

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KEYSIGHT TECHNOLOGIES, INC.
Petitioner,

v.

CENTRIPETAL NETWORKS, LLC,
Patent Owner.

Case IPR2023-00445
Patent No. 10,785,266

PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. THE ’266 PATENT OVERVIEW	3
III. LEVEL OF ORDINARY SKILL IN THE ART	6
IV. CLAIM CONSTRUCTION	6
A. The Preambles of Independent Claims 1, 8, and 15 Are Limiting	6
B. Receiving a Dynamic Security Policy Comprising a First Set of Rules (All Challenged Claims)	8
C. Other Constructions.....	12
V. OVERVIEW OF THE REFERENCES.....	13
A. The Law Reference	13
B. The Wood Reference.....	17
VI. THE CHALLENGED CLAIMS ARE PATENTABLE	17
A. Ground 1: Claims 1-27 Are Patentable Over Law	17
1. Law Does Not Disclose “a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected” (Independent Claims 1, 8, 15).....	17
a. Law’s “Network 150” Does Not Refer to a Combination of Networks 150a and 150b.....	19
b. Petitioner’s Expanded Number of Firewalls Theory Lacks Sufficient Rationale and Succumbs to the Same Network 150 Deficiencies	26

2.	Law Does Not Disclose Applying “a first set of filtering rules” to “all network traversing the boundary” (Independent Claims 1, 8, 15).....	27
a.	Each firewall has a unique set of global rules to protect their respective network and the devices within that network.....	28
b.	Law’s Internet-networks and network-network communication paths are subject to the application of different rules	31
3.	Law Does Not Disclose Nor Render Obvious a Security Policy Management Server That Automatically Creates or Alters Dynamic Security Policies.....	33
a.	Law does not disclose the automatic generation of rulesets by firm 305	34
b.	Skilled artisans would not have found it obvious to incorporate automatic generation techniques in firm 305 because IT personnel are required for the updates	38
4.	Law Does Not Teach or Suggest the “Receiving a Dynamic Security Policy Comprising a First Set of Rules” Limitation.....	42
a.	Law’s operators create initial rulesets with firm 305 only distributing updates to the operator-created initial rulesets.....	43
b.	Petitioner’s evidence and rationale show that firm 305 distributes only updates to the operator-created initial rulesets.....	47
c.	The ’474 Institution Decision’s interpretation of Law finds no support from the record evidence.....	49
B.	Ground 2: Claims 1-24 are Patentable Over Law in View of Wood	53

C.	Ground 3: Claims 6, 13, 19, and 26 are Patentable Over Law in View of Jungck.....	53
D.	Ground 4: Claims 6, 13, 19, and 26 are Patentable Over Law in View of Wood and Jungck.....	54
VII.	CONCLUSION.....	54

TABLE OF AUTHORITIES

	<u>Page(s)</u>
Cases	
<i>ACTV, Inc. v. Walt Disney Co.</i> , 346 F.3d 1082 (Fed. Cir. 2003)	8
<i>Apple Comput., Inc. v. Articulate Sys., Inc.</i> , 234 F.3d 14 (Fed. Cir. 2000)	11
<i>Ariosa Diagnostics v. Verinata Health, Inc.</i> , 805 F.3d 1359 (Fed. Cir. 2015)	38
<i>Banyan Licensing, L.C. v. Orthosupport Int'l, Inc.</i> , 34 F. App'x 696 (Fed. Cir. 2002)	11
<i>Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve, Inc.</i> , 796 F.2d 443 (Fed. Cir. 1986)	30
<i>Catalina Mktg. Int'l, Inc. v. Coolsavings.com, Inc.</i> , 289 F.3d 801 (Fed. Cir. 2002)	7
<i>Chef Am., Inc. v. Lamb-Weston, Inc.</i> , 358 F.3d 1371 (Fed. Cir. 2004)	11
<i>Chemours Co. FC, LLC v. Daikin Indus., Ltd.</i> , 4 F.4th 1370 (Fed. Cir. 2021)	39
<i>Hamilton Beach Brands, Inc. v. f'real Foods, LLC</i> , 908 F.3d 1328 (Fed. Cir. 2018.,)	8
<i>IP Innovation, L.L.C. v. eCollege.com</i> , 156 F. App'x 317 (Fed. Cir. 2005)	27
<i>Keysight Techs., Inc. v. Centripetal Networks, LLC</i> , No. IPR2023-00448, Paper 7 (P.T.A.B. July 24, 2023)	<i>passim</i>
<i>In re Nuvasive, Inc.</i> , 842 F.3d 1376 (Fed. Cir. 2016)	26
<i>Randall Mfg. v. Rea</i> , 733 F.3d 1355 (Fed. Cir. 2013)	40

<i>TQ Delta, LLC v. Cisco Sys., Inc.</i> , 942 F.3d 1352 (Fed. Cir. 2019)	25
<i>Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.</i> , 200 F.3d 795 (Fed. Cir. 1999)	13
<i>In re Wesslau</i> , 353 F.2d 238 (CCPA 1965)	30
<i>Xerox Corp. v. Bytemark, Inc.</i> , No. IPR2022-00624, Paper 9 (P.T.A.B. Aug. 24, 2022)	21

PATENT OWNER'S EXHIBIT LIST

Exhibit	Description
2001	Notice of Intervention by Cisco Systems GmbH in European Patent Office proceedings for EP3550795, dated May 23, 2022
2002	Patent Owner's Response in European Patent Office proceedings for EP3550795, dated September 30, 2022
2003	Preliminary Opinion in European Patent Office proceedings for EP3550795, dated January 9, 2023
2004	Decision Denying Institution, <i>Palo Alto Networks, Inc. v. Centripetal Networks, Inc.</i> , No. IPR2021-01154, Paper 11 (P.T.A.B. Jan. 24, 2022)
2005	Intervention by Keysight Technologies Deutschland GmbH in European Patent Office proceedings for EP3550795, dated May 27, 2022
2006	Correspondence from Patent Owner to European Patent Office, dated October 7, 2022, enclosing Patent Owner's submission from September 30, 2022
2007	Patent Owner's Preliminary Response, <i>Palo Alto Networks, Inc. v. Centripetal Networks, Inc.</i> , No. IPR2021-01154 (P.T.A.B. Oct. 25, 2021)
2008	Patent Owner's Preliminary Sur-Reply, <i>Palo Alto Networks, Inc. v. Centripetal Networks, Inc.</i> , No. IPR2021-01154 (P.T.A.B. Dec. 7, 2021)
2009	Law Insider Webpage – Network Access Device definition, available from https://www.lawinsider.com/dictionary/network-access-device , dated April 26, 2023
2010	Excerpts from Microsoft Computer Dictionary - "Internet" (5th ed. 2002)
2011	Excerpts from The American Heritage Dictionary - "Firm" (4th ed. 2001)

Exhibit	Description
2012	Declaration of Dr. Michael T. Goodrich in Support of Patent Owner's Response
2013	IBM Webpage – Centripetal Networks X-Force Security, available from https://www.ibm.com/case-studies/centripetal-networks-x-force-security , dated April 12, 2022
2014	Transcript of Deposition of Douglas Jacobson, Ph.D., <i>Keysight Technologies, Inc. v. Centripetal Networks, LLC</i> , Nos. IPR2023-00445, IPR2023-00448, taken on October 2, 2023
2015	Portnox Webpage – What is a Network Access Device (NAD)?, available from https://www.portnox.com/cybersecurity-101/network-access-device-nad/ , dated October 15, 2023
2016	RESERVED
2017	Memorandum Opinion and Order, <i>Centripetal Networks, LLC, v. Palo Alto Networks, Inc.</i> , No. 21-cv-00137 (EWH), Dkt. No. 452 (E.D. Va Oct. 11, 2023)

I. INTRODUCTION

The Challenged Claims are patentable because Law (Ex. 1005) does not disclose a “network protected” by “a packet security gateway, of a plurality of packet security gateways that collectively provide an entire interface across a boundary of” the protected network. ’266 Patent (Ex. 1001) at Claims 1, 8, 15. Instead, Law discloses a single firewall protecting a single network, and does not teach that the firewall has the capability of interacting with another firewall to protect a network. Petitioner’s argument that Law teaches an embodiment where LANs 150a and 150b are actually a single network lacks evidentiary support, relying entirely on a misreading of Law, which never refers to the grouping of networks 150a and 150b as network 150. Paper 2 (“Pet.”) at 19 (citing Law ¶¶ at 52, 55).

Law also fails to teach applying “a first set of packet filtering rules” to “all network traffic traversing the boundary” of that protected network (the “all network traffic” limitation). Contrary to the plain language of the claims, which recites applying the same “first set” of rules at each packet security gateway (“PSG”) Law applies a unique rule set (ruleset 147a, 147b) at each firewall. Network access device 149c applies yet another unique set of rules (ruleset 151c) to network traffic as it crosses between networks 150a and 150b. Petitioner’s argument that the firewalls apply “global” rules fails because those rules are only “global” for the particular network that the firewall protects. Law uses the term “global” to distinguish between

rules that are applied at the network boundary to protect all devices on the network and non-global rules that are applied **within** the network and only apply to a subset of all of the network devices. Law at ¶ 51.

The Challenged Claims are also patentable because the '266 Patent is directed to protecting a network with a security policy management server ("SPMS") that automatically creates initial dynamic security policies including a first set of rules that are received by the PSG and applied to all network traffic. *See generally*, '266 Patent at Abstract, 5:54-6:2, 14:9-39, Claims 1, 8, 15, 21. Law, on the other hand, is directed to a Unified Threat Management System ("UTMS") for high-risk or sensitive process control systems (*e.g.*, nuclear reactors) in which rulesets are initially created by operators with intimate knowledge of the process control system. *See* Law at ¶¶ 22-23, 59, 90, 102. A third party with its own staff of IT personnel, firm 305 generates and sends updates to these operator-created rulesets when new threats are detected. *See generally, id.* at ¶¶ 16, 22, 88-89. Further, rather than firm 305 automatically creating rules, Law discloses that IT personnel are "required to update the ruleset when new threats are discovered or upgrades to software components of the system are implemented." *Id.* at ¶ 16.

Law, therefore, does not teach or suggest (i) "receiving, . . . a dynamic security policy comprising a first set of packet filtering rules" which under the correct construction means an initial dynamic security policy including a first set of rules

received by the PSG; or (ii) “one or more first packet filtering rules of the first set of packet filtering rules . . . automatically created or altered by the security policy management server.” ’266 Patent at Claims 1, 8, 15, 21.

Wood (Ground 2) does not cure the above-noted deficiencies. Because Petitioner only relies on Wood for its alleged teaching of providing suspect network addresses, the proposed Law-Wood combination suffers from the same shortfalls as Law taken alone in Ground 1.¹ See Pet. at 65. For these reasons and those that follow, Centripetal respectfully requests the Board find the Challenged Claims patentable.

