

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 PRELIMINARY RESPONSE

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. THE '266 PATENT OVERVIEW	3
A. The '266 Patent	3
B. Prosecution History	6
III. THE BOARD SHOULD EXERCISE ITS DISCRETION TO DENY INSTITUTION UNDER 35 U.S.C. § 314(a).....	7
A. Factor 1: whether the same petitioner previously filed a petition directed to the same claims of the same patent	9
B. Factor 2: whether at the time of filing of the first petition the petitioner knew of the prior art asserted in the second petition or should have known of it	12
C. Factor 3: Whether at the time of filing of the second petition the petitioner already received the patent owner's preliminary response to the first petition or received the Board's decision on whether to institute review in the first petition	13
D. Factor 4: The length of time that elapsed between the time the petitioner learned of the prior art asserted in the second petition and the filing of the second petition	17
E. Factor 5: Whether the petitioner provides adequate explanation for the time elapsed between the filings of multiple petitions directed to the same claims of the same patent	20
F. Factors 6 and 7: The finite resources of the Board	21
IV. LEVEL OF ORDINARY SKILL IN THE ART	22
V. CLAIM CONSTRUCTION	23
A. The Preambles of Independent Claims 1, 8, and 15 are Limiting.....	23

B.	Other Constructions.....	24
VI.	OVERVIEW OF THE REFERENCES.....	25
A.	Law	25
B.	Wood	28
VII.	THE PETITION SHOULD BE DENIED BECAUSE PETITIONER FAILS TO DEMONSTRATE A REASONABLE LIKELIHOOD OF SUCCESS ON ANY CHALLENGED CLAIM	29
A.	Ground 1: Claims 1-27 Are Patentable Over Law	29
1.	Petitioner Fails to Demonstrate that Law Teaches or Suggests the “Entire Interface Across a Boundary” and “All Traffic Traversing the Boundary” Limitations	29
a.	Because Law’s Firewalls 146a and 146b each protect its own network they do not collectively provide “an entire interface across a boundary”	29
b.	Law’s LANs 150a and 150b are Separate Networks Even When Joined With a Network Access Device	33
c.	Petitioner Does Not Sufficiently Explain Its Expanded Number of Firewalls Theory	35
2.	Petitioner Fails to Show that Any Ground Discloses the “All Network Traffic” Requirement	36
3.	Petitioner Fails to Demonstrate that Law Teaches or Suggests “Receiving a First Set of Packet Filtering Rules by the PSG” in which “the First Set of Packet Filtering Rules is Automatically Created or Altered by the SPMS” Limitations	38
a.	Law does not teach or suggest the “receiving a first set of packet filtering rules by the PSG” limitation.....	39

i.	Law’s operators within the process control system create ruleset 147 and a first set of rules	40
ii.	Petitioner’s Only Evidence Is Directed to Law’s UTMS-configured firewall devices receiving updates to ruleset 147	44
b.	Law does not teach or suggest “the first set of packet filtering rules is automatically created or altered by the SPMS” limitation.....	45
i.	Law’s firm 305 does not disclose the claimed SPMS that automatically creates or alters a first set of packet filtering rules.....	46
ii.	Law’s firm 305 does not render obvious the claimed SPMS that automatically creates or alters a first set of packet filtering rules	49
B.	Ground 2: Claims 1-27 are Patentable Over Law in View of Wood	51
C.	Ground 3: Claims 6, 13, 19, and 26 are Patentable Over Law in View of Jungck.....	52
D.	Ground 4: Claims 6, 13, 19, and 26 are Patentable Over Law in View of Wood and Jungck	52
VIII.	CONCLUSION.....	52

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Am. Well Corp. v. Teladoc Health, Inc.</i> , No. IPR2022-00038, Paper 10 (P.T.A.B. Apr. 19, 2022)	13, 16
<i>Ariosa Diagnostics v. Verinata Health, Inc.</i> , 805 F.3d 1359 (Fed. Cir. 2015)	50
<i>Ericsson Inc. v. Uniloc 2017, LLC</i> , No. IPR2019-00420, Paper 7 (P.T.A.B. June 18, 2020)	12, 20
<i>Ericsson Inc. v. Uniloc 2017, LLC</i> , No. IPR2020-01550, Paper 8 (P.T.A.B. Mar. 17, 2020)	9, 10, 11, 21
<i>Gen. Plastic Indus. Co. v. Canon Kabushiki Kaisha</i> , No. IPR2016-01357, Paper 19 (P.T.A.B. Sept. 6, 2017).....	<i>passim</i>
<i>Google Inc. v. Koninklijke Philips N.V.</i> , No. IPR2017-00409, Paper 10 (P.T.A.B. Jun. 5, 2017)	50
<i>In re Magnum Oil Tools Int’l, Ltd.</i> , 829 F.3d 1364 (Fed. Cir. 2016)	50
<i>Mitek Sys., Inc. v. United Servs. Auto. Assoc.</i> , No. IPR2020-01101, Paper 29 (P.T.A.B. Jan. 26, 2021)	10, 20
<i>Oil States Energy Servs., LLC v. Greene’s Energy Grp., LLC</i> , 138 S. Ct. 1365 (2018).....	22
<i>Palo Alto Networks, Inc. v. Centripetal Networks, Inc.</i> , No. IPR2021-01154, Paper 11 (P.T.A.B. Jan. 24, 2022)	<i>passim</i>
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005)	23
<i>Samsung Elecs. Co. v. Elm 3DS Innovations, LLC</i> , No. IPR2017-01305, Paper 11 (P.T.A.B. Oct. 17, 2017).....	10
<i>Seki S.P.A. v. CM2W JSC</i> , No. IPR2020-01636, Paper 9 (P.T.A.B. Jan. 7, 2021)	21

<i>Shanghai Lunion Info. Tech., Ltd. v. Telefonaktiebolaget LM Ericsson</i> , No. IPR2018-00995, Paper 12 (P.T.A.B. Nov. 13, 2018).....	12, 13
<i>Shenzhen Silver Star Intelligent Tech. Co. v. iRobot Corp.</i> , No. IPR2018-00761, Paper 15 (P.T.A.B. Sept. 5, 2018).....	15, 18, 19
<i>TQ Delta, LLC v. Cisco Sys., Inc.</i> , 942 F.3d 1352 (Fed. Cir. 2019)	35
<i>United Fire Protection Corp. v. Eng’d Corrosion Solutions, LLC</i> , No. IPR2018-00991, Paper 18 (P.T.A.B. Oct. 10, 2019).....	11, 12, 17
<i>Valve Corp. v. Elec. Scripting Prods., Inc.</i> , No. IPR2019-00062, Paper 11 (P.T.A.B. Apr. 2, 2019)	9, 11, 20
<i>Xerox Corp. v. Bytemark, Inc.</i> , No. IPR2022-00624, Paper 9 (P.T.A.B. Aug. 24, 2022).....	50

Statutes

35 U.S.C.	
§ 314(a)	7, 10, 18
§ 315(b)	18
§ 325(d)	20

Other Authorities

83 Fed. Reg. 51340, 51341 (Oct. 11, 2018).....	23
--	----

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)

I. INTRODUCTION

The Board should exercise its discretion to deny institution because Petitioner¹ admittedly used the Board's decision denying institution in IPR2021-01154 ("the '1154 decision") as a roadmap to construct this Petition, which challenges the same claims. Petitioner waited until the last possible day to file this Petition in hopes that it would also have access to a not-yet-published decision from the European Patent Office ("EPO"), addressing the application of Law (Ex. 1005) to similar claim elements in a related European application. That decision, which was favorable to Centripetal, published only three days after the one-year bar date. Petitioner's use of an earlier Petition, Centripetal's counter-arguments in two different fora, and the '1154 decision to address identified deficiencies in a follow-on petition that: challenged the same claims that the Board previously confirmed, used the decision denying institution as a roadmap, asserted art that it knew about for at least six months prior to filing, and was delayed in an attempt to gain even more of a strategic advantage than it already had, raises precisely the concerns for abuse outlined in *General Plastic*. See *Gen. Plastic Indus. Co. v. Canon Kabushiki Kaisha*, No. IPR2016-01357, Paper 19 (P.T.A.B. Sept. 6, 2017) (precedential).

