputes Petitioner’s contentions. *See, e.g.*, Resp. 1–2, 11–34; Sur-reply 1–21.

Below, we provide overviews of Law and Golnabi. Then, we consider the obviousness issues. For the reasons explained below, we agree

with Petitioner that claims 1–3, 5, 7, 9–11, 13, 15, 17–19, 21, 23, 25–27, 29, and 31 are unpatentable under § 103 as obvious over Law and Golnabi but disagree that claims 6, 14, 22, 30, and 33 are unpatentable based on these references.

### 1. OVERVIEW OF LAW (EXHIBIT 1005)

Law is a U.S. patent application publication titled “Integrated Unified Threat Management for a Process Control System,” filed on September 23, 2010, and published on March 24, 2011. Ex. 1005, codes (12), (22), (43), (54). Law states that the “application relates generally to process plant control systems,” such as “distributed or scalable process control systems like those used in power generation, chemical, petroleum, or other processes.” *Id.* ¶¶ 2–3. As more specific examples of process control systems, Law identifies “military and government applications,” “nuclear power plants,” “municipal services,” “public communications systems,” “high-energy processes,” and “dangerous or hazardous processes.” *Id.* ¶¶ 15, 93, 102.

Law explains that “firewalls typically provide security for process control networks and mitigate the risk of network attacks.” Ex. 1005 ¶ 11. But “firewalls require detailed configuration of their rulesets.” *Id.* ¶ 12. “As the process control system and various sub-systems evolve, the firewall rulesets must also change to meet any additional security requirements of new devices, software updates, and any other network changes.” *Id.* ¶ 13.

Law describes difficulties in achieving suitable network security at process control systems. *See* Ex. 1005 ¶¶ 14–21. For example, when “network devices are not integrated into the process control system,” system operators lack access to firewall information. *Id.* ¶ 14. So firewall tasks

“such as configuration, ruleset patching, and regular maintenance are left to IT personnel” at process control systems. *Id.*

Law explains that to accomplish those firewall tasks, IT personnel at process control systems should have “detailed knowledge of the network architecture” and should “understand the network topography, network business needs related to the network, permitted devices and services that the business requires within and between local networks, and the various external entities that should be permitted to access the local networks.” Ex. 1005 ¶ 16; *see id.* ¶¶ 17–19. But IT personnel at process control systems “are not typically trained to understand the process control system and its upgrades” and “may not understand how or why the rulesets must also be changed.” *Id.* ¶ 16. “In other circumstances, IT personnel have limited or no detailed understanding of the control system details and how the control system is to properly function to meet control objectives.” *Id.* ¶ 20. “As such, IT personnel may be at a significant disadvantage regarding proper access controls, permission settings, and/or proper firewall rules configuration for the system.” *Id.*

Law also explains that some “commercial off-the-shelf (COTS) firewall systems” for process control systems may “provide a partial solution to network security, but still must be managed outside of the operator environment” by “IT personnel specifically trained to integrate the firewall into the needs of the process control system and configure the various rulesets.” Ex. 1005 ¶ 16. With those conventional firewall systems, “IT personnel are still required to update the ruleset when new threats are discovered or upgrades to software components of the system are implemented.” *Id.*

Law endeavors to (1) overcome the need for specifically trained IT personnel at process control systems to create or update firewall rulesets and (2) enhance “security and management” by providing an operator environment implementing a “Unified Threat Management System (UTMS).” Ex. 1005 ¶ 22; *see id.* at code (57). The UTMS includes “a UTMS-configured firewall, UTMS-configured network access device, and UTMS-configured field devices that are capable of defending against both known and ‘zero day’ vulnerabilities and threats to control systems for both embedded, proprietary devices, and standard, commonly-used devices.” *Id.* ¶ 22.

With the UTMS, system operators may monitor and configure equipment, including firewalls, “from a graphic display of an operator workstation, without IT personnel intervention.” Ex. 1005 ¶ 59; *see id.* ¶ 87. Thus, system operators (not IT personnel) may protect a process control system from “internal and external network threats such as viruses, worms, or any other attack that may induce a fault in one or more network devices, field devices, or other portions of the process control system.” *Id.* ¶ 59; *see id.* ¶ 22.

With the UTMS, operator displays permit system operators (not IT personnel) to:

- (1) “display the current state of the connection”;
- (2) “update the settings, rulesets, and other parameters or variables of the UTMS (and its firewalls, network access devices, and field devices if so configured)”; and
- (3) “perform any other process control system security tasks from the operator display or other workstation.”

Ex. 1005 ¶ 23; *see id.* ¶¶ 26, 60–61, 90–91, 102. Hence, system operators “may easily configure each UTMS-configured device while reducing the risk of mis-configuration and reduced security.” *Id.* ¶ 81; *see id.* ¶ 105.

UTMS-configured devices in the process control system may “communicate with a perpetual service that proactively supplies the UTMS-configured firewalls, network access devices, and configured controllers or field devices with rulesets to meet the latest security threats, threat patterns, and control system vulnerabilities found to exist within the network.”

Ex. 1005 ¶ 22, code (57). These “updates are managed from within the standard control user interface of the plant” by a system operator as if the UTMS-configured devices “were no different than any other control system element or entity.” *Id.* ¶ 22.

The firewall rulesets may “be created based upon continuous or periodic evaluation of the process control system itself to provide immediate system protection from identified threats.” Ex. 1005 ¶ 23. Moreover, the firewall rulesets may come from “a source that is external to the process control system.” *Id.* ¶ 26; *see id.* ¶ 66, code (57).

Each firewall ruleset may “define conditions that, if detected, implement some combination of blocking suspected malicious communications or alerting an operator or other plant personnel through an alarm.” Ex. 1005 ¶ 91; *see id.* ¶¶ 24–25. UTMS-configured devices in the process control system may “use one or more rulesets to inspect and drop malicious packets from the network before the malicious packets can reach their intended destination” and “cause a fault.” *Id.* ¶ 52.

Law's Figure 3 (reproduced below) depicts “a logical block diagram of a method to update rulesets of the UTMS” (Ex. 1005 ¶ 30):

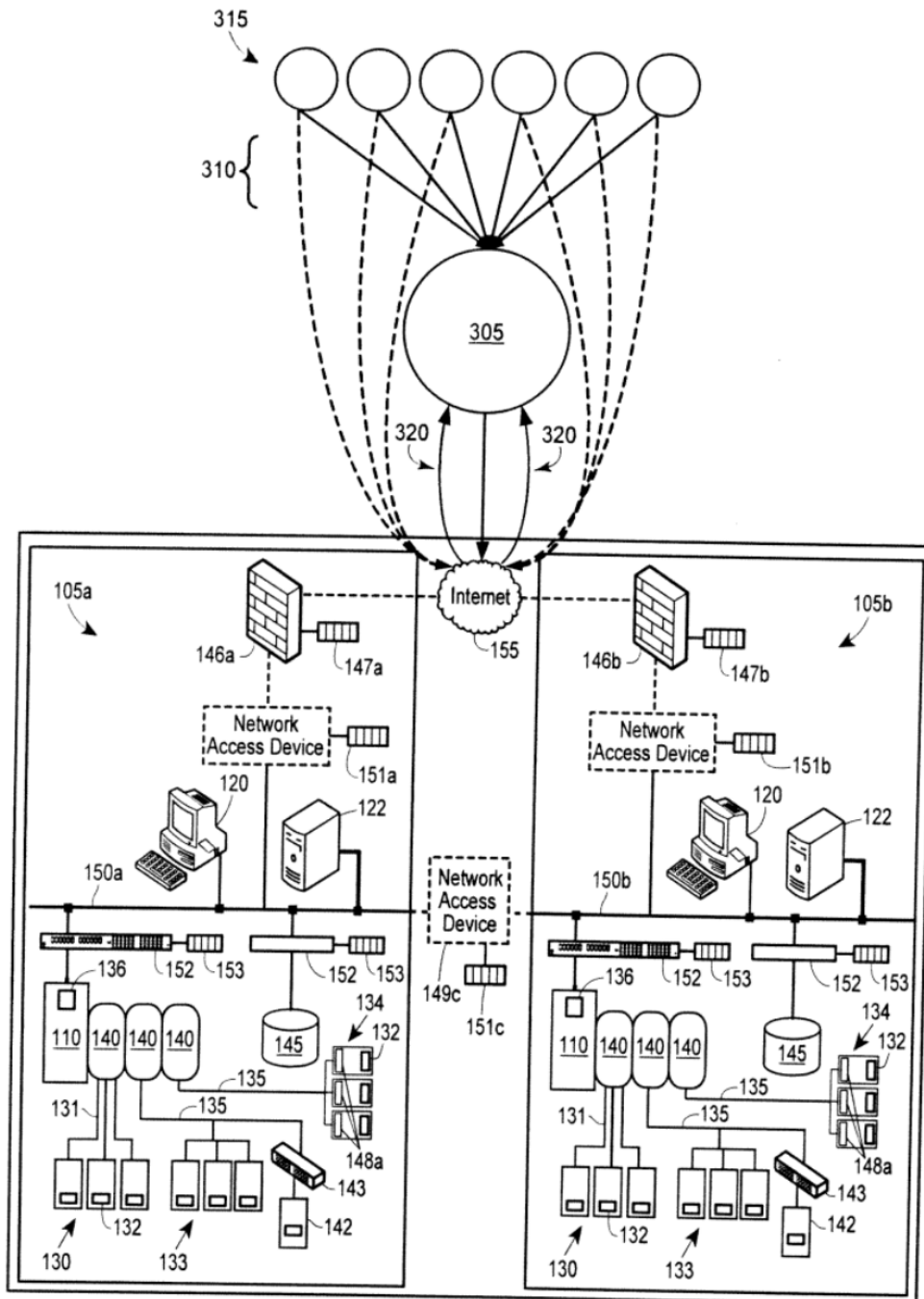


**Fig. 3**

Figure 3 illustrates a process control system including process control sub-systems 105a and 105b “within one or more process plants” communicating

via the Internet 155. Ex. 1005 ¶¶ 51, 53, Fig. 3. The process control system includes perimeter firewalls 146a and 146b protecting communication networks 150a and 150b, respectively. *Id.* ¶ 51, Fig. 3; *see id.* ¶ 92.

The process control system also includes:

- (1) process controllers 110 “communicatively connected” to operator workstations 120;
- (2) field devices 134 “configured to perform many network security functions without direct intervention by system operators or other personnel,” i.e., field devices such as “sensors, valves, transmitters, positioners, etc.”;
- (3) network access devices 149 “positioned downstream” of the firewalls to “supplement the perimeter UTMS functions” of the firewalls or “perform specialized UTMS functions”; and
- (4) network devices 152 to protect particular “areas or subsystems.”

Ex. 1005 ¶¶ 51, 53, 55, 59, 81, Fig. 3. “Each firewall 146 or device 134, 149, 152 may include a ruleset, for example, rulesets 147a, 148a, 147b, 148b, 151a, 151b, 153 defining the communication that may be received or processed by the UTMS-configured device.” *Id.* ¶ 51, Fig. 3. Further, rulesets 147a and 147b for firewalls 146a and 146b, respectively, may “include a global set of rules for access to any device within” communication networks 150a and 150b, respectively. *Id.* ¶ 51.

Law explains that firewalls 146a and 146b “require updates to remain effective against network threats.” Ex. 1005 ¶ 88. Firewalls 146a and 146b may “receive the ruleset data . . . and other update data on a periodic or non-periodic basis via any desired communication link to the device or to a third party source,” such as “cyber security risk management firm 305 as described in relation to” Figure 3. *Id.* ¶ 66; *see id.* ¶¶ 26, 88, 92.

Referencing Figure 3, Law discloses that cyber security risk management firm 305 may “collect threat data 310 from a plurality of various sources 315 to construct the various rulesets 147, 148, 151, 153, validate the rulesets, verify, and distribute the rulesets” to firewalls 146a and 146b and other UTMS-configured devices. Ex. 1005 ¶ 88. Law also discloses that “[r]uleset collecting, constructing, validating, and distributing may be performed using any type of information technology methods suitable for performing such actions using electronic data.” *Id.* To collect threat data 310, Law identifies “various data collection techniques (e.g., robots, crawling, data feeds, collaborative forums, etc.).” *Id.*

Law explains that cyber security risk management firm 305 may:

- (1) “continuously identify network vulnerabilities in any device, sub-system, or software program”;
- (2) create “rules for the various rulesets,” including rules for firewall rulesets, based on an analysis of vulnerabilities; and
- (3) “provide an ongoing remediation update service to the system” including “device updates.”

Ex. 1005 ¶ 89. For example, a “perpetual service” may “proactively” supply firewall rulesets responsive to newly discovered security threats and vulnerabilities. *Id.* ¶ 22, code (57).

Law discloses that sources 315 may “create the threat data 310 by monitoring, defining, and analyzing potential and known threats to the security of” communication networks 150a and 150b. Ex. 1005 ¶ 92. Further, “to name but a few of the sources for firewall ruleset data,” Law identifies sources 315 as including Assurent Secure Technologies, Secunia, and Carnegie Mellon University. *Id.*

Law discloses that firewalls 146a and 146b may “collect and aggregate threat data 310 directly from the firm 305 or plurality of sources 315 to construct, validate, and verify the various rulesets.” Ex. 1005 ¶ 92. Law’s Figure 3 depicts “dotted communication lines to deliver” threat data 310 from sources 315 directly to firewalls 146a and 146b without going through firm 305. *Id.* ¶ 92, Fig. 3.

Law’s Figure 13 (reproduced below) depicts “a ruleset user interface to configure rules for managing network traffic for the process control system” (Ex. 1005 ¶ 40):

1300

|        | 1324                                | 1302     | 1304       | 1305          | 1329                | 1306  | 1308     | 1310                 | 1312 | 1314 |
|--------|-------------------------------------|----------|------------|---------------|---------------------|-------|----------|----------------------|------|------|
|        |                                     | PROTOCOL | FROM       | THRESH.       | T0                  | PORT  | ACTION   | DESCRIPTION          |      | LOG  |
| 1326 → | <input checked="" type="checkbox"/> | UDP ↓    | 10.4.0.0   | n/a           | 232.108.1<br>16.118 | 18515 | Accept ↓ | New Multicast        |      | NO ↓ |
| 1328 → | <input type="checkbox"/>            | UDP ↓    | 10.8.0.0   | n/a           | 0-7                 | 18516 | Accept ↓ | New Multicast        |      | NO ↓ |
|        | <input type="checkbox"/>            | UDP ↓    | 10.8.0.0   | n/a           | n/a                 | 18517 | Accept ↓ | PT_COM_<br>RDS_IP    |      | NO ↓ |
|        | <input type="checkbox"/>            | UDP ↓    | 10.8.0.0   | n/a           | n/a                 | 18518 | Accept ↓ | PT_COM_<br>RDS_IP    |      | NO ↓ |
| 1330 → | <input checked="" type="checkbox"/> | TCP ↓    | A          | < x MB/<br>hr | B                   | 18519 | Accept ↓ | PT_COM_<br>RTRP      |      | NO ↓ |
| 1332 → | <input checked="" type="checkbox"/> | TCP ↓    | B          | n/a           | A                   | 18519 | Accept ↓ | PT_COM_<br>RTRP      |      | NO ↓ |
|        | <input type="checkbox"/>            | UDP ↓    | 10.81.14.9 | 0-2           | n/a                 | 18520 | Accept ↓ | NTP                  |      | NO ↓ |
|        | <input type="checkbox"/>            | ICMP ↓   | ...        | ...           | ...                 | 18521 | Accept ↓ | Remote Login         |      | NO ↓ |
|        | <input type="checkbox"/>            | ICMP ↓   | ...        | ...           | ...                 | 18522 | Accept ↓ | Ping Pri-Act         |      | NO ↓ |
|        | <input type="checkbox"/>            | ICMP ↓   | ...        | ...           | ...                 | 18523 | Accept ↓ | Allow SNMP<br>Access |      | NO ↓ |

|      |                      |      |      |
|------|----------------------|------|------|
| 1316 | DeltaV Profile #14 ↓ | LOAD | 1318 |
| 1320 |                      | SAVE | 1322 |

**Fig. 13**

Figure 13 illustrates a ruleset user interface including rule table 1300 containing “a protocol type column 1302, a from-address column 1304, a threshold parameter column 1305, a to-address column 1306, a port number

column 1308, an action column 1310, a description column 1312, and a log column 1314.” Ex. 1005 ¶ 102, Fig. 13. Each row of rule table 1300 “enforces a rule if a corresponding row selector is active, as shown by an example row selection column 1324.” *Id.* ¶ 103.

The ruleset user interface permits a system operator to:

- (1) select an already existing ruleset from among profiles “generated by a manufacturer of process control equipment” to “reflect firewall settings that are typically common to users”;
- (2) access an already existing ruleset created by cyber security risk management firm 305; and
- (3) “configure and control any of the rules within the rulesets 147, 148, 151, 152 and the network security in the process control system.”

Ex. 1005 ¶¶ 66, 88, 90, 102, Fig. 13.

## 2. OVERVIEW OF GOLNABI (EXHIBIT 1009)

Golnabi is a paper titled “Analysis of Firewall Policy Rules Using Data Mining Techniques” by Korosh Golnabi et al., published in the IEEE/IFIP Network Operations and Management Symposium NOMS 2006 (April 2006). Ex. 1009, 305;<sup>7</sup> *see* Ex. 1013, 1–2. Golnabi explains that a “firewall is the *de facto* core technology of today’s network security and first line of defense against external network attacks and threats.” Ex. 1009, 305. According to Golnabi, however, “the management of firewall rules has been proven to be complex, error-prone, costly and inefficient,” and “firewall

---

<sup>7</sup> For Exhibit 1009 (Golnabi), we follow Petitioner’s practice and cite to the page numbers that appear in the publication rather than the page numbers that Petitioner applied to the exhibit.

security may be limited or compromised by a poor management of firewall policy rules.” *Id.*

To address those deficiencies, Golnabi teaches techniques for analyzing and modifying firewall policy rules to “optimize the firewall policy and efficiency.” Ex. 1009, 305–14. Among other things, Golnabi’s techniques enable network administrators to “optimize and validate firewall rules automatically.” *Id.* at 305.

Golnabi’s techniques include the following:

- (1) a data-mining technique based on an algorithm called “Mining firewall Log using Frequency (MLF)” that “deduce[s] efficient firewall policy rules” by mining a network traffic log;
- (2) an aggregation technique based on an algorithm called “Filtering-Rule Generalization (FRG)” that “reduce[s] the number of policy rules” and “generate[s] a minimum number of firewall policy rules for efficiency”;
- (3) an anomaly-detection technique based on an algorithm called “Anomaly Discovery Algorithm” that detects (i) a shadowing anomaly, (ii) a correlation anomaly, (iii) a generalization anomaly, (iv) a redundancy anomaly, and (v) certain “non-systematic mis-configuration anomalies”; and
- (4) a technique for identifying (i) dominant rules covering “a significant portion of the network traffic” and (ii) decaying or useless rules and then updating “the rule ordering in [the] firewall in order to optimize the filtering matching at real-time.”

*Id.* at 305–14.

In particular, the data-mining technique uses an “initial set of firewall policy rules” specified by a network administrator based on an organization’s security policy where each rule “specifies to accept or drop

(deny) a packet of certain attributes.” Ex. 1009, 307; *see id.* at 312 (Fig. 10 showing example firewall policy rules). Each rule “could consist of up to seven attributes” in the following format: “<direction> <protocol> <source IP> <source port> <destination IP> <destination port> <action>.” *Id.* at 307, 312; *see id.* at 307–08.

With the “initial set of firewall policy rules,” a firewall log file containing “firewall log raw data” is generated. Ex. 1009, 307; *see id.* at 311–12 (“First Step (1)”). As an example, Golnabi describes a firewall log file containing 33,172 records “obtained from a LINUX operating system firewall” based on the “initial set of firewall policy rules.” *Id.* at 311–12; *see id.* at 313.