II. THE ’266 PATENT OVERVIEW

The ’266 Patent is directed to “[m]ethods and systems for protecting a secured network.” ’266 Patent at Abstract, 1:59-60; *see also* Ex. 2012 (“Goodrich Decl.”), ¶¶ 31-33. Because “the path a given packet may take cannot be readily predicted,” (’266 Patent at 5:23-24) PSGs are placed at each boundary between a protected network and one or more other networks. *Id.* at 5:23-34, 3:54-58. For example, as shown in Figure 7, multiple PSGs are placed at the boundaries between a protected network (*i.e.* Network C) and one or more networks other than the network protected by the PSGs (*i.e.* Networks A and B).

¹ Grounds 3 and 4 (challenging the dependent claims) fail for the same reasons.

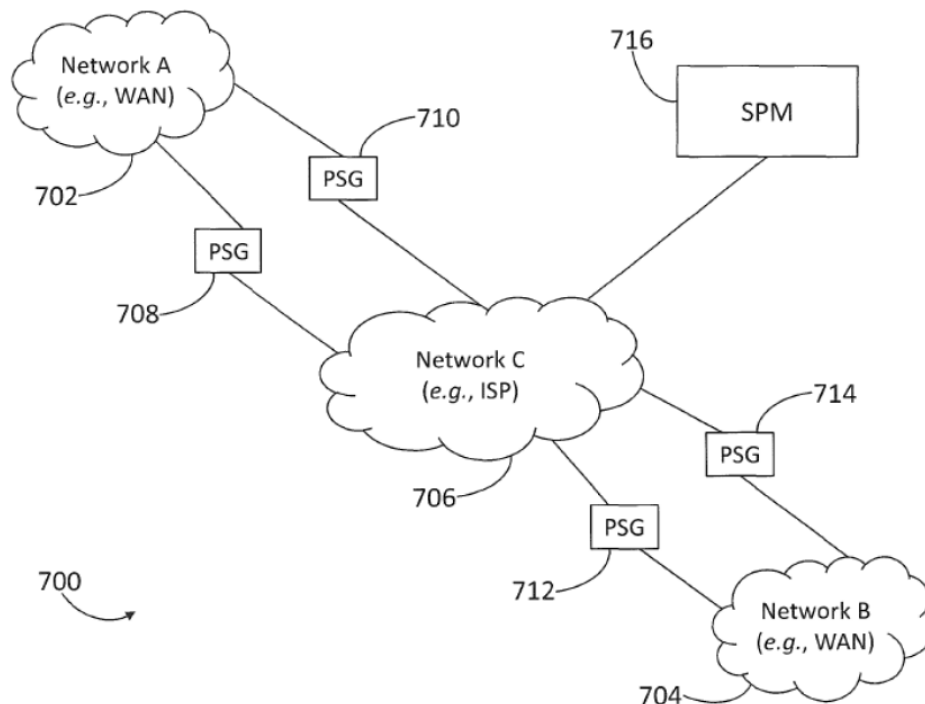


FIG. 7

Id. at Fig. 7; *id.* at 16:44-48, 16:62-17:1. In this way, the '266 Patent discloses “plurality of packet security gateways that collectively provide the entire interface across a boundary” of a protected network. *Id.* at Claims 1, 8, 15.

Each PSG applies a dynamic security policy to packets traversing the boundary. *See id.* at 4:61-5:11, 5:34-53, Claims 1, 8, 15, 21 (receiving “a dynamic security policy comprising a first set of packet filtering rules”). These policies are automatically created at an SPMS and include rules derived from malicious traffic information received from malicious host tracker services. *Id.* at 13:25-34, 14:9-39, 19:38-45, Figs. 1, 5, 9.

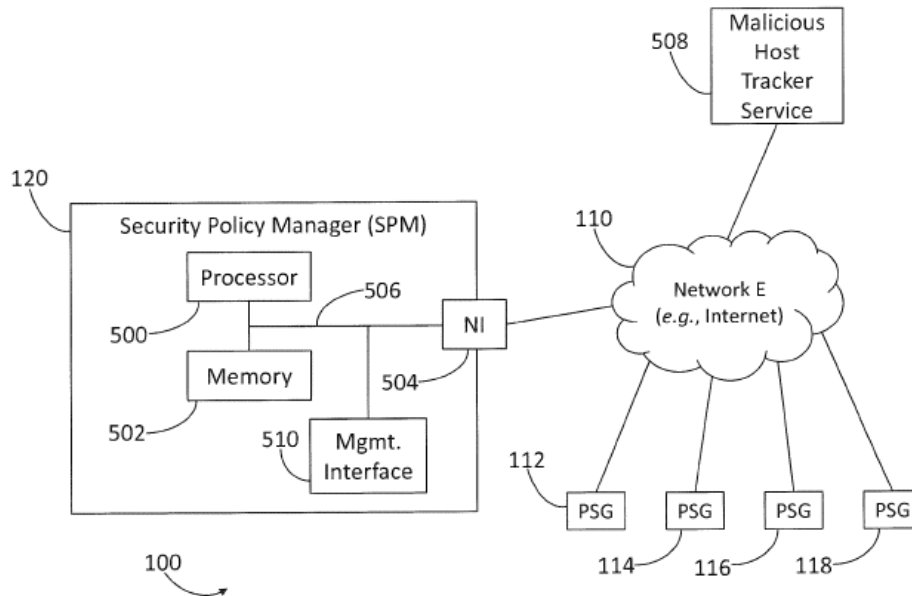


FIG. 5

Id. at Fig. 5. In this manner, the SPMS **(i)** automatically creates or alters a first set of packet filtering rules of a dynamic security policy,² **(ii)** communicates the

² Importantly, the SPMS's automatic creation or alteration of rules is performed without IT intervention, which differentiates traditional security systems from Centripetal's claimed security systems. Ex. 2013 at 6 ("The company's CleanINTERNET service automates threat protection This is the crux of the difference between traditional, manual security postures, and the CleanINTERNET service . . . It's really cool to show traditional security stack people how this all happens without any user intervention") (internal quotation marks omitted).

dynamic security policy and its first set to the PSG, (iii) updates the first set based on information (*e.g.*, network addresses) received from malicious host tracker services, and (iv) communicates an updated second set to the PSGs. *See* '266 Patent at 13:18-14:39, *id.* at Fig. 5; *see also id.* at Claims 1, 8, 15, and 21 (the claimed SPMS carrying out these operations).

III. LEVEL OF ORDINARY SKILL IN THE ART

Centripetal adopts the Board's level of ordinary skill in the art set forth in its decision denying institution in IPR2021-01154, *Palo Alto Networks, Inc. v. Centripetal Networks, Inc.* ("the '1154 decision"), "a person of ordinary skill in the relevant art [a "POSITA" or skilled artisan] on October 22, 2012 (the filing date of the application that matured in the '266 patent), 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." Ex. 2004 at 6; *see also* Goodrich Decl., ¶¶ 25-30.

IV. CLAIM CONSTRUCTION

A. The Preambles of Independent Claims 1, 8, and 15 Are Limiting

The preambles of independent claims 1, 8, and 15 should be treated as limiting. These preambles provide antecedent basis for "packet security gateway,"

“boundary,” “network,” and “one or more other networks.” ’266 Patent at Claims 1, 8, 15; *see also* Goodrich Decl., ¶¶ 38-39.

The preambles also recite the “plurality of packet security gateways that collectively provide an entire interface across a boundary of a [protected] network,” which is “essential to understand” the “all network traffic traversing the boundary” limitation in the body of these claims and thus ““give life, meaning, and vitality”” to the claims. *Catalina Mktg. Int’l, Inc. v. Coolsavings.com, Inc.*, 289 F.3d 801, 808 (Fed. Cir. 2002) (citation omitted); ’266 Patent at Claims 1, 8, 15. The preambles provide the context for the body of the independent claims by defining the arrangement of the “plurality of packet security gateways” relative to the “boundary” of the protected network and thus the basis for applying “packet filtering rules . . . to all network traffic traversing the boundary.” *See, e.g.*, ’266 Patent at Claim 1.

In the ’1154 decision, the Board construed the preambles as limiting because they provide context for the body of the independent claims:

The preambles provide the context for the body of the independent claims by defining the arrangement of the “plurality of packet security gateways” relative to the “boundary” of the protected network and thus the basis for applying “packet filtering rules . . . to all network traffic traversing the boundary.”

Ex. 2004 at 8.

B. Receiving a Dynamic Security Policy Comprising a First Set of Rules (All Challenged Claims)

In the Institution Decision, the Board tacitly interpreted the claim term as referring to an “initial ruleset” created by the PSG with a “first set of packet filtering rules” providing updates, received from the SPMS. Paper 10 (“Institution Decision”) at 25. That interpretation is incorrect. As shown below, by the plain reading and the specification, the term “receiving, by the packet security gateway and from a security policy management server . . . a dynamic security policy comprising a first set of packet filtering rules” (the “receiving a dynamic security policy comprising a first set of rules” limitation) means an initial dynamic security policy, including a first set of rules, that is received by the PSG from the SPMS. See Goodrich Decl., ¶¶ 40-41.

In construing a term, the term must be considered in “the context of the surrounding words,” *ACTV, Inc. v. Walt Disney Co.*, 346 F.3d 1082, 1088 (Fed. Cir. 2003), and “in the context of the entire patent, including the specification.” *Hamilton Beach Brands, Inc. v. f'real Foods, LLC*, 908 F.3d 1328, 1339 (Fed. Cir. 2018). The surrounding claim language recites that the claimed dynamic security policy and its first set of rules is constructed “by the security policy management based on aggregated malicious traffic information . . . that comprises network addresses” with the PSG then receiving the “dynamic security policy comprising a first set of packet filtering rules” and the PSG also receiving “an updated second set

of packet filtering rules for the dynamic security policy . . . wherein the updated second set of packet filtering rules comprises an update to the one or more first packet filtering rules.” ’266 Patent at Claims 1, 8, 15, 21; *see also* Goodrich Decl., ¶ 42.

Where 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. ’266 Patent at Claims 1, 8, 15, 21 (emphasis added). Accordingly, by the plain reading, “receiving a dynamic security policy comprising a first set of rules” refers to receiving an **initial dynamic security policy including a first set of rules from the SPMS**, not a first set of packet filtering rules updating an initial dynamic security policy created by the PSG. *See* Institution Decision at 25; Goodrich Decl., ¶ 42.

The plain reading 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. In every instance, the security policy management server creates or alters dynamic security policies including rules that specify network addresses as malicious network traffic information is received:

[S]ecurity policy management server 120’s memory 502 may include a **dynamic security policy *having one or more rules that specify a list of network addresses*** known to be associated with malicious network traffic. Security policy management server 120 may be **configured to**

automatically create or alter one or more of such rules as new network addresses associated with malicious network traffic are determined.

'266 Patent at 14:13-20 (emphasis added); *id.* at 14:28-31 (“Security policy management server 120 may be configured to create or alter one or more rules **included** within a dynamic security policy. . . .”) (emphasis added). As these passages illustrate, the SPMS creates or alters the first set of rules included within an initial dynamic security policy that is received by the PSG. Goodrich Decl., ¶ 43.