¹ Keysight Technologies, Inc., ("Petitioner") petitioned for IPR of Claims 1-27 (the "Challenged Claims") of U.S. Patent No. 10,785,266 (Ex. 1001, "the '266 Patent").

The Board should also deny institution because, even with the benefit of the '1154 decision, Petitioner could not locate art that discloses an “entire interface” and “all traffic” limitations found missing in the '1154 decision. This feature requires (1) “a network protected by a packet security gateway” (“PSG”) and (2) a plurality of PSGs “that collectively provide an entire interface across a boundary of” that network “and one or more networks other than the network protected by the packet security gateway.” Law’s firewalls 146a and 146b protect separate local area networks (LANs) (networks 150a and 150b, respectively) and, therefore, do not collectively provide an entire interface across either of these protected networks. *See* Pet. at 14-32.

Petitioner also fails to show that Law teaches or suggests “receiving a first set of packet filtering rules by the PSG.” Law’s firm 305, which Petitioner likens to the claimed “security policy management server” (“SPMS”), does not create or distribute the first set of rules to the UTMS-configured firewalls, which petitioner likens to the claimed PSGs. *See id.* at 24, 27, 38-39. Because “each ruleset is specific to the system it protects,” Law’s rulesets are initially created by operators within the process control system environment who have in-depth knowledge about that environment. Law at Abstract; *id.* at ¶¶ 16, 23. Firm 305 only updates these operator-created rulesets, so that they remain effective against network threats over time. *Id.* at ¶ 88 (“[T]he various rulesets . . . associated with the UTMS configured

network devices . . . require updates to remain effective against network threats.”); *id.* at ¶ 30; *id.* at Fig. 3. Accordingly, rather than receiving a first ruleset from firm 305, the UTMS-configured firewall devices only receives updates to already existing, operator-defined ruleset.

Petitioner also fails to show that Law teaches or suggests the SPMS automatically creating or altering “the first set of packet filtering rules” because firm 305 does not automatically update the operator-created rulesets. *See* Pet. at 37-38. Even when updating an existing ruleset, firm 305 requires the use of IT personnel to update the rulesets specific to a process control system to ensure adequate protection. Law at ¶¶ 16, 88. Because IT personnel are necessary to implement these updates, firm 305 does not provide automatic updates.

Wood, which Petitioner cites Wood (Ex. 1006) only for its alleged disclosure of a source providing suspect addresses, does not cure Law’s noted deficiencies. Pet. at 65. For at least these reasons, Centripetal respectfully requests that the Board deny institution.

II. THE ’266 PATENT OVERVIEW

A. The ’266 Patent

The ’266 Patent is directed to “[m]ethods and systems for protecting a secured network.” ’266 Patent at Abstract, 1:59–60. Because “the path a given packet may take cannot be readily predicted,” (*id.* at 5:23-24) PSGs are placed at each boundary

between a protected network and an unprotected network. *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).

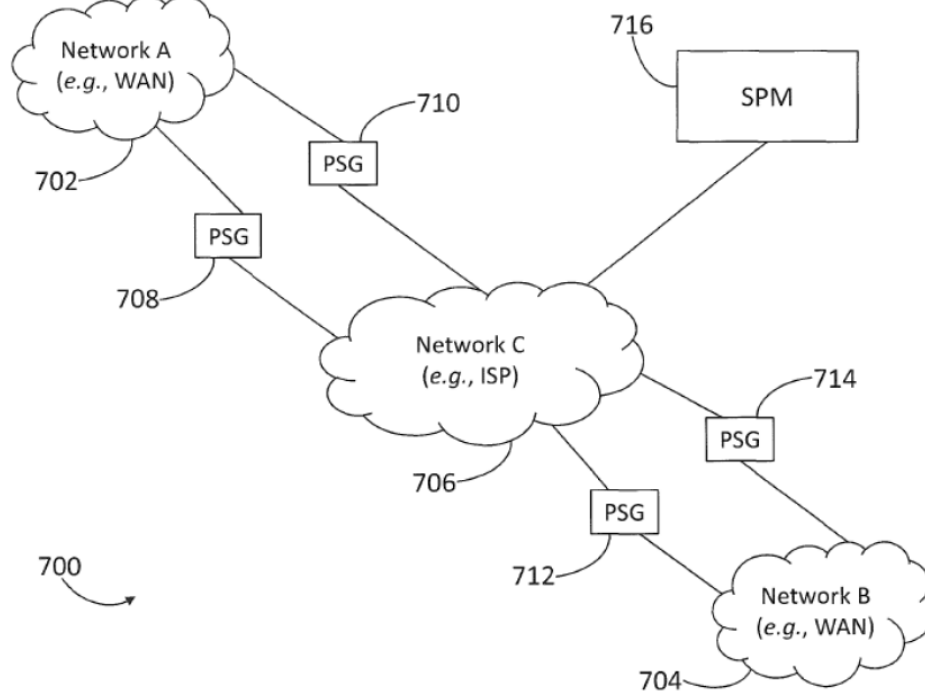


FIG. 7

Id. at Fig. 7; *id.* at 16:44–48, 16:62–17:1.

Critically for purposes of this case, the Challenged Claims explicitly define the scope of the protected network as the network protected by one of a plurality of PSGs:

A method of filtering packets at a **packet security gateway**, of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a **network protected by the packet**

security gateway and one or more networks other than the network protected by the packet security gateway....

Id. at Claim 1 (emphasis added). By definition, any network not protected by “the packet security gateway” is “one or more networks other than the network protected by the packet security gateway.”²

A PSG receives packets and proactively protects a network from malicious attacks based on dynamic security policies³ that are automatically created and/or altered by an SPMS based on malicious traffic information received from a malicious host tracker service. *Id.* at 4:61–5:11, 5:34–53, 13:25–34, 14:9–39, 19:38–45, Figs. 1, 5, 9. Specifically, Figure 5 (reproduced below) illustrates an exemplary SPMS 120, including a processor 500 and memory 502:

² As discussed in more detail later, because Law’s firewall 146a does not protect network 150b, network 150b is, by definition “one or more networks other than the network protected by” firewall 146a rather than part of a single network with network 150a, which firewall 146a does protect.