After the firewall log file is generated, the “MLF algorithm reads each line of [the] firewall log file, extracts the attributes for each log record, counts its occurrence and outputs the count for each unique combination of these attribute-values.” Ex. 1009, 307; *see id.* at 308 (Fig. 4 showing the MLF algorithm with “Input: Firewall Log file” and “Output: Unique Rules and their Frequency”), 312 (“Second step (2)”). Thus, “each log record of a packet in [the] firewall log file” is processed to generate “a primitive rule,” i.e., “a specific firewall policy rule where all of its attributes are instantiated or specified with its value being observed in [the] firewall log file.” *Id.* at 307–08. Further, the “frequency of each rule discovered is kept . . . and used for its probability and statistical processing.” *Id.* at 307.

Next, using the primitive rules determined from the firewall log file by the MLF algorithm, the FRG algorithm “generates a decision tree where each level or branching represents one of the attributes of a primitive rule from [the] log record of a packet which is an instance of a rule to be

processed.” Ex. 1009, 308; *see id.* at 308–09 (Fig. 5 showing the FRG algorithm with “Input: Rules” and “Output: The Tree”), 310 (Fig. 6 showing an example decision tree), 312 (“Third step (3)”). “Each of the rules extracted from [the] firewall log file is then examined to be branched and analyzed, and then to be grouped to be aggregated by combining the common fields to get the superset rules that match with a group of unique rules.” *Id.* at 308. Specifically, “every path on the generated tree would print a generalized rule that supersedes all the existing rules in the input.” *Id.* at 310.

As an example, if multiple input rules have “matching fields with an exception of source port field,” the “rules are then aggregated” by “combining all the source ports as a range of these source ports to get one generalized rule.” Ex. 1009, 308. As another example, “the IP addresses of 129.110.10.7 and 129.110.10.1 can be aggregated to 129.110.10.\*” where the \* character represents a specified range. *Id.* at 308–09. As yet another example, “the filtering rule of a multi-valued field” may be split “into several rules where each rule will have a single-valued field.” *Id.* at 312.

After employing the MLF algorithm, the FRG algorithm, and the Anomaly Discovery Algorithm, the “final result is new policy rules ordered, generalized and anomaly-free to guarantee the correctness and efficiency of policy rule configuration and filtering process.” Ex. 1009, 313.

Further, Golnabi explains that by “reordering or prioritizing” certain frequently used rules, “one may expect a tremendous performance gain as a result.” Ex. 1009, 314.

### 3. INDEPENDENT CLAIM 1

(a) Preamble 1.0

Claim 1 recites “[a] method of filtering packets at a packet security gateway configured for protection of a network, wherein the packet security gateway is capable of receiving a plurality of dynamic security policies and is associated with a security policy management server external from the network.” Ex. 1001, 25:31–35.

Petitioner contends that Law teaches claim 1’s preamble for three related reasons. *See* Pet. 19–28. First, Petitioner asserts that Law teaches a “packet security gateway” because Law discloses enhancing network security by providing “a Unified Threat Management System (UTMS) including a UTMS-configured firewall,” such as “stand-alone network devices located at the perimeter of the . . . network.” *Id.* at 19–20 (alteration by Petitioner) (quoting Ex. 1005 ¶ 22). As examples of UTMS-configured perimeter firewalls, Petitioner identifies firewalls 146a and 146b in Law’s Figure 1A that separate communication networks 150a and 150b, respectively, from the Internet 155. *Id.* at 20–21 (citing Ex. 1005 ¶¶ 51, 54, Fig. 1A). Petitioner also asserts that firewalls 146a and 146b perform packet filtering and may “use one or more rulesets to inspect and drop malicious packets from the network before the malicious packets can reach their intended destination.” *Id.* at 21 (quoting Ex. 1005 ¶ 52). Petitioner further asserts that a firewall ruleset may “define conditions that, if detected, implement some combination of blocking suspected malicious communications or alerting an operator.” *Id.* at 21–22 (quoting Ex. 1005 ¶ 91).

Second, Petitioner asserts that firewalls 146a and 146b are “capable of receiving a plurality of dynamic security policies” because a firewall ruleset:

- (1) “may be a data file that includes known signature, policy, or other rules describing characteristics of network-based threats”;
- (2) “specifies criteria corresponding to one or more packets,” such as the “PROTOCOL,” “FROM,” “TO,” and “PORT” fields;
- (3) “identifies a packet transformation function to be performed on packets corresponding to the specified criteria (actions including accept, block, notify, reroute, and logging)”;
- (4) may be updated to address “known vulnerabilities,” e.g., vulnerabilities that a third party may provide through “an ongoing remediation update service to the system” including “device updates.”

Pet. 27–28 (emphasis omitted) (quoting Ex. 1005 ¶¶ 89–90) (citing Ex. 1003 ¶¶ 66–67; Ex. 1005 ¶¶ 92, 102–103, Fig. 13). Further, Petitioner quotes the following disclosure in Law’s paragraph 83 about certain network conditions triggering automatic or manual action: “Detection of certain network conditions may also trigger an automatic update of the rulesets 147, 148, 151, 153 or an alarm to prompt a user to perform a manual update of the rulesets or another action to fully secure the system 100.” *Id.* at 28 (quoting Ex. 1005 ¶ 83).

Third, Petitioner asserts that firewalls 146a and 146b are “associated with a security policy management server external from the network” because firewalls 146a and 146b may “receive rulesets from cyber security risk management firm 305.” Pet. 23. According to Petitioner, the firewall

rulesets “meet the latest security threats, threat patterns, and control system vulnerabilities found to exist within the network.” *Id.* (quoting Ex. 1005 ¶ 22).

Additionally, Petitioner contends that Law discloses that a “third party, cyber security risk management firm 305 such as Wurldtech Security, Inc. of Vancouver, BC Canada, or other entity, may collect threat data 310 from a plurality of various sources 315 to construct the various rulesets 147, 148, 151, 153, validate the rulesets, verify, and distribute the rulesets” to firewalls 146a and 146b. Pet. 24 (emphases omitted) (quoting Ex. 1005 ¶ 88); *see* Reply 4. According to Petitioner, Law’s Figure 3 “confirms that cyber security risk management firm 305 is external from” communication networks 150a and 150b protected by firewalls 146a and 146b. Pet. 24–25 (citing Ex. 1003 ¶ 63; Ex. 1005 ¶ 26, Fig. 3).

Patent Owner makes no arguments specific to claim 1’s preamble. *See, e.g.*, Resp. 1–2, 11–34; Sur-reply 1–22.

Generally, a preamble does not limit a claim. *Allen Eng’g Corp. v. Bartell Indus., Inc.*, 299 F.3d 1336, 1346 (Fed. Cir. 2002). We need not decide whether claim 1’s preamble limits the claim because, for the reasons stated by Petitioner and supported by Dr. Jacobson’s testimony, we agree with Petitioner that Law teaches claim 1’s preamble. *See* Pet. 19–28; Ex. 1003 ¶¶ 58–68.

(b) Limitation 1.1

Claim 1 recites “receiving, by the packet security gateway and from the security policy management server, a dynamic security policy comprising packet filtering rules.” Ex. 1001, 25:37–39 (limitation 1.1).

Petitioner contends that Law teaches limitation 1.1 because Law discloses that firewalls 146a and 146b may “receive the ruleset data . . . and other update data on a periodic or non-periodic basis via any desired communication link to the device or to a third party source,” such as “cyber security risk management firm 305 as described in relation to” Figure 3. Pet. 28–29 (alteration by Petitioner) (emphases omitted) (quoting Ex. 1005 ¶ 66). Further, Petitioner asserts that the “received rulesets comprise packet filtering rules.” *Id.* at 29 (citing Ex. 1005 ¶¶ 102–103).

Patent Owner makes no arguments specific to limitation 1.1. *See, e.g.,* Resp. 1–2, 11–34; Sur-reply 1–22.

For the reasons stated by Petitioner and supported by Dr. Jacobson’s testimony, we agree with Petitioner that Law teaches limitation 1.1. *See* Pet. 28–29; Ex. 1003 ¶ 69.

(c) Limitation 1.2

Claim 1 recites “wherein one or both of the dynamic security policy or one or more of the packet filtering rules of the dynamic security policy were automatically created or altered, by the security policy management server, based on malicious traffic information received from a plurality of malicious host tracker services.” Ex. 1001, 25:39–45 (limitation 1.2).

(i) Petitioner’s Contentions

Petitioner contends that Law teaches or renders obvious limitation 1.2 for several related reasons. *See* Pet. 23–26, 29–36; Reply 2–8.

a. Security Policy Management Server

Initially, Petitioner asserts that Law’s cyber security risk management firm 305 corresponds to the “security policy management server” required by claim 1. *See* Pet. 23–26, 29–32; Reply 3–4. According to Petitioner,

Law identifies firm 305 as a “third party source” that supplies “ruleset data . . . and other update data on a periodic or non-periodic basis via any desired communication link” to firewalls 146a and 146b. Pet. 23–24 (alteration by Petitioner) (emphases omitted) (quoting Ex. 1005 ¶ 66); *see id.* at 25–26 (citing Ex. 1005 ¶¶ 66, 88). As support, Petitioner quotes the following disclosure in Law’s paragraph 22 about ruleset delivery: “The UTMS firewalls and devices may communicate with a perpetual service that proactively supplies the UTMS-configured firewalls . . . with rulesets to meet the latest security threats, threat patterns, and control system vulnerabilities found to exist within the network.” *Id.* at 23 (alteration by Petitioner) (emphasis omitted) (quoting Ex. 1005 ¶ 22).

As additional support, Petitioner quotes the following disclosure in Law’s paragraph 88 about a “third party source” that supplies rulesets:

With reference to FIG. 3, a third party, cyber security risk management firm 305 such as Wurldtech Security, Inc. of Vancouver, BC Canada, or other entity, may collect threat data 310 from a plurality of various sources 315 to construct the various rulesets 147, 148, 151, 153, validate the rulesets, verify, and distribute the rulesets to the UTMS-configured firewalls 146a, 146b . . . .

Pet. 24 (emphases omitted) (quoting Ex. 1005 ¶ 88).

Further, Petitioner asserts that an ordinarily skilled artisan “would have understood that cyber security risk management firm 305 necessarily comprises a server” because firm 305 distributes rulesets to “firewalls 146a and 146b over the Internet 155.” Pet. 25–26 (citing Ex. 1003 ¶ 63; Ex. 1005 ¶¶ 66, 88).

b. Packet Filtering Rules Automatically Created

Regarding “packet filtering rules of the dynamic security policy” that were “automatically created” by the “security policy management server,” Petitioner asserts that Law discloses that:

- (1) cyber security risk management firm 305 may “collect threat data 310 from a plurality of various sources 315 to construct the various rulesets 147, 148, 151, 153, validate the rulesets, verify, and distribute the rulesets” to firewalls 146a and 146b;
- (2) “[r]uleset collecting, constructing, validating, and distributing may be performed using any type of information technology methods suitable for performing such actions using electronic data”; and
- (3) “collecting the threat data 310 from the World Wide Web” may include “using various data collection techniques (e.g., robots, crawling, data feeds, collaborative forums, etc.).”

Pet. 29–30 (alteration by Petitioner) (emphases omitted) (quoting Ex. 1005 ¶ 88); *see* Reply 4–5.

Petitioner asserts that an ordinarily skilled artisan “would have understood that ruleset constructing using ‘any type of information technology methods suitable for’ ruleset constructing would have included methods of automatically constructing rules.” Pet. 30 (quoting Ex. 1005 ¶ 88) (citing Ex. 1003 ¶ 70); *see* Reply 4–5. As evidence of “known techniques for automatically generating rules,” Petitioner identifies Law’s disclosure that prior-art techniques for creating firewall rulesets include “automatically locating devices and generating rules by passively analyzing traffic on the network.” Pet. 30 (emphases omitted) (quoting Ex. 1005 ¶ 21); *see* Reply 6. Petitioner also asserts that it would have been obvious to an

ordinarily skilled artisan to incorporate such “known techniques for automatically generating rules” for “at least some of the rules in ruleset 147 created by cyber security risk management firm 305.” Pet. 30 (citing Ex. 1003 ¶ 71).

c. Packet Filtering Rules Automatically Altered

Regarding “packet filtering rules of the dynamic security policy” that were “automatically . . . altered” by the “security policy management server,” Petitioner asserts that cyber security risk management firm 305 automatically updates rules in firewall rulesets. Pet. 31; *see* Reply 8. To support that assertion, Petitioner quotes the following disclosure in Law’s paragraph 83 about certain network conditions triggering automatic or manual action: “Detection of certain network conditions may also trigger an automatic update of the rulesets 147, 148, 151, 153 or an alarm to prompt a user to perform a manual update of the rulesets or another action to fully secure the system 100.” Pet. 31 (emphasis omitted) (quoting Ex. 1005 ¶ 83); *see* Reply 8. Petitioner also quotes the disclosure in Law’s paragraph 88 that firewalls 146a and 146b “require updates to remain effective against network threats.” Pet. 31 (emphasis omitted) (quoting Ex. 1005 ¶ 88).

d. Packet Filtering Rules Based on Malicious Traffic Information

Regarding “packet filtering rules of the dynamic security policy” that were “based on malicious traffic information received from a plurality of malicious host tracker services,” Petitioner asserts that Law discloses that a “third party, cyber security risk management firm 305 such as Wurldtech Security, Inc. of Vancouver, BC Canada, or other entity, may collect threat data 310 from a plurality of various sources 315 to construct the various

rulesets 147, 148, 151, 153, validate the rulesets, verify, and distribute the rulesets” to firewalls 146a and 146b. Pet. 32 (emphases omitted) (quoting Ex. 1005 ¶ 88). Petitioner asserts that Law also discloses that sources 315 may “create the threat data 310 by monitoring, defining, and analyzing potential and known threats to the security of” communication networks 150a and 150b. *Id.* at 34 (quoting Ex. 1005 ¶ 92). Petitioner further asserts that Law discloses various sources for “firewall ruleset data” including the following:

- (1) Assurent Secure Technologies that provides a Vulnerability Research Service (VRS);
- (2) Secunia;
- (3) Achilles; and
- (4) the Computer Emergency Response Team (CERT) of Carnegie Mellon University.

*Id.* (citing Ex. 1005 ¶ 92).

(ii) Patent Owner’s Contentions

Patent Owner disputes that Law teaches or renders obvious limitation 1.2 because Patent Owner disagrees that Law discloses or suggests “packet filtering rules of the dynamic security policy” that were “automatically created or altered” by the “security policy management server.” *See* Resp. 1, 11–19; Sur-reply 1, 3–8.

a. Security Policy Management Server

Patent Owner asserts that Law’s cyber security risk management firm 305 is “not a server” but instead “a commercial entity” with “IT personnel” and “IT infrastructure” for “updating rulesets by ‘collecting the threat data,’ ‘constructing data files,’ and ‘executing [] computer implemented algorithm[s] to determine if the rulesets effectively secure the

process control system.” Sur-reply 3–4 (alterations by Patent Owner) (emphasis omitted) (quoting Ex. 1005 ¶ 88) (citing Ex. 2006, 37:2–38:7); *see id.* at 1; Resp. 12–13 (citing Ex. 2006, 35:11–23, 37:2–38:10).

According to Patent Owner, Petitioner “does not identify with any particularity a server within the commercial entity that performs the claimed automatically generating and distributing dynamic security policy functionality.” Sur-reply 1; *see id.* at 4.

b. Packet Filtering Rules Automatically Created

Regarding “packet filtering rules of the dynamic security policy” that were “automatically created” by the “security policy management server,” Patent Owner asserts that Law’s cyber security risk management firm 305 is “a company that includes IT personnel and other infrastructure components.” Resp. 12; *see id.* at 1, 9–10, 12–13; Sur-reply 1, 3–4. Patent Owner asserts that firm 305’s IT personnel are “required to update the ruleset when new threats are discovered or upgrades to software components of the system are implemented.” Resp. 1, 9, 12–13, 18–19 (quoting Ex. 1005 ¶ 16); *see* Sur-reply 1, 5–8.

Patent Owner asserts that firm 305’s IT personnel must update rulesets because the IT personnel:

- (1) have “detailed knowledge” about (i) “the network architecture” and (ii) “the process control system”; and
- (2) “understand how and why the rulesets must be modified to protect the system.”

Resp. 9, 13 (quoting Ex. 1005 ¶ 16) (citing Ex. 2002 ¶ 50); *see* Sur-reply 6 (citing Ex. 2006, 38:1–10). According to Patent Owner, “IT personnel must be involved in managing access to the process control network.” Sur-reply 6–7.

Further, Patent Owner asserts that “Law’s paragraph 16 expressly discloses that ‘specifically trained’ IT personnel are required to manage updates outside the operator environment when new threats are detected.” Resp. 13 (quoting Ex. 1005 ¶ 16) (citing Ex. 1005 ¶¶ 21–22, 88–89; Ex. 2002 ¶ 49); *see id.* at 1; Sur-reply 1, 5, 7–8 (citing Ex. 1005 ¶¶ 16, 88). Also, based on Law’s paragraph 16, Patent Owner asserts that Law teaches away from automatic generation techniques in cyber security risk management firm 305. Resp. 15–16.

Additionally, Patent Owner cites Law’s paragraph 88 as disclosing a “concrete example” where “the IT personnel would construct the updated rulesets and run tests (for example, executing computer-implemented algorithms) to ensure that the ‘rulesets effectively secure the process control systems in a desirable manner.’” Resp. 13–14 (quoting Ex. 1005 ¶ 88); *see* Sur-reply 5 (quoting Ex. 1005 ¶ 88).

c. Packet Filtering Rules Automatically Altered

Regarding “packet filtering rules of the dynamic security policy” that were “automatically . . . altered” by the “security policy management server,” Patent Owner asserts that Petitioner mischaracterizes Law’s paragraph 83 as disclosing that cyber security risk management firm 305 automatically updates rules in firewall rulesets. Resp. 14 (citing Pet. 31); *see* Sur-reply 6. Patent Owner asserts that “Petitioner misses Law’s innovative feature: UTMS-configured elements of graphical displays that allow operators to configure and manage rulesets within the process control system.” Resp. 14 (emphasis omitted) (citing Ex. 1005 ¶ 83; Ex. 2006, 54:17–19, 55:10–56:6).

Patent Owner also asserts that the disclosure in Law’s paragraph 83 about the “[d]etection of certain network conditions” triggering “an automatic update of the rulesets” concerns only UTMS-configured devices implementing automatic updates and not cyber security risk management firm 305 implementing automatic updates. Resp. 14 (citing Ex. 1005 ¶ 83; Ex. 2002 ¶ 51). According to Patent Owner, the disclosure in Law’s paragraph 83 is “unrelated to any activities undertaken by firm 305, which is the alleged SPMS.” Sur-reply 6.

Additionally, Patent Owner contends that Law’s disclosure that “the UTMS-configured devices can receive from firm 305 the ‘update data’ on a continuous basis” does not “mean that the ‘update data’ was automatically generated.” Resp. 15 (citing Ex. 1005 ¶¶ 30, 66, Fig. 3; Ex. 2002 ¶ 52).

(iii) Analysis

For the reasons explained below, we agree with Petitioner that Law teaches or renders obvious limitation 1.2. *See* Pet. 23–26, 29–36; Reply 2–8; Ex. 1003 ¶¶ 61–64, 70–76; Ex. 1017 ¶¶ 5–16.

a. Security Policy Management Server

Law discloses that firewalls 146a and 146b may “receive the ruleset data . . . and other update data on a periodic or non-periodic basis via any desired communication link to the device or to a third party source,” such as “cyber security risk management firm 305 as described in relation to” Figure 3. Ex. 1005 ¶ 66; *see id.* ¶¶ 26, 88, 92; Ex. 1003 ¶¶ 62, 69. Referencing Figure 3, Law discloses that cyber security risk management firm 305 may “collect threat data 310 from a plurality of various sources 315 to construct the various rulesets 147, 148, 151, 153, validate the rulesets,

verify, and distribute the rulesets” to firewalls 146a and 146b and other UTMS-configured devices. Ex. 1005 ¶ 88; *see* Ex. 1003 ¶¶ 62, 70, 75.