Further, in updating (e.g., altering) one or more rules, the claims and specification dictate that the PSG receives the updates in the form of a “second set of packet filtering rules” for the initial dynamic security policy and its first set of rules. '266 Patent at Claims 1, 8, 15, 21, 14:33-37. Thus, the claim language does not encompass nor any embodiments illustrate the PSG first creating “an initial ruleset” and then separately receive “an update” in the form of a “first set of packet filtering rules.” Institution Decision at 25; *see also* Goodrich Decl., ¶ 44.

Given the foregoing, the Board's preliminary interpretation is inconsistent with the claim language and specification. *Id.*; *see also* Goodrich Decl., ¶ 45. By adding the implicit limitations of the PSG creating “**an initial ruleset**” and then receiving from the SPMS a “first set of packet filtering rules . . . [as] **an update to that initial ruleset,**” the Board (1) rendered the “receiving [by the PSG] a dynamic security policy” superfluous and (2) separated the first set of packet filtering rules

from the dynamic security policy, of which it is a part. The claims should be construed as written. *Chef Am., Inc. v. Lamb-Weston, Inc.*, 358 F.3d 1371, 1374 (Fed. Cir. 2004) (“[W]e construe the claim as written”); *Banyan Licensing, L.C. v. Orthosupport Int’l, Inc.*, 34 F. App’x 696, 697 (Fed. Cir. 2002) (“First, we look to the claim language” and then “we look to the rest of the intrinsic evidence”) (citations omitted).

This interpretation is also in error because it ensnares prior art despite there being a more reasonable interpretation that avoids Law. *See Apple Comput., Inc. v. Articulate Sys., Inc.*, 234 F.3d 14, 24 (Fed. Cir. 2000) (explaining that “claims should be read in a way that avoids ensnaring prior art if it is possible to do so”) (citation omitted). As established above, the correct interpretation of the claims— that stays true to the claim language and most naturally aligns with the specification—refers to the PSG receiving an initial dynamic security policy included with a first rule set created at the SPMS, which Law does not satisfy. The Board’s interpretation, however, erroneously ensnares Law’s disclosure of receiving updates to operator-created initial rulesets. Institution Decision at 25 (finding that the interpretation “comports with the system in Law, since an initial ruleset can be created by operators, and the claimed ‘first set of packet filtering rules’ would be an update to the initial ruleset”).

In view of the foregoing, the term “receiving a dynamic security policy comprising a first set of rules” means receiving by the PSG from the SPMS an initial dynamic security policy including a first set of rules, not a first set of rules updating a separate PSG-created initial dynamic security policy. Under the proper construction, Law does not satisfy the claim term because Law’s operators create the initial rulesets with firm 305 (the alleged “SPMS”) distributing only updates to the operator-created initial rulesets, as discussed in greater detail below. See § VI.A.4, *infra*; Goodrich Decl., ¶ 46.

C. Other Constructions

Petitioner requests that the Board adopt the constructions of the claim terms set forth below that have been construed in previous IPR proceedings.

Term	The PTAB’s Constructions
packet security gateway	a gateway computer configured to receive packets and perform a packet transformation function on the packets
packet transformation function	[one or more] operations performed on a packet
rule(s)	a condition or set of conditions that when satisfied causes a specific function to occur
dynamic security policy	any rule, message, instruction, file, data structure, or the like that specifies criteria corresponding to one or more packets and identifies a packet transformation function to be performed on packets corresponding to the specified criteria

Term	The PTAB's Constructions
security policy management server (SPMS)	a server configured to communicate a dynamic security policy to a packet gateway
network layer address	an address that identifies a device for communication on the network layer, such as an IP address

See Pet. at 9-10; Goodrich Decl., ¶¶ 47-48.

The disputes in these proceedings do not turn on these constructions, and thus these constructions are not necessary. *See Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) (“[O]nly those terms need be construed that are in controversy, and only to the extent necessary to resolve the controversy”) (citation omitted). Nevertheless, for the purpose of this proceeding, Centripetal applies the Board's previously adopted constructions.

V. OVERVIEW OF THE REFERENCES

A. The Law Reference

Law discloses an operator environment that enhances the security and management of a process control system³ by providing UTMS-configured devices

³ Process control systems are used for particularly high-risk or sensitive applications, like power generation, chemical processes, petroleum processes, nuclear reactors,

configured and managed by operator workstations within the system. *See, e.g.*, Law at ¶¶ 22-23; Goodrich Decl., ¶¶ 49-54. Before Law, process control systems relied on firewall systems that were managed by third-party “IT personnel specifically trained to integrate the firewall into the needs of the process control system and configure the various rulesets.” Law at ¶ 16. “[S]eparately-trained IT personnel” managed network security leaving process control system operators with “no capability to monitor and manage process control network security from operator workstations.” *Id.* at ¶ 21.

Law overcame the need for separately trained IT personnel with operator workstations for managing UTMS-configured devices. *See id.* at ¶¶ 22-23, 59-60, 83. These workstations enable operators to create and manage rulesets (*i.e.* rulesets 147, 148, 151, and 153) specific to the unique security requirements of their particular process control system “without IT personnel intervention.” *Id.* at ¶ 59; *see id.* at ¶¶ 23, 66, 90, 102.

Although an operator with intimate knowledge of the process control system creates the initial rulesets, third-party IT personnel are “still required to update the

high-energy processes, and/or military and government processes, each of which has its own unique security requirements. *See* Law at ¶¶ 3, 15.

ruleset when new threats are discovered or upgrades to software components of the system are implemented.” *Id.* at ¶ 88; *see also id.* at ¶¶ 16, 22, 31, 89. Law makes clear that because each operator-created ruleset is specific to the system it protects, the third-party IT personnel must “have detailed knowledge of the network architecture that is to be protected” to understand “how or why the rulesets must also be changed” to ensure that the system remains effective. Law at ¶ 16. Accordingly, given the uniqueness of process control systems and the UTMS-configured devices, Law teaches that (i) initial rulesets are created by operators to meet the needs of the particular process control system; and (ii) third-party IT personnel (for example of firm 305) are required to manually update the rulesets when new threats are detected. *See* Law at ¶¶ 16, 22-23, 88-89.

On the other hand, the '266 Patent describes and claims an SPMS that automatically creates initial dynamic security policies that are received by the PSG. *See* '266 Patent at Claims 1, 8, 15, 21; Ex. 2013 at 6 (“The company’s CleanINTERNET service automates threat protection It’s really cool to show traditional security stack people how this all happens without any user intervention,” *i.e.* “manual security postures”) (internal quotation marks omitted).

Additionally, unlike the '266 Patent, which claims a plurality of PSGs that collectively provide an entire interface across a boundary of a single protected network, Law’s system includes **two separate networks** 150a (green) and 150b

(blue) that are each respectively protected by a single firewall 146a (green) and 146b (blue):

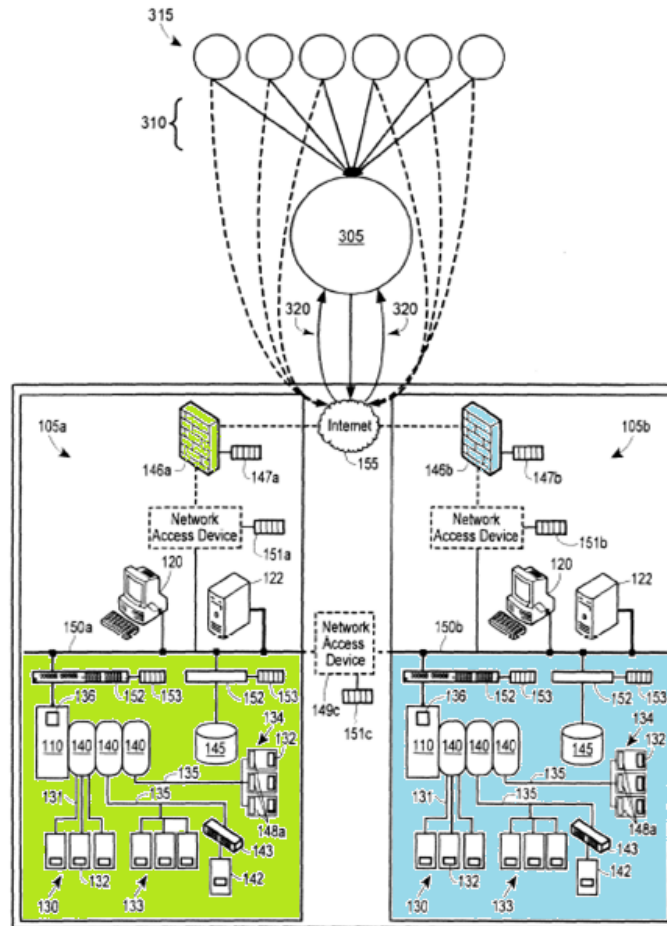


Fig. 3

Law at Fig. 3 (annotated). Network access device 149c controls network access between sub-system 105a and sub-system 105b, each of which has its own separate network 150a and 150b, in the same way that network access devices 149a and 149b controls network access between the Internet and networks 150a and 150b. *Id.* at ¶¶ 94, 96 (explaining that network access device controls network access between the Internet and networks 150a and 150b or between the networks). Thus, contrary to

Petitioner's suggestion, network access device 149c does not join together these separate networks into a single network 150.

B. The Wood Reference

Wood (Ex. 1006) does not cure Law's deficiencies. Wood is only cited for its disclosure of a source providing suspect network addresses. Pet. at 65 (citing Wood for "'one or more suspect address sources 210' providing [sic] 'a feed of suspect addresses from one or more sources on the external network.'") (quoting Wood at ¶¶ 21, 32, 34, *id.* at Fig. 2). Wood's adaptive interrogation module 304, located within the subnetwork, receives "suspect address update[s]" and reconfigures the router "if any changes to the suspect address list have been made." Wood at ¶ 36; *see also id.* at ¶ 34, Fig. 2; Goodrich Decl., ¶ 55.

VI. THE CHALLENGED CLAIMS ARE PATENTABLE

A. Ground 1: Claims 1-27 Are Patentable Over Law

1. Law Does Not Disclose "a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected" (Independent Claims 1, 8, 15)

As a preliminary matter, in *Centripetal Networks, LLC, v. Palo Alto Networks, Inc.*, No. 2:21-CV-00137 (EWH), the district court construed the term "a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network" to mean "***two or more packet security gateways*** arranged such that there is no network path across a boundary of ***a network*** that bypasses the

packet security gateways.” Ex. 2017 at 25-29 (emphasis added). Therefore, as construed, a network is protected by two or more PSGs. *Id.* at 26 (concluding based on the claim language that “the packet security gateways are arranged in such a way that they fully protect a boundary between the protected network and another network”).

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. '266 Patent at Clams 1, 8, 15; *see* Pet. at 19 (reading the preamble as “requir[ing] that a plurality of packet security gateways collectively protect a single network”); Goodrich Decl., ¶ 56.

Petitioner's single network obviousness theory is premised on the mistaken understanding that Law discloses joining networks 150a and 150b together into a single network, *i.e.* network 150. *See* Pet. at 19-21; Institution Decision at 20-21 (finding that Law refers to “‘network 150,’ rather than separately specifying subnetworks 150a and 150b” and that “paired LANs of Law” is “a single network”). Contrary to Petitioner's reading, Law never uses the term “network 150” to refer to any combination of networks 150a and 150b. 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. Goodrich Decl., ¶ 57.