³ A dynamic security policy includes rules that “specify criteria and one or more packet transformation functions that should be performed for packets associated with the specified criteria.” ’266 Patent at 7:23–26.

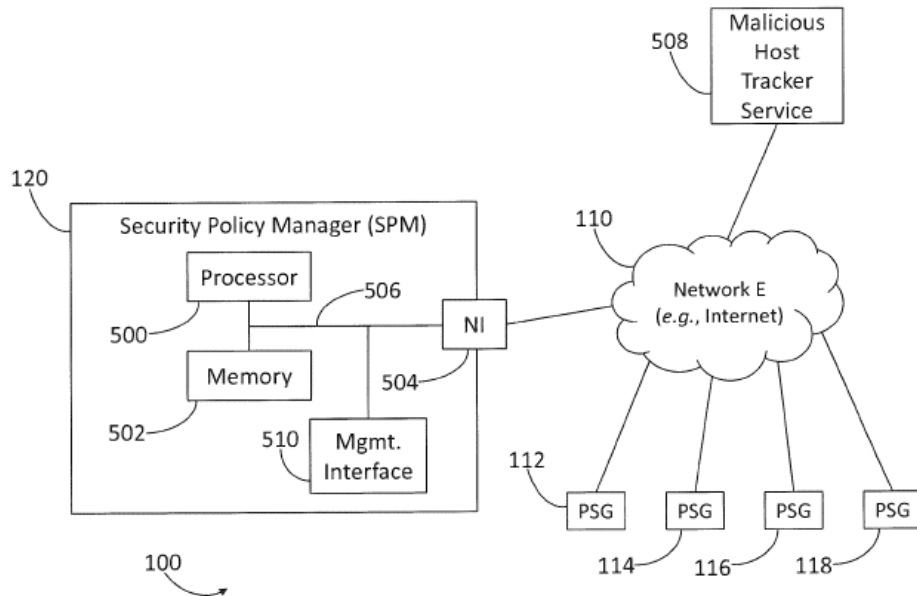


FIG. 5

Id. at Fig. 5. The exemplary SPMS can (i) automatically create or alter a first set of packet filtering rules of a dynamic security policy based on aggregated malicious network traffic from malicious host tracker services, (ii) communicate the first set to the PSGs, (iii) alter the first set based on updates from the malicious host tracker services, and (iv) communicate an updated second set of the packet filtering rules to the PSGs. *See id.* 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).

B. Prosecution History

During prosecution of the application that matured into the '266 Patent, the Examiner rejected then-pending claims as being unpatentable over U.S. Patent Publ. No. 20030118038 to Jalava et al. ("Jalava") in view of U.S. Patent Publ.

No. 20060123481 to Bhatnagar et al. (“Bhatnagar”). Ex. 1002 at 168-214. In response to the Examiner’s rejection, Centripetal distinguished Jalava in view of Bhatnagar by arguing that none of the cited references teach, disclose, or otherwise suggest the claim limitations of automatically creating or altering one or more first packet filtering rules of the first set based on aggregated malicious traffic information. *Id.* at 147-50.

The Examiner found Centripetal’s arguments persuasive and issued a notice of allowance. *Id.* at 59-76.

III. THE BOARD SHOULD EXERCISE ITS DISCRETION TO DENY INSTITUTION UNDER 35 U.S.C. § 314(a)

The Board should exercise its discretion under 35 U.S.C. § 314(a) to deny institution because the *General Plastic* factors weigh in favor of denying institution of this Petition as a follow-on Petition based on a prior proceeding involving the same patent and same challenged claims (IPR2021-01154, “the ’1154 IPR”). *Gen. Plastic*, Paper 19 at 8-10 (enumerating a list of seven factors for considering whether follow-on petitions present inequities to the patent owner or inefficiency of the IPR process).

Despite having the previous challenger’s mistakes spelled out for it in the decision denying institution, Petitioner took more than 11 months to file its serial attack on the ’266 Patent. Petitioner also knew of its primary reference, Law, at least seven months before it filed this Petition. Ex. 2001 at 8, 74-86 (raising Law in

Petitioner's European opposition challenging a related⁴ European patent having many of the same claim elements at issue here). More than that, Petitioner had many months before filing the Petition to study Centripetal's arguments and rebuttals addressing Law in those opposition proceedings. Ex. 2002 at 48-51 (Centripetal's rebuttal addressing Law filed in September 2022).

The timing of Petitioner's filing suggests that it sought a further tactical advantage than it already had given its access to Centripetal's '1154 Preliminary Response, the '1154 decision, and Centripetal's response to Law in the opposition proceedings. By waiting until the last possible day to file its Petition, Petitioner was very nearly also privy to the European opposition panel's preliminary opinion addressing Centripetal's rebuttal arguments to grounds that applied Law. This ploy almost worked out for Petitioner, the opposition panel issued its preliminary opinion just days after this Petition was filed, crediting the same deficiencies of Law that Centripetal had detailed in its response. Ex. 2003 (preliminary opinion of opposition division issued on January 9, 2023) at 53-56 (finding that Law does not disclose feature 1.1.3 reciting the "malicious host tracker service").

⁴ U.S. Patent No. 9,565,213, to which EP Pat. No. 3550795 claims priority, was originally filed as a continuation-in-part of the '205 Patent.

On balance, the *General Plastic* factors weigh strongly in favor of discretionary denial.

A. Factor 1: whether the same petitioner previously filed a petition directed to the same claims of the same patent

Factor 1 weighs in favor of discretionary denial because Petitioner challenged the same claims of the same patent as challenged by prior-petitioner, Palo Alto Networks, Inc. (“PAN”), and used the decision denying institution in this case as a roadmap to address the deficiencies noted in the ’1154 decision. *See* Ex. 2004 at 2 (prior petition also challenging claims 1-27 of the ’266 Patent).

The Board weighs *General Plastic* factor one in favor of discretionary denial even when a previous petition is filed by a different petitioner against the same claims of the same patent, where a “significant relationship” exists between the first and follow-on petitioners. *Valve Corp. v. Elec. Scripting Prods., Inc.*, No. IPR2019-00062, Paper 11 at 10 (P.T.A.B. Apr. 2, 2019) (precedential). Here, Petitioner created an implicit relationship with prior-petitioner PAN when it used the ’1154 decision as a roadmap for its challenge. *See Ericsson Inc. v. Uniloc 2017, LLC* (“*Ericsson I*”), No. IPR2020-01550, Paper 8 at 12 (P.T.A.B. Mar. 17, 2020) (using a prior petition “as a roadmap for its own petition ties the interests of all of the petitioners together.”). In the ’1154 petition, PAN relied on Jungck’s edge server for allegedly satisfying “an entire interface” that protects entire networks by filtering “all network traffic.” Ex. 2004 at 11-12. The Board disagreed. The Board found

that “Jungck teaches network paths that **bypass** its edge servers when carrying network traffic through the POPs.” *Id.* at 12-14 (emphasis added); *see also id.* at 15.

