

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KEYSIGHT TECHNOLOGIES, INC. and
PALO ALTO NETWORKS, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, LLC,
Patent Owner.

IPR2023-00445¹
Patent 10,785,266 B2

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

TURNER, *Administrative Patent Judge*.

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

¹ IPR2023-01329 has been joined with this proceeding.

I. INTRODUCTION

A. *Background and Summary*

In response to a Petition (Paper 2, “Pet.”), on July 24, 2023, we instituted an *inter partes* review of claims 1–27 (“the challenged claims”) of U.S. Patent No. 10,785,266 B2 (Ex. 1001, “the ’266 Patent”). Paper 10 (“Dec. to Inst.”). That decision was the subject of a request by Patent Owner for Director Review (Paper 13), which was later denied (Paper 14). Patent Owner subsequently filed a Patent Owner Response (Paper 17, “PO Resp.”), Petitioner filed a Petitioner Reply (Paper 21, “Pet. Reply”), Patent Owner filed a Patent Owner Sur-reply (Paper 28, “PO Sur-reply”), and a transcript of an oral hearing held on April 22, 2024 (Paper 30, “Hr’g Tr.”) has been entered into the record.

We have jurisdiction under 35 U.S.C. § 6. This Final Written Decision is issued pursuant to 35 U.S.C. § 318(a). We base our decision on the preponderance of the evidence. 35 U.S.C. § 316(e) (2018); 37 C.F.R. § 42.1(d) (2024).

Having reviewed the arguments of the parties and the supporting evidence, we conclude that Petitioner has demonstrated by a preponderance of the evidence that the challenged claims are unpatentable.

B. *Related Proceedings*

The Petition states that the ’266 Patent is asserted in the following litigation: *Centripetal Networks, Inc. v. Keysight Technologies, Inc.*, 2:22-cv-00002 (E.D. Va.) (filed Jan. 1, 2022), where Patent Owner cites to the same. Pet. 1; Paper 4, 1. The ’266 Patent was previously the subject of another potential *inter partes* review, IPR2021-01154, with Palo Alto Networks, Inc. as the prior petitioner, where institution was denied on the basis of that prior petitioner’s petition. *See* Ex. 2004 (“the ’1154 decision”).

C. Real Party-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 4, 1.

D. The '266 Patent

The '266 Patent discloses methods and systems for protecting a secured network. Ex. 1001, code (57). The '266 Patent discloses that “network environment 100 may include networks A-E 102, 104, 106, 108, and 110,” and “may include packet security gateways [“PSGs”] 112, 114, 116, and[] 118 and security policy management server [“SPMS”] 120.” *Id.* at 4:42–43, 5:15–16. An exemplary system is illustrated in Figure 1 and is reproduced below:

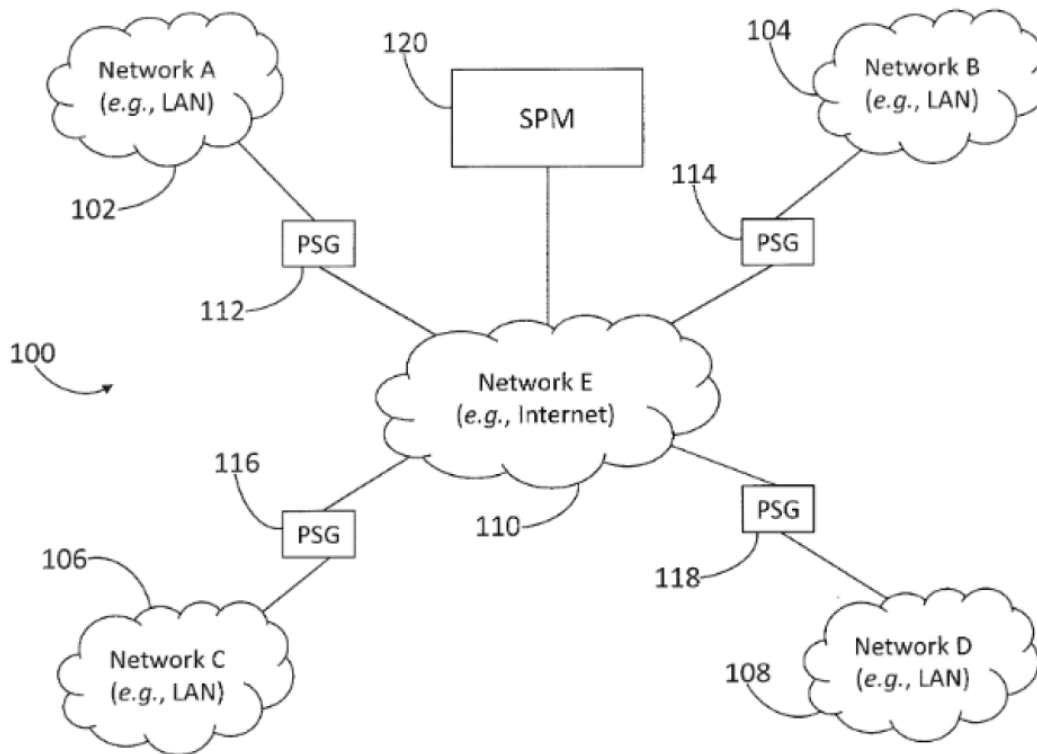


FIG. 1

The PSGs perform packet transformation functions (e.g., actions such as packet forwarding, dropping, or re-routing to a different destination

address) on received packets according to rules in a dynamic security policy that specifies one or more actions that are performed on packets associated with specific criteria. Ex. 1001, 4:59–5:11; 6:24–28; 7:23–26. The dynamic security policies can be added, removed, or altered by SPMS based on information received from third-party services. *Id.* at 14:9–28; Fig. 5. The exemplary SPMS can (i) automatically create or alter a first set of packet filtering rules of a dynamic security policy based on aggregated malicious network traffic from malicious host tracker services, (ii) communicate the first set to the PSGs, (iii) alter the first set based on updates from the malicious host tracker services, and (iv) communicate an updated second set of the packet filtering rules to the PSGs. *Id.* at 13:18–14:39; Fig. 5.