Law explains that cyber security risk management firm 305 may:

- (1) “continuously identify network vulnerabilities in any device, sub-system, or software program”;
- (2) create “rules for the various rulesets,” including rules for firewall rulesets, based on an analysis of vulnerabilities; and
- (3) “provide an ongoing remediation update service to the system” including “device updates.”

Ex. 1005 ¶ 89; *see* Ex. 1003 ¶¶ 67, 72; Ex. 1017 ¶ 8.

When discussing cyber security risk management firm 305, Law does not use the word “server.” *See, e.g.*, Ex. 1005 ¶¶ 66, 88–89, 92. But an obviousness analysis “can take account of the inferences” drawn by an ordinarily skilled artisan who has “common sense, common wisdom, and common knowledge.” *See KSR*, 550 U.S. at 418; *Elektro Ltd. v. ZAP Surgical Sys., Inc.*, 81 F.4th 1368, 1374 (Fed. Cir. 2023). Moreover, “the meaning of a prior art reference requires analysis of the understanding of an artisan of ordinary skill.” *Finisar Corp. v. DirecTV Grp., Inc.*, 523 F.3d 1323, 1336 (Fed. Cir. 2008).

Here, an ordinarily skilled artisan “would have understood that cyber security risk management firm 305 necessarily comprises a server.”

Ex. 1003 ¶ 63. Dr. Jacobson testifies that firm 305 includes “IT infrastructure” with “computers” having “processing power” and “storage.” Ex. 2006, 37:2–38:2. Consistent with Dr. Jacobson’s testimony, Law describes firm 305 as “executing a computer-implemented algorithm” relating to rulesets. Ex. 1005 ¶ 88; *see* Ex. 1003 ¶ 70. Additionally, Law

discloses that (1) firewalls may communicate with firm 305 via “an Internet connection” to access rulesets and (2) firm 305 may respond to an access request by conveying rulesets “to their destination devices” via “a secure Internet interface.” Ex. 1005 ¶¶ 22, 66, 88, Fig. 3. Law also discloses that each “ruleset may be a data file,” e.g., as conveyed by a file server. *See* Ex. 1005 ¶ 90; *see* Ex. 1003 ¶ 63.

That cyber security risk management firm 305 is “a commercial entity,” as Patent Owner asserts, does not preclude firm 305 from employing a server to supply rulesets to firewalls via “a secure Internet interface.” *See* Ex. 1003 ¶ 63; Ex. 1005 ¶¶ 88, 90, Fig. 3; Resp. 12–13; Sur-reply 3–4.

b. Packet Filtering Rules Automatically Created

Regarding “packet filtering rules of the dynamic security policy” that were “automatically created” by the “security policy management server,” Law discloses that:

- (1) cyber security risk management firm 305 may “collect threat data 310 from a plurality of various sources 315 to construct the various rulesets 147, 148, 151, 153, validate the rulesets, verify, and distribute the rulesets” to firewalls 146a and 146b and other UTMS-configured devices;
- (2) “[r]uleset collecting, constructing, validating, and distributing may be performed using any type of information technology methods suitable for performing such actions using electronic data”; and
- (3) prior-art techniques for creating firewall rulesets include “automatically locating devices and generating rules by passively analyzing traffic on the network.”

Ex. 1005 ¶¶ 21, 88; *see* Ex. 1003 ¶¶ 70–71; Ex. 1017 ¶¶ 6–7, 11, 13; Pet. 30–31; Inst. Dec. 31–32; Reply 4–6. Further, Dr. Jacobson testifies that an

ordinarily skilled artisan “would have understood that ruleset constructing using ‘any type of information technology methods suitable for’ ruleset constructing would have included methods of automatically constructing rules.” Ex. 1003 ¶ 70 (quoting Ex. 1005 ¶ 88); Ex. 1017 ¶¶ 6, 11 (quoting Ex. 1005 ¶ 88). We credit Dr. Jacobson’s testimony.

Because Law discloses that cyber security risk management firm 305 may construct rulesets for firewalls using “any type of information technology methods suitable for” ruleset constructing and that such methods include “automatically locating devices and generating rules,” Law teaches “packet filtering rules of the dynamic security policy” that were “automatically created” by the “security policy management server” according to limitation 1.2. Ex. 1005 ¶¶ 21, 88; *see* Ex. 1003 ¶¶ 70–71; Ex. 1017 ¶¶ 6–7, 9–15.

As evidence that prior-art techniques for creating firewall rulesets include “automatically locating devices and generating rules,” Law cites U.S. Patent Application Publication No. 2007/0199061 to Byres et al., titled “Network Security Appliance,” and published in August 2007 (“Byres”).<sup>8</sup> Ex. 1005 ¶ 21; *see* Pet. 30 (quoting Ex. 1005 ¶ 21); Ex. 1003 ¶ 71 (quoting Ex. 1005 ¶ 21). Patent Owner asserts that background art, such as Byres, “cannot be used” to “change the basis” of a proposed combination. Resp. 17 (citing *Randall Mfg. v. Rea*, 733 F.3d 1355, 1362–63 (Fed. Cir. 2013)); *see id.* at 18. But Byres does not “change the basis” of the proposed Law-

---

<sup>8</sup> Law’s identification of U.S. Patent Application Publication No. 2007/0199061 includes an incorrect publication number that omits the last digit in the correct publication number, i.e., the digit “1.”

Golnabi combination. *See* Pet. 30–31; Ex. 1003 ¶¶ 70–71; Ex. 1017 ¶¶ 6, 11.

In particular, an ordinarily skilled artisan’s knowledge constitutes “part of the store of public knowledge that must be consulted when considering whether a claimed invention would have been obvious.” *Randall*, 733 F.3d at 1362. Dr. Jacobson testifies that an ordinarily skilled artisan “would have understood that ruleset constructing using ‘any type of information technology methods suitable for’ ruleset constructing would have included methods of automatically constructing rules.” Ex. 1003 ¶ 70 (quoting Ex. 1005 ¶ 88); Ex. 1017 ¶¶ 6, 11 (quoting Ex. 1005 ¶ 88). Byres properly corroborates Dr. Jacobson’s testimony. *See* Ex. 1005 ¶ 21; *Koninklijke Philips N.V. v. Google LLC*, 948 F.3d 1330, 1337–38 (Fed. Cir. 2020) (deciding that the Board properly relied on expert evidence corroborated by the Hua reference when determining that a claimed feature “was not only in the prior art, but also within the general knowledge of a skilled artisan”).

Patent Owner asserts that Byres “does not provide state-of-the-art evidence of automatic rule generation because Law explicitly explains how and why IT personnel must be involved in managing access to the process control network.” Sur-reply 6–7; *see* Resp. 17. We disagree. As explained later in this section, Law does not indicate that “IT personnel must be involved in managing access to the process control network.” Instead, Law discloses that system operators may monitor and configure equipment, including firewalls, “from a graphic display of an operator workstation, without IT personnel intervention.” Ex. 1005 ¶ 59; *see id.* ¶¶ 22, 87; Ex. 2006, 33:7–34:12; Resp. 9 (quoting Ex. 1005 ¶ 59).

We disagree with Patent Owner that IT personnel at cyber security risk management firm 305 are “required to update the ruleset when new threats are discovered or upgrades to software components of the system are implemented.” *See* Resp. 1, 9, 12–13, 18–19; Sur-reply 1, 5–8. When Law discusses IT personnel, Law refers to IT personnel at process control systems, not IT personnel at cyber security risk management firm 305. Ex. 1005 ¶¶ 14, 16–21, 59.

Specifically, Law describes difficulties in achieving suitable network security at process control systems. *See* Ex. 1005 ¶¶ 14–21. For example, when “network devices are not integrated into the process control system,” system operators lack access to firewall information. *Id.* ¶ 14. So firewall tasks “such as configuration, ruleset patching, and regular maintenance are left to IT personnel” at process control systems. *Id.*

Law explains that to accomplish those firewall tasks, IT personnel at process control systems should have “detailed knowledge of the network architecture” and should “understand the network topography, network business needs related to the network, permitted devices and services that the business requires within and between local networks, and the various external entities that should be permitted to access the local networks.” Ex. 1005 ¶ 16; *see id.* ¶¶ 17–19. But IT personnel at process control systems “are not typically trained to understand the process control system and its upgrades” and “may not understand how or why the rulesets must also be changed.” *Id.* ¶ 16. “In other circumstances, IT personnel have limited or no detailed understanding of the control system details and how the control system is to properly function to meet control objectives.” *Id.* ¶ 20. “As such, IT personnel may be at a significant disadvantage regarding proper

access controls, permission settings, and/or proper firewall rules configuration for the system.” *Id.*

Law also explains that some “commercial off-the-shelf (COTS) firewall systems” for process control systems may “provide a partial solution to network security, but still must be managed outside of the operator environment” by “IT personnel specifically trained to integrate the firewall into the needs of the process control system and configure the various rulesets.” Ex. 1005 ¶ 16; *see* Ex. 1017 ¶ 15. With those conventional firewall systems, “IT personnel are still required to update the ruleset when new threats are discovered or upgrades to software components of the system are implemented.” Ex. 1005 ¶ 16; *see* Ex. 1017 ¶ 15.

Law endeavors to (1) overcome the need for specifically trained IT personnel at process control systems to create or update firewall rulesets and (2) enhance “security and management” by providing an operator environment implementing a “Unified Threat Management System (UTMS).” Ex. 1005 ¶ 22; *see id.* at code (57); Ex. 1017 ¶ 16. The UTMS includes “a UTMS-configured firewall, UTMS-configured network access device, and UTMS-configured field devices that are capable of defending against both known and ‘zero day’ vulnerabilities and threats to control systems for both embedded, proprietary devices, and standard, commonly-used devices.” Ex. 1005 ¶ 22; *see* Ex. 1017 ¶ 16.

With the UTMS, system operators may monitor and configure equipment, including firewalls, “from a graphic display of an operator workstation, without IT personnel intervention.” Ex. 1005 ¶ 59; *see id.* ¶ 87. Thus, system operators (not IT personnel) may protect a process control system from “internal and external network threats such as viruses, worms,

or any other attack that may induce a fault in one or more network devices, field devices, or other portions of the process control system.” *Id.* ¶ 59; *see id.* ¶ 22; Ex. 1003 ¶ 64; Ex. 2006, 33:7–34:12; Resp. 9 (quoting Ex. 1005 ¶ 59).

With the UTMS, operator displays permit system operators (not IT personnel) to:

- (1) “display the current state of the connection”;
- (2) “update the settings, rulesets, and other parameters or variables of the UTMS (and its firewalls, network access devices, and field devices if so configured)”;
- (3) “perform any other process control system security tasks from the operator display or other workstation.”

Ex. 1005 ¶ 23; *see id.* ¶¶ 26, 60–61, 90–91, 102; Ex. 2006, 33:7–34:12.

Hence, system operators “may easily configure each UTMS-configured device while reducing the risk of mis-configuration and reduced security.”

Ex. 1005 ¶ 81; *see id.* ¶ 105.

As Patent Owner concedes, “UTMS-configured elements of graphical displays that allow operators to configure and manage rulesets within the process control system” constitute “Law’s innovative feature.” *See* Resp. 14 (emphasis omitted).

When Law discusses cyber security risk management firm 305, Law does not mention any IT personnel or any other individuals at firm 305, such as someone who obtains threat data or someone who constructs rulesets.

Ex. 1005 ¶¶ 66, 88–89, 92; *see* Ex. 1017 ¶¶ 14–15. Law does not discuss what anyone at firm 305 does to support the firm’s mission. *See* Ex. 1005 ¶¶ 66, 88–89, 92. Patent Owner wrongly attributes Law’s discussion of IT personnel at process control systems to individuals at firm 305. *See* Resp.

1, 9, 12–13, 18–19; Sur-reply 1, 5–8; Ex. 1005 ¶¶ 14, 16–21, 59, 66, 88–89, 92; Ex. 1017 ¶¶ 14–15.

Also, Patent Owner’s assertion that IT personnel at cyber security risk management firm 305 have “detailed knowledge” about each process control system receiving rulesets from firm 305 leads to an incredible conclusion: IT personnel at firm 305 would have knowledge about the intricacies of each of a wide variety of “very individualized” process control systems including “distributed or scalable process control systems like those used in power generation, chemical, petroleum, or other processes.” *See* Resp. 13; Tr. 23:13–14; Ex. 1005 ¶ 3. For example, those process control systems include “military and government applications,” “nuclear power plants,” “municipal services,” “public communications systems,” “high-energy processes,” and “dangerous or hazardous processes” that IT personnel at firm 305 would have “detailed knowledge” about according to Patent Owner. Ex. 1005 ¶¶ 15, 93, 102; *see* Resp. 13.

Additionally, we disagree with Patent Owner that Law teaches away from automatic generation techniques in cyber security risk management firm 305. *See* Resp. 15–16. A “reference does not teach away” if “it merely expresses a general preference for an alternative invention but does not ‘criticize, discredit, or otherwise discourage’ investigation into the invention claimed.” *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 567 F.3d 1314, 1327 (Fed. Cir. 2009) (quoting *In re Fulton*, 391 F.3d 1195, 1201 (Fed. Cir. 2004)).

Law does not “criticize, discredit, or otherwise discourage” automatic generation techniques in cyber security risk management firm 305. *See, e.g.*, Ex. 1005 ¶¶ 16, 66, 88–89, 92. Instead, Law explains that “[r]uleset

collecting, constructing, validating, and distributing” by firm 305 may be “performed using any type of information technology methods suitable for performing such actions using electronic data.” *Id.* ¶ 88; *see* Ex. 1003 ¶¶ 70–71; Ex. 1017 ¶¶ 6–7, 11, 13. Additionally, Law explains that prior-art techniques for creating firewall rulesets include “automatically locating devices and generating rules.” Ex. 1005 ¶ 21; *see* Ex. 1003 ¶ 71; Ex. 1017 ¶¶ 7, 13.

c. Packet Filtering Rules Automatically Altered

Regarding “packet filtering rules of the dynamic security policy” that were “automatically . . . altered” by the “security policy management server,” Law explains that firewalls 146a and 146b “require updates to remain effective against network threats.” Ex. 1005 ¶ 88; *see* Ex. 1003 ¶¶ 49, 72; Ex. 1017 ¶ 8; Ex. 1018, 17:22–18:16. Law also explains that firewalls 146a and 146b may “receive the ruleset data . . . and other update data on a periodic or non-periodic basis via any desired communication link to the device or to a third party source,” such as “cyber security risk management firm 305 as described in relation to” Figure 3. Ex. 1005 ¶ 66; *see id.* ¶¶ 26, 88, 92; Ex. 1003 ¶¶ 62, 69. Law describes Figure 3 as depicting “a logical block diagram of a method to update rulesets of the UTMS.” Ex. 1005 ¶ 30; *see* Ex. 1003 ¶ 50.

Law explains that cyber security risk management firm 305 may:

- (1) “continuously identify network vulnerabilities in any device, sub-system, or software program”;
- (2) create “rules for the various rulesets,” including rules for firewall rulesets, based on an analysis of vulnerabilities; and

- (3) “provide an ongoing remediation update service to the system” including “device updates.”

Ex. 1005 ¶ 89; *see* Ex. 1003 ¶¶ 67, 72; Ex. 1017 ¶ 8. Law also explains that the service may “proactively” supply firewall rulesets to “meet the latest security threats, threat patterns, and control system vulnerabilities found to exist within the network.” Ex. 1005 ¶ 22, code (57); *see* Ex. 1003 ¶¶ 49, 62; Ex. 2006, 35:11–23, 36:12–18.

By explaining that firm 305 may “continuously identify network vulnerabilities in any device,” “provide an ongoing remediation update service,” and “proactively” supply firewall rulesets to “meet the latest security threats,” Law teaches that firm 305 automatically alters (updates) firewall rulesets. *See* Ex. 1003 ¶¶ 49, 62, 67, 72–73; Ex. 1005 ¶¶ 22, 89, code (57); Ex. 1017 ¶¶ 8, 16; Ex. 2006, 35:11–23, 36:12–18.

As for Patent Owner’s contention that Law’s disclosure that “the UTMS-configured devices can receive from firm 305 the ‘update data’ on a continuous basis” does not “mean that the ‘update data’ was automatically generated,” Law includes other disclosures concerning firm 305 and the “perpetual service” for “proactively” supplying firewall rulesets. *See* Ex. 1005 ¶¶ 22, 66, 88–89, code (57), Fig. 3; Resp. 15 (citing Ex. 1005 ¶¶ 30, 66, Fig. 3; Ex. 2002 ¶ 52). For the reasons discussed above, Law’s disclosures concerning firm 305 collectively teach that firm 305 automatically alters (updates) firewall rulesets. Ex. 1005 ¶¶ 22, 66, 83, 88–89, code (57), Fig. 3; *see* Ex. 1003 ¶¶ 49, 62, 67, 72–73; Ex. 1017 ¶¶ 8, 16.

d. Packet Filtering Rules Based on  
Malicious Traffic Information

Regarding “packet filtering rules of the dynamic security policy” that were “based on malicious traffic information received from a plurality of malicious host tracker services,” Law discloses that cyber security risk management firm 305 may “collect threat data 310 from a plurality of various sources 315 to construct the various rulesets 147, 148, 151, 153, validate the rulesets, verify, and distribute the rulesets” to firewalls 146a and 146b and other UTMS-configured devices. Ex. 1005 ¶ 88; *see* Ex. 1003 ¶¶ 62, 70, 75. Law also discloses that sources 315 may “create the threat data 310 by monitoring, defining, and analyzing potential and known threats to the security of” communication networks 150a and 150b. Ex. 1005 ¶ 92; *see* Ex. 1003 ¶ 76. Further, “to name but a few of the sources for firewall ruleset data,” Law identifies sources 315 as including Assurent Secure Technologies, Secunia, and Carnegie Mellon University, i.e., “a plurality of malicious host tracker services” according to limitation 1.2. Ex. 1005 ¶ 92; *see* Ex. 1003 ¶ 76.

(d) Limitation 1.3

Claim 1 recites “wherein at least two of the plurality of malicious host tracker services are managed by different organizations.” Ex. 1001, 25:45–47 (limitation 1.3).

Petitioner contends that Law teaches limitation 1.3 because Law discloses various sources for “firewall ruleset data,” such as Assurent Secure Technologies, Secunia, and Carnegie Mellon University, that are “managed by different organizations.” Pet. 36 (citing Ex. 1005 ¶ 92); *see id.* at 34 (quoting Ex. 1005 ¶ 92).

Patent Owner makes no arguments specific to limitation 1.3. *See, e.g.,* Resp. 1–2, 11–34; Sur-reply 1–22.

For the reasons stated by Petitioner and supported by Dr. Jacobson’s testimony, we agree with Petitioner that Law teaches limitation 1.3. *See* Pet. 12, 34, 36; Ex. 1003 ¶¶ 49, 76–77.

(e) Limitation 1.4

Claim 1 recites “wherein one or more of the packet filtering rules were added, removed, or altered by the security policy management server based on a correlation between portions of the malicious traffic information.” Ex. 1001, 25:47–51 (limitation 1.4).

(i) Petitioner’s Contentions

Petitioner contends that Law alone renders obvious limitation 1.4 and alternatively that the combined disclosures in Law and Golnabi teach limitation 1.4. *See* Pet. 36–38; Reply 8–15.

a. Law Alone

Regarding Law alone, Petitioner asserts that Law discloses “receiving malicious traffic information (threat data 310) from several different third-party sources 315.” Pet. 37 (citing Ex. 1005 ¶ 92, Fig. 3); Reply 9. Petitioner asserts that sources 315 include (1) “at least three named sources 315,” i.e., Assurent, Secunia, and Carnegie Mellon, and (2) “at least three additional unnamed sources.” Reply 10 (citing Ex. 1005 ¶ 92, Fig. 3); *see id.* at 9; Pet. 34 (quoting Ex. 1005 ¶ 92). According to Petitioner, Law describes “sources 315 of threat data 310 to be ‘sources for firewall ruleset data.’” Reply 11 (quoting Ex. 1005 ¶ 92) (citing Ex. 1017 ¶ 20); *see id.* at 13. Petitioner asserts that an ordinarily skilled artisan would have

understood that “‘firewall ruleset data’ may have included rules.” *Id.* at 11 (citing Ex. 1017 ¶ 20).