Petitioner explicitly used the ’1154 decision as a guide to identify and address the ’1154 petition’s deficiencies. Pet. at 21-23, 30-31 (addressing Law’s bypass embodiments in an attempt to show why Law does not succumb to the same deficiencies as in Jungck). Indeed, Petitioner devotes roughly 18 pages to these preamble limitations in an attempt to show how Law’s firewalls 146a and 146b allegedly “serve as the entire interface” that “all network traffic between joined LANs 150a and 150b and the Internet must pass through.” *Id.* at 18-19, 21; *see also generally id.* at 14-32. Just like in *Samsung* where the petitioner replaced unsuccessful prior art with a new reference, Petitioner does the same thing here which “evinces benefit Petitioner . . . derived from th[e] prior proceeding[.]” *Samsung Elecs. Co. v. Elm 3DS Innovations, LLC*, No. IPR2017-01305, Paper 11, at 20 (P.T.A.B. Oct. 17, 2017). This commonality between petitions “ties the interests of all of the petitioners together.” *Ericsson I*, Paper 8 at 12.

In another example, the Board exercised its discretion under § 314(a) to deny institution to a follow-on petition, where a different petitioner challenged the same claims of the same patent as an earlier petitioner. *Mitek Sys., Inc. v. United Servs. Auto. Assoc.*, No. IPR2020-01101, Paper 29 at 3 (P.T.A.B. Jan. 26, 2021). There, the Board found the complete overlap in challenged claims, together with evidence

that the petitioner “closely monitor[ed]” the proceedings of the earlier petitioner created a significant relationship between petitioners, weighed in favor of discretionary denial. *Id.* at 23. The Board also found that because the follow-on petition had used the Board’s prior decision denying institution as a roadmap, implicating the fairness concerns discussed in *General Plastic*, and that the petitioner’s delay of seven months was “unreasonable,” the particular circumstances weighed in favor of discretionary denial. *Id.* at 30, 33-34.

Because there is a complete overlap between the challenged claims, and because Petitioner created an implicit relationship with prior-petitioner PAN, *General Plastic* Factor 1 weighs in favor of denial. *See Valve*, Paper 11 at 9-10 (finding that “[t]he complete overlap in the challenged claims and significant relationship between Valve and HTC favor denying institution”); *see also Ericsson I*, Paper 8 at 12 (finding that “[p]etitioner and the prior petitioners in this case are similar to petitioners discussed in *Valve Corp.*” given the implicit relationship).

Even if the Board determines that Petitioner’s actions did not create an implicit relationship with PAN, the Board nonetheless exercises its discretion to deny institution when other *General Plastic* factors weigh in favor of denial. *See United Fire Protection Corp. v. Eng’d Corrosion Solutions, LLC*, No. IPR2018-00991, Paper 18 at 13 (P.T.A.B. Oct. 10, 2019) (“The potential for abuse of follow-on petitions exists not only with overlapping petitions by the same petitioner, . . . but

also with any follow-on petitions.”). For instance, in *United Fire*, the Board exercised its discretion to deny institution of a follow-on petition despite a lack of relationship between different petitioners, where *General Plastic* factors three and five “weigh[ed] strongly in favor of invoking [its] discretion to deny institution.” *United Fire*, Paper 10 at 15, 17 (P.T.A.B. Nov. 15, 2018); see also *Ericsson Inc. v. Uniloc 2017, LLC* (“*Ericsson IP*”), No. IPR2019-00420, Paper 7 at 13 (P.T.A.B. June 18, 2020) (finding “factor five urges in factor of denying the [p]etition” despite the follow-on petition being filed by a party unrelated to the first petition). The Board considered evidence that the petitioner received “substantial potential benefit . . . to tailor its arguments” using the prior decisions “as a roadmap” and cure the deficiencies that the Board identified in the earlier challenge. *United Fire*, Paper 10 at 13-15. The Board also faulted the petitioner for providing no explanation of a delay of nearly one year long, similar to the instant Petition. *Id.* at 16.

Given the foregoing, Factor 1 weighs in favor of denying institution or is, at worst, neutral.

B. Factor 2: whether at the time of filing of the first petition the petitioner knew of the prior art asserted in the second petition or should have known of it

Factor two is neutral because this factor has “little probative value” where the instant petitioner was not the petitioner in the prior proceedings. See *Shanghai*

Lunion Info. Tech., Ltd. v. Telefonaktiebolaget LM Ericsson, No. IPR2018-00995, Paper 12 at 17-18 (P.T.A.B. Nov. 13, 2018).

C. Factor 3: Whether at the time of filing of the second petition the petitioner already received the patent owner's preliminary response to the first petition or received the Board's decision on whether to institute review in the first petition

General Plastic Factor 3 weighs strongly in favor of discretionary denial because Petitioner received Centripetal's preliminary response and the Board's decision to deny trial in the '1154 IPR long before it filed this Petition. It also received Centripetal's response to the European opposition proceedings applying Law to the claims of a related patent and tailored its Petition explicitly to address deficiencies noted in both of these earlier challenges.

General Plastic case law discourages follow-on petitions in which petitioner delays filing and tailors their arguments to address issues identified in the previous proceeding because "[t]he absence of any restrictions on follow-on petitions would allow petitioners the opportunity to strategically stage their prior art and arguments in multiple petitions, using our decisions as a roadmap." *Gen. Plastic*, Paper 19 at 17-18; *see also Am. Well Corp. v. Teladoc Health, Inc.*, No. IPR2022-00038, Paper 10 at 21-22 (P.T.A.B. Apr. 19, 2022) (finding that *General Plastic* Factor 3 weighed against institution because petitioner used the prior institution decision as a roadmap to present "updated arguments and evidence" which "raise the fairness and efficiency concerns discussed in *General Plastic*."). This is the case here.

In its '1154 preliminary response, Centripetal demonstrated that the primary reference, Jungck (Ex. 1008), failed to satisfy the claimed “entire interface” and “all network traffic” requirements. Ex. 2007, *Palo Alto Networks, Inc. v. Centripetal Networks, Inc.*, No. IPR2021-01154, Paper 7 at 32-47 (P.T.A.B. Oct. 25, 2021); Ex. 2008, No. IPR2021-01154, Paper 9, Prelim. Sur-Reply at 8-10 (P.T.A.B. Dec. 7, 2021). At the time of filing this follow-on Petition, the entirety of the prior proceedings, from the initial petition through institution, had been available to Petitioner for just shy of a year. In denying the 'first petition, the Board credited Centripetal's argument that the main reference, Jungck, did not disclose the claimed “entire interface” and “all network traffic” requirements because network traffic bypassed Jungck's edge servers, which the previous challenger relied on to show the claimed “packet security gateways.” Ex. 2004 ('1154 decision) at 12-15. To avoid the same mistakes that led to the denial of the first petition, Petitioner attempts to distinguish Law's alleged non-bypass embodiment from the deficient disclosures in Jungck. Pet. at 21-23, 30-31; *see supra* (General Plastic Factor 1).

Petitioner also tailored its arguments to address deficiencies noted in Centripetal's successful arguments made in the European opposition proceedings.⁵ *See Gen. Plastic*, Paper 19 at 18 ("additional factors may arise in other cases for consideration, where appropriate"). For example, Petitioner backstopped its main ground, which relies on Law alone, with an additional ground that relies on Wood for the same claim element that Centripetal argued is missing from Law in the European opposition proceedings. Pet. at 63-68; Ex. 2002 at 48, 50-51 (Centripetal arguing that Law does not disclose the claimed "malicious host tracker service").