Petitioner also has submitted no evidence that could support a conclusion that a POSITA would have recognized network 150a, network 150b, and network access device 149c to be a single network. Indeed, that conclusion is contrary to Law's disclosure that perimeter devices, like network access device 149c, are **outside** of networks 150a and 150b. Law at ¶ 51 ("Where the UTMS-configured device is a perimeter device (i.e., outside of the process control network 150a or 150b), the rulesets 147 and 151 may include a global set of rules for access to any device within the subsystems 105a, 105b."). Petitioner's backup argument, that it would have been obvious to expand Law's system to include any number of PSGs, is conclusory and ultimately succumbs to the same deficiencies as its primary argument. Goodrich Decl., ¶ 58.

a. Law's "Network 150" Does Not Refer to a Combination of Networks 150a and 150b

Law discloses two separate networks, protected by two separate firewalls that do not interact with each other:

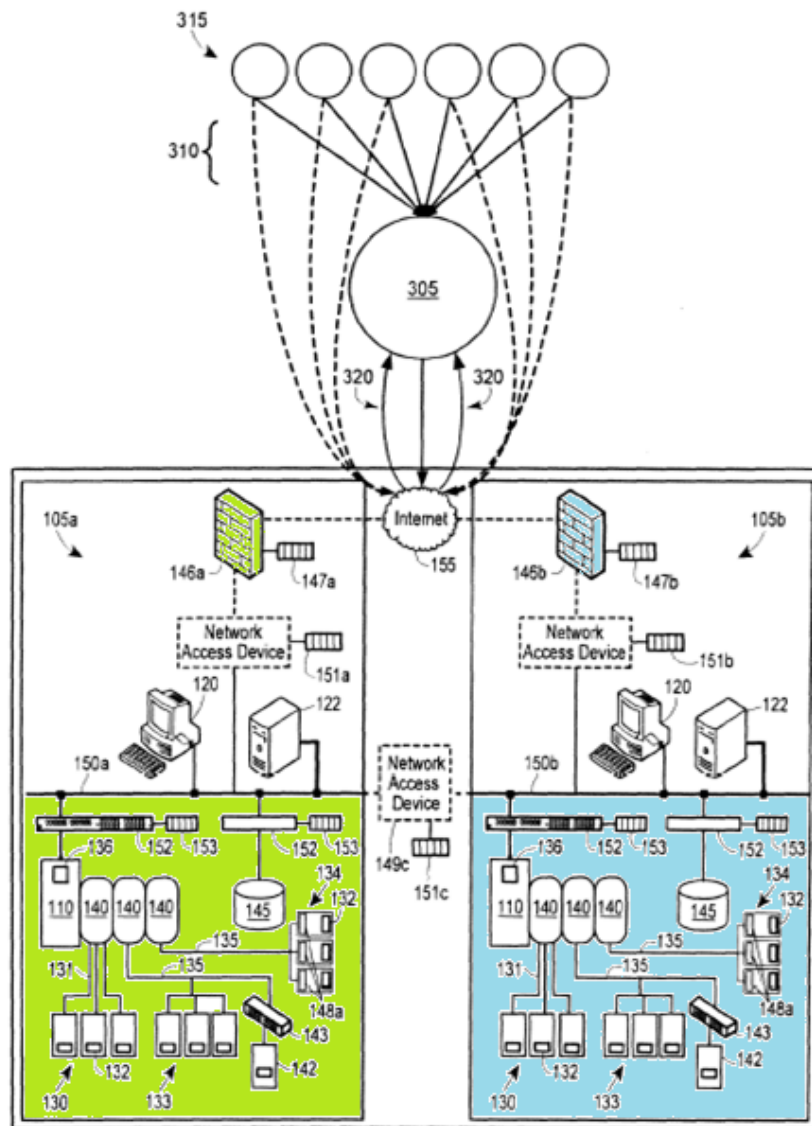


Fig. 3

Law at Fig. 3 (annotated, depicting networks 150a and 150b); see also *id.* at ¶¶ 51, 53; Goodrich Decl., ¶ 59. Networks 150a and 150b are “process control networks.” Law at ¶¶ 51, 53. When necessary to distinguish between these two process control networks, Law refers to “process control network 150a or 150b.” *Id.* at ¶ 51. When discussing both process control networks, Law refers to “one or more process control networks 150a, 150b.” *Id.* at ¶ 53. When it is not necessary to differentiate between

the two networks, Law refers to “a process control network 150.” *Id.*; see also Goodrich Decl., ¶ 59.

As depicted in figure 9 (reproduced below), Law uses network 150 when showing a single network that encompass devices 130-134 that are communicatively connected to operator workstations and computers 120-122 that relay information via a firewall 146.

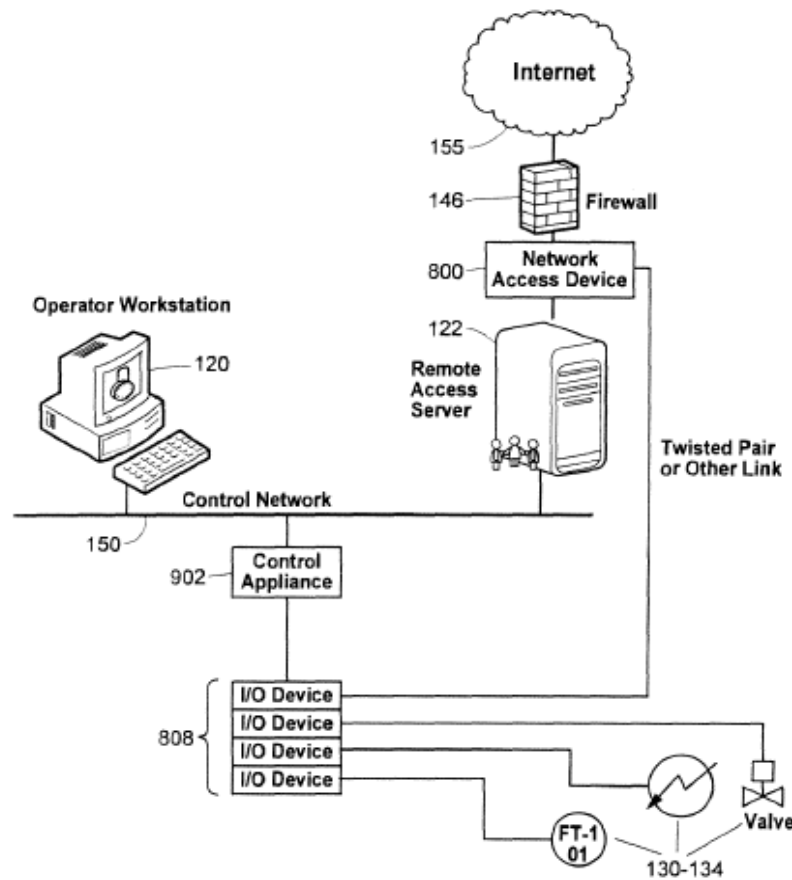


Fig. 9

Law at Fig. 9; *see also* Figs. 6, 9, 12; Goodrich Decl., ¶ 60. Similarly, figure 3 depicts networks 150a and 150b, each including the entire host of network components depicted in the illustrative single network 150 of figure 3 (*i.e.* remote access server 122, firewall 146, operator workstation 120, and devices 130-134). Law at Fig. 3; *see also id.* at ¶¶ 51, 53-54. Thus, “[t]he network 150 and devices” represents an example of either network 150a or 150b and the components of each, not the combination of networks 150a and 150b, as Petitioner suggests. *See* Law at ¶ 55; Goodrich Decl., ¶ 60.

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. *Compare* Pet. at 19-21 (citing Law at ¶ 55) *with* Ex. 1003 at ¶ 64 (citing Law at ¶ 55); *see also Xerox Corp. v. Bytemark, Inc.*, No. IPR2022-00624, Paper 9 at 15 (P.T.A.B. Aug. 24, 2022) (precedential) (determining that testimony of a declarant that merely repeats, verbatim, conclusory assertions from a petition, without citing additional supporting evidence or providing technical reasoning to support the testimony, is entitled to little weight). Dr. Jacobson cites no evidence or articulated reasoning in support of his conclusion. In fact, during cross-examination, Dr. Jacobson testified that the **only** evidence supporting his opinion is Law's use of the term “network 150.” Ex. 2014 (“Jacobson Tr.”) at 51:3-

21 (testifying that the evidence he relied on came from Law's use of "network 150" in paragraphs 51 and 55); Goodrich Decl., ¶ 61.

However, as established above, "network 150" is not the combination of networks 150a and 150b, and when questioned about how Law's network access device 149c transforms networks 150a and 150b into a single network, Petitioner's counsel objected to the entire line of questioning as being outside the scope of his declaration. See, e.g., Jacobson Tr. at 40:16-20, 45:9-46:9, 50:1-7; Goodrich Decl., ¶ 62. Because Petitioner's *prima facie* obviousness theory requires the use of network access device 149c to join networks 150a and 150b into a single network, Petitioner was required to support that theory with evidence that Patent Owner could evaluate.

Contrary to Petitioner's conclusory argument, Law explains that network access device 149c controls network access between two networks (e.g., network 150b of system 105B and network 150a of system 105A), as depicted in figure 5.

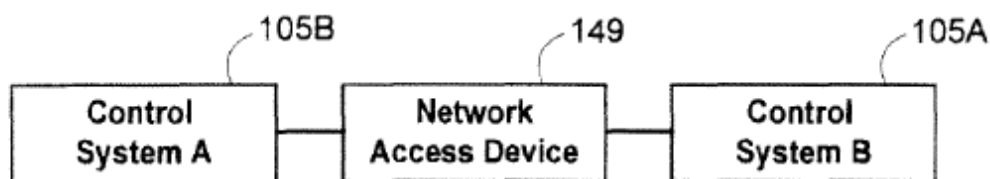


Fig. 5

Law at Fig. 5, ¶ 94 (explaining that the device “may be used by the operator . . . to control network access between . . . sites”); Goodrich Decl., ¶ 62. As further illustrated in Figure 3, network access device 149c is a perimeter device that functions as the interface between the two networks:

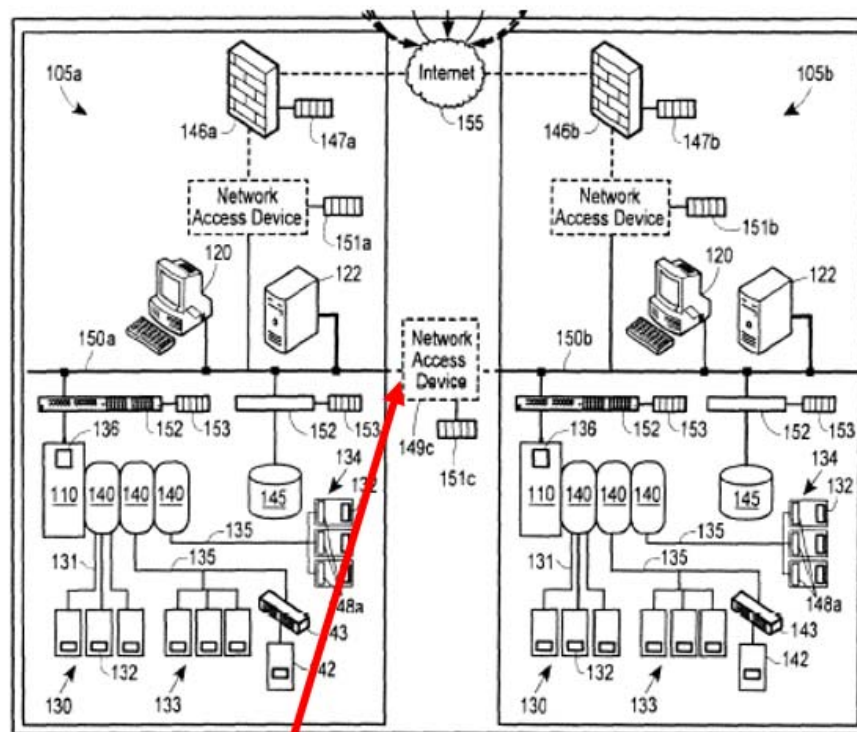


Fig. 3

perimeter device

Law at Fig. 3 (annotated); *id.* at ¶¶ 51, 52, 92 (explaining that the network access device is a perimeter device that sits outside networks 150a and 150b); Ex. 2015 at 1 (explaining that a router is a network access device “used to connect multiple

networks together”).⁴ And rather than Law describing network access device 149c as a device that combines two separate networks into a single network 150, Law explicitly discloses that such perimeter devices are **outside** of networks 150a and 150b. Law at ¶ 51 (“Where the UTMS-configured device is a perimeter device (i.e., outside of the process control network 150a or 150b), the rulesets 147 and 151 may include a global set of rules for access to any device within the subsystems 105a, 105b.”); *see also id.* at ¶ 92 (referring to network access device 149 as perimeter device); Goodrich Decl., ¶ 63.

Because Dr. Jacobson does not provide any supporting evidential basis for how network access device 149 combines networks 150a and 150b into a single network 150, his conclusory, unsupported testimony cannot support an obviousness conclusion. *TQ Delta, LLC v. Cisco Sys., Inc.*, 942 F.3d 1352, 1359 (Fed. Cir. 2019) (reversing the Board’s obviousness determination because the “conclusory expert testimony is inadequate to support an obviousness determination”).

⁴ Because network access device 149c is a perimeter device that allows for communications between networks, network traffic traverses the perimeter at multiple locations, *e.g.*, firewall 146a and network access device 149c, with each location supplying its own set of rules, *e.g.* firewall 146 applying ruleset 147a and network access device 149c applying ruleset 151c. *See* § VI.A.2, *infra*.

b. Petitioner's Expanded Number of Firewalls Theory Lacks Sufficient Rationale and Succumbs to the Same Network 150 Deficiencies

Petitioner's alternative argument, that it would have been obvious "to expand Law's disclosure to any number" of firewalls (the alleged "packet security gateways") (Pet. at 23), is conclusory and insufficient on its face to alter the conclusion reached above. *See In re Nuvasive, Inc.*, 842 F.3d 1376, 1383 (Fed. Cir. 2016) ("conclusory statements alone are insufficient and, instead, the finding must be supported by a reasoned explanation.") (internal quotation marks omitted and citation omitted).

Moreover, Petitioner's argument that Law's "process control system 100 may include any number of sub-systems as well as devices, modules and components" does not suggest that a skilled artisan would have added additional firewalls to any one of the sub-systems. Pet. at 23 (quoting Law at ¶ 53). Instead, expanding Law to include more than two sub-systems, as discussed in Law and alleged in the Petition, would result in a system with the same exact deficiencies as the two sub-systems embodiment discussed directly above. That is, even if Law disclosed 100 subsystems, each subsystem would require 100 firewalls, and none of those firewalls has the capability of interacting together. Goodrich Decl., ¶¶ 64-65.

Additionally, Petitioner's citation to vague boilerplate language stating that the "process control system 100 may include any number of . . . devices" is

insufficient to support Petitioner's allegation that "it would have been obvious to a POSITA to expand Law's disclosure to any number of packet security gateways." Pet. at 23; *cf. IP Innovation, L.L.C. v. eCollege.com*, 156 F. App'x 317, 321-22 (Fed. Cir. 2005) (explaining that "common boilerplate" language did not effectively disclose an alternative embodiment to support a broader construction). There are notably many devices disclosed in Law, and nothing in this vague, boilerplate language contemplates implementing more than two firewalls devices in the process control system, let alone in each network 150a and 150b. See Law at ¶ 53; Goodrich Decl., ¶ 66. Accordingly, Petitioner falls short of providing articulated reasoning with rationale underpinning as to how a POSITA a POSITA would have implemented any number of firewall devices in Law's system.

2. Law Does Not Disclose Applying "a first set of filtering rules" to "all network traversing the boundary" (Independent Claims 1, 8, 15)

Law also does not teach applying a "first set of filtering rules" to "all network traffic traversing the boundary" of the single protected network because (i) firewalls 146a and 146b each have its own set of rules to protect their respective networks; and (ii) network traffic traverses the perimeters at network access device 149c that applies its own set of rules in addition to network traffic traversing the perimeters at the firewalls. Goodrich Decl., ¶ 67.

a. Each firewall has a unique set of global rules to protect their respective network and the devices within that network

The Petition relies on Law's global set of rules in alleging that "[a] POSITA would have understood that perimeter UTMS firewalls 146a and 146b would have applied ruleset 147 to all network traffic passing therethrough." Pet. at 30; Institution Decision at 23 (relying on this passage in instituting review). This allegation misapprehends what Law's "global" rule sets are and how Law's UTMS-system operates. Goodrich Decl., ¶ 68.

Law refers to global ruleset as one that applies to all of the devices within a subsystem. Law at ¶ 51. Because they are broadly applicable to all of the devices within a subsystem, they can be applied at a perimeter device, like firewall 146 or network access device 149. On the other hand, a subset of this global ruleset might only control access to a "particular internal device." *Id.* Accordingly, Law's "global" ruleset is not one that is applied to all traffic traversing the boundaries of a protected network. Rather, firewall 146a will apply a different global set of rules for access to devices in subsystem 105a, and firewall 146b will apply a global set of rules for access to devices in subsystem 105b. But because each of these global rulesets is unique to the particular devices in the subsystem, the "global" ruleset for subsystem 105a will be different from the "global" ruleset for subsystem 105b. Goodrich Decl., ¶ 69.

Law's key contribution to the art concerns how to adequately protect process control systems with unique network topologies and different requirements. Law at ¶¶ 3-4, 16, 89; Goodrich Decl., ¶ 70. Thus, as Law recognized, the rules applied in any particular process control network must depend on the particular features, configurations, and permissions of the devices on that network. Law at ¶¶ 19-20. This is why Law describes a ruleset as being "specific to the system it protects" and as including rules to protect against "vulnerabilities of specific devices within [a] network." *Id.* at ¶¶ 11, 16, 22 (discussing "rulesets to meet the latest security threats, threat patterns, and control system vulnerabilities found to exist within the network"), ¶ 55 (recognizing "known vulnerabilities of the device itself"), ¶ 89 (describing rules to address "specific system vulnerabilities"); Goodrich Decl., ¶ 70.

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. Goodrich Decl., ¶ 71. But Petitioner provides no reason why a skilled artisan would have understood those subsystems and networks to include the exact same devices with the exact same configurations and permissions such that the exact same ruleset would have been suitable for both firewalls.

A skilled artisan, possessed with an understanding of the full scope of Law's teachings, would have recognized that Law's firewalls (146a, 146b) apply unique rulesets to their respective networks (150a, 150b) in order to protect them against the specific threats and vulnerabilities that arise from the particular devices, configurations, and permissions present at those networks. Goodrich Decl., ¶ 71; *see also Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve, Inc.*, 796 F.2d 443, 448 (Fed. Cir. 1986) ("It is impermissible within the framework of section 103 to pick and choose from any one reference only so much of it as will support a given position to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one skilled in the art") (quoting *In re Wesslau*, 353 F.2d 238, 241 (CCPA 1965)).

The Institution Decision's common ruleset theory does not cure the above deficiencies. Institution Decision at 23. This theory is predicated upon Law's networks 150a and 150b being joined together to form single network 150. *Id.* (viewing "subsystems 105a, 105b as a single network"). However, they are not. Rather they are separate networks that protect different features, configurations, and permissions of devices located at separate sites (*i.e.* subsystems). Law at ¶ 10 (describing that process control systems have "different steps of the process are executed, monitored, and controlled, etc., in physically separate locations"), *id.* at ¶ 96 (equating "sites" to subsystems 105a, 105b); Goodrich Decl., ¶ 72. Petitioner

fails to show that a skilled artisan would have understood that firewalls 146a, 146b would fully or even partially apply a common ruleset to all network traffic traversing the perimeters of each network that protects categorically different systems.

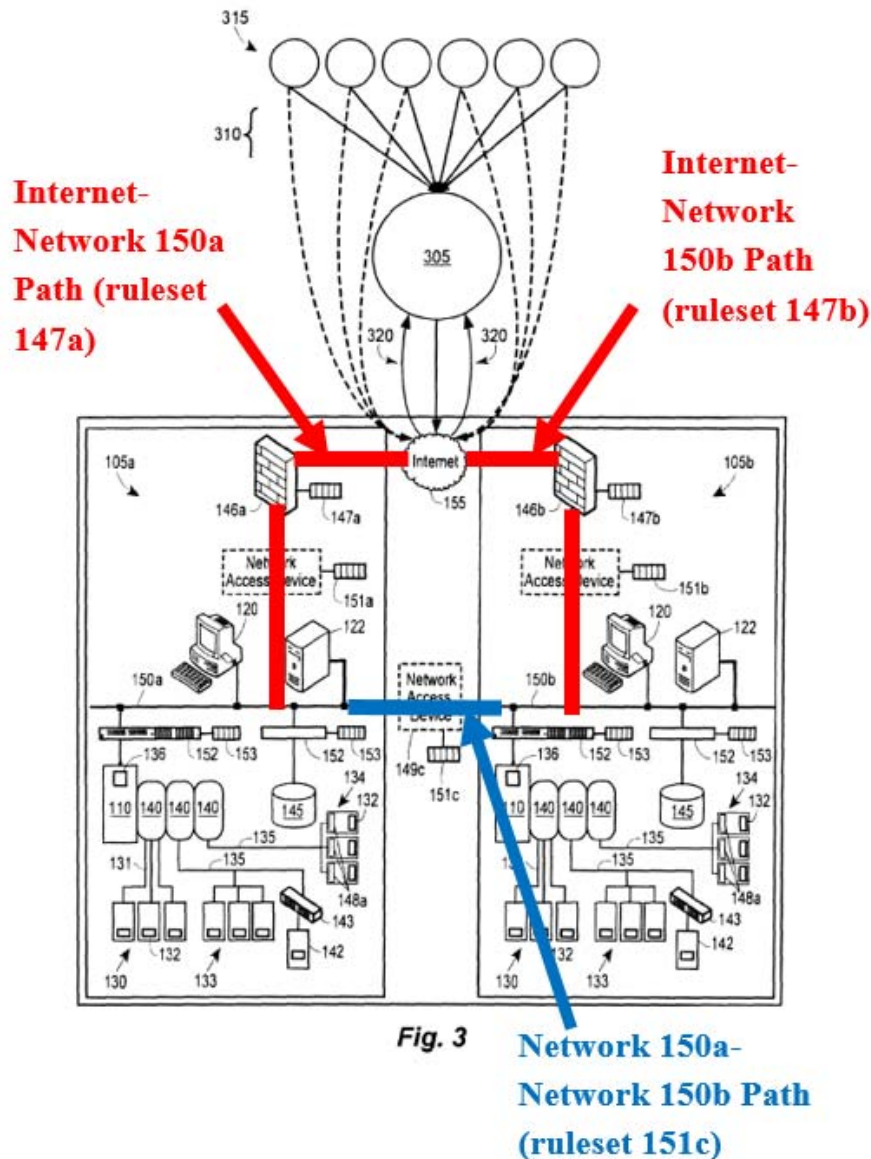
Given that Law's firewalls (146a, 146b) do not work together and would have applied unique rulesets to the network traffic each receives, Law cannot satisfy the "all network traffic" requirement regardless of whether Law's networks (150a, 150b) were connected together under Petitioner's joined network theory or remained unconnected. Goodrich Decl., ¶ 73.