Further, Petitioner asserts that an ordinarily skilled artisan would have understood (1) the “potential overlap in the threat data provided by sources 315” and (2) the “high likelihood of duplicates in the received threat data.” Pet. 37 (citing Ex. 1003 ¶ 79); Reply 9–11 (quoting Ex. 1018, 83:11–23); *see* Pet. 18–19. According to Petitioner, it would have been obvious to an ordinarily skilled artisan to “remove duplicate rules in order to avoid the inefficiency, wasted processing power, and slower execution speed of not doing so.” Pet. 37 (citing Ex. 1003 ¶ 79); *see* Reply 9–11.

Additionally, Petitioner contends that given (1) “Law’s disclosure of the likelihood of duplicate threat data existing across the threat data aggregated from the numerous independent sources” and (2) “Law’s disclosure that the threat data includes firewall ruleset data” that “may have included rules,” the “problem of duplicate rules arising from Law’s aggregation of threat data follows directly from the text of Law.” Reply 11–12 (citing Ex. 1017 ¶ 20). According to Petitioner, an ordinarily skilled artisan would have been aware “based exclusively” on Law’s teachings that “Law’s system of aggregating threat data and ruleset data from multiple independent sources would have given rise to duplicate rules.” *Id.* at 10.

Also, contrary to Patent Owner’s position, Petitioner contends that Dr. Jacobson’s supporting testimony that Law alone renders obvious limitation 1.4 does not rest on hindsight gleaned from the ’474 patent. Reply 10; *see infra* § III.D.3(e)(ii).a.

b. The Combined Disclosures in Law and Golnabi

Regarding the combined disclosures in Law and Golnabi, Petitioner asserts that Golnabi teaches:

- (1) filtering out “any unwanted traffic coming into or going from the secure network”;
- (2) “merging a plurality of rules using ‘an aggregation algorithm to generate a minimum number of firewall policy rules for efficiency’”;
- (3) combining “a group of similar rules”; and
- (4) combining rules “to get one generalized rule.”

Pet. 38 (emphasis omitted) (quoting Ex. 1009, 308) (citing Ex. 1003 ¶ 80); Reply 9, 12–13 (quoting Ex. 1009, 305, 308).

Petitioner asserts that it would have been obvious to an ordinarily skilled artisan to “combine rules as Golnabi teaches, when constructing rulesets as Law teaches using threat data 310 from a plurality of sources 315, because the appropriate combining of rules can minimize total rules thereby providing processing efficiency.” Pet. 38 (citing Ex. 1003 ¶ 80); Reply 9–10, 13 (citing Ex. 1003 ¶ 80; Ex. 1017 ¶ 22).

Petitioner also asserts that an ordinarily skilled artisan would have:

- (1) “appreciated that Golnabi’s technique, which may provide ‘a tremendous performance gain as a result,’ operates on rules”;
- (2) understood that Golnabi’s teachings apply to “rule optimization at any time”;
- (3) “recognized that it is desirable to process the rule sets, as Golnabi teaches, by merging, separating, and ordering rules of the rule sets such that they provide optimized performance during operational processing”;

(4) “been motivated to implement Golnabi’s processes for ‘combining, separating, and ordering of rules’ in Law” to “achieve optimized performance”; and

(5) “had success doing so.”

Reply 13–15 (citations omitted) (citing Ex. 1003 ¶ 57; Ex. 1005 ¶¶ 52, 88; Ex. 1009, 305, 313–14; Ex. 1017 ¶ 26).

Petitioner further asserts that an ordinarily skilled artisan would have understood that “any inefficiencies from having aggregated duplicate rules” relating to malicious traffic information “would have been more than outweighed by the tremendous performance gains achieved using Golnabi’s technique.” Reply 13–14 (citing Ex. 1017 ¶ 24).

(ii) Patent Owner’s Contentions

Patent Owner disputes that Law alone renders obvious limitation 1.4 and that the combined disclosures in Law and Golnabi teach limitation 1.4. *See* Resp. 1–2, 19–27; Sur-reply 1–2, 8–13.

a. Law Alone

Regarding Law alone, Patent Owner contends that “Petitioner concedes that Law does not disclose an SPMS that adds, removes, or alters packet-filtering rules based on a correlation between portions of malicious traffic information.” Resp. 20 (citing Pet. 36–38); *see* Sur-reply 8. According to Patent Owner, Law’s cyber security risk management firm 305 “updates rules based on aggregated threat data 310 with no contemplation of removing duplicate rules.” Resp. 21 (citing Ex. 1005 ¶ 88); *see* Sur-reply 10.

Patent Owner asserts that Law does not describe a duplicate-rules problem. Sur-reply 9; *see id.* at 2, 10. According to Patent Owner, “Law simply discloses collecting and aggregating the threat data, nothing more.”

*Id.* at 10. Patent Owner further asserts that even if Law described a duplicate-rules problem, “knowledge of a problem and motivation to solve it does not provide the motivation to modify Law alone” to reach the claimed invention. *Id.* at 9 (citing *Innogenetics, N.V. v. Abbott Lab’ys*, 512 F.3d 1363, 1373 (Fed. Cir. 2008)); *see id.* at 10–11.

Patent Owner asserts that an ordinarily skilled artisan considering Law alone “would have found it more efficient to analyze the received threat data and ‘remove’ any duplicate information before constructing updates to ruleset 147, as opposed to constructing (potentially numerous) duplicate rules, comparing the received threat data and then removing the constructed duplicate rules in the updated ruleset 147.” Resp. 24 (quoting Inst. Dec. 40 (quoting Prelim. Resp. 20)) (citing Ex. 2002 ¶¶ 64–66); *see* Sur-reply 11.

Patent Owner also asserts that Petitioner’s “only record support” for the contention that Law alone renders obvious limitation 1.4 is “Dr. Jacobson’s conclusory, unsupported testimony, which merely parrots the Petition.” Resp. 21 (citing Pet. 37; Ex. 1003 ¶ 79). According to Patent Owner, the Board should give Dr. Jacobson’s testimony on this point “very little weight.” *Id.* (citing *Xerox Corp. v. Bytemark, Inc.*, IPR2022-00624, Paper 9 at 15–16 (PTAB Aug. 24, 2022) (precedential)).

Additionally, Patent Owner contends that Dr. Jacobson’s testimony that Law alone renders obvious limitation 1.4 rests on hindsight gleaned from the ’474 patent’s “recognition of and solution to the problem of duplicate information coming from multiple malicious host tracker services.” Resp. 22 (emphases omitted); *see id.* at 24; Sur-reply 8–10. Patent Owner asserts that “there is no record evidence” other than the ’474 patent that an ordinarily skilled artisan “would have considered solving

this problem by correlating malicious traffic information at an SPMS and then adding, removing, or altering rules based on that correlation.”

Resp. 23. Patent Owner also asserts that “Petitioner may not simply ‘retrace’ the inventor’s path and call it obvious.” *Id.* (citing *Ortho-McNeil Pharm., Inc. v. Mylan Lab’ys, Inc.*, 520 F.3d 1358, 1364 (Fed. Cir. 2008)).

b. The Combined Disclosures in Law and Golnabi

Regarding the combined disclosures in Law and Golnabi, Patent Owner asserts that an ordinarily skilled artisan “setting out to improve Law’s system with Golnabi’s teachings would not have reached the claimed invention.” Resp. 25 (citing Ex. 2002 ¶¶ 67–71); *see id.* at 27; Sur-reply 12–13. Patent Owner asserts that “Golnabi discloses implementing a ruleset on a protected network, running traffic through the ruleset to create firewall log data, and processing the firewall log data to find and combine similar rules.” Resp. 25. Patent Owner asserts that because “Golnabi’s technique requires implementing the ruleset on a protected network and analyzing the resulting firewall logs,” an ordinarily skilled artisan “seeking to improve Law would have implemented the ruleset (as taught in Law and Golnabi) and then used resulting log data to make the ruleset more efficient.” *Id.* at 25–26.

Further, Patent Owner asserts that using Golnabi’s technique in the Law-Golnabi combination would have removed “duplicate data from the threat data itself” and would not have removed duplicate rules from the firewall rulesets. Sur-reply 12–13. Therefore, according to Patent Owner, the Law-Golnabi combination would not have satisfied the “requirement of adding, removing, or altering rules from the dynamic security policy.” *Id.* at 13 (emphasis omitted); *see id.* at 2.

Additionally, Patent Owner contends that “[n]either Law nor Golnabi suggests correlating malicious traffic information at all.” Resp. 26. Patent Owner also contends that “Petitioner does not explain how or why” an ordinarily skilled artisan “would have modified Golnabi’s technique to correlate malicious traffic information at an SPMS instead of simply following Golnabi’s teachings of analyzing firewall logs generated on a protected network.” *Id.* According to Patent Owner, Petitioner does not explain how an ordinarily skilled artisan “would have been able to use malicious traffic information correlations” to generate “a minimum number of firewall policy rules for efficiency.” *Id.* at 27.

(iii) Analysis

We agree with Petitioner that the combined disclosures in Law and Golnabi teach limitation 1.4. *See* Pet. 18–19, 38; Reply 9–10, 12–15; Ex. 1003 ¶¶ 53–57, 80; Ex. 1017 ¶¶ 18, 21–26. Specifically, Golnabi teaches techniques for analyzing and modifying firewall policy rules to “optimize the firewall policy and efficiency.” Ex. 1009, 305–14; *see* Ex. 1003 ¶¶ 53–54; Ex. 1017 ¶¶ 18, 22, 26. Golnabi’s techniques include the following:

- (1) a data-mining technique based on an algorithm called “Mining firewall Log using Frequency (MLF)” that “deduce[s] efficient firewall policy rules” by mining a network traffic log;
- (2) an aggregation technique based on an algorithm called “Filtering-Rule Generalization (FRG)” that “reduce[s] the number of policy rules” and “generate[s] a minimum number of firewall policy rules for efficiency”;
- (3) an anomaly-detection technique based on an algorithm called “Anomaly Discovery Algorithm” that detects (i) a shadowing anomaly, (ii) a correlation anomaly,

- (iii) a generalization anomaly, (iv) a redundancy anomaly, and (v) certain “non-systematic mis-configuration anomalies”; and
- (4) a technique for identifying (i) dominant rules covering “a significant portion of the network traffic” and (ii) decaying or useless rules and then updating “the rule ordering in [the] firewall in order to optimize the filtering matching at real-time.”

Ex. 1009, 305–14; *see* Ex. 1003 ¶¶ 53–54, 80; Ex. 1017 ¶¶ 18, 22.

As an example of the aggregation technique, if multiple rules have “matching fields with an exception of source port field,” the “rules are then aggregated” by “combining all the source ports as a range of these source ports to get one generalized rule.” Ex. 1009, 308; *see* Ex. 1003 ¶ 53; Ex. 1017 ¶¶ 18, 22, 26. As another example of the aggregation technique, “the IP addresses of 129.110.10.7 and 129.110.10.1 can be aggregated to 129.110.10.\*” where the \* character represents a specified range. Ex. 1009, 308–09; *see* Ex. 1017 ¶ 26; Prelim. Resp. 22 (quoting Ex. 1009, 308–09).

The ’474 patent discloses an analogous process for combining rules having similar characteristics. *See* Ex. 1001, 24:27–50. The patent explains that “security policy management server 120 may combine the two rules of dynamic security policy 300” that each specify (1) common network addresses and (2) distinct network addresses “into a rule that specifies a range of network addresses” encompassing both the common network addresses and the distinct network addresses. *Id.* at 24:40–49. For instance, if a first rule specifies network addresses A, B, C, and F and a second rule specifies network addresses A, B, C, and G, the combined rule may specify the range of network address A through G. *Id.* at 24:40–50.

Like Golnabi, the '474 patent explains that by reducing the size of one or more dynamic security policies, security policy management server 120 may improve a packet security gateway's performance because its performance may depend on "the size of and/or correlations within [the] dynamic security policies." Ex. 1001, 15:48–52; *see* Ex. 1009, 308.

We disagree with Patent Owner that an ordinarily skilled artisan seeking to improve Law with Golnabi's teachings "would not have reached the claimed invention." *See* Resp. 25–26. In particular, Golnabi's data-mining technique uses an "initial set of firewall policy rules" specified by a network administrator based on an organization's security policy where each rule "specifies to accept or drop (deny) a packet of certain attributes." Ex. 1009, 307; *see id.* at 312 (Fig. 10 showing example firewall policy rules). With the "initial set of firewall policy rules," a firewall log file containing "firewall log raw data" is generated. *Id.* at 307; *see id.* at 311–12 ("First Step (1)").

After the firewall log file is generated, Golnabi's "MLF algorithm reads each line of [the] firewall log file, extracts the attributes for each log record, counts its occurrence and outputs the count for each unique combination of these attribute-values." Ex. 1009, 307; *see id.* at 308 (Fig. 4 showing the MLF algorithm with "Input: Firewall Log file" and "Output: Unique Rules and their Frequency"), 312 ("Second step (2)"). Thus, "each log record of a packet in [the] firewall log file" is processed to generate "a primitive rule," i.e., "a specific firewall policy rule where all of its attributes are instantiated or specified with its value being observed in [the] firewall log file." *Id.* at 307–08.

Next, using the primitive rules determined from the firewall log file by the MLF algorithm, Golnabi's FRG algorithm "generates a decision tree where each level or branching represents one of the attributes of a primitive rule from [the] log record of a packet which is an instance of a rule to be processed." Ex. 1009, 308; *see id.* at 308–09 (Fig. 5 showing the FRG algorithm with "Input: Rules" and "Output: The Tree"), 310 (Fig. 6 showing an example decision tree), 312 ("Third step (3)"). "Each of the rules extracted from [the] firewall log file is then examined to be branched and analyzed, and then to be grouped to be aggregated by combining the common fields to get the superset rules that match with a group of unique rules." *Id.* at 308. Specifically, "every path on the generated tree would print a generalized rule that supersedes all the existing rules in the input." *Id.* at 310.

By using packet filtering rules "based on malicious traffic information" according to Law as the "initial set of firewall policy rules" for Golnabi's data-mining technique and then using Golnabi's MLF algorithm and FRG algorithm to aggregate rules, the "security policy management server" (firm 305) would have "removed" or "altered" one or more of the packet filtering rules "based on a correlation between portions of the malicious traffic information" according to limitation 1.4. *See* Ex. 1001, 24:26–50; Ex. 1003 ¶ 80; Ex. 1005 ¶¶ 88, 92; Ex. 1009, 307–13; *supra* § III.D.3(c)(iii).d. For instance, the "security policy management server" (firm 305) would have generated the "initial set of firewall policy rules" for a firewall "based on malicious traffic information," and the firewall would have returned a firewall log file to the "security policy management server" (firm 305) for processing according to Golnabi's techniques. Because the

input rules would have been “based on malicious traffic information,” the correlations determined by Golnabi’s techniques would also have been “based on malicious traffic information.”

Additionally, Law discloses logging packets. Ex. 1005 ¶¶ 102–104, Fig. 13; *see* Ex. 1003 ¶ 162. As Patent Owner contends, an ordinarily skilled artisan “could have analyzed Law’s log data.” *See* Resp. 26. By using packet filtering rules “based on malicious traffic information” according to Law and then processing the resulting log data at the “security policy management server” (firm 305) using Golnabi’s MLF algorithm and FRG algorithm to aggregate rules, an ordinarily skilled artisan would have arrived at the claimed invention. *See* Ex. 1005 ¶¶ 88, 92; Ex. 1009, 307–13.

As for Patent Owner’s assertion that using Golnabi’s technique in the Law-Golnabi combination would have removed “duplicate data from the threat data itself” and would not have removed duplicate rules from the firewall rulesets, we disagree. *See* Sur-reply 12–13. As explained earlier in this section, Golnabi’s MLF algorithm and FRG algorithm aggregate rules, not threat data, when applied to firewall log data as Golnabi teaches. *See* Ex. 1003 ¶ 80; Ex. 1009, 307–13.

As for Patent Owner’s contention that “[n]either Law nor Golnabi suggests correlating malicious traffic information at all,” Law discloses packet filtering rules “based on malicious traffic information,” and Golnabi discloses correlating packet filtering rules. Ex. 1005 ¶¶ 88, 92; Ex. 1009, 305–13; *see* Ex. 1003 ¶¶ 70, 76, 80; Resp. 26; *supra* § III.D.3(c)(iii).d. Thus, the combined disclosures in Law and Golnabi teach limitation 1.4. Where an obviousness challenge rests on the combined disclosures in references, a patent owner cannot establish nonobviousness by attacking the

references individually. *See In re Merck & Co.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986).

As for Patent Owner’s contention that “Petitioner does not explain how or why” an ordinarily skilled artisan “would have modified Golnabi’s technique to correlate malicious traffic information at an SPMS,” Petitioner does not propose modifying Golnabi’s technique. *See* Pet. 18–19, 38; Resp. 26; Reply 9–10, 12–13, 15. Rather, Petitioner proposes applying Golnabi’s techniques to the rules in Law’s firewall rulesets to achieve “processing efficiency” and “optimized performance.” Pet. 18–19, 38; Reply 9–10, 12–13, 15; *see* Ex. 1003 ¶¶ 55–57, 80; Ex. 1017 ¶¶ 18, 22, 26.

Because we determine that the combined disclosures in Law and Golnabi teach limitation 1.4, we do not reach the question whether Law alone renders obvious limitation 1.4.

(f) Limitation 1.5

Claim 1 recites “wherein a first packet matching rule of the packet filtering rules comprises: at least one packet matching criterion, a corresponding packet transformation function, and an indication of a feed managed by at least one of the plurality of malicious host tracker services.” Ex. 1001, 25:51–56 (limitation 1.5).

(i) Petitioner’s Contentions

Petitioner contends that Law teaches or renders obvious limitation 1.5 for several related reasons. *See* Pet. 38–43; Reply 15–22.

a. At Least One Packet Matching Criterion

For a “packet matching rule” comprising “at least one packet matching criterion,” Petitioner asserts that Law discloses that a firewall ruleset may “define conditions that, if detected, implement some

combination of blocking suspected malicious communications or alerting an operator.” Pet. 39 (emphasis omitted) (quoting Ex. 1005 ¶ 91). Petitioner asserts that the rule conditions include “PROTOCOL,” “FROM,” “TO,” and “PORT” fields corresponding to “a single packet matching criterion for a single packet filtering rule within ruleset 147.” *Id.* at 39–40 (citing Ex. 1003 ¶ 84; Ex. 1005 ¶¶ 102–103, Fig. 13).

b. A Corresponding Packet Transformation Function

For a “packet matching rule” comprising “a corresponding packet transformation function,” Petitioner asserts that Law discloses that firewalls 146a and 146b may “use one or more rulesets to inspect and drop malicious packets from the network before the malicious packets can reach their intended destination.” Pet. 41 (quoting Ex. 1005 ¶ 52). Petitioner asserts that Law also discloses “other operations that each rule may perform on a packet,” including “accept,” “notify,” and “re-route.” *Id.* (citing Ex. 1003 ¶ 85; Ex. 1005 ¶ 103, Fig. 13).

c. An Indication of a Feed

i. A Protocol Providing an Indication of a Feed

For a “packet matching rule” comprising “an indication of a feed managed by at least one of the plurality of malicious host tracker services,” Petitioner asserts that Law discloses protocol types including “UDP, TCP, ICMP, HART, and/or SCPI.”<sup>9</sup> Pet. 42 (quoting Ex. 1005 ¶ 102); *see* Reply 18. Petitioner asserts that an ordinarily skilled artisan would have

---

<sup>9</sup> The acronym “UDP” stands for “User Datagram Protocol.” The acronym “TCP” stands for “Transmission Control Protocol.” The acronym “ICMP” stands for “Internet Control Message Protocol.” The acronym “HART” stands for “Highway Addressable Remote Transducer.” The acronym “SCPI” stands for “Standard Commands for Programmable Instruments.”

understood that some feeds of threat data 310 from sources 315 “may have been uniquely associated with a particular combination of rule parameters.” Pet. 42 (citing Ex. 1003 ¶ 86). Petitioner identifies “a rule featuring” SCPI as the protocol type applied to a feed “specialized in the SCPI protocol” as providing “an indication of that particular feed.” *Id.* (citing Ex. 1003 ¶ 86).

