

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KEYSIGHT TECHNOLOGIES, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, LLC,
Patent Owner.

Case IPR2023-00445¹
Patent No. 10,785,266

PATENT OWNER'S SUR-REPLY

¹ IPR2023-01329 has been joined with this proceeding.

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	THE CHALLENGED CLAIMS ARE PATENTABLE	3
A.	Law Does Not Render Obvious Claims 1-27 (Ground 1).....	3
1.	Law Does Not Teach or Suggest “A Plurality of Packet Security Gateways That Collectively Provide an Entire Interface Across a Boundary of a Network Protected”	3
a.	Claim Construction: the Preambles of Independent Claims 1, 8, and 15 are Limiting	3
b.	Law’s Network Access Device 149c Does Not Join Together Networks 150a and 150b Into a Single Network 150 Protected by a Plurality of PSGs	3
c.	Law’s “Network 150” is One Process Control Network, Not a Combination of Networks 150a and Network 150b.....	7
2.	Each of Law’s Subsystems Has its Own Global Set of Rules Unique to Devices Within the Subsystem With Different Rulesets Applied to Traffic	10
a.	Each Subsystem Has its Own Global Set of Rules Unique to its Devices.....	10
b.	The Subsystems Apply Different Rulesets to Traffic Traversing Their Network Boundaries.....	13
3.	Law’s Firm 305 is Not a “Security Policy Management Server” That Distributes Initial Rulesets And Automatically Updates the Rulesets	15
a.	Firm 305 is Not a “Security Policy Management Server” But a Commercial Entity	15
b.	Firm 305 Does Not Automatically Update Rulesets as IT Personnel Are Required in the Updates	16

c.	Firm 305 Does Not Distribute “a Dynamic Security Policy Comprising a First Set of Rules”	20
i.	Claim Construction: “Receiving a Dynamic Security Policy Comprising a First Set of Rules”	20
ii.	Firm 305 Only Distributes Updates to Operator-Created Initial Rulesets	22
B.	Law in View of Wood Does Not Render Obvious Claims 1-24 (Ground 2)	25
C.	Law in view of Wood and/or Jungck Fails to Render Obvious the Dependent Claims (Grounds 3 and 4)	25
III.	CONCLUSION.....	25

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>3M Innovative Props. Co. v. Avery Dennison Corp.</i> , 350 F.3d 1365 (Fed. Cir. 2003)	22
<i>Ariosa Diagnostics v. Verinata Health, Inc.</i> , 805 F.3d 1359 (Fed. Cir. 2015)	19, 20
<i>Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.</i> , 800 F.3d 1375 (Fed. Cir. 2015)	17
<i>Henny Penny Corp. v. Frymaster LLC</i> , 938 F.3d 1324 (Fed. Cir. 2019)	19
<i>Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.</i> , 821 F.3d 1359 (Fed. Cir. 2016)	16
<i>Xerox Corp. v. Bytemark, Inc.</i> , No. IPR2022-00624, Paper 9 (P.T.A.B. Aug. 24, 2022).....	6
Statutes	
35 U.S.C. § 312(a)(3).....	16
35 U.S.C. § 316(e)	18

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)

Exhibit	Description
2011	Excerpts from The American Heritage Dictionary - "Firm" (4th ed. 2001)
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)
2018	Transcript of Deposition of Douglas Jacobson, Ph.D., <i>Keysight Technologies, Inc. v. Centripetal Networks, LLC</i> , Nos. IPR2023-00445, IPR2023-00448, taken on March 27, 2024

I. INTRODUCTION

The Challenged Claims are patentable over Law. First, rather than disclosing “a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected,” Law discloses a single firewall architecture. Recognizing that networks 150a and 150b are each protected by a single firewall, Petitioner paints network access device (“NAD”) 149c as something it is not: a device that joins two networks into a single network. Paper 21 (“Reply”) at 4-6, 9-10. To the contrary, Law’s NAD 149c is a perimeter device that, by definition, sits outside of and controls access between the two different networks. *See* Law (Ex. 1005), ¶¶ 51, 52, 92, 94. Because networks 150a and 150b are different networks each protected by a single firewall, Law does not disclose a “a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected.”

Law also fails to teach or suggest applying a “first set of packet filtering rules” to “all network traffic traversing the boundary” because firewalls 146a and 146b apply separate, independent, rulesets that are unique to subsystems 105a and 105b, respectively. Paper 17 (“POR”) at 27-28 (citing Law, ¶ 51). Undisputed expert testimony establishes that this basic premise underlying Law’s system architecture extends even to its “global” rulesets, which are only “global” in the sense that they apply to all of the devices in a particular subsystem. Ex. 1015 (“Goodrich Tr.”) at

11:16-12:23. There simply is no “global” set of rules that is applied at firewalls 146a and 146b that could qualify as the claimed “first set of packet filtering rules.” *Cf.* Reply at 11.