b. Law's Internet-networks and network-network communication paths are subject to the application of different rules

In addition to each firewall having its own unique set of rules, Law also explains that network traffic traverses the perimeter of the network at the network access device 149c, with these devices applying their own set of rules. See Law at ¶ 51, Fig. 3 (applying ruleset 151c to network traffic crossing the perimeter via network access device 149c to control network access); *see also id.* ¶¶ 51, 52, 92 (explaining that network access device functions as a perimeter device); Goodrich Decl., ¶ 74.

As depicted in annotated figure 3 reproduced below, rulesets 147a and 147b are applied to network traffic following the Internet-Network 150a and Internet-Network 150b communication paths (**shown in red**), respectively. The annotation

further demonstrates that ruleset 151c is applied to network traffic following the Network 150a-Network 150b communication path (**shown in blue**).



Law at Fig. 3 (annotated). As the above illustration shows, network traffic crosses the perimeter at different locations for which different rulesets are applied (for example, Internet-Network 150a pathway applies ruleset 147a and Network 150a-

Network 150b pathway applies ruleset 151c to control network access). Because network traffic crosses the perimeters at different locations and is subject to the application of different rules, the same set of rules is not applied to “all network traffic” that “travers[es] an entire interface across a boundary,” as required by the Challenged Claims. ’266 Patent at Claim 1 (reciting a “dynamic security policy comprising a **first set of packet filtering rules to be applied to all network traffic traversing the boundary**”) (emphasis added); *see also id.* at Claims 8, 15; Goodrich Decl., ¶ 75.

* * *

In view of the foregoing, Law fails to teach applying a “first set of filtering rules” to “all network traffic traversing the boundary.” Goodrich Decl., ¶ 76.

3. Law Does Not Disclose Nor Render Obvious a Security Policy Management Server That Automatically Creates or Alters Dynamic Security Policies

The Board should also confirm the patentability of the Challenged Claims because Law does not disclose or render obvious an SPMS that automatically generates rulesets. Goodrich Decl., ¶ 77.

Petitioner alleges that firm 305 is a server that automatically generates rules (or that it would have been obvious to modify firm 305 to automatically generate rulesets). *See* Pet. at 29, 36-38. This allegation cannot be supported because Law expresses that: (1) firm 305 is a company that includes IT personnel and other

infrastructure components; and (2) IT personnel of third-party firms, like firm 305, are still required to manually update the rulesets of process control systems. See Law at ¶¶ 16, 88-89; Goodrich Decl., ¶ 78.

a. Law does not disclose the automatic generation of rulesets by firm 305

Petitioner asserts that firm 305 is a server that automatically generates rules. See Pet. at 36-38 (citing Law, ¶¶ 83, 88, and 89). But firm 305 is a company that employs IT personnel who are required to update rulesets specific to each process control system. Thus, Law explicitly discloses firm 305 to be a commercial entity, *e.g.*, Wurldtech Security, Inc., with IT personnel and various components involved in updating rulesets. Law at ¶ 88 (“a third party, cyber security risk management firm 305 such as Wurldtech Security, Inc.”); *see also* Ex. 2011 at 3 (defining “firm” as meaning “[a] commercial partnership of two or more persons.”); Goodrich Decl., ¶¶ 79-80.

During cross-examination, Dr. Jacobson testified that firm 305 is a business with various components and staff involved in updating rulesets:

So it would have to have a place to store that information

It would need then necessary processing power to work with the various -- the information that got from the 315s you have a staff to manage the infrastructure, typically these firms will also **have staff that understand, you know, something about the 315s and understand, you know, issues about threats**, et cetera. And so you're going to have

some **security type personnel in the 305** and then of course that's all.
You know, **I mean, I'm going to completely ignore everybody else
that you need to run a business.**

Jacobson Tr. at 37:2-38:10 (emphasis added); *see also id.* at 35:11-23 (testifying that firm 305 is a service that “supplies the UTMS-configured firewalls with updated rulesets.”). In fact, 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. *See* § V.A, *supra*; *see also* Law at ¶ 16; *see also id.* at ¶¶ 21-22, 88-89; Goodrich Decl., ¶ 81.

Accordingly, skilled artisans reading these paragraphs would understand that updating rulesets at third-party firm 305 (a commercial business) necessarily requires IT personnel involvement. Goodrich Decl., ¶ 82. Particularly, skilled artisans would have appreciated that third-party IT personnel who have detailed knowledge of the process control system are required to update rulesets when new threats are detected because they understand how and why the rulesets must be modified to protect the system. *Id.* As a concrete example, 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.” Law at ¶ 88; *see also id.* at ¶ 16; Goodrich Decl., ¶ 82.

Critically, 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. See Law at ¶ 83; Jacobson Tr. at 54:17-19, 55:10-56:6 (testifying that paragraph 83 is directed to the process control system). Rather than firm 305 automatically generating rules, Law's internal UTMS-configured elements implement "automatic update[s]" under certain network conditions. Law at ¶ 83 (detailing that the UTMS-configured elements that detect network conditions in which the graphic display elements may trigger either automatic updates or an "alarm to prompt a user to perform a manual update of the rulesets."); Goodrich Decl., ¶ 83.

The '474 Institution Decision's interpretation (in IPR2023-00448)⁵ of paragraph 83 is misaligned with Law's express disclosure. *Keysight Techs., Inc. v.*

⁵ The claim requirement of an SPMS that automatically creates or alters dynamic security policies is also found in U.S. Patent 11,012,474 challenged in IPR2023-00445, which also advances Law. See IPR2023-00445, Paper 2 (Petition) at 29-31 (alleging that Law discloses or renders obvious an SPMS that automatically creates or alters dynamic security policies, as required by the claims of '474 Patent). Accordingly, the '474 Institution Decision also addressed Law's alleged disclosure

Centripetal Networks, LLC, No. IPR2023-00448, Paper 7 at 31, 33-34 (P.T.A.B. July 24, 2023) (the “’474 Institution Decision”). Particularly, the decision concluded that “we disagree . . . that paragraph 83 concerns ‘the process control system, not firm 305’” because firm 305 may continuously identify network vulnerabilities and update rulesets. ’474 Institution Decision at 33-34 (internal quotation marks omitted). That firm 305 continuously identifies network vulnerabilities and updates rulesets does not mean that it does so automatically, and nothing paragraph 83 says that it does. The decision ignores the critical context that firm 305 is a service that includes separately-trained IP personnel who “are still required to update the ruleset[s]” when the updates occur outside the operator environment. Law at ¶¶ 16, 83, 88-89. In this regard, the UTMS-configured devices can receive from firm 305 the “update data” on a continuous basis, as shown in Figure 3’s “logical block diagram of a method to update rulesets of the UTMS,” but that does not mean that the “update data” was automatically generated. *Id.* at ¶¶ 30, 66, Fig. 3; Goodrich Decl., ¶ 84.

of automatic ruleset generation by firm 305 amongst other alleged disclosures in Law. Therefore, the ’474 Institution Decision is referenced throughout the Response.

In view of the foregoing, Law does not disclose automatic generation of rulesets by firm 305. Goodrich Decl., ¶ 85.

b. Skilled artisans would not have found it obvious to incorporate automatic generation techniques in firm 305 because IT personnel are required for the updates

Petitioner asserts, in the alternative, that it would have been obvious for skilled artisans to incorporate in firm 305 the alleged automatic generation technique as referenced in paragraph 21 of Law. Pet. at 38. In making this argument, Petitioner relied on the background art for documenting what skilled artisans would allegedly be armed with when reading Law. *Id.*; Goodrich Decl., ¶ 86.

While art can be considered to show the state of the art at the time of the invention, a petitioner must “provide adequately developed explanations when relying on background knowledge based on cited art.” *Ariosa Diagnostics v. Verinata Health, Inc.*, 805 F.3d 1359, 1366 (Fed. Cir. 2015). Petitioner failed to do so here. Other than saying that automatic generation was allegedly known, Petitioner does not provide any explanation or basis for how or why a skilled artisan would have ignored Law’s disclosure that trained IT personnel are “**still required to update the ruleset when new threats are discovered.**” Law at ¶ 16 (emphasis added); *see also id.* at ¶ 88 (disclosing that the third party firm provides updates to the rules “to remain effective against network threats.”).

In fact, Petitioner ignores this express disclosure that teaches away from the '266 Patent and relied on an alleged technique without concern of how or why a POSITA would have implemented the technique in third-party firm 305. See *Chemours Co. FC, LLC v. Daikin Indus., Ltd.*, 4 F.4th 1370, 1376 (Fed. Cir. 2021) (reversing the Board's obviousness determination because "the Board appear[ed] to have ignored the express disclosure in Kaulbach that teaches away from the claimed invention and relied on teachings from other references that were not concerned with the particular problems Kaulbach sought to solve"). As established above, firm 305 includes IT personnel who are required to update the rulesets for process control systems. See Law at ¶¶ 16, 88-89. Moreover, Dr. Jacobson testified that firm 305 necessarily includes "staff that understand . . . something about the 315s and understand, you know, issues about threats," and thus are intimately involved in the update process. Jacobson Tr. at 38:1-10; Goodrich Decl., ¶ 87.

Petitioner's failure to comply with Federal Circuit precedent as seemingly excused by the '474 Institution Decision cannot stand scrutiny at trial because background art cannot be used to change the basis of the combination, and the alleged technique in Law does not provide state-of-the-art evidence. See '474 Institution Decision at 31-32 (citing Law, ¶ 21). **First**, the '474 Institution Decision used the background art's alleged automatic technique to effectively supply the automatic limitation. However, background art cannot be used for the purpose of

changing a petition's combinations. *See Randall Mfg. v. Rea*, 733 F.3d 1355, 1362-63 (Fed. Cir. 2013) (emphasizing that while background art can provide evidence of the state-of-the-art, it cannot change the prior art combination that forms the basis of the asserted ground).