Petitioner further asserts that Law’s firewall rulesets include rule parameters corresponding to the following columns in Figure 13’s rule table 1300: protocol type column 1302, from-address column 1304, to-address column 1306, and port number column 1308. Reply 17–18 (citing Ex. 1005 ¶ 102, Fig. 13). Petitioner explains that if “one of Law’s sources 315 was known to be the only source of a set of sources that provided rules with a less-common protocol, such as the SCPI protocol,” an ordinarily skilled artisan would have understood that:

- (1) “a rule featuring that protocol in the protocol type column 1302 would have identified that particular feed”;  
and
- (2) “Law’s from-address column 1304, to-address column 1306, and port number column 1308 still would have satisfied” limitation 1.5’s distinct requirement for “at least one packet matching criterion.”

*Id.* at 18 (citing Ex. 1017 ¶ 29).

Petitioner also asserts that even if one of sources 315 “would not always have been” the “only source providing rules under a particular protocol,” such as the SCPI protocol, an ordinarily skilled artisan would have understood that “on the occasions where that would have been the case, the unusual protocol in the protocol type column 1302 would have been sufficient to identify that particular feed.” Reply 18 (citing Ex. 1017 ¶ 29;

*Hewlett-Packard Co. v. Mustek Sys., Inc.*, 340 F.3d 1314, 1326 (Fed. Cir. 2003)).

ii. A Rule Table Providing an Indication of a Feed

Alternatively, if “an indication of a feed” requires “an identification of a feed,” Petitioner asserts that including “an indication of a feed” in a packet matching rule would have been obvious in view of Law. Pet. 42–43 (citing Ex. 1003 ¶ 87); *see* Reply 19–22. Petitioner asserts that Law’s Figure 13 “illustrates a [sic] ‘a ruleset user interface such as a protocol rule table 1300’ that ‘may allow a user to access one or more user interfaces to configure and control any of the rules within the rulesets 147, 148, 151, 152.’” Pet. 42 (quoting Ex. 1005 ¶ 102); Reply 19.

Petitioner asserts that “some sources 315 may be more trustworthy or reliable than others.” Pet. 42–43 (citing Ex. 1003 ¶ 87); Reply 19–20 (citing Ex. 1003 ¶ 87). Petitioner cites Dr. Goodrich’s testimony that “the threat data provided by any source” is not “necessarily correct.” Reply 20 (citing Ex. 1018, 84:21–24). Petitioner asserts that given Law’s express disclosure of three named sources, i.e., Assurent, Secunia, and Carnegie Mellon, and Law’s additional disclosure of unnamed sources, an ordinarily skilled artisan “would have understood that it is impossible to say that the unnamed sources are equally as reliable and trustworthy as the three named sources.” *Id.* at 22 (citing Ex. 1005 ¶ 92, Fig. 3; Ex. 1017 ¶ 36).

Further, Petitioner asserts that “information regarding the source 315 of each rule may be helpful to a user when using the ruleset interface to configure and control any of the rules” given “Law’s disclosure of receiving threat data 310 from several sources 315.” Pet. 42 (citing Ex. 1003 ¶ 87); Reply 19 (citing Ex. 1003 ¶ 87).

Additionally, Petitioner contends that “it would have been obvious to communicate” source-identifying information to a user by “adding a column to the rule table 1300 shown in Fig. 13 to indicate, for each rule, the source[s] 315 upon which the rule is based.” Pet. 43 (brackets in original) (citing Ex. 1003 ¶ 87); Reply 19–20 (citing Ex. 1003 ¶ 87). Petitioner contends that when adding a column to the rule table 1300 to indicate “the source[s] 315 upon which the rule is based,” an ordinarily skilled artisan would have understood that “it would have been as easy to have identified multiple sources 315 in that column as it would have been to have identified a single source.” Reply 20 (brackets in original) (citing Ex. 1017 ¶ 32). According to Petitioner, an ordinarily skilled artisan would have understood that “identifying multiple sources for a particular rule in a column added to the rule table 1300 would have given an operator viewing the rule table even greater confidence in the accuracy of” a particular rule due to the “possibility of errors” in ruleset information. *Id.* at 20–21 (citing Ex. 1017 ¶ 32).

Also, Petitioner asserts that Law discloses that firewalls 146a and 146b may receive threat data 310 “directly from” sources 315, “thereby identifying the source of the threat data to Law’s firewalls.” Reply 21 (quoting Ex. 1005 ¶ 92) (citing Ex. 1017 ¶ 34). Petitioner asserts that cyber security risk management firm 305 receives the same source-identifying information from sources 315. *Id.* at 21–22. Petitioner explains that it would have been obvious to include source-identifying information in the firewall rulesets distributed by firm 305 to firewalls 146a and 146b because the firewalls may receive the same source-identifying information “directly

from” sources 315. *Id.* at 21–22 (citing Ex. 1005 ¶ 92, Fig. 3; Ex. 1017 ¶ 34).

(ii) Patent Owner’s Contentions

Patent Owner disputes that Law teaches or renders obvious limitation 1.5 because Patent Owner disagrees that Law discloses or suggests “an indication of a feed managed by at least one of the plurality of malicious host tracker services.” *See* Resp. 2, 28–34; Sur-reply 2–3, 14–21. According to Patent Owner, “an indication of a feed” requires “an identification of a feed.” *See* Resp. 30; Tr. 24:11–25:2.

a. A Protocol Providing an Indication of a Feed

Regarding Petitioner’s contention that a “less-common protocol, such as the SCPI protocol,” could provide “an indication of a feed” if “one of Law’s sources 315 was known to be the only source” of that less-common protocol, Patent Owner asserts that rule parameters, such as “UDP, TCP, ICMP, HART, and/or SCPI,” are “part of the rules that cause actions to be performed on packets if met.” Resp. 28 (citing Ex. 1001, 2:56–60, 7:54–59, 8:34–44, 10:59–66; Ex. 2002 ¶ 73). Patent Owner asserts that an ordinarily skilled artisan would have understood that “a ‘combination of rule parameters’ in the rules would not and could not identify particular feeds the rules come from” due to the “high likelihood” of duplicate rules from different sources. *Id.* at 29 (quoting Pet. 42) (citing Ex. 2002 ¶¶ 73–75). Patent Owner also asserts that due to the “high likelihood” that “a number of sources provide duplicate rules under a particular protocol type, there is no factual basis for Petitioner’s assumption that Law’s protocol would, or even could, identify a particular feed from one source.” Sur-reply 17.

Further, Patent Owner asserts that Petitioner improperly “identifies Law’s protocol for both the claimed ‘packet matching criterion’ and ‘indication of a feed.’” Sur-reply 15 (citing Inst. Dec. 45–46); *see id.* at 14. Patent Owner asserts that “[w]here a claim provides for two separate elements, these two elements ‘logically cannot be one and the same.’” *Id.* at 14 (quoting *Engel Indus., Inc. v. Lockformer Co.*, 96 F.3d 1398, 1405 (Fed. Cir. 1996)).

Patent Owner contends that “Petitioner’s conclusory statement that some sources ‘may have been uniquely associated with a particular combination of rule parameters’ to indicate a feed lacks an evidentiary basis.” Resp. 28 (quoting Pet. 42); *see* Sur-reply 15–16. Patent Owner also contends that Petitioner’s “only support” for that statement “comes from Dr. Jacobson who merely repeats, verbatim, the statement for which his testimony is offered to support, without any supporting evidence or technical reasoning.” Resp. 28–29 (citing Pet. 42; Ex. 1003 ¶ 86; *Xerox*, IPR2022-00624, Paper 9 at 15); *see* Sur-reply 15–16. According to Patent Owner, “Dr. Jacobson admitted that he did not even know what the SCPI protocol is used for.” Sur-reply 16 (citing Ex. 2007, 43:9–22).

b. A Rule Table Providing an Indication of a Feed

Patent Owner contends that Figure 13’s rule table 1300 “does not include an indication column” and that Petitioner relies on the table “as the basis for modifying the table with a column including information regarding the source 315 of each rule.” Resp. 31, 33 (citing Pet. 42–43; Ex. 2002 ¶ 78; Ex. 2006, 62:8–65:6); *see* Sur-reply 18.

Patent Owner asserts that modifying Figure 13’s rule table 1300 to add an indication column would also require modifying cyber security risk

management firm 305 (“the alleged SPMS”). Resp. 31; *see* Sur-reply 18. According to Patent Owner, Figure 13’s rule table 1300 requires a modification to add an indication column, and the firewall rulesets supplied by firm 305 require a modification to add source-identifying information. Sur-reply 18; *see* Resp. 31–32.

Patent Owner asserts that “Petitioner fails to provide articulated reasoning grounded in evidence for why a skilled artisan would have (or even could have) modified firm 305” to supply firewall rulesets with source-identifying information. Resp. 32; *see id.* at 34; Sur-reply 18, 20–21. Patent Owner also asserts that “Petitioner’s alleged rationale focuses only on the modification of the rule table, not the updated rulesets themselves that are distributed by firm 305.” Sur-reply 18 (citing Pet. 42–43).

Regarding reliability and trustworthiness as a reason to modify Figure 13’s rule table 1300, Patent Owner asserts that an ordinarily skilled artisan “would not care what source the threat originated from and whether it is reliable or trustworthy” because “a threat is a threat.” Sur-reply 20 (citing Ex. 1018, 84:12–20). According to Patent Owner, Dr. Jacobson admitted that a process control system would “accept firm 305’s assessment of source trustworthiness” and that system operators “would not care where the threat originated from because trustworthiness of the sources has been accepted.” *Id.* (citing Ex. 2007, 51:5–52:22).

Patent Owner concedes that Law discloses that firewalls 146a and 146b may receive threat data 310 “directly from” sources 315. Resp. 33 (citing Ex. 1005 ¶ 92); *see* Sur-reply 19. But Patent Owner contends that Law “does not teach or otherwise contemplate” (1) incorporating source-identifying information into firewall rulesets and (2) “distributing the

rulesets to a modified rule table.” Resp. 33–34 (citing Ex. 1005 ¶ 92; Ex. 2002 ¶ 81); *see* Sur-reply 19. According to Patent Owner, “there stands no articulated reasoning grounded in evidence that a skilled artisan, with no knowledge of the claimed invention, would have modified both Law and third-party firm 305” to arrive at the claimed invention “absent hindsight.” Resp. 34; Sur-reply 21.

Regarding Petitioner’s explanation that it would have been obvious to include source-identifying information in the firewall rulesets distributed by firm 305 to firewalls 146a and 146b because the firewalls may receive the same source-identifying information “directly from” sources 315, Patent Owner contends that the “directly from” embodiment “does nothing to show that the updated rulesets would include the source information nor that the rule table would include a column to display such information, which is ultimately required for Petitioner’s theory.” Sur-reply 19.

Patent Owner notes that Figure 13’s rule table 1300 lacks source-identifying information. Sur-reply 19. Patent Owner contends that “Law would have described the rule table as including” source-identifying information if the threat data supplied by sources 315 directly to a process control system included source-identifying information. *Id.*

Further, Patent Owner asserts that “Petitioner’s rationale based on the ‘possibility of errors’ is new and improper and likewise fails to supply a reason that would have prompted” an ordinarily skilled artisan to modify Figure 13’s rule table 1300 to add an indication column or modify the firewall rulesets supplied by firm 305 to add source-identifying information. Sur-reply 20–21.

(iii) Analysis

For the reasons explained below, we agree with Petitioner that Law teaches or renders obvious limitation 1.5. *See* Pet. 38–43; Reply 19–22; Ex. 1003 ¶¶ 82–85, 87–88; Ex. 1017 ¶¶ 30–36.

a. At Least One Packet Matching Criterion

Regarding a “packet matching rule” comprising “at least one packet matching criterion,” Law discloses that a firewall ruleset may “define conditions that, if detected, implement some combination of blocking suspected malicious communications or alerting an operator.” Ex. 1005 ¶ 91; *see* Ex. 1003 ¶¶ 59, 65, 83. Further, Law discloses a ruleset user interface including rule table 1300 containing “a protocol type column 1302, a from-address column 1304, a threshold parameter column 1305, a to-address column 1306, a port number column 1308, an action column 1310, a description column 1312, and a log column 1314.” Ex. 1005 ¶ 102, Fig. 13; *see* Ex. 1003 ¶¶ 51, 65–66, 83–84. Each row of rule table 1300 “enforces a rule if a corresponding row selector is active.” Ex. 1005 ¶ 103; *see* Ex. 1003 ¶ 84. Each row of rule table 1300 “corresponds to a single packet matching criterion for a single packet filtering rule within ruleset 147.” Ex. 1003 ¶ 84 (citing Ex. 1005 ¶ 103).

b. A Corresponding Packet Transformation Function

Regarding a “packet matching rule” comprising “a corresponding packet transformation function,” Law discloses that firewalls 146a and 146b may “use one or more rulesets to inspect and drop malicious packets from the network before the malicious packets can reach their intended destination” and “cause a fault.” Ex. 1005 ¶ 52; *see* Ex. 1003 ¶¶ 48, 59, 64, 85. Law also discloses that firewalls 146a and 146b may perform other

actions, such as “accept, . . . block, notify, and/or re-route.” Ex. 1005 ¶ 103; *see* Ex. 1003 ¶¶ 60, 65–66, 85.

c. An Indication of a Feed

Regarding a “packet matching rule” comprising “an indication of a feed managed by at least one of the plurality of malicious host tracker services,” we agree with Petitioner that “it would have been obvious to communicate” source-identifying information to a user by “adding a column to” Figure 13’s rule table 1300 “to indicate, for each rule, the source[s] 315 upon which the rule is based.” Ex. 1003 ¶ 87 (brackets in original); Ex. 1017 ¶¶ 30, 32; *see* Pet. 43; Reply 19–20.

As Petitioner asserts, “some sources 315 may be more trustworthy or reliable than others,” and “information regarding the source 315 of each rule may be helpful to a user when using the ruleset interface to configure and control any of the rules.” Ex. 1003 ¶ 87; Ex. 1017 ¶¶ 30, 32, 36; *see* Pet. 42–43; Reply 19–20. Dr. Jacobson explains that sources of threat data have “different methods of collecting threats” and “different levels of trust” depending on “the nature of the actual provider of that threat data.” Ex. 2007, 47:4–11, 49:12–24, 51:5–11. Dr. Goodrich agrees that “the threat data provided by any source” is not “necessarily correct.” Ex. 1018, 84:21–24.

Also, when adding a column to Figure 13’s rule table 1300 to indicate “the source[s] 315 upon which the rule is based,” an ordinarily skilled artisan would have understood that “it would have been just as easy to identify multiple sources 315 in that column as it would have been to identify a single source.” Ex. 1017 ¶ 32 (brackets in original); *see* Reply 20. Further, an ordinarily skilled artisan would have understood that “identifying

multiple sources for a particular rule” in a column added to rule table 1300 would have given an operator viewing the rule table “greater confidence in the accuracy of” a particular rule due to the “possibility of errors” in ruleset information. Ex. 1017 ¶ 32 (citing Ex. 1018, 84:21–24); *see id.* ¶ 34; Reply 20–21. Hence, a “high likelihood” of duplicate rules from different sources does not undermine the proposed modification. *See* Ex. 1017 ¶¶ 31–32.

We disagree with Patent Owner that “Petitioner’s rationale based on the ‘possibility of errors’ is new and improper.” *See* Sur-reply 20. In the Petition, Petitioner asserted that “some sources 315 may be more trustworthy or reliable than others.” Pet. 42–43. In the Reply, Petitioner further explained that “there may be errors in the ruleset information provided by Law’s sources 315” and cited Dr. Goodrich’s testimony as support. Reply 20 (citing Ex. 1018, 84:21–24). Petitioner’s further explanation does not amount to a new theory of unpatentability. *See, e.g., Apple Inc. v. Andrea Elecs. Corp.*, 949 F.3d 697, 706 (Fed. Cir. 2020); *Ericsson Inc. v. Intell. Ventures I LLC*, 901 F.3d 1374, 1379–81 (Fed. Cir. 2018). Also, Petitioner obtained Dr. Goodrich’s supporting testimony after filing the Petition. *See* Ex. 1018, 3:1–4.

Further, we disagree with Patent Owner that “Petitioner fails to provide articulated reasoning grounded in evidence for why a skilled artisan would have (or even could have) modified firm 305” to supply firewall rulesets with information identifying sources 315. *See* Resp. 32, 34; Reply 21–22; Sur-reply 18, 20–21; Ex. 1017 ¶¶ 33–34. Specifically, Petitioner identifies Law’s disclosures that firewalls 146a and 146b may receive threat data 310 “directly from” sources 315 including source-identifying information and that cyber security risk management firm 305 receives the

same source-identifying information from sources 315. Reply 21–22 (citing Ex. 1005 ¶ 92, Fig. 3; Ex. 1017 ¶ 34). Petitioner explains that it would have been obvious to include source-identifying information in the firewall rulesets distributed by firm 305 to firewalls 146a and 146b because the firewalls may receive the same source-identifying information “directly from” sources 315. *Id.* at 21–22.

Consistent with Petitioner’s explanation, Law discloses that firewalls 146a and 146b may “collect and aggregate threat data 310 directly from the firm 305 or plurality of sources 315 to construct, validate, and verify the various rulesets.” Ex. 1005 ¶ 92; *see* Ex. 1017 ¶ 34. Law’s Figure 3 depicts “dotted communication lines to deliver” threat data 310 from sources 315 directly to firewalls 146a and 146b without going through firm 305. Ex. 1005 ¶ 92, Fig. 3; *see* Ex. 1017 ¶ 34.

“If a firewall collected threat data 310 directly from one of the sources 315, the firewall would receive an identification of that feed directly from that source.” Ex. 1017 ¶ 34. Providing “that same information indirectly through the rulesets distributed by firm 305” would have been obvious to an ordinarily skilled artisan. *Id.* This is “the predictable use of prior art elements according to their established functions.” *See KSR*, 550 U.S. at 417.

As for Patent Owner’s contention that the “directly from” embodiment “does nothing to show that the updated rulesets would include the source information nor that the rule table would include a column to display such information,” Petitioner does not rely on that embodiment alone to establish obviousness. *See* Pet. 42–43 (citing Ex. 1003 ¶ 87; Ex. 1005 ¶ 102, Fig. 13); Reply 21–22 (citing Ex. 1005 ¶ 92, Fig. 3; Ex. 1017 ¶ 34);

Sur-reply 19. Petitioner relies on the “directly from” embodiment to show the obviousness of modifying the embodiment where firm 305 receives threat data 310 from sources 315 and firm 305 distributes firewall rulesets to firewalls 146a and 146b to include source-identifying information in the firewall rulesets. *See* Reply 21–22; Ex. 1017 ¶ 34.

Patent Owner’s contention that “Law would have described the rule table as including” source-identifying information if the threat data supplied by sources 315 directly to a process control system included source-identifying information rests on the unsupported premise that Figure 13’s rule table 1300 represents the “directly from” embodiment. *See* Sur-reply 19. Moreover, that premise conflicts with Figure 3.