Petitioner had many months before filing the Petition to study Centripetal's arguments and rebuttals addressing Law in those opposition proceedings. Ex. 2002 at 48-51 (Centripetal's rebuttal addressing Law filed in September 2022). Further, the timing of Petitioner's filing suggests that it sought a tactical advantage by waiting until the last possible day to file its Petition in the hopes that the European opposition

⁵ Petitioner failed to mention the European opposition proceedings, in which the opposition grounds applying Law substantially mirror Petitioner's primary challenge, despite the Board having previously instructed parties to "draw attention to relevant information regarding related litigation that provides a context for the filings before [it]." *Shenzhen Silver Star Intelligent Tech. Co. v. iRobot Corp.*, No. IPR2018-00761, Paper 15 at 19 (P.T.A.B. Sept. 5, 2018).

panel would issue its preliminary opinion addressing Centripetal's rebuttal arguments to the opposition grounds that applied Law. This would further allow for Petitioner's strung-out and piecemeal approach, with the unjustified delay hopefully providing Petitioner another opinion on what not to argue. And this plan almost worked out for Petitioner, because the opposition panel issued its preliminary opinion just days after this Petition was filed, crediting the same deficiencies of Law that Centripetal had detailed in its response. Ex. 2003 (preliminary opinion of opposition division issued on January 9, 2023) at 53-56 (finding that Law does not disclose feature 1.1.3 reciting the "malicious host tracker service").

Factor 3 therefore weighs in favor of denying institution because Petitioner updated its arguments and art after having an opportunity to review numerous briefs and decisions directly bearing on the patentability of the '266 Patent. In *American Well*, the Board determined that these very actions "rais[ed] the fairness and efficiency concerns discussed in *General Plastic*," and thus found that Factor 3 weighed in favor of denial. *Am. Well*, Paper 10 at 21-22. Petitioner's actions here also raise fairness concerns which weigh in favor of denial. For example, Petitioner had close to a year to study the deficiencies identified in the Board's '1154 decision and Centripetal's '1154 preliminary response to update the arguments and evidence before filing the instant Petition and waited as long as it possibly could wait for even more relevant arguments and conclusions of law. Notice of Filing Date Accorded,

Paper 3 (petition filing date of January 6, 2023); Ex. 2004 at Cover ('1154 decision entered January 24, 2022); Ex. 1011 at 3 (complaint served on January 6, 2022). The Board has found that this type of delayed filing “raises the potential for abuse because [p]etitioner had ample opportunity to study the [previous] arguments . . . and the Board’s findings and conclusions of law.” *United Fire*, Paper 10 at 13-14 (denying institution in part because the petitioner had roughly two years to study the patent owner’s arguments and the Board’s decision).

In view of the foregoing, *General Plastic* Factor 3 weighs strongly in favor of discretionary denial. *See id.* at 14-15 (finding that factor 3 “weighs strongly in favor of invoking our discretion” because the petitioner used the prior petitions as roadmaps and the delay in filing the petition).

D. Factor 4: The length of time that elapsed between the time the petitioner learned of the prior art asserted in the second petition and the filing of the second petition

Factor 4 weighs in favor of denying institution given that Petitioner had Law and knew of its relevance for more than seven months before filing this follow-on Petition on the last possible day, yet Petitioner provides no explanation for the timing of its filing. Ex. 2001 at 8, 74-86. During that seven-month period, Petitioner had ample opportunity to study the manner in which its co-party to the European opposition proceedings (Cisco) applied Law to substantially similar claim elements. *See supra* (*General Plastic* Factor 3). Indeed, Petitioner’s German subsidiary was

already aware of Cisco's grounds of opposition applying Law at the time that subsidiary filed its notice of intervention in the opposition proceedings on May 27, 2022, a mere four days after Cisco filed its notice of intervention on May 23, 2022. Ex. 2005 at 1, 79 (relying on a reference applied by co-party Cisco to challenge the dependent European claims); Ex. 2001 at 1, 97, 99-100, 7-8.⁶

The unexplained seven-month stretch of time during which Petitioner was aware of each reference relied on in its Petition falls squarely within the amount of time that the Board has found "weighs strongly against institution." *Shenzhen*, Paper 15 at 13-15 (denying institution where the petitioner was aware of the asserted references **more than five months** before filing its petition); *id.* at 18 n.2 ("the time bar of 35 U.S.C. § 315(b) . . . provide[s] a hard ceiling, which we [the Board] are free to lower as fairness dictates under our general authority not to institute a petition that may otherwise be instituted, under § 314(a)") (concurring). The substantial overlap in how both Petitioner and its opposition co-party (Cisco) map Law to the claim elements exacerbates Petitioner's unexplained delay in filing its Petition. See *supra* (General Plastic Factor 3); see also *infra*. (General Plastic Factor 5).

⁶ Petitioner's subsidiary, Ixia, also received notification of Cisco's intervention applying Law. Ex. 2006 at 1-2, 49-52.

In fact, the timing of Petitioner's filing suggests it sought an ***additional*** tactical advantage by waiting to file its Petition on the last possible day before being statutorily barred. Ex. 1011 at 3 (complaint served on January 6, 2022); Notice of Filing Date Accorded, Paper 3 (Petition filed on January 6, 2023). The panel in the European opposition proceedings issued its preliminary opinion only three days after Petitioner's statutory bar date. Ex. 2003 at cover page. By tactically delaying its filing, Petitioner increased the chances that the opposition panel would issue its preliminary opinion which would allow Petitioner to strengthen its own Petition based on the opposition panel's reaction to Centripetal's arguments addressing Law.

Given that Petitioner provides no explanation for its delay, the only conclusion is that the Petition "was filed at the time it was filed solely for the tactical reason of using the [opposition proceedings] as a test case." *Shenzhen*, Paper 15 at 19 (concurring); *see also id.* ("Our decision above puts parties on notice that such tactics may result in denials under *General Plastic*"). That Petitioner simply ran out of time before the opposition panel issued its preliminary opinion does not detract from Petitioner's intentional delay or the harm to Centripetal by this apparent gamesmanship. Factor 4, therefore, weighs strongly in favor of denying institution.

E. Factor 5: Whether the petitioner provides adequate explanation for the time elapsed between the filings of multiple petitions directed to the same claims of the same patent

General Plastic Factor 5 weighs strongly for discretionary denial. When the *General Plastic* considerations are applied to petitions filed by different petitioners, factor five is “reasonably read to refer to when Petitioner first had a reason to file a petition” and “factor five probes why Petitioner took as long as it did to file this Petition.” *Ericsson II*, Paper 7 at 12-13.

The instant Petition was filed on January 6, 2023, over 11 months after the -’1154 decision was issued on January 24, 2022. *See* Ex. 2004. Petitioner’s substantial delay after learning of the outcome of the prior proceedings weighs strongly in favor of exercising the Board’s discretion to deny institution of the present proceeding. *See Valve*, Paper 11 at 14 (finding the petitioner’s filing delay of five months from the prior petitioner’s petition weighed in favor of discretionary denial); *Ericsson II*, Paper 7 at 13 (finding that factor five “urges in factor of denying the [p]etition” where the petitioner waited nearly ten months from when it became aware of its infringement accusation); *Mitek Sys.*, Paper 30 at 33-34 (finding the petitioner’s “unreasonable” delay of at least seven months weighed in factor of discretionary denial).