E. Illustrative Claim

As noted above, Petitioner challenges claims 1–27, with claims 1, 8, 15, and 21 being independent claims. Claim 1 is illustrative of the challenged claims and is reproduced below:

1. **[1.0]** A method of filtering packets at a packet security gateway, of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway and one or more networks other than the network protected by the packet security gateway, the method comprising:
 - [1.1]** receiving, by the packet security gateway and from a security policy management server external from the network protected by the packet security gateway, a dynamic security policy comprising a first set of packet filtering rules to be applied to all network traffic traversing the boundary, wherein:
 - [1.2]** each packet filtering rule of the first set of packet filtering rules comprises at least one packet matching criterion and a corresponding packet transformation function, and

- [1.3] 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 and were automatically created or altered by the security policy management server based on aggregated malicious traffic information received from at least one third party malicious host tracker service located in the one or more networks other than the network protected by the packet security gateway, that comprises network addresses that have been determined, by the at least one third party malicious host tracker service, to be associated with malicious network traffic;
- [1.4] performing, on a packet by packet basis, packet filtering on a first portion of packets corresponding to network traffic traversing the boundary via the packet security gateway based on the first set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets;
- [1.5] receiving, by the packet security gateway and after performing packet filtering on the first portion of the packets, an updated second set of packet filtering rules for the dynamic security policy from the security policy management server, wherein the updated second set of packet filtering rules comprises an update to the one or more first packet filtering rules created or altered by the security policy management server based on updated malicious traffic information received from the at least one third party malicious host tracker service; and
- [1.6] performing, on a packet by packet basis, packet filtering on a second portion of the packets corresponding to network traffic traversing the boundary via the packet security gateway based on the updated second set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the second set of packet filtering rules on the second portion of packets.

Ex. 1001, 20:64–21:52 (with annotations provided by Petitioner,
Ex. 1009, 1–2).

F. Grounds of Institution

Trial was instituted on the following grounds:

References	35 U.S.C. § ²	Claims Challenged
Law ³	§ 103(a)	1–27
Law, Wood ⁴	§ 103(a)	1–27
Law, Jungck ⁵	§ 103(a)	6, 13, 19, 26
Law, Wood, Jungck	§ 103(a)	6, 13, 19, 26

Dec. to Inst. 27. Petitioner relies on the declarations of Dr. Doug W. Jacobson (Exs. 1003, 1014), and Patent Owner relies on the declaration of Dr. Michael T. Goodrich (Ex. 2012), with two depositions of Dr. Jacobson (Exs. 2014, 2018) and one deposition of Dr. Goodrich (Ex. 1015).

II. ANALYSIS

A. Level of Ordinary Skill in the Art

The level of ordinary skill in the pertinent art at the relevant time is a factor in how we construe patent claims. *See Phillips v. AWH Corp.*, 415

² The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011), amended 35 U.S.C. § 103 effective March 16, 2013. Because the '266 Patent has an effective filing date prior to the effective date of the applicable AIA amendment, we refer to the pre-AIA version of § 103.

³ U.S. Patent Publication No. 2011/0072506 A1 (filed Sept. 23, 2010) (published Mar. 24, 2011) (Ex. 1005, “Law”).

⁴ U.S. Patent Publication No. 2007/0097976 A1 (filed May 19, 2006) (published May 3, 2007) (Ex. 1006, “Wood”).

⁵ U.S. Patent Publication No. 2009/0262741 A1 (filed June 29, 2009) (published Oct. 22, 2009) (Ex. 1008, “Jungck”).

F.3d 1303, 1312–13 (Fed. Cir. 2005) (en banc). It is also one of the factors we consider when determining whether a patent claim is obvious over the prior art. *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

To assess the level of ordinary skill, we construct a hypothetical “person of ordinary skill in the art,” from whose vantage point we assess obviousness and claim interpretation. *See In re Rouffet*, 149 F.3d 1350, 1357 (Fed. Cir. 1998). This legal construct “presumes that all prior art references in the field of the invention are available to this hypothetical skilled artisan.” *Id.* (citing *In re Carlson*, 983 F.2d 1032, 1038 (Fed. Cir. 1993)).

Petitioner, supported by Dr. Jacobson’s testimony, proposes that a person of ordinary skill in the art at the time of the invention “would have had a bachelor’s degree in computer science, 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 (citing Ex. 1003 ¶ 33). Patent Owner cites to the ’1154 decision, and that panel’s assertion regarding the level of ordinary skill in the art, stating it is the level that it adopts. PO Resp. 6 (citing Ex. 2012 ¶¶ 25–30). Reviewing both statements, we determine no substantive differences between the two, and continue to adopt the level adopted in the Decision to Institute. *See* Dec. to Inst. 12–13.

B. Claim Construction

In an *inter partes* review, we construe a patent claim “using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b).” 37 C.F.R. § 42.100(b). In applying such standard, claim terms are generally given their ordinary and customary

meaning, as would be understood by a person of ordinary skill in the art, at the time of the effective filing date of the patent application and in the context of the entire patent disclosure. *Phillips*, 415 F.3d at 1312–13. “In determining the meaning of the disputed claim limitation, we look 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).

Patent Owner argues that the preambles of independent claims 1, 8, and 15 should be found to be limiting because those preambles provide antecedent basis for multiple limitations recited later in the claims, and because the limitations in the preambles “give life, meaning, and vitality” to the claims. PO Resp. 6–7 (citing Ex. 2012 ¶¶ 38–39; *Catalina Mktg. Int’l, Inc. v. Coolsavings.com, Inc.*, 289 F.3d 801, 808 (Fed. Cir. 2002)). Per the Institution Decision, we continue to find the preambles of the independent claims to be limiting. *See* Dec. to Inst. 14.

Patent Owner also takes exception to an implicit claim construction determined in the Institution Decision, namely a construction of “receiving . . . a dynamic security policy comprising a first set of packet filtering rules.” PO Resp. 8 (citing Dec. to Inst. 25). Patent Owner asserts that the limitation should be construed as “an initial dynamic security policy, including a first set of rules, that is received by the PSG from the SPMS.” *Id.* (citing Ex. 2012 ¶¶ 40–41). Patent Owner argues that we interpreted the claim term as “an ‘initial ruleset’ created by the PSG with a ‘first set of packet filtering rules’ providing updates, received from the SPMS,” which Patent Owner argues to be incorrect. *Id.*

Patent Owner also argues that “[w]here the inventors intended to specify ‘an update’ they did so expressly by reciting ‘receiving, by the packet security gateway . . . **update[s]**’ for the received dynamic security policy and its first set of rules.” PO Resp. 9 (emphasis in original). Patent Owner also argues that its interpretation of the claim language is supported by the specification that describes the initial dynamic security policy and first set of rules originating from the SPMS. *Id.* at 9–10 (citing Ex. 1001, 14:13–20, 28–31). Based on this, Patent Owner argues that the claim language does not encompass nor do any embodiments illustrate the PSG first creating “an initial ruleset” and then separately receiving “an update” in the form of a “first set of packet filtering rules. *Id.* at 10.