Here, instead of viewing the background art as evidence for what a skilled artisan would allegedly bring when reading Law's passing reference to third-party firms (*e.g.*, the cyber security risk management firm 305), the '474 Institution Decision used the background art for supplying the alleged automatic technique. *See* '474 Institution Decision at 32 (focusing on the alleged techniques disclosed in paragraph 21 of Law and a U.S. patent application publication ("the Xie publication") for the automatic limitation). But the basis of Petitioner's proposal rested on the automatic implementation in firm 305. In fact, the Xie publication was not even included in Petition's referenced background art. Thus, at trial, Petitioner cannot change the basis of its proposal and rely on alleged techniques in paragraph 21 or the Xie publication to supply the missing automatic generation limitation.

Second, the alleged technique in paragraph 21 does not provide state-of-the-art evidence of automatic generation by a third-party firm. During cross-examination, Dr. Jacobson admitted that he had not read the reference cited in paragraph 21, let alone in view of firm 305 that as a business requires IT personnel to understand the threat updates. *See* Jacobson Tr. at 58:3-25; Goodrich Decl., ¶ 88.

Reading paragraph 21 in view of third-party firms, a skilled artisan would appreciate that “separately-trained IT personnel” are still required to update rules to meet the needs of industrial environments they service. Goodrich Decl., (citing Law at ¶ 21 (describing that “separately-trained IT personnel” are required to “quickly and accurately manage” the industrial environment)), Similarly, in Law, separately trained IT personnel of third-party firm 305 are leveraged to update rulesets when new threats are discovered to ensure that the updates meet the needs of the particular process control system. *See, e.g.,* Law at ¶¶ 16, 88; *see also* Jacobson Tr. at 37:2-12, 38:1-10 (testifying that IT staff of firm 305 are involved in the process as they understand issues about threats). Thus, the third-party IT management referenced in paragraph 21 further supports the necessary involvement of third-party firm 305’s IT personnel when rulesets are updated to ensure that Law’s process control system’s needs are met. Goodrich Decl., ¶ 89.

In view of the foregoing, Petitioner cannot show that a POSITA armed with this state-of-the-art evidence 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.*, ¶ 90.

* * *

At bottom, there is no rational connection between Petitioner's theory and Law's disclosure to support a finding that firm 305 employs automatic updating of rulesets. Law, therefore, does not disclose nor render obvious "one or more first packet filtering rules of the first set of packet filtering rules . . . automatically created or altered by the security policy management server." *Id.* at ¶ 91.

4. Law Does Not Teach or Suggest the "Receiving a Dynamic Security Policy Comprising a First Set of Rules" Limitation

The term "receiving . . . a dynamic security policy comprising a first set of rules" refers to "an initial dynamic security policy including a first set of rules that is received by the PSG from the SPMS." *See* § IV.B, *supra*. Law does not satisfy the claim limitation under the correct construction because, as the record evidence demonstrates, Law's system (the alleged PSG end) only receives **updates** to its operator-created initial rulesets (*i.e.* ruleset 147)⁶ from firm 305. Goodrich Decl., ¶ 92.

In the Institution Decision, the Board implicitly interpreted this term to mean encompass updating an initial ruleset created by the PSG with a "'first set of packet filtering rules'" received from the SPMS. Institution Decision at 25 (finding that

⁶ Petitioner alleges that ruleset 147 is the claimed "dynamic security policy." *See* Pet. at 23-24.

“since an initial ruleset can be created by operators, and the claimed ‘first set of packet filtering rules’ would be an update to the initial ruleset, received from firm 305”). In construing the term in this way, the Board interpreted Law as teaching that firm 305 distributes updates to the operator-created initial rulesets of Law’s system. *Id.*; see also *id.* at 18 (interpreting firm 305 as a “‘perpetual service that proactively supplies the UTMS-configured firewalls . . . with’ updated ‘rulesets to meet the latest security threats.’”) (citing Law at ¶¶ 22, 88) (emphasis added).

Accordingly, under the Board’s interpretation of Law, operators create the initial rulesets while firm 305 distributes updates to the operator-created initial rulesets. Goodrich Decl., ¶ 93. Thus, under this interpretation of Law, Law does not satisfy “receiving a dynamic security policy comprising a first set of rules” when the correct construction is applied.

a. Law’s operators create initial rulesets with firm 305 only distributing updates to the operator-created initial rulesets

With process control systems “each ruleset is specific to the system it protects.” Law at ¶ 16. Law discloses that operators within the process control system create ruleset 147, along with rulesets 148, 151, and 153, particular to its protected system. See *id.* at ¶¶ 16, 23, 81, 90; Goodrich Decl., ¶ 94. Accordingly, initial rulesets are created by operators within the process control system, as recognized by the Board. Institution Decision at 25 (finding that “since an initial

ruleset can be created by operators, and the claimed ‘first set of packet filtering rules’ would be an update to the initial ruleset, received from firm 305”).

Critical to Law’s invention are graphical display applications that allow operators to create rulesets specific to the process control system. Law at Abstract (operators utilize “a workstation within a graphical process control system environment.”). By leveraging graphic display interfaces, operators create and manage rulesets specific to the security needs of the process control system. *See id.* at ¶ 21 (recognizing the need for operators to manage and monitor rulesets); *id.* at ¶ 23 (operators through graphic displays can create rulesets specific to the process control system); *id.* at ¶ 81 (employing pull-down menus to configure rulesets based on the sub-system); Goodrich Decl., ¶ 95.

Specifically, Law’s graphic display application allows an operator to configure rulesets based on various characteristics of the process control system:

Because the UTMS-configured network device 134, 146, 149, 152 is configured as a process variable (as described above), **the rulesets 148, 147, 151, 153 may be configurable by an operator or other personnel from a graphic display 129 at a workstation 120.** For example, based on various characteristics of the process control system 100 the user may individually configure and manage the network security of any portion of the process control system 100.

Law at ¶ 90 (emphasis added); *id.* at ¶ 23 (disclosing that “[o]perator displays for each component of the UTMS may be displayed within the DeltaV™ environment

or another graphical process control environment [T]he rulesets may be created based upon continuous or periodic evaluation of the process control system itself to provide immediate system protection from identified threats.”); *see also id.* at ¶¶ 81, 102. Given that an operator within the process control system creates rulesets, the system also includes a first set of rules in the operator-created rulesets. Thus, contrary to Petitioner’s theory (*see* Pet. at 27, 36-37, 39), ruleset 147 (and a first set of rules) is not created and distributed by firm 305 to the firewall devices. Law at ¶¶ 23, 81, 90, 102; *see also* Goodrich Decl., ¶ 96.

This analysis is confirmed by Law’s teaching of firm 305 as a remediation service that updates the various rulesets to remain effective against network threats:

[T]he various rulesets (e.g., rulesets 147, 148, 151, 153) associated with the UTMS configured network devices 146, 134, 149, 152 **require updates** to remain effective against network threats.

Law at ¶ 88 (emphasis added); *see also id.* at ¶ 89. Accordingly, Law describes a “method to **update** rulesets of the UTMS,” with firm 305 collecting threat data to construct updates to ruleset 147. *Id.* at ¶ 30 (emphasis added); *see also id.* at ¶ 88 (disclosing that “the various rulesets (e.g., ruleset[] 147 . . .) associated with the UTMS configured network devices . . . require updates to remain effective With reference to FIG. 3, . . . [firm 305] may collect threat data 310 from a plurality of various sources 315 to construct the various ruleset[] 147”); *id.* at Fig. 3. For instance, Law describes that the process control system sends domain-specific

information (*e.g.*, network infrastructure information) to firm 305 which based on this information collects data and identifies vulnerabilities that then can be translated into mitigations or rules for ruleset 147. *See id.* at ¶ 89 (“Each of these known vulnerabilities may then be translated into mitigations or rules for the various rulesets”). In this way, firm 305 acts as a remediation service to update the operator-created rulesets, including ruleset 147. *Id.*; *see also* Goodrich Decl., ¶¶ 97-98.

By leveraging firm 305 (and its IT personnel) as a remediation service to update the operator-created initial rulesets, the process control system's firewalls can either access the **operator-created ruleset data** (*e.g.*, including a first set of rules) as in figure 1A or **receive updates to ruleset data** (*e.g.*, updated sets) as in figure 3:

The UTMS-configured device or entity may receive the ruleset data and the UTMS-configured process object 204e may be configured or programmed to access the ruleset data 147, 148, 151, 153, (FIG. 1a) 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 FIG. 3, [])

Law at ¶ 66; *see also id.* at ¶ 26 (describing that the parameters of the UTMS-configured devices include “the ruleset[] and a ruleset update.”); Goodrich Decl., ¶ 98.

In view of the foregoing, operators within the process control system create initial rulesets (ruleset 147), with firm 305 simply providing updates to the operator-created rulesets. Goodrich Decl., ¶ 99. Accordingly, Law does not disclose “receiving a dynamic security policy comprising a first set of rules,” under the correct construction. See § IV.B, *supra* (proposing a construing meaning “an initial dynamic security policy, including a first set of rules, that is received by the PSG from the SPMS.”).

b. Petitioner's evidence and rationale show that firm 305 distributes only updates to the operator-created initial rulesets

In appreciating Law's full disclosure, it is readily apparent that Law describes operator-created ruleset 147 (including a first set of rules), with firm 305 simply providing remedial updates by constructing updates to ruleset 147. See Law at ¶ 88. Petitioner recognized this fact in the Petition:

The 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.”

Pet. at 13 (emphasis added) (citing Law at ¶ 22, Abstract, ¶ 88); *see also* Jacobson Tr. at 35:11-23 (testifying that firm 305 is a perpetual service that provides the process control system with updated rulesets); Goodrich Decl., ¶ 100. With this understanding, Petitioner and its expert acknowledge that figure 3 of Law is directed to firm 305 and its remediation service of updating rulesets. Pet. at 50

(acknowledging that figure 3 is directed to a “block diagram of a method to **update rulesets** of the UTMS.”) (quoting Law at ¶ 30).

Significantly, all of Petitioner's arguments rely on figure 3's method of updating the operator-created ruleset 147 with newly constructed or altered rules. *See, e.g.*, Pet. at 12-13, 23-27, 36-41, 44, 49-51 (citing Law's Figure 3 and/or paragraph 88, directed to updating the operator-created ruleset 147 of the process control system, for the “receiving a first set of packet filtering rules by the PSG” limitation, among others). Accordingly, while firm 305 (and its IT personnel) can construct the various rulesets in figure 3, those constructions only update the operator-created ruleset in order to remain effective against network threats. Law at ¶ 30 (“FIG. 3 is a logical block diagram of a method to update rulesets of the UTMS.”), *id.* at FIG. 3; ¶¶ 20, 66, 88; Goodrich Decl., ¶ 101.