The instant Petition does not mention or discuss the *General Plastic* factors at all. *See* Pet. at 11-12 (discussion limited to *Fintiv* and § 325(d) discretionary denial).

Petitioner does not provide *any* explanation as to when it learned of the Law and Wood references or as to the length of time elapsed between the filing of the Petition and when it first learned of its infringement accusation. To the extent that a reasonable explanation exists for Petitioner's delay, "it was incumbent upon Petitioner to identify those circumstances to the Board in the Petition itself." *Seki S.P.A. v. CM2W JSC*, No. IPR2020-01636, Paper 9 at 9-10 (P.T.A.B. Jan. 7, 2021) (finding factors four and five in favor of exercising its discretion to deny institution); *see also id.* at Paper 8 (P.T.A.B. Dec. 2, 2020) (denying the petitioner's motion for additional briefing and finding it was reasonably foreseeable that the patent owner would argue *General Plastic* and that the petitioner should have addressed the factors in the petition).

Given the objectively long time between the two petitions and Petitioner's wholesale failure to address the delay (or any factors relevant to discretionary denial under *General Plastic*), factor five weighs strongly in favor of discretionary denial.

F. Factors 6 and 7: The finite resources of the Board

General Plastic Factor 6 also weighs against institution. The sixth *General Plastic* factor considers "the finite resources of the Board." *Gen. Plastic*, Paper 9 at 9-10, 16. The Board's resources would be more fairly expended on initial petitions rather than on the instant Petition. *Id.* at 10. This is indeed true as the validity of the '266 Patent has been thoroughly tested during the initial prosecution and the '1154

IPR, with the Board determining that a reconsideration of the patent grant is not warranted. *See Oil States Energy Servs., LLC v. Greene's Energy Grp., LLC*, 138 S. Ct. 1365, 1374 (2018) (inter partes review is simply a reconsideration of the patent grant). The Board need not entertain a third challenge to the '266 Patent's confirmed validity as its resources are better spent reviewing petitions asking for the first time for the Office to reconsider the initial patent grant. Accordingly, factor 6 weighs in favor of discretionary denial, and factor 7 is neutral because Centripetal has no reason to believe that the Board could not issue a final determination in this case within one year of institution.

IV. LEVEL OF ORDINARY SKILL IN THE ART

For the purpose of this Preliminary Response only, Centripetal adopts the Board's level of ordinary skill in the art set forth in its '1154 decision, "a person of ordinary skill in the relevant art 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.

V. CLAIM CONSTRUCTION

Under *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005), patent claims are interpreted in light of the intrinsic evidence, including the specification and file history, and “the ordinary and customary meaning of a claim term is the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention, *i.e.*, as of the effective filing date of the patent application.” *Id.* at 1313, 1317 (citations omitted); *see also* 83 Fed. Reg. 51340, 51341 (Oct. 11, 2018) (adopting *Phillips* standard for AIA proceedings before the Board).

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

In the '1154 decision, the Board concluded that the preambles are 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. Indeed, the preamble’s recitation of “plurality of packet security gateways that collectively provide an entire interface across a boundary of a [protected] network” is essential to understand the “all traffic traversing the boundary” limitation in the body of the claims. Thus, the Board should likewise construe the preambles as limiting here.

B. Other Constructions

Petitioner requests that the Board adopt the constructions of the following claim terms that have been construed in previous IPR proceedings:

Term	The PTAB's construction
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
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. For the purpose of this Preliminary Response only, Centripetal adopts and applies these constructions.

VI. OVERVIEW OF THE REFERENCES

A. Law

While the '266 Patent leverages a plurality of PSGs to provide an “entire interface across a boundary” of a protected network to apply packet filtering rules to “all traffic traversing the boundary” along with an SPMS that automatically creates or alters a first set of packet filtering rules received by a PSG, Law does neither. *See* § II.A, *supra*; '266 Patent at Claims 1, 8, 15, 21.

Instead of locating a plurality of PSGs at the boundary of a network protected by a PSG, Law discloses using individual firewalls to protect separate networks. Specifically, Law teaches that firewall 146a protects LAN 150a of sub-system 105a while firewall 146b separately protects LAN 150b of sub-system 105b. *See* Law at ¶¶ 51, 53, 72, Figs. 1A, 1B, and 3.

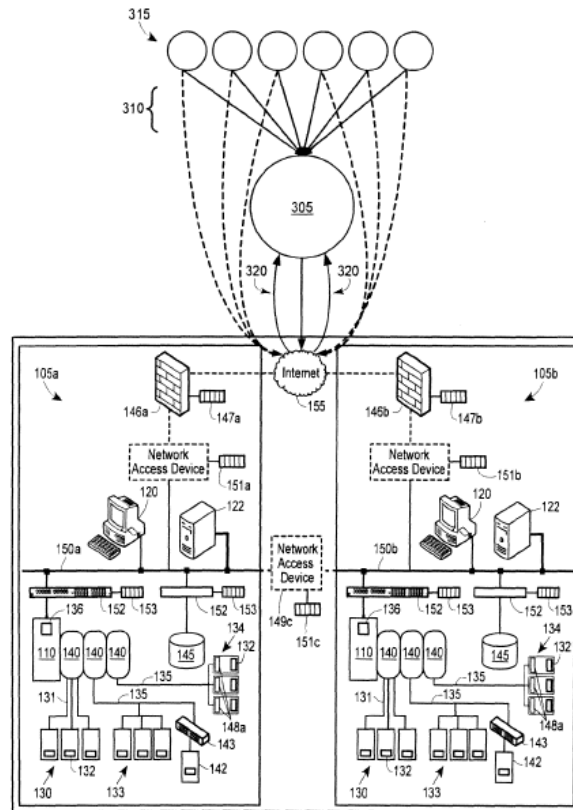


Fig. 3

Id. at Fig. 3. Because Law's firewall 146a does not protect LAN 150b, LAN 150b cannot be considered "a network protected by the packet security gateway," whether or not it is connected to LAN 150a via Network Access Device 149c. Because LAN 150b is not "a network protected by" firewall 146a, it is (by the terms of the Challenged Claims) "one or more networks other than the network protected by the packet security gateway." As a result, Law does not disclose a plurality of PSGs at the boundary between a network protected by firewall 146a and one or more other networks, as claimed.

Law also does not disclose an SPMS to create rulesets including a first set of rules that is received by either firewall 146a or 146b. Rather, operators within the process control system environment (*e.g.*, a nuclear plant) create the “rulesets [] specific to the system it protects.” *See id.* at ¶ 16 (disclosing that “each ruleset is specific to the system it protects.”); *id.* at ¶ 23 (disclosing that operators using a graphical process control system creates rulesets); *id.* at ¶ 90 (disclosing that the rulesets may be configured based on the operator or other personnel from a graphic display at a workstation in the process control system environment). Using the graphical displays, the operators create the initial ruleset that protects each particular process control system.