Petitioner disagrees, arguing that Patent Owner’s proposed construction seeks to add an additional limitation that the “first set of packet filtering rules” be limited to an initial dynamic security policy. Pet. Reply 20. Limitation [1.1] recites “receiving . . . a dynamic security policy comprising a first set of packet filtering rules,” without any restriction that the “first set of packet filtering rules” be limited to an initial dynamic security policy. *Id.* Petitioner also asserts that “first” need not connote “initial,” as asserted by Patent Owner, but can be understood as “a common patent-law convention to distinguish between repeated instances of an element or limitation.” *Id.* at 21 (quoting *3M Innovative Props. Co. v. Avery Dennison Corp.*, 350 F.3d 1365, 1371 (Fed. Cir. 2003)).

Patent Owner responds that the intrinsic record does not support Petitioner’s reading of the claims, that would allow for the dynamic security policy to be generated at the PSG rather than being received at the PSG from the SPMS. PO Sur-reply 21. Patent Owner also argues that persons of ordinary skill in the art would have recognized that the “first set of packet

filtering rules” is the “initial” rule set because it is received as part of the dynamic security policy, and the use of the word “initial” signifies that the dynamic security policy can be updated at a later time. *Id.*

We are not persuaded by Patent Owner’s arguments. A review of the ’266 Patent does not show the disclosure of “initial dynamic security policy,” or equivalent, and the cited sections (Ex. 1001, 14:13–31) also do not discuss such extra limitations. The ’266 Patent provides:

Security policy management server **120** may be configured to communicate *one or more* dynamic security policies to one or more packet security gateways within network environment **100**. ... For example, security policy management server **120** may be configured to communicate one or more dynamic security policies to one or more of packet security gateways **112**, **114**, **116**, and **118** on a periodic basis, under specified network conditions, whenever security policy management server **120** receives a new dynamic security policy, whenever a dynamic security policy stored on security policy management server **120** is changed or altered, or in response to a request from one or more of packet security gateways **112**, **114**, **116**, and **118**.

Ex. 1001, 13:35–50 (emphasis added). Per this disclosure, the PSGs may receive multiple DSPs from the SPMS, with different PSGs receiving different DSPs. This disclosure undercuts the argument that the first set of packet filtering rules needs to be an initial set. We also disagree that this would require the PSGs to produce DSPs; rather, the SPMS would still create and update the DSPs, on an on-going basis, such that a second set can be updated by third set, with that second set being an initial set with respect to the third set, etc.

Additionally, the structure of independent claim 1, for example, is directed to a method of filtering packets, such that the claim may read upon a network environment where the plurality of PSGs already contain a DSP,

prior to the first step of that claim, and a change is made through the application of another DSP with a first set of packet rules, that are subsequently updated. As such, we are unpersuaded that the implicit claim construction determined in the Institution Decision was incorrect and not in keeping with the language of the claim and the scope of the disclosure of the '266 Patent.

Patent Owner also cites claim constructions that have been adopted in previous IPR proceedings (PO Resp. 12–13), but asserts that “these proceedings do not turn on these constructions, and thus these constructions are not necessary. *Id.* (citing *See Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)). We agree with Patent Owner with respect to the additional listed claim limitations and determine that no other claim terms need to be construed expressly for purposes of this Decision.

C. Legal Standards

The question of obviousness is resolved on the basis of underlying factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) objective evidence of nonobviousness. *See Graham*, 383 U.S. at 17. Additionally, the obviousness inquiry typically requires an analysis of “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) (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006) (requiring “articulated reasoning with some rational underpinning to support the legal conclusion of obviousness”)); *see In re Warsaw Orthopedic, Inc.*, 832 F.3d 1327, 1333 (Fed. Cir. 2016) (citing *DyStar Textilfarben GmbH & Co. Deutschland KG v. C. H. Patrick Co.*, 464 F.3d 1356, 1360 (Fed. Cir. 2006)).

An obviousness analysis “need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ.” *KSR*, 550 U.S. at 418; accord *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1259 (Fed. Cir. 2007). Petitioner cannot satisfy its burden of proving obviousness by employing “mere conclusory statements.” *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016). Instead, Petitioner must articulate a reason why a person of ordinary skill in the art would have combined or modified the prior art. *In re NuVasive, Inc.*, 842 F.3d 1376, 1382 (Fed. Cir. 2016).

A reason to combine or modify the prior art may be found explicitly or implicitly in market forces; design incentives; the “interrelated teachings of multiple patents”; “any need or problem known in the field of endeavor at the time of invention and addressed by the patent”; and the background knowledge, creativity, and common sense of the person of ordinary skill. *Perfect Web Techs., Inc. v. InfoUSA, Inc.*, 587 F.3d 1324, 1328–29 (Fed. Cir. 2009) (quoting *KSR*, 550 U.S. at 418–21).

In determining whether a claim is obvious in light of the prior art, when in evidence, we consider any relevant objective evidence of non-obviousness. See *Graham*, 383 U.S. at 17. Notwithstanding what the teachings of the prior art would have suggested to one of ordinary skill in the art at the time of the invention, the totality of the evidence submitted, including objective evidence of non-obviousness, may lead to a conclusion that the challenged claims would not have been obvious to one of ordinary skill. *In re Piasecki*, 745 F.2d 1468, 1471–72 (Fed. Cir. 1984).

We analyze the asserted grounds of unpatentability in accordance with these principles to determine whether Petitioner has met its burden to

establish unpatentability of the challenged claims by a preponderance of the evidence.

D. Obviousness over Law

Petitioner asserts that claim 1–27 are unpatentable over Law. Pet. 12. Petitioner addresses each limitation of claim 1 and provides the testimony of Dr. Jacobson in support of its position with respect to them. Pet. 14–52; Ex. 1003 ¶¶ 59–110. Petitioner also addresses the limitations of independent claims 8, 15, and 21, referencing the analysis of independent claim 1, as well as addressing the subject matter of the challenged, dependent claims. Pet. 52–63.