The Challenged Claims are also patentable because cyber security risk management firm 305 is not a “security policy management server” (“SPMS”) but rather a commercial entity, which consists of IT personnel and various IT infrastructure components. In fact, Petitioner’s expert, Dr. Jacobson, acknowledged this very fact. *See* Ex. 2014 at 37:2-38:7. Thus, for this basis alone, Law’s firm 305 does not correspond to the claimed SPMS.

Firm 305 also does not distribute a dynamic security policy comprising a first set of rules because operators *within* the process control system create the initial policies rather than a server as claimed. POR at 42-53; *see* Law, ¶¶ 22, 66, 88 (disclosing that firm 305 only provides updates to the operator-created policies).

Finally, firm 305 does not automatically update the operator-created rulesets because firm 305’s IT personnel are “required to update the ruleset[s] when new threats are discovered” to ensure that the desired protection is provided, and therefore does not meet the automatic update requirement of the claims. Law, ¶¶ 16, 88.

II. THE CHALLENGED CLAIMS ARE PATENTABLE

A. Law Does Not Render Obvious Claims 1-27 (Ground 1)

Most of the errors in Petitioner's Reply stem from its efforts to: (1) make NAD 149c do things it does not, including joining two separate networks into one; (2) manufacture a "global" set of rules that would be applied at firewalls 150a and 150b, despite Law's requirement that each separate subsystem be protected by its own unique ruleset; and (3) turning firm 305 into a "security policy management server" despite it being a commercial entity with humans (not servers) who are responsible for updating operator-defined policies.

1. Law Does Not Teach or Suggest "A Plurality of Packet Security Gateways That Collectively Provide an Entire Interface Across a Boundary of a Network Protected"

a. Claim Construction: the Preambles of Independent Claims 1, 8, and 15 are Limiting

Petitioner does not dispute that the preambles of Independent Claims 1, 8, and 15 are limiting. *See generally* Reply. Therefore, the Board should conclude the preambles as limiting and find that Law does not render obvious the preamble limitations, as discussed in detail below.

b. Law's Network Access Device 149c Does Not Join Together Networks 150a and 150b Into a Single Network 150 Protected by a Plurality of PSGs

Law does not disclose "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” because Law discloses a single firewall protecting each process control network rather than a plurality of firewalls that are designed to implement common rule sets sent from security policy management server. POR at 17-25; Law, ¶¶ 51, 52 (disclosing that firewall 146a protects network 150a of subsystem 105a, and firewall 146b protects network 150b of subsystem 105b).

Petitioner's attempt to transform Law's networks 150a and 150b into a single network runs headlong into Law's explicit disclosure that NAD 149c is a “perimeter device” that is, by definition, “outside of the process control network 150a or 150b.” Law, ¶ 51, *see also id.* at ¶¶ 22, 52, 92. If NAD 149c is “**outside** of the process control network 150a or 150b,” then it cannot simultaneously be **within** the single process control network that the NAD allegedly creates. Law, ¶ 51 (emphasis added). Petitioner's expert agrees. Ex. 2018 at 21:1-9 (Dr. Jacobson agreeing that NAD 149c sits outside the process control subsystems and respective networks).

Petitioner has no answer to this determinative fact, and no amount of hindsight-tainted textual gymnastics supports its contention that NAD 149c joins process control network 150a and process control network 150b into a single process control network. Reply at 9. Rather than join networks together, Law's NADs “control network access” between different networks. *See* Law, ¶¶ 51, 94 (“[D]evice 149 may be used by the operator or other authenticated personnel to **control**

network access between the site and the internet and, as shown in FIG. 5, between sites, or, as shown in FIG. 6, within sites.”) (emphasis added). Law’s NADs are “perimeter devices” that are located “outside” of the process control networks, not “internal” devices, as Petitioner represents. *Compare id. with* Reply at 9.

And contrary to Petitioner’s claim that Dr. Goodrich agreed that the NAD joins together the networks and therefore “a device that is internal” (Reply at 9), Dr. Goodrich testified the opposite:

Q. So let’s assume that those communications, all of the communications flowing through network access device 149c are part of the local network, a LAN embodiment as described in figure 1b and not over the internet, as I think you just said is a possibility. In that situation, couldn’t subnetworks 150a and 150b be considered a combined network?