Law discloses using a third-party company, firm 305, as a remediation service to update already-existing, operator-created rulesets. *Id.* ¶¶ 30, 88, 89. Specifically, with respect to Figure 3, Law describes a method “to update rulesets of the UTMS” in which firm 305 receives threat data 310 from various sources 315 and constructs rules in the various rulesets. *Id.* In this manner, Law’s UTMS-configured devices receive only updates to the operator-created rulesets, not a first set of rules as required by the Challenged Claims.

Moreover, unlike the claimed SPMS that automatically creates or alters packet filtering rules, Law’s firm 305 is a company, such as Wurldtech Security, Inc., that employs IT personnel to update the operator-created rulesets when new threats are

discovered. *Id.* at ¶¶ 16, 88. Specifically, because “each ruleset is specific to the system it protects,” IT personnel “are still required to update the ruleset when new threats are discovered” to ensure that the update provides the required protection. *See id.* at ¶ 16 (disclosing that “IT personnel are still required to update the ruleset when new threats are discovered”); *id.* at ¶ 88 (“With reference to FIG. 3, a third party, cyber security risk management firm 305 such as Wurldtech Security, Inc. of Vancouver, BC Canada” provides the updates).

B. Wood

Wood 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 [] ‘a feed of suspect addresses from one or more sources on the external network.’”) (quoting Wood at ¶¶ 21, 32, 34, *id.* at Fig. 2). Specifically, 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.

VII. THE PETITION SHOULD BE DENIED BECAUSE PETITIONER FAILS TO DEMONSTRATE A REASONABLE LIKELIHOOD OF SUCCESS ON ANY CHALLENGED CLAIM

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

1. Petitioner Fails to Demonstrate that Law Teaches or Suggests the “Entire Interface Across a Boundary” and “All Traffic Traversing the Boundary” Limitations

Independent Claims 1, 8, and 15 recite, *inter alia*:

- “a plurality of packet security gateways that collectively provide an entire interface across a boundary” (“entire interface across a boundary” limitation); and
- “packet filtering rules to be applied to all network traffic traversing the boundary” (“all traffic traversing the boundary” limitation).

'266 Patent at Claims 1, 8, 15. Like prior-petitioner PAN, Petitioner also fails to demonstrate that its asserted art teaches or suggests the “entire interface across a boundary” and “all traffic traversing the boundary” limitations.

a. Because Law's Firewalls 146a and 146b each protect its own network they do not collectively provide “an entire interface across a boundary”

Independent Claims 1, 8, and 15 of the '266 Patent recite a “plurality of packet security gateways that collectively provide the entire interface across a boundary” of a protected network:

a packet security gateway, of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway and one or more

networks other than the network protected by the packet security gateway

Id. at Claims 1, 8, 15 (emphasis added). By the plain language of the claims, “the network protected by the packet security gateway” is literally the group of networked computers protected by one of the plurality of PSGs. Any network not “protected by the PSG” is, by definition, “one or more networks other than the network protected by the packet security gateway.” Applying this plain-language understanding of the claims to Law, Law cannot possibly disclose “a plurality of packet security gateways that collectively provide an entire interface across a boundary of” that network.

Law's firewalls 146a (outlined in purple) and 146b (outlined in blue) each protects its own network, *i.e.* LAN 150a (outlined in purple) and LAN 150b (outlined in blue), respectively. *See* Law at ¶¶ 51, 53, 72, Figs. 1A, 1B, 3. As Figure 3 illustrates, LAN 150b is not part of “the network protected by” firewall 146a and *vice versa*:

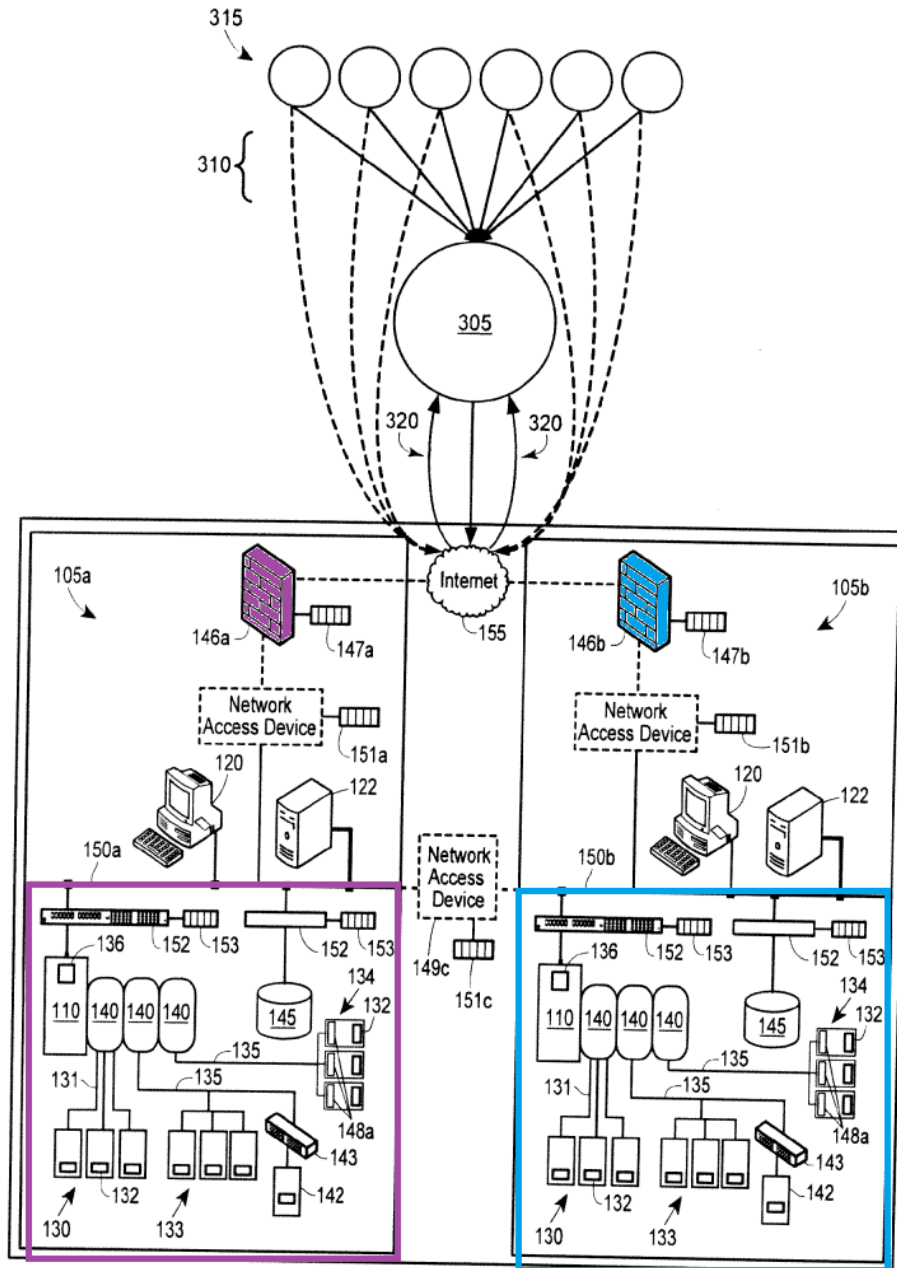


Fig. 3

Id. at Fig. 3 (annotated); *id.* at ¶ 53. Accordingly, if firewall 146a is then taken to be “the packet security gateway” then LAN 150a is the “network protected by the packet security gateway.” Because network 150b is not (and is not part of) the

“network protected by” firewall 146a, network 150b can only be “one or more networks other than the network protected by the packet security gateway.”