Patent Owner argues that the challenged claims are patentable over Law based on specific arguments: (1) that Law does not disclose a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected (PO Resp. 17–27; PO Sur-reply 3–10; “entire network interface”); (2) that Law does not disclose applying a first set of filtering rules to all network traffic traversing the boundary (PO Resp. 27–33; PO Sur-reply 10–15; “common set of filtering rules”); (3) that Law does not teach or suggest a security policy management server that automatically creates or alters dynamic security policies (PO Resp. 33–42; PO Sur-reply 15–20; “automatic generation by a server”); and (4) that Law does not teach or suggest receiving a dynamic security policy comprising a first set of rules (PO Resp. 42–53; PO Sur-reply 20–25; “only distributes updates”). All of Patent Owner’s arguments address specific elements of independent claim 1, namely [1.0], [1.1] and [1.3]. Patent Owner does not provide separate arguments with respect to the other independent claims, nor the dependent claims. *See* PO Resp.; PO Sur-reply.

We begin with a discussion of Law, then consider Petitioner's assertions regarding the reference's teachings with respect to independent claim 1, then consider Patent Owner's arguments countering those assertions, based on its specific arguments, and finally address the instant ground with respect to the other independent and dependent claims.

1. Overview of Law

Law is directed to a Unified Threat Management System ("UTMS") for securing network traffic in a process control system. Ex. 1005, codes (54), (57). Law explains that "firewalls typically provide security for process control networks and mitigate the risk of network attacks." *Id.* ¶ 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 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.

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. An exemplary implementation of the system is provided in Figure 3 and is reproduced below:

Law discloses that cyber security risk management firm 305 may distribute rulesets to Law's firewalls over the Internet. *Id.* ¶¶ 66, 88, Fig. 3. In turn, cyber security risk management firm 305 may formulate rulesets based on aggregated threat data 310 from various third-party sources 315, which include cyber-security threat intelligence providers such as “the Vulnerability Research Service (VRS) of Assurent Secure Technologies.” *Id.* ¶ 92. Cyber security risk management firm 305 is a “perpetual service that proactively supplies the UTMS-configured firewalls . . . with” updated “rulesets to meet the latest security threats.” *Id.* ¶¶ 22, 88 (disclosing that “the various rulesets . . . require updates to remain effective against network threats”).

Law also provides its UTMS in the context of protecting a “process control network,” such as a communication network implemented in the context of “process control systems like those used in power generation, chemical, petroleum, or other processes.” Ex. 1005 ¶ 3. Petitioner asserts that persons of ordinary skill in the art would have understood the applicability of Law's UTMS to protecting any network. Pet. 13 (citing Ex. 1003 ¶ 58).

2. Independent Claim 1

a. Petitioner's Assertions

Claim limitation [1.0], the preamble of independent claim 1, is directed to a method of filtering packets. Petitioner asserts that Law discloses the filtering of packets, with Law's firewalls 146a and 146b each corresponding to the claimed “packet security gateways,” and located at the perimeter of a network. Pet. 14 (citing Ex. 1005 ¶ 22, Fig. 1A; Ex. 1003 ¶ 59). Petitioner points to Law's disclosure that “[t]he communication network 150a, 150b may be a local area network (LAN) . . . and may be

implemented using hardwired or wireless technology” including “standard protocols such as Ethernet.” *Id.* at 15 (quoting Ex. 1005 ¶ 55).

Petitioner also asserts that persons of ordinary skill in the art would have understood that Law’s perimeter UTMS firewalls 146a and 146b are gateways, as they are firewalls that separate a LAN (e.g., LANs 150a and 150b) from the Internet. Pet. 17 (citing Ex. 1003 ¶ 61). In addition, the firewalls are configured to perform one or more operations on a packet. *Id.* (citing Ex. 1005 ¶ 103; Ex. 1003 ¶ 61). Petitioner also asserts that firewall 146a provides the entire interface across a boundary of a network protected by the firewall 146a (LAN 150a) and one or more networks other than the network protected by firewall 146a (Internet 155). *Id.* at 18 (citing Ex. 1005, Fig. 1A; Ex. 1003 ¶ 62). In addition, Petitioner asserts that, based on the descriptions in Law, one of ordinary skill in the art would have understood the firewalls to provide the entire interface, because it was acknowledged that any external connection into a process control system network presents a possible point of attack into the system. *Id.* at 19 (citing Ex. 1005 ¶ 10). Petitioner also asserts that Law’s express disclosure of an alternative “bypass” embodiment further confirms that the non-bypass embodiments, such as those illustrated in Figures 1A and 3, necessarily provide the entire interface across the boundary of the network protected by firewalls. *Id.* at 21 (citing Ex. 1003 ¶ 65).

Claim limitation [1.1] is directed to the step of receiving from a security policy management server, external from the network, a first set of packet filtering rules to be applied to all network traffic traversing the boundary. Petitioner asserts that Law’s cyber security risk management firm 305 corresponds to the claimed “security policy management server,” and is located on an external network (i.e., Internet 155), and distributes to Law’s

perimeter UTMS firewalls 146a and 146b a dynamic security policy comprising a first set of packet filtering rules to be applied to all network traffic traversing the boundary between protected network 150 and Internet 155. Pet. 23–24 (citing Ex. 1005 ¶¶ 22, 66, 88, 92, Fig. 3; Ex. 1003 ¶ 69).

Petitioner also asserts that because cyber security risk management firm 305 distributes ruleset 147 to perimeter UTMS firewalls 146a and 146b over the Internet 155 (Ex. 1005 ¶¶ 66, 88), a person of ordinary skill in the art would have understood that firm 305 necessarily comprises a server. Pet. 26–27 (citing Ex. 1003 ¶ 71). In addition, although Law details that specific rulesets correspond to specific firewalls, persons of ordinary skill in the art would have understood that firewalls 146a and 146b may apply the same ruleset, which Law also identifies as “ruleset[] 147.” *Id.* at 27 (citing Ex. 1005 ¶ 88; Ex. 1003 ¶ 71).

Claim limitation [1.2] details that each packet filtering rule comprises at least one packet matching criterion and a corresponding packet transformation function. Petitioner asserts that each packet filtering rule in ruleset 147 applied by the perimeter UTMS firewalls 146a and 146b comprises at least one packet matching criterion and a corresponding packet transformation function. Pet. 32 (citing Ex. 1005 ¶¶ 52, 91, 102–103, Fig. 13; Ex. 1003 ¶ 81).

Claim limitation [1.3] details that the first packet filtering rules include packet matching criteria corresponding to one or more network addresses and were automatically created or altered by the SPMS based on aggregated malicious traffic information. Petitioner asserts that Law details that each packet filtering rule in ruleset 147 applied by the perimeter UTMS firewalls 146a and 146b comprises packet matching criteria. Pet. 35–36 (citing Ex. 1005 ¶¶ 102–103; Ex. 1003 ¶ 86).