Petitioner's evidence and rationale pertaining to threat data 310 further support that Law simply provides updates to the operator-created initial rulesets. Particularly, Petitioner's obviousness theory is based on firm 305 receiving threat data 310 used for updating rulesets. Pet. at 42-43 (threat data 310 “provides rapid **updates to rulesets**. . . [to] stay protected against emerging and changing network security threats.”) (citing Ex. 1007 at 5 (“**vulnerability data** [that] enables security product vendors to deliver product **updates**”) (emphases added)). That is, based on the received threat data, firm 305 (and its IT personnel) merely provides **updates**

to the operator-created initial rulesets in order for Law's system to "stay protected against emerging and changing network security threats." Pet. at 42-43; *see also* Goodrich Decl., ¶ 102.

Hence, under Petitioner's own evidence-backed theory, firm 305 simply distributes updates, not initial rulesets and rules as the proper construction requires. *See* § IV.B, *supra*; Goodrich Decl., ¶ 103.

c. The '474 Institution Decision's interpretation of Law finds no support from the record evidence

In the '474 Institution Decision, the Board disagreed "with Patent Owner that [] 'operators create the rulesets' in Law's system," and therefore coming to the opposite interpretation of Law as in the '266 Institution Decision. '474 Institution Decision at 34, 35 (concluding that Law's operators access "already existing ruleset created by . . . firm 305."). That Law's operators access already existing rulesets created by firm 305, as opposed to creating initial rulesets, is contradicted by Law's own teachings and extends and alters Law's disclosure. Goodrich Decl., ¶ 104.

First, the interpretation is contradicted by Law's own teachings that its system configures initial rulesets without outside IT personnel intervention, which the Decision even acknowledged. '474 Institution Decision at 34 (acknowledging that Law overcomes the need for separately-trained IT personnel to create rulesets by providing operator workstations within the process control system that do so). The '474 Institution Decision went so far as acknowledging that Law's operators

configure and monitor the Law's process control equipment “**without [outside or external] IT personnel intervention.**” *Id.* (citing Law at ¶ 59) (emphasis added). That acknowledgment aligns with Centripetal's evidence-backed argument: operators using workstations create the initial rulesets (*i.e.* ruleset 147) without firm 305's involvement. See Paper 7 (Prelim. Response, “POPR”) at 40-43; Law at ¶¶ 21-23, 59, 81, 90, 102; *see also* Goodrich Decl., ¶ 105.

Second, such an interpretation extends and alters Law's disclosure by inserting the language of an operator “access[ing] an already existing ruleset created by cyber security risk management firm 305.” '474 Institution Decision at 34-35 (citing Law at ¶¶ 66, 88, 90, 102). In coming to this interpretation, the Decision cited paragraphs 66, 88, 90, and 102 of Law, however, the cited paragraphs do not recite that language or even similar language. Goodrich Decl., ¶¶ 106-111.

Specifically, Law's paragraphs 90 and 102 detail that operators may configure the rulesets (*i.e.* ruleset 147) from graphic displays of operator workstations:

Because the UTMS-configured network device 134, 146, 149, 152 is configured as a process variable (as described above), the rulesets 148, 147, 151, 153 may be configurable by an operator or other personnel from a graphic display 129 at a workstation 120.

Law at ¶ 90.

For example, a UTMS-configured process object 204e (FIG. 2) 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 and the network security in the process control system.

Id. at ¶ 102.

With respect to Law's paragraph 88, that passage details a method of a third-party firm updating the operator-created initial rulesets to remain effective against newly detected threats:

As previously described, **the various rulesets** (e.g., rulesets 147, 148, 151, 153) associated with the UTMS configured network devices 146, 134, 149, 152 **require updates** to remain effective against network threats.

Id. at ¶ 88 (emphasis added).

Finally, paragraph 66 details that the UTMS-configured devices can access the operator-created ruleset data (Fig. 1a) and other “**update data**” from a third-party source (Fig. 3):

The UTMS-configured device or entity may receive the ruleset data and the UTMS-configured process object 204e may be configured or programmed to access the ruleset data 147, 148, 151, 153, (FIG. 1a) **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 FIG. 3, below).

Id. at ¶ 66 (emphasis added).

The above paragraphs do not recite or otherwise contemplate an operator “access an already existing ruleset created by cyber security risk management firm 305.” ’474 Institution Decision at 35. Instead, they plainly show that operators via workstations configure initial rulesets (*i.e.* ruleset 147) with Law’s system simply receiving updates from firm 305, as Law’s figure 3 illustrates. Law at Fig. 3, ¶ 30 (“FIG. 3 is a logical block diagram of a method to **update rulesets of the UTMS**”) (emphasis added); Goodrich Decl., ¶ 110. Indeed, as confirmed by Petitioner’s own evidence-backed theory. *See* § VI.A.4.b, *supra*.

As such, no record evidence supports an interpretation of Law in which operators access already existing rulesets created by firm 305 rather than create initial rulesets themselves. To the contrary, all the record evidence confirms the Board’s interpretation in the ’266 Institution Decision—that operators create initial rulesets while firm 305 merely provides updates to the rulesets. Goodrich Decl., ¶ 111.

* * *

At bottom, Law’s operator-created initial rulesets does not meet “receiving a dynamic security policy comprising a first set of rules,” under the correct construction, which is, an initial dynamic security policy, including a first set of

rules, that is received by the PSG from the SPMS. *See* § IV.B, *supra* Goodrich Decl., ¶¶ 106-111.

B. Ground 2: Claims 1-24 are Patentable Over Law in View of Wood

Petitioner references Wood only for its alleged disclosure of “one or more suspect address sources 210’ providing [sic] ‘a feed of suspect addresses from one or more sources on the external network.’” Pet. at 65 (quoting Wood at ¶¶ 21, 32, 34, *id.* at Fig. 2). Whether or not Wood provides suspect network addresses from an external source does not cure any of Law’s deficiencies as set forth above. *See* § VI.A, *supra*. Accordingly, Ground 2 fails for the same reasons Ground 1 fails. Goodrich Decl., ¶ 112.

Therefore, Petitioner fails to show by a preponderance of the evidence that Law in view of Wood renders obvious the Challenged Claims.

C. Ground 3: Claims 6, 13, 19, and 26 are Patentable Over Law in View of Jungck

As established above, Petitioner fails to demonstrate by a preponderance of the evidence that Independent Claims 1, 8, 15 and 21 are obvious over Law, and Petitioner cites Jungck (Ex. 1008) only for the dependent claims. *See* Pet. at 2-3. Thus, Jungck does not cure any of the above-noted deficiencies. *See* § VI.A, *supra*.

Therefore, Petitioner also fails to show by a preponderance of the evidence that Law in view of Jungck renders obvious Claims 6, 13, 19, and 26, which depend

from the independent claims, are unpatentable over Law in view of Jungck. Goodrich Decl., ¶ 113.

D. Ground 4: Claims 6, 13, 19, and 26 are Patentable Over Law in View of Wood and Jungck

As established above, Petitioner fails to demonstrate by a preponderance of the evidence that Independent Claims 1, 8, 15 and 21 are obvious over Law and Wood, and neither Wood nor Jungck cure any of Law's deficiencies as set forth above. *See* §§ VI.A, VI.B, *supra*.

Therefore, Petitioner also fails to show by a preponderance of the evidence that Law in view of Jungck renders obvious Claims 6, 13, 19, and 26, which depend from the independent claims, are unpatentable over Law in view of Wood and Jungck. Goodrich Decl., ¶ 114.

VII. CONCLUSION

For all of these reasons, Centripetal respectfully requests that the Board hold patentable the Challenged Claims.

Respectfully submitted,

Dated: October 20, 2023

By: /James Hannah/

James Hannah (Reg. No. 56,369)
Jenna Fuller (Reg. No. 74,212)
Kramer Levin Naftalis & Frankel LLP
333 Twin Dolphin Drive, Suite 700
Redwood Shores, CA 94065
Tel: (650) 752-1700 Fax: (650) 752-1800
Email: jhannah@kramerlevin.com
Email: jfuller@kramerlevin.com

Jeffrey H. Price (Reg. No. 69,141)
Kramer Levin Naftalis & Frankel LLP
1177 Avenue of the Americas
New York, NY 10036
Tel: (212) 715-7502 Fax: (212) 715-8302
Email: jprice@kramerlevin.com

Scott M. Kelly (Reg. No. 65,121)
Bradley C. Wright (Reg. No. 38,061)
John R. Hutchins (Reg. No. 43,686)
BANNER & WITCOFF, Ltd.
1100 13th Street, NW, Suite 1200
Washington, DC 20005
Email: skelly@bannerwitcoff.com
Email: bwright@bannerwitcoff.com
Email: jhutchins@bannerwitcoff.com

Attorneys for Patent Owner

CERTIFICATE OF COMPLIANCE

The undersigned hereby certifies that the portions of the foregoing **PATENT OWNER'S RESPONSE** specified in 37 C.F.R. § 42.24 has 11,306 words in compliance with the 14,000-word limit set forth in C.F.R. § 42.24(b)(2). This word count was prepared using the Microsoft Word word-processing system used to prepare this paper.

Dated: October 20, 2023

By: /James Hannah/

James Hannah (Reg. No. 56,369)
Jenna Fuller (Reg. No. 74,212)
Kramer Levin Naftalis & Frankel LLP
333 Twin Dolphin Drive, Suite 700
Redwood Shores, CA 94065
Tel: (650) 752-1700 Fax: (650) 752-1800
Email: jhannah@kramerlevin.com
Email: jfuller@kramerlevin.com

Jeffrey H. Price (Reg. No. 69,141)
Kramer Levin Naftalis & Frankel LLP
1177 Avenue of the Americas
New York, NY 10036
Tel: (212) 715-7502 Fax: (212) 715-8302
Email: jprice@kramerlevin.com

Scott M. Kelly (Reg. No. 65,121)
Bradley C. Wright (Reg. No. 38,061)
John R. Hutchins (Reg. No. 43,686)
BANNER & WITCOFF, Ltd.
1100 13th Street, NW, Suite 1200
Washington, DC 20005
Email: skelly@bannerwitcoff.com
Email: bwright@bannerwitcoff.com
Email: jhutchins@bannerwitcoff.com

Attorneys for Patent Owner

CERTIFICATE OF SERVICE

The undersigned certifies, in accordance with 37 C.F.R. § 42.6(e), and pursuant to agreement by the parties that filing with the Board through the Patent Trial and Appeal Case Tracking System (P-TACTS) constitutes electronic service, that service was made on Petitioner as detailed below.

<i>Date of service</i>	October 20, 2023
<i>Manner of service</i>	Electronic Filing with the Board
<i>Documents served</i>	PATENT OWNER'S RESPONSE
<i>Persons served</i>	Gerard M. Donovan Peter J. Chassman Jonathan I. Detrixhe Sidharth Kapoor gdonovan@reedsmith.com pchassman@reedsmith.com jdetrixhe@reedsmith.com skapoor@reedsmith.com

By: /James Hannah/
James Hannah (Reg. No. 56,369)
Lead Counsel for Patent Owner