In particular, Figure 3 depicts “dotted communication lines to deliver” threat data 310 from sources 315 directly to firewalls 146a and 146b. Ex. 1005 ¶ 92, Fig. 3; *see* Ex. 1017 ¶ 34. In contrast to that alternative embodiment, Figure 3 depicts solid lines to deliver threat data 310 from sources 315 to firm 305 and another solid line to deliver firewall rulesets from firm 305 to firewalls 146a and 146b. Ex. 1005 ¶¶ 88–89, Fig. 3; *see* Ex. 1003 ¶¶ 50, 63. In view of Figure 3, Figure 13’s rule table 1300 more likely represents the preferred embodiment depicted by solid lines in Figure 3 rather than the alternative “directly from” embodiment depicted by dotted lines in Figure 3.

Additionally, we disagree with Patent Owner that an ordinarily skilled artisan “would not care what source the threat originated from and whether it is reliable or trustworthy” because “a threat is a threat.” *See* Sur-reply 20. As explained earlier in this section, “some sources 315 may be more trustworthy or reliable than others,” and “information regarding the

source 315 of each rule may be helpful to a user when using the ruleset interface to configure and control any of the rules.” Ex. 1003 ¶ 87; Ex. 1017 ¶¶ 30, 32, 36.

We also disagree with Patent Owner that Dr. Jacobson admitted that a process control system would “accept firm 305’s assessment of source trustworthiness” and that system operators “would not care where the threat originated from because trustworthiness of the sources has been accepted.” *See* Sur-reply 20 (citing Ex. 2007, 51:5–52:22). In the testimony Patent Owner cites, Dr. Jacobson did not discuss what system operators would or would not care about. *See* Ex. 2007, 51:5–52:22. Dr. Jacobson stated that “if you’re buying your service from [firm] 305, you are assuming that you also have a trust of [firm] 305,” and that “[i]f the service comes external to you, there’s a certain level of trust and business process that you need to go through.” *Id.* at 52:15–21. But buying a ruleset from firm 305 and, therefore, accepting that firm 305’s multiple data sources are adequately trustworthy does not mean that firm 305’s multiple data sources are equally trustworthy. Dr. Jacobson’s testimony does not undermine the proposed modification.

Because we determine that “it would have been obvious to communicate” source-identifying information to a user by “adding a column to” Figure 13’s rule table 1300, we do not reach the question whether a protocol may provide “an indication of a feed” as required by limitation 1.5.

(g) Limitation 1.6

Claim 1 recites “performing, based on the packet filtering rules, packet filtering on individual packets of a plurality of packets associated

with the network protected by the packet security gateway.” Ex. 1001, 25:57–60 (limitation 1.6).

Petitioner contends that Law teaches limitation 1.6 because Law discloses that firewalls 146a and 146b “enforce rulesets, such as ruleset 147, to perform the packet transformation function (e.g., blocking packets) when the packet-matching criteria is satisfied.” Pet. 43–44 (citing Ex. 1005 ¶¶ 52, 91, 103). Further, Petitioner asserts that a firewall ruleset may “define conditions that, if detected, implement some combination of blocking suspected malicious communications or alerting an operator.” *Id.* at 43 (quoting Ex. 1005 ¶ 91).

Patent Owner makes no arguments specific to limitation 1.6. *See, e.g.,* Resp. 1–2, 11–34; Sur-reply 1–22.

For the reasons stated by Petitioner and supported by Dr. Jacobson’s testimony, we agree with Petitioner that Law teaches limitation 1.6. *See* Pet. 43–44; Ex. 1003 ¶¶ 89–90.

(h) Limitation 1.7

Claim 1 recites “wherein the packet filtering comprises: inspecting individual packets.” Ex. 1001, 25:60–62 (limitation 1.7).

Petitioner contends that Law teaches limitation 1.7 because Law discloses “inspecting individual packets to determine whether [the] conditions of any rule are satisfied.” Pet. 44 (citing Ex. 1005 ¶¶ 52, 91, Fig. 13). Further, Petitioner asserts that an ordinarily skilled artisan “would have understood that determining whether the conditions of any rule are satisfied would have necessarily required inspecting individual packets.” *Id.* (citing Ex. 1003 ¶ 91).

Patent Owner makes no arguments specific to limitation 1.7. *See, e.g.,* Resp. 1–2, 11–34; Sur-reply 1–22.

For the reasons stated by Petitioner and supported by Dr. Jacobson’s testimony, we agree with Petitioner that Law teaches limitation 1.7. *See* Pet. 44; Ex. 1003 ¶ 91.

(i) Limitation 1.8

Claim 1 recites “filtering each packet based on content determined from the inspection of that individual packet.” Ex. 1001, 25:63–64 (limitation 1.8).

Petitioner contends that Law teaches limitation 1.8 because Law discloses that:

- (1) firewalls 146a and 146b may “use one or more rulesets to inspect and drop malicious packets from the network before the malicious packets can reach their intended destination”; and
- (2) a firewall ruleset may “define conditions that, if detected, implement some combination of blocking suspected malicious communications or alerting an operator.”

Pet. 44–45 (quoting Ex. 1005 ¶¶ 52, 91).

Patent Owner makes no arguments specific to limitation 1.8. *See, e.g.,* Resp. 1–2, 11–34; Sur-reply 1–22.

For the reasons stated by Petitioner and supported by Dr. Jacobson’s testimony, we agree with Petitioner that Law teaches limitation 1.8. *See* Pet. 44–45; Ex. 1003 ¶ 92.

(j) Alleged Reason to Combine the Teachings of the References

Petitioner identifies a reason that would have prompted an ordinarily skilled artisan to combine Golnabi’s teachings with Law’s teachings in the way Petitioner proposes, i.e., to achieve “processing efficiency” and

“optimized performance.” *See* Pet. 18–19, 38; Reply 9–10, 12–13, 15. Also, Petitioner asserts that an ordinarily skilled artisan “would have had success” and produced “predictable” and “beneficial” results when combining Golnabi’s teachings with Law’s teachings. Pet. 18–19; *see* Reply 15. Dr. Jacobson’s testimony supports Petitioner’s positions. *See* Ex. 1003 ¶¶ 53–57, 80; Ex. 1017 ¶¶ 18–22, 26.

For instance, Dr. Jacobson testifies that an ordinarily skilled artisan would have been motivated to apply Golnabi’s techniques for “combining, separating, and ordering” to the rules in Law’s firewall rulesets to “optimize performance” of the rulesets. Ex. 1003 ¶ 57; Ex. 1017 ¶ 26; *see* Ex. 1003 ¶¶ 53–55. He explains that Golnabi teaches combining rules having similar characteristics, such as rules having “matching fields with an exception of source port field,” using “an aggregation algorithm to generate a minimum number of firewall policy rules for efficiency.” Ex. 1003 ¶¶ 53, 80 (quoting Ex. 1009, 308); *see* Ex. 1017 ¶¶ 18, 22. He also explains that Golnabi teaches splitting a rule into multiple rules and “reordering or prioritizing” certain frequently used rules to obtain “a tremendous performance gain as a result.” Ex. 1003 ¶ 54 (emphasis omitted) (quoting Ex. 1009, 314).

Dr. Jacobson also testifies that an ordinarily skilled artisan “would have been motivated to combine the teachings of Law and Golnabi to produce the obvious, beneficial, and predictable result of implementing Law’s rulesets by merging, separating, and ordering as taught by Golnabi so as to avoid inefficient ruleset processing” by Law’s firewalls 146a and 146b. Ex. 1003 ¶ 55; *see id.* ¶ 57; Ex. 1017 ¶ 26. He explains that an ordinarily skilled artisan “would have recognized the likelihood for duplication and overlap in the threat information received by cyber security risk

management firm 305” since Law discloses “receiving threat information from numerous independent third-party sources.” Ex. 1003 ¶ 57 (citing Ex. 1005 ¶ 92); *see* Ex. 1017 ¶¶ 18–20. He also explains that “[g]iven the likelihood of duplication and overlap in the received threat information that is used in construct[ing] Law’s rulesets,” an ordinarily skilled artisan “would have recognized that it is desirable to process the rule sets, by merging, separating, and ordering rules of the rule sets such that they provide optimized performance during operational processing.” Ex. 1003 ¶ 57; Ex. 1017 ¶ 26.

Dr. Jacobson further testifies that it would have been obvious to an ordinarily skilled artisan to “combine rules as Golnabi teaches, when constructing rulesets as Law teaches using threat data 310 from a plurality of sources 315, because the appropriate combining of rules can minimize total rules thereby providing processing efficiency.” Ex. 1003 ¶ 80; *see* Ex. 1017 ¶¶ 18, 22.

Patent Owner disputes that an ordinarily skilled artisan would have been motivated to combine Golnabi’s teachings with Law’s teachings to reach the claimed invention. *See* Resp. 26–27; Sur-reply 9, 12. According to Patent Owner, “Petitioner’s allegations fail even to allege ‘that a person of ordinary skill in the art would have been motivated to combine or modify the teachings in the prior art and would have had a reasonable expectation of success in doing so.’” Resp. 27 (quoting *OSI Pharms., LLC v. Apotex Inc.*, 939 F.3d 1375, 1382 (Fed. Cir. 2019)).

Further, Patent Owner asserts that Petitioner fails to explain why an ordinarily skilled artisan would have “modified Golnabi’s teachings in order to perform correlations on Law’s threat analysis data when it could have

analyzed Law’s log data instead.” Resp. 26 (citing *Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064, 1073 (Fed. Cir. 2015)). Patent Owner also asserts that “correlating malicious traffic information at the SPMS” as claimed relinquishes “certain advantages” of Golnabi’s techniques, such as “the ability to order the rules to ensure that the most frequently satisfied rules are applied first.” *Id.* at 26–27 (citing Ex. 2002 ¶ 69; *Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve, Inc.*, 796 F.2d 443, 448 (Fed. Cir. 1986)).

We agree with Petitioner that an ordinarily skilled artisan would have had a reason to combine Golnabi’s teachings with Law’s teachings in the way Petitioner proposes. *See* Pet. 18–19, 38; Reply 9–10, 12–13, 15; Ex. 1003 ¶¶ 53–57, 80; Ex. 1017 ¶¶ 18–22, 26. Specifically, Golnabi teaches techniques for analyzing and modifying firewall policy rules to “optimize the firewall policy and efficiency.” Ex. 1009, 305–14; *see* Ex. 1003 ¶¶ 53–54; Ex. 1017 ¶¶ 18, 22, 26. Among other things, Golnabi’s techniques enable network administrators to “optimize and validate firewall rules automatically.” Ex. 1009, 305; *see* Ex. 1003 ¶ 57.

As an example, Golnabi discloses combining rules having similar characteristics using “an aggregation algorithm to generate a minimum number of firewall policy rules for efficiency,” e.g., “aggregated by combining the common fields” in multiple rules. Ex. 1009, 308; *see* Ex. 1003 ¶¶ 53, 80; Ex. 1017 ¶¶ 18, 22. For instance, if multiple rules have “matching fields with an exception of source port field,” the “rules are then aggregated” by “combining all the source ports as a range of these source ports to get one generalized rule.” Ex. 1009, 308; *see* Ex. 1003 ¶ 53; Ex. 1017 ¶¶ 18, 22, 26. Similarly, “the IP addresses of 129.110.10.7 and 129.110.10.1 can be aggregated to 129.110.10.\*” where the \* character

represents a specified range. Ex. 1009, 308–09; *see* Ex. 1017 ¶ 26; Prelim. Resp. 22 (quoting Ex. 1009, 308–09).

As another example, Golnabi discloses splitting “the filtering rule of a multi-valued field into several rules where each rule will have a single-valued field.” Ex. 1009, 312; *see* Ex. 1003 ¶ 54. Further, Golnabi explains that by “reordering or prioritizing” certain frequently used rules, “one may expect a tremendous performance gain as a result.” Ex. 1009, 314; *see* Ex. 1003 ¶ 54; Ex. 1017 ¶ 24.

As Dr. Jacobson testifies, an ordinarily skilled artisan “would have been motivated to combine the teachings of Law and Golnabi to produce the obvious, beneficial, and predictable result of implementing Law’s rulesets by merging, separating, and ordering as taught by Golnabi so as to avoid inefficient ruleset processing” by Law’s firewalls 146a and 146b. Ex. 1003 ¶ 55; *see id.* ¶ 57; Ex. 1017 ¶ 26. As Dr. Jacobson further testifies, it would have been obvious to an ordinarily skilled artisan to “combine rules as Golnabi teaches, when constructing rulesets as Law teaches using threat data 310 from a plurality of sources 315, because the appropriate combining of rules can minimize total rules thereby providing processing efficiency.” Ex. 1003 ¶ 80; Ex. 1017 ¶¶ 18, 22. We credit Dr. Jacobson’s testimony.

A motivation to combine “can be found explicitly or implicitly in the prior art references themselves, in market forces, in design incentives, or in ‘any need or problem known in the field of endeavor at the time of invention and addressed by the patent.’” *Forest Lab ’ys, LLC v. Sigmapharm Lab ’ys, LLC*, 918 F.3d 928, 934 (Fed. Cir. 2019) (quoting *Arctic Cat Inc. v. Bombardier Recreational Prods. Inc.*, 876 F.3d 1350, 1359 (Fed. Cir. 2017)). Here, Petitioner identifies a motivation to combine “in the prior art

references themselves,” i.e., in Golnabi’s disclosures about modifying firewall policy rules for efficiency. Pet. 15–19, 38 (citing Ex. 1009, 305, 308, 312–14); *see* Ex. 1003 ¶¶ 53–57, 80 (citing Ex. 1009, 305, 308, 312–14); Ex. 1017 ¶¶ 18, 22, 26 (citing Ex. 1009, 305, 308, 312).

As for Patent Owner’s assertion that Petitioner fails to explain why an ordinarily skilled artisan would have “modified Golnabi’s teachings in order to perform correlations on Law’s threat analysis data when it could have analyzed Law’s log data instead,” Petitioner does not propose modifying Golnabi’s teachings. *See* Pet. 18–19, 38; Resp. 26; Reply 9–10, 12–13, 15. Rather, Petitioner proposes applying Golnabi’s techniques to the rules in Law’s firewall rulesets to achieve “processing efficiency” and “optimized performance.” Pet. 18–19, 38; Reply 9–10, 12–13, 15; *see* Ex. 1003 ¶¶ 55–57, 80; Ex. 1017 ¶¶ 18, 22, 26. The “normal desire of artisans to improve upon” known products and processes “can provide the motivation to optimize” known aspects of the products and processes. *In re Ethicon, Inc.*, 844 F.3d 1344, 1351 (Fed. Cir. 2017).

Moreover, “[t]here is a motivation to combine when a known technique ‘has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way,’ using the ‘prior art elements according to their established functions.’” *Intel Corp. v. PACT XPP Schweiz AG*, 61 F.4th 1373, 1380–81 (Fed. Cir. 2023) (citations omitted) (quoting *KSR*, 550 U.S. at 417; *Intel Corp. v. Qualcomm Inc.*, 21 F.4th 784, 799–800 (Fed. Cir. 2021)). Here, Petitioner identifies Golnabi’s known techniques used to improve firewall rulesets that would improve similar firewall rulesets in Law in the same way

when used according to Golnabi's teachings. *See* Pet. 18–19, 38; Reply 9–10, 12–13, 15; Ex. 1003 ¶¶ 55–57, 80; Ex. 1017 ¶¶ 18, 22, 26.

As for Patent Owner's assertion that "correlating malicious traffic information at the SPMS" as claimed relinquishes "certain advantages" of Golnabi's techniques, such as "the ability to order the rules to ensure that the most frequently satisfied rules are applied first," Golnabi does not describe rule ordering as mutually exclusive from Golnabi's other techniques. Ex. 1009, 305–14; *see* Resp. 26. For instance, Golnabi includes separate sections discussing (1) the MLF algorithm and the FRG algorithm "used to generate, filter, and generalize policies" (section A titled "Dataset Analysis & Process") and (2) rule ordering based on decaying rules and dominant rules (section B titled "Decaying Rules and Dominant Rules"). Ex. 1009, 312–14. Hence, an ordinarily skilled artisan could have employed rule ordering according to Golnabi after using Golnabi's MLF algorithm and FRG algorithm to aggregate rules. *See id.* at 305–14.

In any event, a "given course of action often has simultaneous advantages and disadvantages, and this does not necessarily obviate motivation to combine." *Medichem, S.A. v. Rolabo, S.L.*, 437 F.3d 1157, 1165 (Fed Cir. 2006). The "benefits, both lost and gained, should be weighed against one another." *Winner Int'l Royalty Corp. v. Wang*, 202 F.3d 1340, 1349 n.8 (Fed. Cir. 2000). Here, an ordinarily skilled artisan "would have understood that any inefficiencies from having aggregated duplicate rules would have been more than outweighed by the tremendous performance gains achieved using Golnabi's technique." Ex. 1017 ¶ 24.

Additionally, we disagree with Patent Owner that "Petitioner's allegations fail even to allege 'that a person of ordinary skill in the art would

have been motivated to combine or modify the teachings in the prior art and would have had a reasonable expectation of success in doing so.” *See* Resp. 27. Petitioner asserts that a person of ordinary skill in the art would have been motivated to combine Golnabi’s teachings with Law’s teachings. Pet. 18–19; Reply 15. Petitioner also asserts that an ordinarily skilled artisan “would have had success” and produced “predictable” and “beneficial” results when combining Golnabi’s teachings with Law’s teachings. Pet. 18–19; Reply 15. Dr. Jacobson’s testimony supports Petitioner’s assertions. *See* Ex. 1003 ¶¶ 55–57; Ex. 1017 ¶¶ 18–22, 26.

(k) Conclusion About Obviousness for Claim 1

For the reasons discussed above, the combined disclosures in Law and Golnabi teach the invention covered by claim 1. *See supra* §§ III.D.3(a)–(i). Moreover, an ordinarily skilled artisan would have been motivated to combine Golnabi’s teachings with Law’s teachings in the way Petitioner proposes and would have predicted success. *See supra* § III.D.3(j). Hence, Petitioner has shown by a preponderance of the evidence that claim 1 is unpatentable under § 103 as obvious over Law and Golnabi.

4. INDEPENDENT CLAIMS 9, 17, AND 25

Independent claims 9, 17, and 25 recite subject matter similar to claim 1. *Compare* Ex. 1001, 25:31–64, *with id.* at 26:39–27:8, *and id.* at 27:54–28:19, *and id.* at 29:3–52; *see* Prelim. Resp. 10 (referencing “similar claim limitations” (emphasis omitted)). Claims 9, 17, and 25 also recite computer or system components, such as a “processor,” a “memory,” and a “server.” *See id.* at 26:39–27:8, 27:54–28:19, 29:3–52.

Petitioner explains how Law teaches the computer and system components recited in claims 9, 17, and 25. *See* Pet. 45–53. Dr. Jacobson’s

testimony supports Petitioner’s positions. *See* Ex. 1003 ¶¶ 94–95, 104–105, 114–117, 125–126.

Patent Owner disputes that the combined disclosures in Law and Golnabi teach the inventions covered by claims 9, 17, and 25 for the reasons Patent Owner disputes that the combined disclosures teach the invention covered by claim 1. *See, e.g.*, Resp. 1–2, 11–34.

For the reasons discussed above, we consider Patent Owner’s patentability arguments about claim 1 unavailing. *See supra* §§ III.D.3(c)(iii), III.D.3(e)(iii), III.D.3(f)(iii), III.D.3(j). For (1) the reasons stated by Petitioner and supported by Dr. Jacobson’s testimony and (2) the reasons discussed above for claim 1, we agree with Petitioner that the combined disclosures in Law and Golnabi teach the inventions covered by claims 9, 17, and 25. *See* Pet. 45–53; Ex. 1003 ¶¶ 93–130; *supra* §§ III.D.3(a)–(i). Moreover, an ordinarily skilled artisan would have been motivated to combine Golnabi’s teachings with Law’s teachings in the way Petitioner proposes and would have predicted success. *See supra* § III.D.3(j). Hence, Petitioner has shown by a preponderance of the evidence that claims 9, 17, and 25 are unpatentable under § 103 as obvious over Law and Golnabi.