Petitioner also asserts that Law discloses rules that were automatically created by the security policy management server, and that persons of ordinary skill in the art would have found it obvious for at least a portion of the constructed rules to have been constructed automatically. Pet. 36–38 (citing Ex. 1003 ¶ 89). Additionally, Petitioner asserts that Law expressly discloses automatically updating (i.e., altering) rulesets in response to detected conditions. *Id.* at 38–39 (citing Ex. 1005 ¶¶ 83, 88–89).

Claim limitation [1.4] details that packet filtering is performed on a packet by packet basis on a first portion of packets based on the first set of packet filtering rules by performing at least one packet transformation function specified by the filtering rules. Petitioner asserts that Law discloses that perimeter UTMS firewalls 146a and 146b perform, on a packet by packet basis, packet filtering on a first portion of packets corresponding to network traffic traversing the boundary via UTMS firewalls 146a and 146b 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 in Figure 13, including actions such as block, accept, re-route, and notify) on the first portion of packets. Pet. 48 (citing Ex. 1005 ¶¶ 52, 59, 91, 102–103, Figs. 1A, 3, 13; Ex. 1003 ¶ 100).

Claim limitation [1.5] details that the packet security gateway subsequently receives an updated second set of packet filtering rules, updating one or more of the first packet filtering rules based on updated malicious traffic information received from the third party malicious host tracker service. Petitioner asserts that Law discloses that perimeter UTMS firewalls 146a and 146b receive from cyber security risk management firm 305 a dynamic security policy comprising a first set of packet filtering rules,

ruleset 147, where the ruleset 147 includes one or more rules created or altered by cyber security risk management firm 305 based on aggregated malicious traffic information (threat data 310) received from at least one third party malicious host tracker service (sources 315, including threat-provider services from Assurent, Secunia, and Carnegie Mellon). Pet. 49 (citing Ex. 1005 ¶¶ 22, 51–52, 59, 66, 83, 88–89, 91–92, 102–103; *id.*, Figs. 1A, 3, 13; Ex. 1003 ¶ 104).

Petitioner also asserts that Law discloses or renders obvious that perimeter UTMS firewalls 146a and 146b receive a second, updated ruleset from cyber security risk management firm 305 that comprises an update to the one or more packet filtering rules in first ruleset 147 created or altered by the cyber security risk management firm 305 based on updated malicious traffic information received from at least one of the sources 315, including threat-provider services from Assurent, Secunia, and Carnegie Mellon. Pet. 50 (citing Ex. 1003 ¶ 105).

Claim limitation [1.6] details that packet filtering is performed on a packet-by-packet basis on a second portion of packets based on the updated second set of packet filtering rules by performing at least one packet transformation function specified by the filtering rules. Petitioner asserts that Law discloses receiving an updated second set of packet filtering rules and that the second set would be used to perform packet filtering, per the analysis of limitation [1.4], discussed above. Pet. 51–52 (citing Ex. 1005 ¶¶ 52, 59, 66, 83, 88–89, 91, 102–103, Figs. 1A, 3, 13; Ex. 1003 ¶ 109).

b. Patent Owner's Arguments

1) "entire network interface"

Patent Owner argues that Law does not disclose a plurality of packet security gateways that collectively provide an entire interface across a

boundary of a network protected. PO Resp. 17–27; PO Sur-reply 3–10. Patent Owner argues that the challenged claims are patentable because Petitioner has not demonstrated that Law’s networks 150a and 150b are a single “network protected” by a plurality of PSGs. PO Resp. 18; PO Sur-reply 7. Patent Owner argues that Law does not refer to 150 as a combination of the networks 150a and 150b and only uses 150 when there is only one relevant network and/or it is not necessary to distinguish between the separate networks. PO Resp. 18 (citing Ex. 2012 ¶ 57); *see also id.* at 19–25. Patent Owner also argues that the “only support for Petitioner’s argument that networks 150a and 150b are joined together to form a single network 150 is Dr. Jacobson’s conclusory testimony, which merely repeats, verbatim, the conclusory interpretation of Law’s teachings for which it is offered to support.” *Id.* at 22–23 (citing Ex. 2014, 51:3–21). Additionally, Patent Owner argues that Law explicitly discloses that perimeter devices, such as network access device 149c, are outside of networks 150a and 150b. *Id.* at 24–25 (citing Ex. 1005 ¶¶ 51, 91; Ex. 2012 ¶ 63); PO Sur-reply 4–5.

Petitioner responds that Figure 3 of Law shows that network access device 149c may optionally be provided to join LANs 150a and 150b together into a single network 150, such that firewalls 146a and 146b collectively provide the entire interface across the boundary of the network protected. Pet. Reply 4–6 (citing Ex. 1005 ¶ 51, Figs. 1A, 3). Petitioner also points out that Law uses the terms “networks 150a and 150b” and “network 150” in the same sentence, making clear that “network 150” refers to the single network formed from the combination of sub-networks. *Id.* at 6–7 (citing Ex. 1014 ¶ 10). Petitioner also argues that network access device 149c directly connects subnetworks 150a and 150b to provide communications between them, to which Petitioner asserts that Patent

Owner's expert (Dr. Goodrich) agreed. *Id.* at 8–10 (citing Ex. 1005 ¶ 51; Ex. 1003 ¶ 64; Ex. 1014 ¶ 13; Ex. 1015, 48:8–49:10).

Patent Owner responds that Dr. Goodrich testified to the opposite, testifying that subnetworks 150a and 150b would not have been considered a combined network because network access device 149c has rulesets associated with it for communications and the networks included specialized devices that performed specialized functionalities. PO Sur-reply 5–6 (citing Ex. 1015, 49:11–19, 49:21–51:1, 51:8–14). Patent Owner also traverses Petitioner's interpretation of the sections of Law cited to support a single network 150. PO Sur-reply 7–9.

We continue to be persuaded that one of ordinary skill in the art would have regarded the paired LANs of Law as viewable as a single network, when compared to the Internet, and each firewall would provide protections to the single network. *See* Dec. to Inst. 20–21. Law makes clear that in one of its embodiments, i.e., an “alternative embodiment,” there is “a *cross-system connection* between sub-systems 105a and 105b including a UTMS-configured network access device 149c that *may or may not* include a ruleset.” Ex. 1005 ¶ 51 (emphases added). As illustrated in Figure 3 of Law, the Internet 155 is connected to the paired LANs only through firewalls 146a, 146b. From the vantage point of the Internet, the sub-systems appear as one and are connected to each other through network access device 149c. As noted in the quoted section of Law, the network access device 149c may or may not include a ruleset, with the latter embodiment having a network access device 149c that does not play a role in packet handling, i.e., being without a ruleset to guide such processing. In such an embodiment, i.e., without a ruleset, network access device 149c

would only act to direct communications between sub-systems 105a and 105b, as illustrated in Figure 3 of Law.