A. No.

Goodrich Tr. at 49:11-19 (emphasis added). In support of this answer, Dr. Goodrich gave several reasons that Petitioner does not rebut. For example, he explained that because the NAD “has rulesets associated with it for communications” to thereby block traffic, it does not join networks. *See id.* at 51:8-14; Law, ¶¶ 51, 102 (describing that the NAD is associated with rulesets to control network communication). Dr. Goodrich further explained that the NAD does not join together the networks because each is understood to include specialized devices and

perform specialized functionalities. *See* Goodrich Tr. at 49:21-51:1. On the other hand, Dr. Jacobson's Reply Declaration offers unsupported, conclusory testimony that parrots the Reply with no independent analysis or evidentiary support. *See* Ex. 1014, ¶¶ 8-9, 12-13; Reply at 4-6, 9-10. As such, it should be entitled to little or no weight. *See Xerox Corp. v. Bytemark, Inc.*, No. IPR2022-00624, Paper 9 at 15 (P.T.A.B. Aug. 24, 2022) (precedential).

Petitioner's contention that NAD 149c joins the two separate networks into a single network is also self-contradictory. Reply at 4-6, 9-10; Ex. 2018 at 13:24-14:13. Law defines the NAD as a device that controls network access between networks 150a and 150b, just as it controls access between the Internet and those networks. *See* Law, ¶ 94 (defining the NADs as controlling network access between networks), Figs. 4-5. If the Board were to agree that NAD 149c joins networks 150a and 150b into a single network 150 merely because it "provide[s] communications between them" (Reply at 9), then NAD 149a would likewise join the Internet and process control network 150a into a single combined network. Not only is that an illogical result, but it contradicts Petitioner's argument that there is a boundary between network 150a and the Internet. *See* Pet. at 14-15.

In view of the foregoing, Law does not disclose or otherwise suggest that “network 150” refers to a “single network” “joined” by “sub-networks 150a and 150b.”² Reply at 9; *see also id.* 6-8 (citing Law at ¶¶ 53, 57).

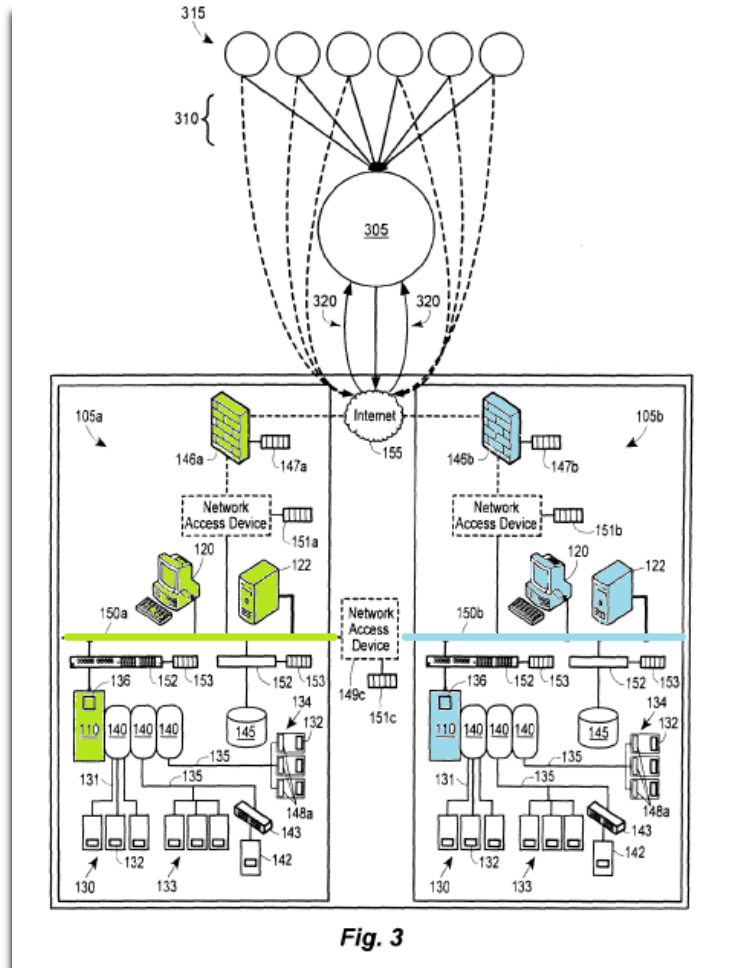
c. Law’s “Network 150” is One Process Control Network, Not a Combination of Networks 150a and Network 150b

Contrary to Petitioner’s contentions, Law only uses the term “a process control network 150”/“network 150” (*see* Law ¶¶ 53, 57) when referring to a single process control network and when it is not necessary to distinguish between two or more different process control networks. *See* POR at 18. The specification never refers to “process control network 150” as the *combination* of two or more process control networks, as Petitioner claims. Reply at 6-8.

In paragraph 53, Law describes a system that includes process control networks 150a and 150b and “one or more process controllers 110 communicatively connected to one or more host workstations or computers 120-122 . . . over a process control network 150.” Law, ¶ 53. In this context, Law uses the term “over [] network

² Petitioner mislabels networks 150a and 150b as “sub-networks 150a and 150b” in an effort to distort the record. *See* Reply at 9; *see also id.* at 1, 3, 7, 9. To be clear, Law never refers to networks 150a and 150b as sub-networks. They are uniformly referred to as “process control network 150a” and “process control network 150b.”