5. DEPENDENT CLAIMS 2, 3, 5–7, 10, 11,  
13–15, 18, 19, 21–23, 26, 27, 29–31, AND 33

(a) Claims 2, 10, 18, and 26

Claim 2 depends directly from claim 1 and specifies that “the at least one packet matching criterion comprises at least one network address associated with an indication of malicious network traffic.” Ex. 1001, 25:65–67. Claims 10, 18, and 26 depend directly from independent

claims 9, 17, and 25, respectively, and include limitations similar to claim 2. *Id.* at 27:9–12, 28:20–23, 30:1–4.

Petitioner contends that Law teaches the limitations in claims 2, 10, 18, and 26 because Law discloses that “the one or more first packet filtering rules of the first set of packet filtering rules comprise packet matching criteria corresponding to one or more network addresses.” Pet. 54. As support, Petitioner cites Law’s Figure 13. *Id.*

Petitioner asserts that Law’s Figure 13 shows rule table 1300 including “from-address column 1304 and to-address column 1306, which ‘correspond to one or more addresses associated with a given protocol type,’ such as ‘IP addresses’ that are ‘typically employ[ed]’ by the ‘TCP, UDP, and ICMP protocols.’” Pet. 54 (alteration by Petitioner) (quoting Ex. 1005 ¶ 102). Petitioner also asserts that an ordinarily skilled artisan “would have understood that an IP address is a network address.” *Id.* (citing Ex. 1003 ¶ 133).

Patent Owner makes no arguments specific to claims 2, 10, 18, and 26. *See, e.g.*, Resp. 1–2, 11–34; Sur-reply 1–22.

For the reasons stated by Petitioner and supported by Dr. Jacobson’s testimony, we agree with Petitioner that Law teaches the limitations in claims 2, 10, 18, and 26. *See* Pet. 53–54; Ex. 1003 ¶¶ 131–133.

(b) Claims 3, 11, 19, and 27

Claim 3 depends directly from claim 1 and specifies that “at least one packet transformation function comprises a network protection action.” Ex. 1001, 26:1–3. Claims 11, 19, and 27 depend directly from independent claims 9, 17, and 25, respectively, and include limitations similar to claim 3. *Id.* at 27:13–15, 28:24–26, 30:5–7.

Petitioner contends that Law teaches the limitations in claims 3, 11, 19, and 27 because Law discloses that:

- (1) “rulesets 147, 148, 151, 153 may define conditions that, if detected, . . . block[] suspected malicious communications”; and
- (2) “perimeter UTMS-configured devices 146 . . . may include any number of additional rule tables to monitor and/or protect a control system 100 from unwanted access and/or malicious attack.”

Pet. 55 (alterations by Petitioner) (quoting Ex. 1005 ¶¶ 91, 102) (citing Ex. 1003 ¶ 135).

Patent Owner makes no arguments specific to claims 3, 11, 19, and 27. *See, e.g.*, Resp. 1–2, 11–34; Sur-reply 1–22.

For the reasons stated by Petitioner and supported by Dr. Jacobson’s testimony, we agree with Petitioner that Law teaches the limitations in claims 3, 11, 19, and 27. *See* Pet. 55; Ex. 1003 ¶¶ 134–135.

(c) Claims 5, 13, 21, and 29

Claim 5 reads as follows (with bracketed numbers added for reference purposes):<sup>10</sup>

5. [5.0] The method of claim 1, further comprising:  
receiving, by the packet security gateway and using an interface that is not addressed at the network layer, packets in a network layer transparent manner; and

[5.1] performing at least one packet transformation function at the network layer.

---

<sup>10</sup> We use the same numbers that Petitioner uses to identify the claim language. *See* Pet. 55–56; Ex. 1012 (Listing of Claims), 2.

Ex. 1001, 26:16–21. Claims 13, 21, and 29 depend directly from independent claims 9, 17, and 25, respectively, and include limitations similar to claim 5. *Id.* at 27:28–35, 28:40–48, 30:22–30.

Petitioner contends that Law teaches limitation 5.0 and the similar limitations in claims 13, 21, and 29 because Law discloses that:

- (1) “[t]he network 150 and devices may also . . . support[] any communications protocol”;
- (2) Figure 13’s rule table 1300 includes first row 1326 employing “IP version 4 addresses”; and
- (3) “any addressing scheme may be employed including, but not limited to, IP version 6, hardware specific addressing (e.g., GPIB device addresses).”<sup>11</sup>

Pet. 55–56 (alterations by Petitioner) (emphases omitted) (quoting Ex. 1005 ¶¶ 55, 103) (citing Ex. 1003 ¶ 136).

Petitioner asserts that an ordinarily skilled artisan would have understood that:

- (1) “any communications protocol” according to Law includes “communication protocols using an interface that is not addressed at the network layer”; and
- (2) addresses for hardware-specific addressing “may not have been at the network layer.”

Pet. 55–56 (citing Ex. 1003 ¶ 136; Ex. 1005 ¶¶ 55, 103). Petitioner also asserts that it would have been obvious to an ordinarily skilled artisan that “firewalls 146a and 146b may have received packets using an interface addressed using hardware-specific addressing,” i.e., with addresses not at the network layer. *Id.* at 56 (citing Ex. 1003 ¶ 136).

---

<sup>11</sup> The acronym “GPIB” stands for “General Purpose Interface Bus.”

Petitioner contends that Law teaches limitation 5.1 and the similar limitations in claims 13, 21, and 29 because Law discloses that firewalls 146a and 146b:

- (1) support “any communications protocol”;
- (2) support “any addressing scheme”; and
- (3) “perform packet filtering on a first portion of packets based on a first set of packet filtering rules (ruleset 147) by performing at least one packet transformation specified by at least one of the packet filtering rules in ruleset 147 (action column 1310, including actions such as block, accept, re-route, and notify) on the first portion of packets, including at the network layer.”

Pet. 56 (citing Ex. 1003 ¶ 137; Ex. 1005 ¶¶ 52, 55, 59, 91, 102–103, Figs. 1A, 3, 13).

Patent Owner makes no arguments specific to claims 5, 13, 21, and 29. *See, e.g.*, Resp. 1–2, 11–34; Sur-reply 1–22.

For the reasons stated by Petitioner and supported by Dr. Jacobson’s testimony, we agree with Petitioner that Law teaches the limitations in claims 5, 13, 21, and 29. *See* Pet. 55–56; Ex. 1003 ¶¶ 136–137.

(d) Claims 6, 14, 22, and 30

Claim 6 depends directly from claim 1 and specifies that “the packet security gateway is a LAN switch.” Ex. 1001, 26:22–23. Claims 14, 22, and 30 depend directly from independent claims 9, 17, and 25, respectively, and include limitations similar to claim 6. *Id.* at 27:36–37, 28:49–51, 30:31–32.

The Petition identifies claims 6, 14, 22, and 30 as challenged claims allegedly unpatentable under § 103 as obvious over Law and Golnabi. Pet. 2–3; *see id.* at i–ii. But the Petition does not address the obviousness of

these claims. *See, e.g., id.* at 11–58. Nor does the Reply address the obviousness of these claims. *See, e.g.,* Reply 2–22. Additionally, Dr. Jacobson does not address the obviousness of these claims. *See, e.g.,* Ex. 1003 ¶¶ 58–139; Ex. 1017 ¶¶ 5–36.

When questioned about claims 6, 14, 22, and 30 at the oral hearing, Petitioner’s counsel made a new unpatentability argument, i.e., that Law’s paragraph 54 equates a network switch and a firewall to a packet security gateway. Tr. 21:3–24, 41:9–18. At an oral hearing, however, a party may not advance new arguments. Paper 21, 4; *see Dell Inc. v. Acceleron, LLC*, 884 F.3d 1364, 1369 (Fed. Cir. 2018) (noting that the “Board was obligated to dismiss [a party’s] untimely argument . . . raised for the first time during oral argument”).

Based on the evidence presented with the Petition, the evidence introduced during the trial, and Petitioner’s timely arguments, Petitioner has not shouldered its burden to prove the unpatentability of claims 6, 14, 22, and 30 by a preponderance of the evidence. *See Dynamic Drinkware*, 800 F.3d at 1378.

(e) Claims 7, 15, 23, and 31

Claim 7 reads as follows (with bracketed numbers added for reference purposes):<sup>12</sup>

7. [7.0] The method of claim 1, wherein the filtering each packet comprises: filtering one packet at a time; and

[7.1] performing a packet digest logging function with respect to each filtered packet.

---

<sup>12</sup> We use the same numbers that Petitioner uses to identify the claim language. *See* Pet. 56–58; Ex. 1012 (Listing of Claims), 2.

Ex. 1001, 26:24–28. Claims 15, 23, and 31 depend directly from independent claims 9, 17, and 25, respectively, and include limitations similar to claim 7. *Id.* at 27:38–43, 28:52–58, 30:33–38.

Petitioner contends that Law teaches limitation 7.0 and the similar limitations in claims 15, 23, and 31 because Law discloses that:

- (1) each row in Figure 13’s rule table 1300 “enforces a rule if a corresponding row selector is active”;
- (2) firewalls 146a and 146b “use one or more rulesets to inspect and drop malicious packets from the network before the malicious packets can reach their intended destination”; and
- (3) a firewall ruleset “may define conditions that, if detected, implement some combination of blocking suspected malicious communications or alerting an operator.”

Pet. 56–57 (quoting Ex. 1005 ¶¶ 52, 91, 103) (citing Ex. 1003 ¶ 138).

Petitioner contends that Law teaches limitation 7.1 and the similar limitations in claims 15, 23, and 31 because Law discloses that each row in Figure 13’s rule table 1300 includes a log column 1314 and that a user interface may include log information. Pet. 57–58 (citing Ex. 1005 ¶¶ 102, 108, Fig. 13). Petitioner also contends that “Law explains that certain conditions can cause a log to be generated.” *Id.* at 58 (citing Ex. 1005 ¶ 104).

Patent Owner makes no arguments specific to claims 7, 15, 23, and 31. *See, e.g.*, Resp. 1–2, 11–34; Sur-reply 1–22.

For the reasons stated by Petitioner and supported by Dr. Jacobson’s testimony, we agree with Petitioner that Law teaches the limitations in claims 7, 15, 23, and 31. *See* Pet. 56–58; Ex. 1003 ¶¶ 138–139.

(f) Claim 33

Claim 33 depends directly from independent claim 25 and specifies that “at least one packet transformation function is configured to route associated packets to a monitoring device.” Ex. 1001, 30:49–51.

The Petition identifies claim 33 as a challenged claim allegedly unpatentable under § 103 as obvious over Law and Golnabi. Pet. 2–3; *see id.* at i–ii. But the Petition does not address the obviousness of claim 33. *See, e.g., id.* at 11–58. Nor does the Reply address the obviousness of claim 33. *See, e.g.,* Reply 2–22. Additionally, Dr. Jacobson does not address the obviousness of claim 33. *See, e.g.,* Ex. 1003 ¶¶ 58–139; Ex. 1017 ¶¶ 5–36.

When questioned about claim 33 at the oral hearing, Petitioner’s counsel made a new unpatentability argument, i.e., that Law teaches claim 33’s limitation for the reason that Law teaches limitation 8.3 in the challenge based on Law, Golnabi, and Johnson. Tr. 21:3–24, 41:25–42:7; *see* Pet. 73. At an oral hearing, however, a party may not advance new arguments. Paper 21, 4; *see Dell*, 884 F.3d at 1369.

Based on the evidence presented with the Petition, the evidence introduced during the trial, and Petitioner’s timely arguments, Petitioner has not shouldered its burden to prove the unpatentability of claim 33 by a preponderance of the evidence. *See Dynamic Drinkware*, 800 F.3d at 1378.

(g) Summary for Dependent Claims 2, 3, 5–7, 10, 11, 13–15, 18, 19, 21–23, 26, 27, 29–31, and 33

For the reasons discussed above, the combined disclosures in Law and Golnabi teach the inventions covered by claims 2, 3, 5, 7, 10, 11, 13, 15, 18, 19, 21, 23, 26, 27, 29, and 31. *See supra* §§ III.D.3(a)–(i), III.D.4,

III.D.5(a)–(c), III.D.5(e). Moreover, an ordinarily skilled artisan would have been motivated to combine Golnabi’s teachings with Law’s teachings in the way Petitioner proposes and would have predicted success. *See supra* § III.D.3(j). Hence, Petitioner has shown by a preponderance of the evidence that claims 2, 3, 5, 7, 10, 11, 13, 15, 18, 19, 21, 23, 26, 27, 29, and 31 are unpatentable under § 103 as obvious over Law and Golnabi.

For the reasons discussed above, Petitioner has not shown that the combined disclosures in Law and Golnabi teach the inventions covered by claims 6, 14, 22, 30, and 33. *See supra* §§ III.D.5(d), III.D.5(f). Hence, Petitioner has not shown by a preponderance of the evidence that claims 6, 14, 22, 30, and 33 are unpatentable under § 103 as obvious over Law and Golnabi.

*E. Alleged Obviousness over Law, Golnabi,  
and Ke: Claims 4, 12, 20, and 28*

Petitioner contends that claims 4, 12, 20, and 28 are unpatentable under § 103 as obvious over Law, Golnabi, and Ke. *See, e.g.*, Pet. 2–3, 64–67. Patent Owner disputes Petitioner’s contentions. *See, e.g.*, Resp. 1–2, 11–34, 11 n.6.

Above, we provided overviews of Law and Golnabi. *See supra* §§ III.D.1–III.D.2. Below, we provide an overview of Ke. Then, we consider the obviousness issues. For the reasons explained below, we agree with Petitioner that claims 4, 12, 20, and 28 are unpatentable under § 103 as obvious over Law, Golnabi, and Ke.

1. OVERVIEW OF KE (EXHIBIT 1010)

Ke is a U.S. patent titled “Internet Security Device and Method,” filed on March 28, 2002, and issued on August 22, 2006. Ex. 1010, codes (12),

(22), (45), (54). Ke states that the “invention relates to an Internet security system.” *Id.* at 1:12.

Ke explains that “network designers have either incorporated security appliances, such as firewalls and traffic management devices in their systems or enhanced their routers with these functionalities” to “ensure security of communications.” Ex. 1010, 1:43–46. In “many cases,” however, “such appliances, although necessary from a security point of view, tend to act like bottlenecks in the network in terms of throughput.” *Id.* at 1:52–54.

Ke endeavors to provide improved throughput in an Internet security device and “meet increasing bandwidth requirements using a single device.” *See* Ex. 1010, 1:58–3:30, code (57). The Internet security device may be employed in a computer environment where users “are connected to a wide area network (WAN),” such as the Internet. *Id.* at 3:57–61.

Ke's Figure 3 (reproduced below) depicts a switching board for an Internet security device:

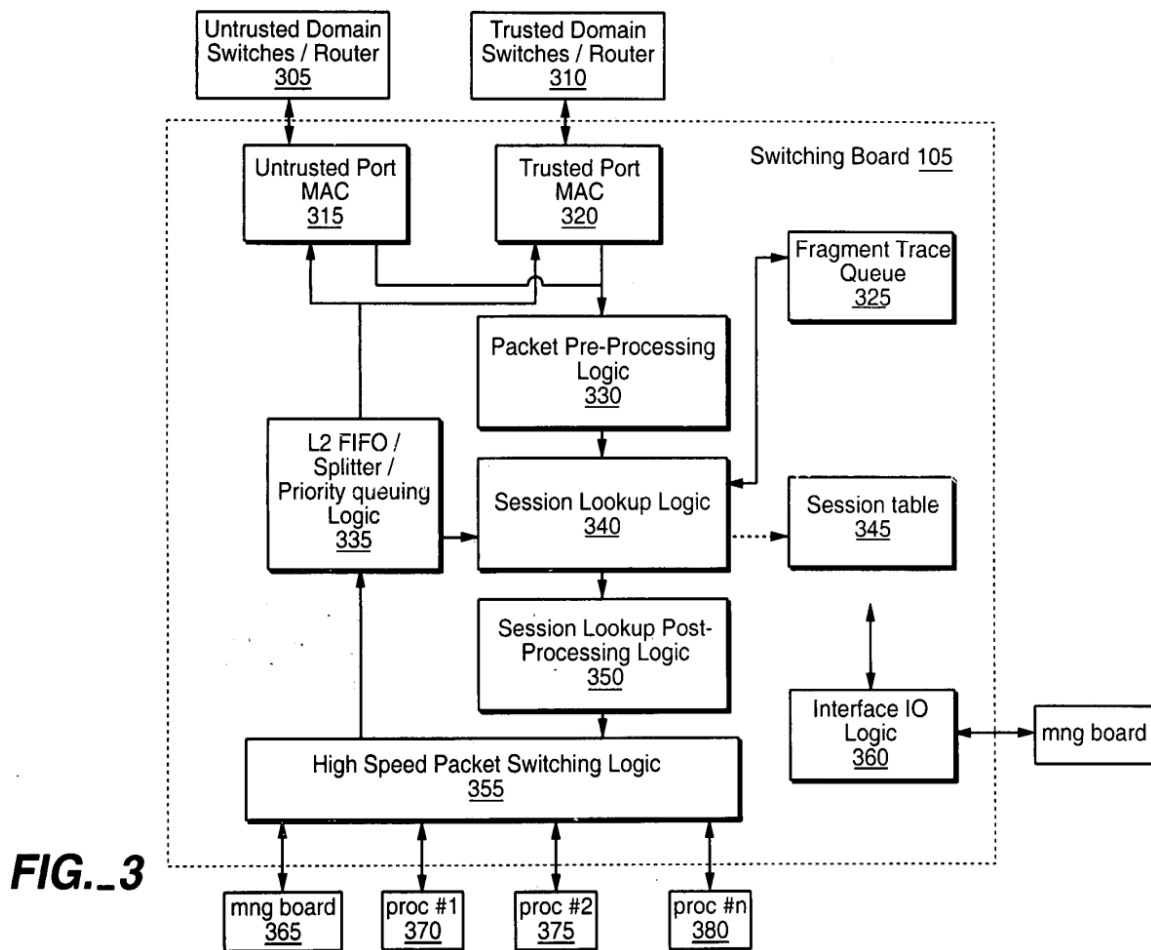


Figure 3 illustrates switching board 205 including the following components:

- (1) untrusted domain switcher/router port 305;
- (2) trusted domain switcher/router port 310;
- (3) untrusted port MAC 315;<sup>13</sup>
- (4) trusted port MAC 320;

<sup>13</sup> According to Ke, the acronym “MAC” refers to “media access connection.” Ex. 1010, 4:63–64.

- (5) pre-processing logic unit 330 to “examine if a packet is an IP packet”;
- (6) splitter and priority queuing logic unit 335 to “buffer packets, determine if a packet is a session control packet, and queue packets in a priority queue so that certain packets get priority over others”;
- (7) session lookup logic unit 340 to “determine if a packet is a non-first fragment packet using” session table 345;
- (8) post-processing logic unit 350 to “switch packets to a management board port” via high-speed packet switching logic unit 355; and
- (9) interface I/O logic unit 360 that “handles the communication between” the management board and the switching board.

Ex. 1010, 4:33–53, 4:63–67, Fig. 3.

For splitter and priority queuing logic unit 335, the “priority mechanisms for the priority queue can be configured by a system user according to any criterion he or she may select.” Ex. 1010, 4:53–55. For example, “control packets can have priority over normal packets.” *Id.* at 4:55–56. “The priority queuing mechanism ensures quality of service and high throughput.” *Id.* at 4:56–57.

## 2. DIFFERENCES BETWEEN THE CLAIMED INVENTION AND THE PRIOR ART

Claim 4 reads as follows (with formatting added for clarity and with bracketed numbers added for reference purposes):<sup>14</sup>

- 4. [4.0] The method of claim 1, wherein the dynamic security policy specifies that a first plurality of packets should

---

<sup>14</sup> We use the same numbers that Petitioner uses to identify the claim language. *See* Pet. 66–67; Ex. 1012 (Listing of Claims), 2.

be placed in a first forwarding queue and a second plurality of packets should be placed in a second forwarding queue,

[4.1] wherein the first forwarding queue has a higher forwarding rate than the second forwarding queue, and

[4.2] wherein the method further comprises:

sending, by the packet security gateway, the first plurality of packets in the first forwarding queue; and

sending, by the packet security gateway, the second plurality of packets in the second forwarding queue.