In addition to an exercise in line drawing, that is making a determination what constitutes inside and outside of a network, we also have dueling interpretations of how Law would have been viewed by those of ordinary skill in the art. Dr. Goodrich, Patent Owner's declarant, testifies that such a person "reading Law would understand that Law never uses the term 'network 150' to refer to any combination of networks 150a and 150b," and that "Law only uses that term when there is only one relevant network and/or it is not necessary to distinguish between networks 150a and 150b." Ex. 2012 ¶ 57. Dr. Jacobson, Petitioner's declarant, testifies that "Law explicitly discloses, and at the very least renders obvious, that one of ordinary skill in the art would [have] understood that LANs 150a and 150b are joined together to form a single network 150 protected by perimeter UTMS firewalls 146a and 146b, as shown in Fig. 3." Ex. 1014 ¶ 8; *see also id.* ¶ 15.

We find Dr. Jacobson's testimony more persuasive in view of Law Figure 3, and the supporting disclosure, that make clear that the sub-systems may be connected, with the firewalls 146a, 146b being the only interfaces with the Internet. We are also persuaded that one of ordinary skill in the art reviewing Law would have interpreted "network 150" to connote a combination of networks 150a, 150b collectively, as that is the clearest inference because no element is identified by "150" in any of the drawings, and it is clear that "150" is not a typographical error, where only one of the sub-systems was intended. One of ordinary skill in the art reviewing Law would have encountered "network 150" in its disclosure and would have naturally interpreted it as a combination of the sub-networks. "The use of

patents as references is not limited to what the patentees describe as their own inventions or to the problems with which they are concerned. They are part of the literature of the art, relevant for all they contain.” *In re Heck*, 699 F.2d 1331, 1332–33 (Fed. Cir. 1983) (quoting *In re Lemelson*, 397 F.2d 1006, 1009 (CCPA 1968)).

2) “*common set of filtering rules*”

Patent Owner argues that Law does not disclose applying a first set of filtering rules to all network traffic traversing the boundary. PO Resp. 27–33; PO Sur-reply 10–15. Patent Owner argues that Law’s “global” ruleset is not one that is applied to all traffic traversing the boundaries of a protected network, but rather, that each firewall, 146a and 146b, has different sets of global rules for access to devices in each subsystem. PO Resp. 28; PO Sur-reply 10–11. Additionally, Patent Owner argues that those global rulesets are unique to the particular devices in the subsystem, with the global ruleset for subsystem 105a would be different from the global ruleset for subsystem 105b. PO Resp. 28 (citing Ex. 2012 ¶ 69). Patent Owner also argues that Petitioner’s argument that Law’s firewalls would have applied the same global set of rules for each subsystem “ignores Law’s very contribution to the art and suggests, without evidence, that Law’s subsystems (105a, 105b) and networks (150a, 150b) necessarily would have been identical.” *Id.* at 29 (citing Ex. 2012 ¶ 71). In addition, Patent Owner argues that Law discloses that network traffic traverses the perimeter of the network at the network access device 149c, with these devices applying their own set of rules. *Id.* at 31–33 (citing Ex. 1005 ¶¶ 51–52, 92, Fig. 3; Ex. 2012 ¶¶ 74–75).

Petitioner responds that Law’s description of the ruleset implemented by both firewalls as “ruleset[] 147,” such that both firewalls apply the same ruleset. Pet. Reply 11 (citing Ex. 1005 ¶¶ 51, 88; Ex. 1014 ¶ 21). Petitioner

also quotes Law as providing that “the rulesets 147 and 151 may include a global set of rules for access to any device within the subsystems 105a, 105b,” thereby disclosing single set of global rules for both subsystems. *Id.* (quoting Ex. 1005 ¶ 51) (emphasis omitted). Petitioner also argues that Patent Owner’s arguments in this section are predicated on Patent Owner’s argument that subnetworks 150a and 150b are not joined together as a single network, as discussed above. *Id.* at 12.

Patent Owner responds that Petitioner’s argument that firewalls 146a and 146b would apply the same set of rules to traffic is wrong because Law discloses that each subsystem has its own “unique and device specific features” with “rules and/or access privileges for each of the devices.” PO Sur-reply 11 (citing Ex. 1005 ¶¶ 18–19). Patent Owner also responds that the testimony of Dr. Goodrich, Patent Owner’s declarant, with respect to recitations of ruleset 147 referring to generically either the ruleset 147a or 147b, is unrebutted, and that Petitioner is merely citing to Dr. Jacobson’s reply declaration, which provides no additional reasoning of analysis. PO Sur-reply 12–13 (citing Ex. 1015, 9:22–25, 11:16–12:23).

We continue to be persuaded that one of ordinary skill in the art would have understood that perimeter UTMS firewalls 146a and 146b would have applied ruleset 147 to all network traffic passing therethrough. *See* Dec. to Inst. 22–23. We find persuasive the disclosure of Law that “the various rulesets 147, 148, 151, 153, ... [are distributed] to the UTMS-configured firewalls 146a [and] 146b.” Ex. 1005 ¶ 88. With respect to Patent Owner’s citation of paragraphs 18 and 19 of Law, we note that while Law discloses different rules for different devices, that section of Law is directed to a “Description of the Related Art,” Law does not specify that the rulesets applied in its embodiments actually differentiate between sub-

sections 150a, 150b. We remain persuaded that Law is clear that “the rulesets 147 and 151 may include a global set of rules for access to any device within subsystems 105a, 105b.” Ex. 1005 ¶ 51. We are persuaded that one of ordinary skill in the art, in view of Law, would have applied the ruleset 147 to all incoming traffic bound for devices in the subsystems.

As discussed above, we have determined that one embodiment of Law discloses that network access device 149c need not employ its own ruleset, and would only act to direct communications between sub-systems 105a and 105b. Although we agree that in an alternate embodiment, with network access device 149c coordinating network traffic with its own ruleset, Law might not subject all traffic to a first set of filtering rules, we are not persuaded that the Petition is relying on such an alternate embodiment. As such, we do not find Patent Owner’s latter arguments to be persuasive.