150” in shorthand notation in reference to either network 150a *or* 150b and their respective devices in communication with one another. For instance, as shown in Figure 3 reproduced below, controller 110 (green of subsystem 105a) communicates with computers 120-122 (green) over the process control network 150a (as indicated by the green line), while controller 110 (blue of subsystem 105b) communicates with computers 120-122 (blue) over the process control network 150b (as indicated by the blue line).



Law at Fig. 3 (annotated). Accordingly, the controllers are communicatively coupled to devices via their respective networks 150a, 150b, with “network 150” used as shorthand to describe the intra-communications.

Law’s paragraph 57 is also consistent with Law’s usage of “network 150” in describing network 150a *or* 150b, depending on the context. Law, ¶ 57. Accordingly, just as with paragraph 53, controller 110 (green) communicates with devices within subsystem 105a through its relevant “network 150” (*i.e.* network 150a) while controller 110 (blue) communicates with devices within subsystem 105b through its relevant “network 150” (*i.e.* network 150b), as the above figure depicts. *See id.* at ¶ 57 (the controller communicates with devices “through the network 150.”). Significantly, when controller 110 (green) communicates with firewall 146b (blue of subsystem 105b), the communication occurs through both networks 150a and 150b, as Petitioner acknowledges. Reply at 7 (acknowledging that “communications between the controller 110 and firewall 146b occur through both sub-network 150a and sub-network 150b”). Accordingly, this type of inter-communication occurs through the two networks rather than within a single combined network. *See* Ex. 2018 at 24:7-25:9 (Dr. Jacobson describing the communication between the two networks).

On the full record, Petitioner fails to show by a preponderance of the evidence that Law teaches or suggests a plurality of packet security gateways that collectively provide an entire interface across a boundary.

2. Each of Law's Subsystems Has its Own Global Set of Rules Unique to Devices Within the Subsystem With Different Rulesets Applied to Traffic

Law also does not disclose applying "a first set of filtering rules" to network traffic traversing the boundary because each firewall works independently and applies different rulesets. POR at 27-33.

a. Each Subsystem Has its Own Global Set of Rules Unique to its Devices

Petitioner's entire argument for this limitation relies on the false premise that all of Law's firewalls apply the same "global" ruleset 147. Reply at 11 (alleging that each subsystem implements "ruleset 147"). As established in the POR, however Law's reference to a "global" set of rules is one that applies to all of the devices *within* a single subsystem:

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.

Law, ¶ 51; POR at 28.

Law contrasts these “global” rule sets, which are applied at perimeter devices like firewalls, with “a subset of the global set of rules that only defines access to the particular internal device.” Law, ¶ 51. Thus, each subsystem has its own global ruleset, and there is no ruleset that applies to multiple subsystems. *Id.* Unrebutted testimony and Law itself, therefore, contradict Petitioner’s argument that the same global set of rules (ruleset 147) applies to both subsystems because each subsystem has a unique typology and needs, requiring its own global set of rules. *Cf.* Reply at 11-12.

Petitioner does not deny that Law’s contribution to the art concerns how to adequately protect process control systems by providing rulesets unique to each subsystem’s features, configurations, and permissions. POR at 28-31. Given this basic undisputed fact, Petitioner is left to suggest firewalls 146a and 146b would apply the same set of rules to traffic because the devices in the subsystems could be identical. Reply at 12. To the contrary, however, Law discloses that each subsystem has its own “unique and device specific features” with “rules and/or access privileges for each of the devices.” Law, ¶¶ 18, 19; *see also* POR at 28-29 (citing Law, ¶¶ 11, 16, 22, 55, 89). Accordingly, given the uniqueness of the devices, a global set of rules for subsystem 105a would be different than the global set of rules for subsystem 105b.

Petitioner also suggests that firewalls 146a and 146b apply the same ruleset 147. Reply at 11. However, as it does with the term “network 150,” Law uses the term “ruleset 147” as shorthand when it is not necessary to distinguish between the ruleset applied by firewall 146a and firewall 146b. Yet, when it is necessary to distinguish the rulesets applied by those firewalls, Law explicitly refers to rulesets 147a or 147b, respectively. See POR at 31-32 (depicting that the communication paths apply different rulesets). Dr. Goodrich testified to the same effect:

A. So to answer your question, the ruleset 146, 147 that is referenced here in paragraph 51, ***person of ordinary skill in the art would understand that this is referring to generically either the ruleset 147a or 147b***

Goodrich Tr. at 11:16-20 (emphasis added); *see also id.* at 9:22-25 (counsel asking whether ruleset 147 “may include a global set of rules”), 11:16-12:23 (Dr. Goodrich explaining that ruleset 147a is associated with firewall 146a while ruleset 147b is associated with firewall 146b). Thus, Dr. Goodrich confirms that a POSITA would understand that a global set of rules (ruleset 147a) is used by subsystem 105a and is *separate* from a global set of rules (ruleset 147b) used by subsystem 105b. See POR at 32 (citing Fig. 3 (annotated)).