Ex. 1001, 26:4–15. Claims 12, 20, and 28 depend directly from independent claims 9, 17, and 25, respectively, and include limitations similar to claim 4. *Id.* at 27:16–27, 28:27–39, 30:8–21.

Petitioner contends that Ke teaches the limitations in claims 4, 12, 20, and 28 because Ke discloses that:

- (1) a first set of the packets (e.g., “session control packet[s]”) should be placed in a first forwarding queue (e.g., a priority queue) for “high throughput”;
- (2) a second set of the packets (e.g., “normal packets”) should be placed in a second forwarding queue (e.g., a non-priority queue);
- (3) the first forwarding queue has a higher forwarding rate than the second forwarding queue (e.g., implementation of “priority mechanisms” through “priority queuing logic”); and
- (4) packets are sent based on the forwarding queue.

Pet. 66–67 (alteration by Petitioner) (citing Ex. 1003 ¶¶ 151–153; Ex. 1010, 4:50–57, Fig. 3).

Patent Owner asserts that the reasons why the independent claims are patentable over the Law-Golnabi combination “apply equally” to the Law-Golnabi-Ke combination. Resp. 11 n.6; *see* Sur-reply 3 n.1.

For the reasons stated by Petitioner and supported by Dr. Jacobson’s testimony, we agree with Petitioner that Ke teaches the limitations in claims 4, 12, 20, and 28. *See* Pet. 64, 66–67; Ex. 1003 ¶¶ 147–148, 151–153. For the reasons discussed above, we consider Patent Owner’s patentability arguments about the independent claims unavailing. *See supra* §§ III.D.3–III.D.4.

### 3. ALLEGED REASON TO COMBINE THE TEACHINGS OF THE REFERENCES

Petitioner identifies a reason that would have prompted an ordinarily skilled artisan to combine the teachings of Law, Golnabi, and Ke. *See* Pet. 65–66. Dr. Jacobson’s testimony supports Petitioner’s position. *See* Ex. 1003 ¶¶ 149–150.

For instance, Dr. Jacobson testifies that an ordinarily skilled artisan would have appreciated that:

- (1) the traffic traversing Law’s network 150 “would have vastly different priority levels” for different devices, such as “sensors, valves, transmitters, positioners, etc.”; and
- (2) “the information from some sensors may have been critical to the functioning of the process control system, whereas others may not have been important at all.”

Ex. 1003 ¶ 149 (quoting Ex. 1005 ¶ 55).

Dr. Jacobson also testifies that an ordinarily skilled artisan would have been motivated to include Ke’s queuing techniques in Law’s system to obtain the advantages of those queuing techniques and “prevent a disaster

that could occur if a critical sensor was unable to communicate due to a network bottleneck.” Ex. 1003 ¶ 150 (citing Ex. 1010, 3:14–32).

Patent Owner makes no arguments against combining the teachings of Law, Golnabi, and Ke. *See, e.g.*, Resp. 1–2, 11–34, 11 n.6; Sur-reply 1–22.

We agree with Petitioner that an ordinarily skilled artisan would have had a reason, i.e., as articulated by Dr. Jacobson, to combine the teachings of Law, Golnabi, and Ke. *See* Pet. 65–66; Ex. 1003 ¶¶ 149–150.

#### 4. CONCLUSION ABOUT OBVIOUSNESS

For the reasons discussed above, the combined disclosures in Law, Golnabi, and Ke teach the inventions covered by claims 4, 12, 20, and 28. *See supra* §§ III.D.3–III.D.4, III.E.2. Moreover, an ordinarily skilled artisan would have been motivated to combine the teachings of Law, Golnabi, and Ke. *See supra* § III.E.3. Hence, Petitioner has shown by a preponderance of the evidence that claims 4, 12, 20, and 28 are unpatentable under § 103 as obvious over Law, Golnabi, and Ke.

##### *F. Alleged Obviousness over Law, Golnabi, and Johnson: Claims 7, 8, 15, 16, 23, 24, 31, and 32*

Petitioner contends that claims 7, 8, 15, 16, 23, 24, 31, and 32 are unpatentable under § 103 as obvious over Law, Golnabi, and Johnson. *See, e.g.*, Pet. 2–3, 69–73. Patent Owner disputes Petitioner’s contentions. *See, e.g.*, Resp. 1–2, 11–34, 11 n.6.

Above, we provided overviews of Law and Golnabi. *See supra* §§ III.D.1–III.D.2. Below, we provide an overview of Johnson. Then, we consider the obviousness issues. For the reasons explained below, we agree with Petitioner that claims 7, 8, 15, 16, 23, 24, 31, and 32 are unpatentable under § 103 as obvious over Law, Golnabi, and Johnson.

1. OVERVIEW OF JOHNSON (EXHIBIT 1011)

Johnson is a U.S. patent application publication titled “Framer,” filed on December 18, 2002, and published on June 24, 2004. Ex. 1011, codes (12), (22), (43), (54). Johnson explains that a “framer” arranges data “into a logical organization of bits known as a frame” for transmission over a network. *Id.* ¶ 2. After receiving a transmission, a “framer identifies frames within the bit stream and can extract packets stored within the frames.” *Id.* ¶ 3.

Johnson discloses a “framer” that “extracts packets from within a received frame and generates digests of the extracted packets.” Ex. 1011, code (57). Among other things, “the digest could speed a search for information in the payload, for instance, where the location of the information is not fixed with regard to the start of the packet.” *Id.* ¶ 21; *see id.* ¶ 10. A variety of devices may incorporate a “framer,” including “routers, switches, firewalls, line cards, network interface cards (NICs), or storage area network (SAN) components, among others.” *Id.* ¶ 22.

Johnson's Figure 1 (reproduced below) depicts "a block diagram illustrating logical operation of a framer that generates a packet digest" (Ex. 1011 ¶ 5):

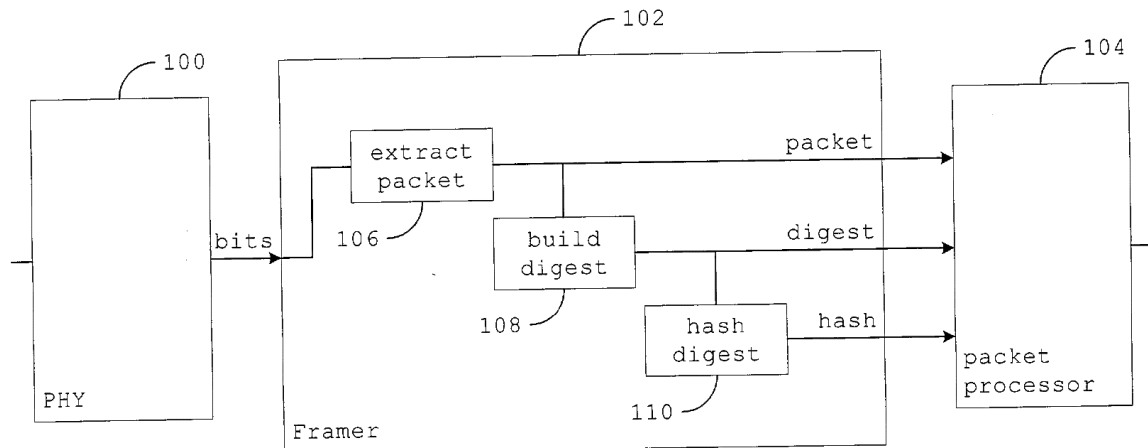


FIG. 1

Figure 1 illustrates framer 102 including logic that (1) "extracts 106 packets from identified frames," (2) "generates 108 digests of the packets," and (3) "computes 110 a hash of the digest." Ex. 1011 ¶ 9, Fig. 1. Framer 102 receives a bit stream from "physical layer component (PHY) 100 that interfaces to a network connection." *Id.* ¶ 11.

Framer 102 may generate digests that "vary based on a packet classification scheme being used." Ex. 1011 ¶ 14. As an example, "the digest may concatenate a packet's source Internet Protocol (IP) address, destination IP address, transport protocol (e.g., Transport Control Protocol (TCP) or User Datagram Protocol (UDP)) from the packet's IP header with the source port, and destination port from a packet's transport header." *Id.* As another example, "the digest may feature the IP source and destination address, transport protocol, and security parameter." *Id.*

Additionally, “the digest may include packet data other than data from the packet’s header.” Ex. 1011 ¶ 14. For instance, “a digest may be formed from bytes of a Universal Resource Locator (URL) included within a packet’s payload.” *Id.* Further, “a digest may include information not included within the packet (e.g., data from one or more previous packets, network status information, and so forth).” *Id.*

## 2. DIFFERENCES BETWEEN THE CLAIMED INVENTION AND THE PRIOR ART

Claims 7 and 8 read as follows (with formatting added for clarity and with bracketed numbers added for reference purposes):<sup>15</sup>

7. [7.0] The method of claim 1, wherein the filtering each packet comprises: filtering one packet at a time; and

[7.1] performing a packet digest logging function with respect to each filtered packet.

8. [8.0] The method of claim 7, wherein, the packet digest logging function comprises: identifying a subset of information in each packet that is also specified by the packet digest logging function;

[8.1] generating, for each packet, a record comprising the subset of information;

[8.2] reformatting, for each packet, the subset of information according to a logging system standard; and

[8.3] routing, based on the subset of information in the identified packet, each packet to a monitoring device.

Ex. 1001, 26:24–38.

Claims 15 and 16 depend directly or indirectly from independent claim 9 and include limitations similar to claims 7 and 8, respectively.

---

<sup>15</sup> We use the same numbers that Petitioner uses to identify the claim language. *See* Pet. 70–73; Ex. 1012 (Listing of Claims), 2–3.

Ex. 1001, 27:38–53. Claims 23 and 24 depend directly or indirectly from independent claim 17 and include limitations similar to claims 7 and 8, respectively. *Id.* at 28:52–29:2. Claims 31 and 32 depend directly or indirectly from independent claim 25 and include limitations similar to claims 7 and 8, respectively. *Id.* at 30:33–48.

Petitioner contends that Johnson teaches the limitations in claims 7, 15, 23, and 31 because Johnson discloses “a packet digest logging function performed on packets.” Pet. 70. Further, Petitioner asserts that Johnson’s packet digest logging function may use the following:

- (1) “a variety of types of information, including a packet’s source IP address, destination IP address, transport protocol, source port or destination port (the ‘five-tuple’); and
- (2) “application-layer packet-header information, such as an HTTP (application layer) packet header.”

*Id.* at 70–71 (citing Ex. 1011 ¶ 14).

Petitioner contends that Johnson teaches limitations 8.0 and 8.1 and the similar limitations in claims 16, 24, and 32 because Johnson discloses that (1) “the digest may feature the IP source and destination address, transport protocol, and security parameter” and (2) “the digest may include packet data other than data from the packet’s header.” Pet. 71–72 (quoting Ex. 1011 ¶ 14) (citing Ex. 1003 ¶¶ 165–166).

Petitioner contends that limitations 8.2 and 8.3 and the similar limitations in claims 16, 24, and 32 would have been obvious “in view of Law and Johnson.” *See* Pet. 72–73. Specifically, Petitioner asserts that an ordinarily skilled artisan “would have understood that it would have been obvious to reformat log data into a standard log format, such as ‘syslog,’

which was well known prior to 2014.” *Id.* at 72 (citing Ex. 1003 ¶ 167). Petitioner also asserts that Law discloses “re-route” as an action performed on a logged packet. *Id.* at 73 (citing Ex. 1003 ¶ 168; Ex. 1005 ¶ 103).

Patent Owner asserts that the reasons why the independent claims are patentable over the Law-Golnabi combination “apply equally” to the Law-Golnabi-Johnson combination. Resp. 11 n.6; *see* Sur-reply 3 n.1.

For the reasons stated by Petitioner and supported by Dr. Jacobson’s testimony, we agree with Petitioner that Johnson teaches the limitations in claims 7, 15, 23, and 31 and that the combined disclosures in Law and Johnson teach the limitations in claims 8, 16, 24, and 32. *See* Pet. 69–73; Ex. 1003 ¶¶ 160, 163–168. For the reasons discussed above, we consider Patent Owner’s patentability arguments about the independent claims unavailing. *See supra* §§ III.D.3–III.D.4.

### 3. ALLEGED REASON TO COMBINE THE TEACHINGS OF THE REFERENCES

Petitioner identifies a reason that would have prompted an ordinarily skilled artisan to combine the teachings of Law, Golnabi, and Johnson. *See* Pet. 70–72. Dr. Jacobson’s testimony supports Petitioner’s position. *See* Ex. 1003 ¶¶ 162, 165.

For instance, Dr. Jacobson testifies that (1) Law discloses packet digesting generally and (2) Johnson teaches a “specific implementation” of that known technique. Ex. 1003 ¶ 162 (citing Ex. 1005 ¶¶ 102, 104, 108, Fig. 13). According to Dr. Jacobson, Johnson’s teachings “represent an obvious extension of Law’s disclosure.” *Id.* ¶ 165.

Patent Owner makes no arguments against combining the teachings of Law, Golnabi, and Johnson. *See, e.g.*, Resp. 1–2, 11–34, 11 n.6; Sur-reply 1–22.

We agree with Petitioner that an ordinarily skilled artisan would have had a reason, i.e., as articulated by Dr. Jacobson, to combine the teachings of Law, Golnabi, and Johnson. *See* Pet. 70–72; Ex. 1003 ¶¶ 162, 165. “There is a motivation to combine when a known technique ‘has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way,’ using the ‘prior art elements according to their established functions.’” *Intel*, 61 F.4th at 1380–81 (citations omitted). Here, Petitioner identifies Johnson’s known technique used to improve packet digesting that would improve similar packet digesting in Law in the same way when used according to Johnson’s teachings. *See* Pet. 70–72; Ex. 1003 ¶¶ 162, 165.

#### 4. CONCLUSION ABOUT OBVIOUSNESS

For the reasons discussed above, the combined disclosures in Law, Golnabi, and Johnson teach the inventions covered by claims 7, 8, 15, 16, 23, 24, 31, and 32. *See supra* §§ III.D.3–III.D.4, III.F.2. Moreover, an ordinarily skilled artisan would have been motivated to combine the teachings of Law, Golnabi, and Johnson. *See supra* § III.F.3. Hence, Petitioner has shown by a preponderance of the evidence that claims 7, 8, 15, 16, 23, 24, 31, and 32 are unpatentable under § 103 as obvious over Law, Golnabi, and Johnson.

*G. Petitioner's Other Patentability Challenges:  
Claims 2, 5, 10, 13, 18, 21, 26, and 29*

As noted above, Petitioner contends that claims 2, 10, 18, and 26 are unpatentable under § 103 as obvious over Law, Golnabi, and Wood. *See* Pet. 2–3, 59–63; *supra* § II.G. As also noted above, Petitioner contends that claims 5, 13, 21, and 29 are unpatentable under § 103 as obvious over Law, Golnabi, and Jungck. *See* Pet. 2–3, 67–69; *supra* § II.G.

The challenge based on Law and Golnabi resolves the patentability questions for claims 2, 5, 10, 13, 18, 21, 26, and 29. *See supra* §§ III.D.5(a), III.D.5(c), III.D.5(g). Hence, we need not reach the challenge based on Law, Golnabi, and Wood or the challenge based on Law, Golnabi, and Jungck. *See SAS Inst. Inc. v. Iancu*, 138 S. Ct. 1348, 1359 (2018) (holding that a petitioner “is entitled to a final written decision addressing all of the claims it has challenged”); *Bos. Sci. Scimed, Inc. v. Cook Grp. Inc.*, 809 F. App’x 984, 990 (Fed. Cir. 2020) (agreeing that the Board “need not address issues that are not necessary to the resolution of the proceeding”).

#### IV. CONCLUSION

Based on the evidence presented with the Petition, the evidence introduced during the trial, and the parties’ respective arguments, Petitioner has shown by a preponderance of the evidence that:

- (1) claims 1–3, 5, 7, 9–11, 13, 15, 17–19, 21, 23, 25–27, 29, and 31 are unpatentable under § 103 as obvious over Law and Golnabi;
- (2) claims 4, 12, 20, and 28 are unpatentable under § 103 as obvious over Law, Golnabi, and Ke; and

- (3) claims 7, 8, 15, 16, 23, 24, 31, and 32 are unpatentable under § 103 as obvious over Law, Golnabi, and Johnson.<sup>16</sup>

But Petitioner has not shown by a preponderance of the evidence that claims 6, 14, 22, 30, and 33 are unpatentable under § 103 as obvious over Law and Golnabi.

In summary:

| Claims                                                                  | 35<br>U.S.C. § | Reference(s)/<br>Basis              | Claims<br>Shown<br>Unpatentable                                | Claims Not<br>Shown<br>Unpatentable |
|-------------------------------------------------------------------------|----------------|-------------------------------------|----------------------------------------------------------------|-------------------------------------|
| 1–3, 5–7,<br>9–11,<br>13–15,<br>17–19,<br>21–23,<br>25–27,<br>29–31, 33 | 103            | Law, Golnabi                        | 1–3, 5, 7,<br>9–11, 13, 15,<br>17–19, 21, 23,<br>25–27, 29, 31 | 6, 14, 22,<br>30, 33                |
| 2, 10,<br>18, 26                                                        | 103            | Law, Golnabi,<br>Wood <sup>17</sup> |                                                                |                                     |
| 4, 12,<br>20, 28                                                        | 103            | Law, Golnabi,<br>Ke                 | 4, 12, 20, 28                                                  |                                     |

---

<sup>16</sup> Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding after the issuance of this Final Written 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. 16,654 (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).

<sup>17</sup> In view of our determination that claims 2, 10, 18, and 26 are unpatentable under § 103 as obvious over Law and Golnabi, we do not reach this challenge to patentability. *See supra* §§ III.D.5(a), III.D.5(g), III.G.

| <b>Claims</b>                      | <b>35<br/>U.S.C. §</b> | <b>Reference(s)/<br/>Basis</b>        | <b>Claims<br/>Shown<br/>Unpatentable</b> | <b>Claims Not<br/>Shown<br/>Unpatentable</b> |
|------------------------------------|------------------------|---------------------------------------|------------------------------------------|----------------------------------------------|
| 5, 13,<br>21, 29                   | 103                    | Law, Golnabi,<br>Jungck <sup>18</sup> |                                          |                                              |
| 7, 8, 15,<br>16, 23,<br>24, 31, 32 | 103                    | Law, Golnabi,<br>Johnson              | 7, 8, 15, 16,<br>23, 24, 31, 32          |                                              |
| <b>Overall<br/>Outcome</b>         |                        |                                       | 1–5, 7–13,<br>15–21, 23–29,<br>31, 32    | 6, 14, 22,<br>30, 33                         |

## V. ORDER

Accordingly, it is

ORDERED that claims 1–5, 7–13, 15–21, 23–29, 31, and 32 in the '474 patent are determined to be unpatentable;

ORDERED that claims 6, 14, 22, 30, and 33 in the '474 patent are not determined to be unpatentable; 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.

---

<sup>18</sup> In view of our determination that claims 5, 13, 21, and 29 are unpatentable under § 103 as obvious over Law and Golnabi, we do not reach this challenge to patentability. *See supra* §§ III.D.5(c), III.D.5(g), III.G.

IPR2023-00448  
Patent 11,012,474 B2

For PETITIONER:

Gerard M. Donovan  
Peter J. Chassman  
Jonathan I. Detrixhe  
Sidharth Kapoor  
REED SMITH LLP  
gdonovan@reedsmith.com  
pchassman@reedsmith.com  
jdetrixhe@reedsmith.com  
skapoor@reedsmith.com

For PATENT OWNER:

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

Bradley C. Wright  
Scott M. Kelly  
John. R. Hutchins  
BANNER & WITCOFF, LTD.  
bwright@bannerwitcoff.com  
skelly@bannerwitcoff.com  
jhutchins@bannerwitcoff.com