3) *“automatic generation by a server”*

Patent Owner argues that Law does not teach or suggest a security policy management server that automatically creates or alters dynamic security policies. PO Resp. 33–42; PO Sur-reply 15–20. Patent Owner argues that Law does not disclose or render obvious the firm 305 automatically generating rulesets because firm 305 would be a company that includes IT personnel and other infrastructure components. PO Resp. 33–34; PO Sur-reply 15. Because of this, Patent Owner argues that skilled artisans reading Law would have understood that updating rulesets at third-party firm 305, a commercial business, necessarily requires IT personnel involvement. PO Resp. 35 (citing Ex. 2012 ¶ 82). Patent Owner also argues that while UTMS-configured devices in Law can receive from firm 305 the “update data” on a continuous basis, that does not mean that the “update

data” was automatically generated. *Id.* at 35 (citing Ex. 1005 ¶¶ 30, 66, Fig. 3; Ex. 2012 ¶ 84).

Patent Owner also argues that IT personnel are still required to manually update the rulesets of process control systems, such that skilled artisans would not have found it obvious to incorporate automatic generation techniques to firm 305. *Id.* at 38–39. Additionally, Patent Owner argues that Petitioner cannot show that a person of ordinary skill in the art would have understood that automatic generation techniques could be implemented in third-party firm 305, as the firm is not simply a server but a service that leverages IT personnel and other infrastructure components to manage updates for Law’s process control systems. *Id.* at 41 (citing Ex. 2012 ¶ 90).

Petitioner responds that firm 305 comprises a security policy management server, as it asserted in its Petition. Pet. Reply 14 (citing Pet. 23–27; Ex. 1003 ¶¶ 69–71). Additionally, Petitioner asserts that Patent Owner’s argument, that the firm 305 could have included IT personnel overseeing the distributed rulesets, does not negate Law’s teachings that rules within the constructed rulesets may have been created automatically. *Id.* at 16 (citing Ex. 1014 ¶ 34). Petitioner also argues that the claim language only requires that “one or more” rules of the set of packet filtering rules have been automatically created or altered by the SPMS, and that Dr. Goodrich admitted that so long as one or more rules in the rulesets distributed by firm 305 were automatically created or altered, the claim language would be satisfied even if a security policy is subsequently modified by a person. *Id.* (citing Ex. 1015, 75:14–76:16). Lastly, Petitioner asserts that Patent Owner relies extensively on background paragraph 16 of Law for its assertions that firm 305 requires IT personnel to generate rulesets, but Law describes that having IT personnel being required to

update the ruleset is a disadvantage of the prior art to be avoided, which is the opposite of Patent Owner's narrative. *Id.* at 17–19 (citing PO Resp. 35, 37, 41; Ex. 1005 ¶ 16).

Patent Owner responds that firm 305 is not a server, and the claims require a server to perform certain functionalities, and that Petitioner has not identified any such server. PO Sur-reply 15–16. Patent Owner also argues that Law does not disclose automatically creating or altering rulesets, and it does not disclose any methods that would or even could forego the required manual input of IT personnel. *Id.* at 17–18. In addition, Patent Owner argues that Petitioner's reliance on alleged state-of-the-art techniques is unavailing because Law explicitly explains how and why IT personnel must be involved in managing access to the process control network. *Id.* at 18–19.

We continue to be persuaded that one of ordinary skill in the art would have understood that Law expressly discloses automatically updating (i.e., altering) rulesets in response to detected conditions, and that those updated rulesets would have been distributed for use. *See* Dec. to Inst. 24–25.

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 ¶¶ 70–71. 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 ¶¶ 70–72.

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 ¶ 71. Dr. Jacobson testifies that firm 305 includes “IT infrastructure” with “computers” having “processing power” and “storage.” Ex. 2014, 37:2–38:10. 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 ¶ 74.

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 ¶ 70; Ex. 1005 ¶¶ 88, 90, Fig. 3; PO Resp. 33–42; PO Sur-reply 15–20.

4) “*only distributes updates*”

Patent Owner argues that Law does not teach or suggest receiving a dynamic security policy comprising a first set of rules. PO Resp. 42–53; PO Sur-reply 20–25. This is based, in part, on Patent Owner’s interpretation of “receiving . . . a dynamic security policy comprising a first set of packet filtering rules,” discussed above. *See supra* II.B. Patent Owner argues that initial rulesets are created by operators within the process control system, and that Petitioner acknowledges that Figure 3 of Law is directed to firm 305 and its remediation service of updating rulesets, such that only updates are distributed. PO Resp. 42–49. Petitioner responds that we should continue to reject Patent Owner’s claim construction position, and that even under that construction, Law still renders obvious the receiving limitation. Pet. Reply 19–23. Patent Owner responds that firm 305 distributes only updates to the operator-created rulesets that were created on the PSG, and does not meet the language of the challenged claims. PO Sur-reply 22–24.

We continue to not be persuaded that the received packet filtering rules (limitation [1.1]) need to be the first set of rules to be applied or modified by the PSGs. *See* Dec. to Inst. 25. This comports with the prior discussion of this limitation in the claim construction section. *See supra* II.B. We continue to determine that Law allows for an initial ruleset to be created by operators, and the claimed “first set of packet filtering rules” to be an update to that initial ruleset, received from firm 305. We continue to be persuaded that Law expressly discloses automatically updating (i.e., altering) rulesets in response to detected conditions, and that those updated rulesets would have been distributed for use.

c. Conclusion Regarding Obviousness of Claim 1

Based on the record presented and for the foregoing reasons, we determine that Petitioner has demonstrated that Law teaches or suggests all the limitations of independent claim 1 and conclude that a preponderance of the evidence establishes that claim 1 is unpatentable as being obvious over Law.

3. Independent Claims 8, 15, and 21

As noted above, Petitioner also addresses the limitations of independent claims 8, 15, and 21, referencing the analysis of independent claim 1. Pet. 52–56. Patent Owner does not provide separate arguments with respect to the elements of independent claims 8, 15, and 21, except with respect to similar elements argued with respect to claim 1. *See* PO Resp. 53–54; PO Sur-reply 25. We find persuasive Petitioner’s arguments regarding the correspondences of elements of independent claims 8, 15, and 21, with those of independent claim 1. Pet. 52–56.

Thus, for the same reasons discussed above with respect to claim 1, based on the current record, Petitioner has demonstrated that Law teaches or suggests of all the limitations of independent claims 8, 15, and 21, and conclude that a preponderance of the evidence establishes that claims 8, 15, and 21 are unpatentable as being obvious over Law.