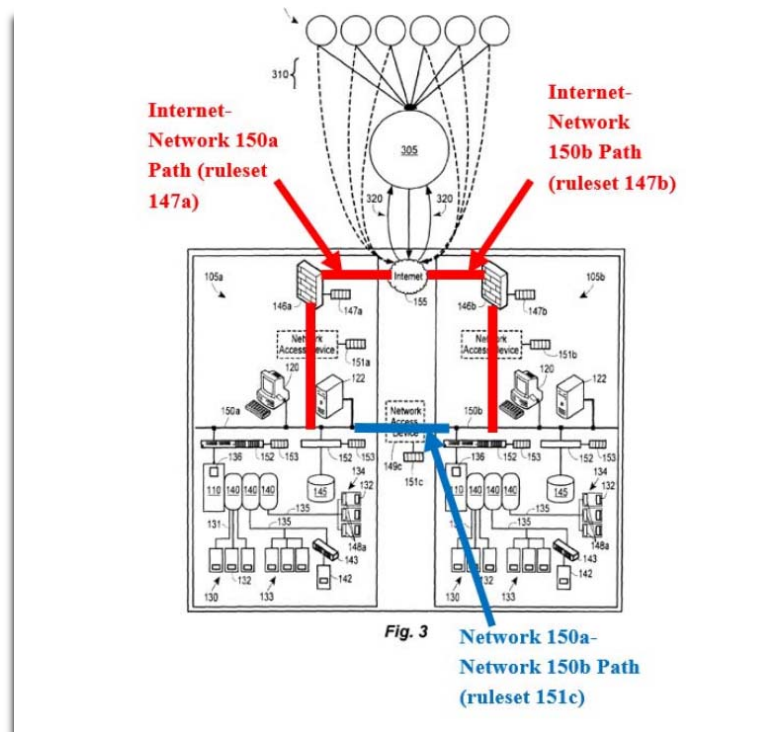
Petitioner leaves this testimony un rebutted. Petitioner simply reiterates paragraph 51’s disclosure while citing Dr. Jacobson’s reply declaration, a carbon copy of the Reply with no additional reasoning or analysis of how Dr. Jacobson

would interpret Law's reference to ruleset 147 in paragraph 51. Reply at 11 (citing Ex. 1014, ¶ 22).

b. The Subsystems Apply Different Rulesets to Traffic Traversing Their Network Boundaries

To the extent that Petitioner suggests that NAD 149c is one of the claimed plurality of PSGs, the Board should find the Challenged Claims patentable because if the NAD applies any ruleset at all, it is different than the rulesets applied at the other alleged PSGs (Law's firewalls). See POR at 31-33 (showing that Law applies different rulesets to traffic). Law, therefore, does not disclose applying "a first set of packet filtering rules" to network traffic traversing the boundary. '266 Patent at Claims 1, 8, 15. Indeed, when it is convenient, Petitioner argues that NAD 149c may not apply any rulesets whatsoever, let alone the same "first" ruleset as another alleged PSG. Reply at 12-13; *see also* POR at 31-33.

Because NAD 149c is a perimeter device that controls network access between networks 150a and 150b, traffic crossing the boundary of network 150a to network 150b, or vice versa, is subject to the NAD's sets of rules, including ruleset 151c, that monitors and controls traffic. Law, ¶ 94; *see also id.* at ¶¶ 51, 102 (disclosing that the NAD includes rulesets associated with it); Ex. 2018 at 18:21-20:19. This set of rules is different from the set of rules applied at the other communication paths.



POR at 32 (citing Law at Fig. 3 (annotated)).

Accordingly, given that the NAD is a perimeter device with its own set of rules, Law's communication paths are subject to the application of different rulesets because the firewalls do not work together or apply a common rule set. Petitioner's admission that NAD may or may not apply ruleset 151c to traffic should also be taken as further evidence that Law does not apply rulesets, let alone the same set, to traffic traversing the boundary as in the Challenged Claims. *See* '266 Patent at Claim 1.

* * *

On the full record, Petitioner fails to show by a preponderance of the evidence Law teaches or suggests applying “a first set of packet filtering rules” to traffic traversing the boundary.