4. Dependent Claims 2–7, 9–14, 16–20, and 22–27

Petitioner asserts that dependent claims dependent claims 2–7, 9–14, 16–20, and 22–27 are obvious under 35 U.S.C. § 103(a) over Law. *See* Pet. 57–63. We address these dependent claims in groups, per the discussions in the Petition.

With respect to dependent claims 2, 9, 16, and 22, each of those claims recites, in part, that the at least one packet matching criterion is one or more network addresses. Petitioner explains that Law discloses that each of its packet filtering rules includes from-address and to-address columns, which may identify one or more network addresses. Pet. 57 (citing Ex. 1005 ¶¶ 102–103, Fig. 13; Ex. 1003 ¶ 137). We agree with Petitioner and determine that Law also teaches or suggests the limitations of dependent claims 2, 9, 16, and 22.

With respect to dependent claims 3, 10, 17, and 23, each of those claims recites, in part, that the third party malicious host tracker service is a subscription service that aggregates information associated with malicious network traffic. Petitioner explains that the sources 315 in Law that provide threat data 310, including Assurent, Secunia, and Carnegie Mellon, correspond to a third party malicious host tracker services, and that it would have been obvious to offer such services through a subscription service. Pet. 58 (citing Ex. 1005 ¶¶ 88, 92; Ex. 1003 ¶ 141). We agree with Petitioner and determine that Law also teaches or suggests the limitations of dependent claims 3, 10, 17, and 23.

With respect to dependent claims 4, 11, and 24, each of those claims recites, in part, that the one or more network addresses were associated with malicious network traffic by a subscription service. Petitioner explains that the sources 315 in Law provide threat data 310 that would have included one or more network addresses, such as IP addresses, associated with malicious network traffic, and per the discussion in the previous paragraph, could be through a subscription service. Pet. 60 (citing Ex. 1005 ¶ 92; Ex. 1003 ¶¶ 143–145). We agree with Petitioner and determine that Law also teaches or suggests the limitations of dependent claims 4, 11, and 24.

With respect to dependent claims 5, 12, 18, and 25, each of those claims recites, in part, that at least one packet transformation is a network protective action. Petitioner explains that Law discloses a blocking action that would constitute a network protective action. Pet. 60 (citing Ex. 1005 ¶¶ 91, 102; Ex. 1003 ¶ 147). We agree with Petitioner and determine that Law also teaches or suggests the limitations of dependent claims 5, 12, 18, and 25.

With respect to dependent claims 6, 13, 19, and 26, each of those claims recites, in part, that the packets are received in a network layer transparent manner and the packet transformation function acts at the network level. Petitioner asserts that “while Law discloses addressing schemes at the network layer (e.g., by using IP addresses), Law also discloses other addressing schemes, such as hardware-specific addressing, which a [person of ordinary skill in the art] would have understood may not have been at the network layer.” Pet. 61 (citing Ex. 1005 ¶ 103; Ex. 1003 ¶ 148). Additionally, Petitioner asserts that Law discloses that the conditions used to identify packets to block may include IP addresses, which ordinarily skilled artisans would have recognized as blocking packets at the network layer. *Id.* at 62 (citing Ex. 1005 ¶¶ 102–104, Fig. 13, 102; Ex. 1003 ¶ 151). We agree with Petitioner and determine that Law also teaches or suggests the limitations of dependent claims 6, 13, 19, and 26.

With respect to dependent claims 7, 14, 20, and 27, each of those claims recites, in part, that the packet transformation function is other than forwarding or dropping of corresponding packets. Petitioner explains that Law discloses that operations performed on packets include, in addition to forwarding and blocking, other operations that “notify” and “re-route.” Pet. 62 (citing Ex. 1005 ¶ 103). We agree with Petitioner and determine that

Law also teaches or suggests the limitations of dependent claims 7, 14, 20, and 27.

Patent Owner does not provide separate arguments with respect to the elements of the dependent claims, except with respect to elements argued with respect to claim 1. *See generally* PO Resp. As such, we conclude that Petitioner has demonstrated that Law teaches or suggests all the limitations of claims 2–7, 9–14, 16–20, and 22–27, and that a preponderance of the evidence establishes that claims 2–7, 9–14, 16–20, and 22–27 are unpatentable as being obvious over Law.

E. Petitioner’s Other Patentability Challenges

As noted above, Petitioner contends that claims 1–27 are unpatentable under § 103(a) as obvious over Law and Wood, that claims 6, 13, 19, and 26 are unpatentable under § 103(a) as obvious over Law and Jungck, and that claims 6, 13, 19, and 26 are unpatentable under § 103(a) as obvious over Law, Wood, and Jungck. *See* Pet. 63–70; *supra* § I.F.

The challenge based on Law alone resolves the patentability questions for all challenged claims. *See supra* §§ II.D.2–4. Additionally, we determine that the consideration of additional references, such as Wood and Jungck, is not necessary to demonstrate the obviousness of claims 1–27. Hence, we need not reach the remaining challenges. *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”).

III. CONCLUSION⁶

Having reviewed all the evidence and arguments of record, we determine that Petitioner has demonstrated by a preponderance of the evidence that claims 1–27 of the '266 Patent are unpatentable. In summary:

Claims	35 U.S.C. §	Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1–27	103(a)	Law	1–27	
1–24	103(a)	Law, Wood ⁷		
6, 13, 19, 26	103(a)	Law, Jungck ⁷		
6, 13, 19, 26	103(a)	Law, Wood, Jungck ⁷		
Overall Outcome			1–27	

IV. ORDER

In consideration of the above it is:

ORDERED that claims 1–27 of the '266 Patent are unpatentable; and

FURTHER ORDERED that, because this is a Final Written Decision, 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.

⁶ Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner's attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. See 84 Fed. Reg. 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).

⁷ In view of our determination that claims 1–27 are unpatentable under § 103(a) as obvious over Law, we do not reach this challenge to patentability. See *supra* §§ II.D–II.E.

IPR2023-00445
Patent 10,785,266 B2

FOR PETITIONER (Keysight Technologies):

Gerard 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 PETITIONER (Palo Alto Networks):

James L. Davis, Jr.
ROPES & GRAY LLP
james.l.davis@ropesgray.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 Wright
Scott M. Kelly
John. R. Hutchins
BANNER & WITCOFF, LTD.
bwright@bannerwitcoff.com
skelly@bannerwitcoff.com
jhutchins@bannerwitcoff.com