3. Law's Firm 305 is Not a “Security Policy Management Server” That Distributes Initial Rulesets And Automatically Updates the Rulesets

The Challenged Claims are also patentable because Petitioner attempts to make firm 305 into something it is not, *i.e.*, an SPMS that distributes a dynamic security policy, including a first set of packet filtering rules. Not only is firm 305 not a server, but it also fails to automatically generate rulesets and distribute dynamic security policies.

a. Firm 305 is Not a “Security Policy Management Server” But a Commercial Entity

Petitioner contends that “Law's cyber security risk management firm 305 corresponds to the claimed ‘security policy management server.’” Pet. at 23; Ex. 2018 at 38:2-39:3. It does not.

Firm 305 is a **commercial entity**, not a server, that includes IT personnel staff and various other components that are involved in updating rulesets. POR at 34-35 (citing Ex. 2011 at 3). On cross-examination, Dr. Jacobson acknowledged that firm 305 operates as a service comprising various IT infrastructure and staff. Ex. 2014 at 37:2-38:7. Accordingly, firm 305 leverages IT staff and various IT infrastructure components in updating rulesets by “collecting the threat data,” “constructing data

files,” and “executing [] computer-implemented algorithm[s] to determine if the rulesets effectively secure the process control systems.” Law, ¶ 88.

In reply, Petitioner’s only counter is to assert that the claimed “security policy management server” may be **part** of that commercial entity. See Reply at 14. This argument misses the point, which is that the Challenged Claims require a server to perform certain functionality—regardless of whether it is part of a commercial entity—and Petitioner cannot identify any such server. See ’266 Patent at Claims 1, 8, 15, 21. The parties agree that firm 305 is not a server, and Petitioner has not identified any server within firm 305 that automatically generates and distributes dynamic security policies. See *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1369 (Fed. Cir. 2016) (“It is of the utmost importance that petitioners in the IPR proceedings adhere to the requirement that the initial petition identify ‘with particularity’ the ‘evidence that supports the grounds for the challenge to each claim.’”) (quoting 35 U.S.C. § 312(a)(3)).

Petitioner, therefore, fails to demonstrate that firm 305 satisfies the claimed SPMS.

b. Firm 305 Does Not Automatically Update Rulesets as IT Personnel Are Required in the Updates

Law’s firm 305 does not “automatically create[] or alter[] one or more packet filtering rules,” as required by the Challenged Claims. See ’266 Patent at Claims 1, 8, 15, 21. Petitioner’s arguments otherwise are meritless because Law does not

disclose automatic updates by firm 305 or establish that it would have been obvious to modify Law in light of its express disclosure that requires IT personnel to update rulesets. *See* Reply at 13-18.

First, Law does not disclose automatically creating or altering rulesets. *See id.* at 15-19 (citing paragraphs 83 and 88 of Law, neither of which discloses that firm 305 provides automatic updates of rulesets). Although paragraph 88 discloses performing ruleset updates using “any type of information technology methods” (*id.* at 15-17 (citing Law at ¶ 88)), it does not disclose any methods that would or even could forego the required manual input of IT personnel. Law, ¶ 88. On the contrary, Law is clear that IT personnel are “still required to update the ruleset when new threats are discovered.” POR at 14-15, 34-35; Law, ¶¶ 16, 88.

Rather than confronting this determinative fact, Petitioner tries to shift the burden onto Centripetal, claiming that Centripetal failed to “explain what role IT personnel would have had, if any, in the constructing of rulesets.” Reply at 16. But it is Petitioner’s burden to show that Law discloses firm 305 providing updates without IT personnel involvement, and that burden does not shift to Centripetal to prove otherwise. *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015) (“In an *inter partes* review, the burden of persuasion is on the petitioner to prove “unpatentability by a preponderance of the evidence,” 35 U.S.C. § 316(e), and that burden never shifts to the patentee.”).

Nonetheless, Centripetal did show that firm 305's IT personnel are involved in constructing updates and running tests (for example, executing computer-implemented algorithms), because, as Dr. Jacobson asserted, they "understand . . . something about 315s and understand, you know, issues about threats" and have knowledge of the protection required by the control system. Ex. 2014 at 38:1-10; POR at 35, 39.

Law's paragraph 83 also does not support Petitioner's position because it is unrelated to any activities undertaken by firm 305, which is the alleged SPMS. See POR at 36-37. Dr. Jacobson confirms that although certain network conditions can trigger the process control system to automatically update a ruleset, that process is unrelated to the manner in which firm 305 generates ruleset updates. Law, ¶ 83; Ex. 2014 at 54:17-19, 55:10-23. Petitioner has not, therefore, established that Law discloses an SPMS that automatically creates or alters a ruleset, as claimed.

Second, Petitioner's reliance on alleged state-of-the-art techniques is unavailing. Reply at 16-17. Petitioner fails to address, let alone rebut, Centripetal's argument that paragraph 21 in Law does not provide state-of-the-art evidence of automatic rule generation because Law explicitly explains how and why IT personnel must be involved in managing access to the process control network. See POR at 40-41 (citing Law, ¶ 21 ("'[S]eparately-trained IT personnel' are required to 'quickly and accurately manage' the industrial environment"); *id.* at ¶ 20 (IT

personnel are involved in configuring ruleset updates so as to “account for the unique needs of the control system)).

Similarly, Petitioner fails to explain **why** a POSITA would have implemented automatic ruleset updates in firm 305 when Law explains that IT personnel of firms are still required to update rulesets of the process control system or demonstrate **how** automatic updates would have overcome its stated need for manual updates by third-party IT personnel. See POR at 38-39 (citing *Ariosa Diagnostics v. Verinata Health, Inc.*, 805 F.3d 1359, 1366 (Fed. Cir. 2015) (a petitioner must “provide adequately developed explanations when relying on background knowledge based on cited art”); see also *id.* at 14-15 (establishing that Law’s invention still leverages IT personnel of third party firms to perform manual updates). Instead, Petitioner selectively cherry-picks Law’s “any type of information technology method” passage to argue that this would have *suggested* to a POSITA to use automatic techniques (see Reply at 17). This cherry-picking fails because it excludes Law’s teaching that third-party IT personnel are still required for updating process control system. *Henny Penny Corp. v. Frymaster LLC*, 938 F.3d 1324, 1331-32 (Fed. Cir. 2019) (articulating the “longstanding principle that the prior art must be considered for all its teachings, not selectively.”) (citations omitted).

Petitioner’s other allegation, that firm 305’s employment of IT personnel “does not negate the obviousness of incorporating Law’s teachings with respect to

the automatic generation of rules,” (Reply at 17) similarly fails because it does not explain why a POSITA would have removed the IT personnel who are required to ensure that each process control system receives the desired protection from the update process. Law, ¶¶ 16, 88; *Ariosa Diagnostics*, 805 F.3d at 1366.

c. Firm 305 Does Not Distribute “a Dynamic Security Policy Comprising a First Set of Rules”

i. Claim Construction: “Receiving a Dynamic Security Policy Comprising a First Set of Rules”

The term “receiving a dynamic security policy comprising a first set of rules,” means that PSG must receive a dynamic security policy, including a first set of rules, from the SPMS, which is then updated. *See* POR at 8-10. Petitioner’s contention that the “first set of packet filtering rules” is not within the dynamic security policy is contrary to the claims. Reply at 20-22.

Centripetal’s construction accounts for the difference between a “dynamic security policy” and updates to a dynamic security policy. Both constructions of this term to date capture the idea that the dynamic security policy is a changeable entity that tells a PSG what to do with packets that meet certain criteria. Pet. at 10. For example, the dynamic security policy can include a set of rules—like the claimed first set of rules—that specifies packet-matching criteria and packet transformation functions. *Id.* The dynamic, or “changeable,” nature of the dynamic security policy contemplates that the policy being applied at the PSG will be updated over time. *See*

POR at 8-12. In the context of the plain language and specification, the dynamic security policy—*i.e.*, what gets implemented at the PSG and what can be changed over time—must be received from the SPMS. *See id.* at 8-10.

The intrinsic record does not support Petitioner's overbroad reading of the claims, which would allow for the dynamic security policy to be **generated** at the PSG rather than being **received** at the PSG from the SPMS. Reply at 20-21; Institution Decision at 25. Not only is that scenario contrary to the plain language of the claims, the specification never suggests that any entity besides the SPMS could, would, or should generate and disseminate dynamic security policies. Thus, in the scenario discussed in the Institution Decision—where the claimed “first set of packet filtering rules” is sent as “an update to [the] initial ruleset”—the alleged dynamic security policy is already at the firewall. Institution Decision at 25. It is not received from the alleged SPMS, firm 305.

Rather than address Centripetal's argument or the intrinsic evidence, Petitioner attacks a strawman. *See* Reply at 21-22 (suggesting that Centripetal's argument depends on narrow constructions of the terms “first” and “second” recited in the claims). But Centripetal made no such argument. Instead, a POSITA recognizes 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. '266 Patent

at Claim 1. Similarly, a POSITA recognizes that the “second set of packet filtering rules” is not the “initial” ruleset because it is received as an update to the existing dynamic security policy. *Id.* This understanding of the claims finds support throughout the intrinsic record. For example, in every embodiment, the SPMS generates a dynamic security policy, including a first set of rules. *See* '266 Patent at 14:13-20; *see also* POR at 9-10. There are no embodiments in which the dynamic security policy is generated at the PSG.

Accordingly, the claims and specification describe the first set of packet filtering rules as being included in the dynamic security policy that is sent from the SPMS to the PSG, therefore ascribing a significance to the “first set of packet filtering rules” other than the “common patent-law convention to distinguish between repeated instances of an element or limitation.” *3M Innovative Props. Co. v. Avery Dennison Corp.*, 350 F.3d 1365, 1371 (Fed. Cir. 2003) (citations omitted).

ii. Firm 305 Only Distributes Updates to Operator-Created Initial Rulesets

Although Petitioner asserts that Law distributes initial rulesets, its assertion is contradicted by its admission made elsewhere and Law itself describing firm 305 as only distributing updates to operator-created initial rulesets. Reply at 22-23.

Significantly, Petitioner admitted that Law's invention is directed to a process control system that “overcome[s] the ***need for specifically trained IT personnel to create . . . firewall rulesets.***” *Id.* at 18 (emphasis added). Rather than trying to

ensure that the IT personnel employed by firm 305 have all of the knowledge necessary to implement Law's UTMS for specialized process control systems, Law discloses assigning that task to operators within the process control system. See Law at ¶¶ 23, 59, 60, 81 90, 91; POR at 43-45. Accordingly, by Petitioner's own admission, Law's firm 305 does not distribute initial rulesets that can be updated. Reply at 18. This concession ends the analysis because it establishes that the firm does not send dynamic security policies to Law's firewalls, it only sends updates to the policies that were created on the PSG.

This is the very technique disclosed in Law's paragraphs 22, 66, and 88, which Petitioner cites in reply. Reply at 22-23 (citing Law ¶¶ 22, 66, 88).³ Specifically, paragraph 22 describes a perpetual service that supplies process control systems with updated rulesets. Law, ¶ 22 ("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 **These updates** are managed from within the standard control user interface of the

³ Petitioner leaves unrebutted Centripetal's showing that the '474 Institution Decision extends and alters Law, inserting the language "access[ing] an already existing ruleset created by cyber security risk management firm 305." See POR at 49-52.

plant”) (emphasis added). Indeed, Petitioner previously relied on this very paragraph for the proposition that firm 305 supplies “updated rulesets”:

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). Accordingly, the Petition’s assessment of firm 305 contradicts its Reply argument.

Paragraphs 66 and 88 likewise disclose that firm 305 distributes updated to existing rulesets created on the PSG rather than dynamic security policies that are sent from the security policy management server. See Law, ¶ 66 (providing “**update data**” via “a third party source (such as cyber security risk management firm 305 as described in relation to FIG. 3”)), ¶ 88 (describing FIG. 3 as a method that provides “updates” to the rulesets); see also *id.* at ¶ 30 (“FIG. 3 is a logical block diagram of ***a method to update rulesets of the UTMS.***”) (emphases added); Goodrich Tr. at 14:11-15:13 (explaining that in paragraph 66 Law receives updates to the operator-created rulesets), 17:22-20:1 (explaining that operators configure the rulesets with firm 305 providing updates as in paragraph 88).

Given Petitioner’s admission and Law’s disclosure, firm 305 distributes only updates to the operator-created rulesets that were created on the PSG. Therefore, Law does not teach or suggest that firm 305 creates and distributes a dynamic security policy, including a first set of rules, as required by the Challenged Claims.

* * *

On the full record, Petitioner fails to show by a preponderance of the evidence that firm 305 is a “security policy management server” which “automatically creates or alters one or more packet filtering rules” and distributes “a dynamic security policy comprising a first set of rules” under the correct construction.

**B. Law in View of Wood Does Not Render Obvious Claims 1-24
(Ground 2)**

As explained in the POR, Wood does not cure the deficiencies of Law. Petitioner does not dispute this in reply. Therefore, Ground 2 does not render obvious the Challenged Claims.

**C. Law in view of Wood and/or Jungck Fails to Render Obvious the
Dependent Claims (Grounds 3 and 4)**

Because Grounds 3 and 4 challenge the dependent claims, these grounds fail for the same reasons Grounds 1 and 2 fail. *See* POR at 53-54.

III. CONCLUSION

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

Respectfully submitted,

Dated: April 3, 2024

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 SUR-REPLY** specified in 37 C.F.R. § 42.24 has 5,464 words in compliance with the 5,600-word limit set forth in 37 C.F.R. § 42.24(c)(4). This word count was prepared using the Microsoft Word word-processing system used to prepare this paper.

Dated: April 3, 2024

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>	April 3, 2024
<i>Manner of service</i>	Electronic Filing with the Board
<i>Documents served</i>	PATENT OWNER'S SUR-REPLY
<i>Persons served</i>	REED SMITH LLP Gerard M. Donovan Peter J. Chassman Jonathan I. Detrixhe Sidharth Kapoor gdonovan@reedsmith.com pchassman@reedsmith.com jdetrixhe@reedsmith.com skapoor@reedsmith.com ROPES & GRAY LLP James L. Davis, Jr. Andrew Radsch james.l.davis@ropesgray.com andrew.radsch@ropesgray.com

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