Accordingly, if network 150a is “the network protected by the packet security gateway,” firewall 146b (which protects network 150b) cannot be one of the claimed “plurality of packet security gateways that collectively provide an entire interface across a boundary of” that network with “one or more networks other than the network protected by the packet security gateway.” To the contrary, every network besides network 150a must be one of the “one or more networks other than the network protected by the packet security gateway.”

Given the foregoing, Petitioner's reliance on “an embodiment in which LANs 150a and 150b are optionally joined together to form a single network protected by perimeter UTMS firewalls 146a and 146b” fails. *See* Pet. at 19-21, 29-32. Even granting Petitioner's unsupported allegation that the presence of network access device 149c transforms these two separate LANs into “a single network,” the claims do not recite “a plurality of packet security gateways that collectively provide an entire interface across a boundary of” *a single network*. *Id.* at 17-18. They recite “a packet security gateway, of a plurality of packet security gateways that collectively provide an entire interface across a boundary of *a network protected by the packet security gateway* and one or more networks other than the network protected by the packet security gateway.” '266 Patent at Claims 1, 8, and 15 (emphasis added).

Because firewall 146a does not protect LAN 150b, the alleged “single network” cannot be considered “a network protected by the packet security gateway” even when those separate LANs are connected via network access device 149c.

**b. Law's LANs 150a and 150b are Separate Networks
Even When Joined With a Network Access Device**

Nor Law does not teach or suggest that network access device 149c joins LANs 150a and 150b into a single network because these networks still need to communicate with each other over yet another network, such as the Internet. *See id.* at 19-21. Law describes that network access device 149 controls Internet access and enables cross-system communication connection between the two sub-systems. Law at ¶ 32 (“Figure 5 is a simplified block diagram of a UTMA-configured network device for cross-system communication connections”); *id.* at ¶ 94 (an operator uses the network access device 149c “to control network access between the site [as shown in Fig. 4] and the internet and, as shown in Fig. 5, between sites”):

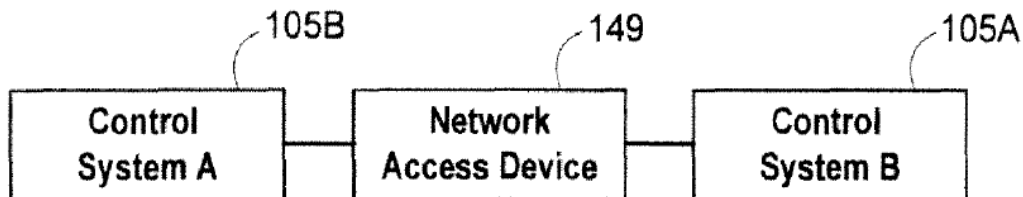


Fig. 5

Id. at Fig. 5; *id.* at ¶ 94; Ex. 2009 at 1 (defining “network access device” as meaning a device that enables communication between devices on local area networks over a wide-area network).

A device that controls network access between two sub-systems or a sub-system and the Internet does not transform two separate networks into one. Law at ¶¶ 32, 94, Fig. 5. Granting Petitioner's argument, every device that connects two networks together would transform those two networks into “a single network,” including, for example, Law's LAN 150a and the Internet. To the contrary, POSITAs use the term “internetwork” to refer to the kind of network of networks disclosed in Law. Ex. 2010 at 3 (definition of internet “[s]hort for internetwork” as meaning “[a] set of computer networks that may be dissimilar and are joined together by means of gateways that handle data transfer and conversion of messages from the sending networks' protocols to those of the receiving network.”). In Law, network access device 149c represents the gateway that connects LANs 150a and 150b. Law at ¶ 94 (an operator uses the network access device 149c “to control network access between the site [as shown in Fig. 4] and the internet and, as shown in Fig. 5, between sites”).

Because Law's network access device 149c does not join LANs 150a and 150b into a single network, let alone the “network protected by the packet security

gateway,” Law does not teach or suggest a plurality of PSGs that protect the claimed network.

c. Petitioner Does Not Sufficiently Explain Its Expanded Number of Firewalls Theory

Petitioner's 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. *TQ Delta, LLC v. Cisco Sys., Inc.*, 942 F.3d 1352, 1361 (Fed. Cir. 2019) (reversing the Board's obviousness determination because the “conclusory and unsupported expert testimony” does not support substantial evidence).

More importantly, 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 even allege that a POSITA would have added more firewalls to any one of the sub-systems. Pet. at 23 (citing Law at ¶ 53). Instead, expanding Law to include more than two sub-systems, as described 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 only be protected by a single firewall rather than the required plurality of PSGs.

For at least the foregoing reasons, Petitioner fails to show that Law teaches or suggests the “entire interface across a boundary limitation.

2. Petitioner Fails to Show that Any Ground Discloses the “All Network Traffic” Requirement

Because Law does not disclose a plurality of PSGs that collectively provide an entire interface across the boundary of a protected network, it also does not disclose “a dynamic security policy comprising a first set of packet filtering rules to be applied to all network traffic traversing the boundary.” *See* §§ VII.A.1.a-c, *supra*. Petitioner's arguments for this limitation also fail because each of Law's firewalls applies a different ruleset tailored to the particular network it protects.

Even granting its position that Law's network access device 149c joins LANs 150a and 150b into a single network, firewalls 146a and 146b apply different rulesets to traffic. Law at ¶ 16 (“In a process control system, each ruleset is specific to the system it protects.”). This means that traffic received at firewall 146a is subject to different rules than traffic received at firewall 146b. Consequently, Petitioner has failed to identify “a first set of packet filtering rules to be applied to all network traffic traversing the boundary,” even if Law's firewalls (146a, 146b) are considered to be located at the claimed “boundary of a network protected by the packet security gateway.”

Law recognizes that each device or application is vulnerable to unique threats. Law at ¶ 22 (explaining that Law's devices are “capable of defending against both known and ‘zero day’ vulnerabilities and threats to control systems for both embedded, proprietary devices, and standard, commonly-used devices”). To address

such unique threats, Law explains that its process control system sends, to a “cyber security risk management firm” (305), “domain-specific information” that includes “information related to the topography” of Law’s process control system such as “the manufacturer, model, state, software/hardware versions, etc., of the types of physical devices in the system.” *Id.* at ¶¶ 88, 89. Firm (305) then uses this “domain-specific information” to “identify network vulnerabilities in any device, sub-system, or software program” and provide “rules for the various rulesets” that Law’s firewalls apply. *Id.* at ¶ 89 (“In this way, each time a new device or code application is introduced to the system 100, any exposure to bugs or other vulnerabilities may be reduced or eliminated.”). These teachings of Law, therefore, show that its firewalls (146a, 146b) would have included unique rulesets having rules that target the specific threats and vulnerabilities of the particular devices, applications, and other components deployed in the respective sub-systems that they protect.

Petitioner’s argument that “a POSITA would have understood that perimeter [] firewalls 146a and 146b apply the received ruleset 147 to all network traffic traversing the boundary” (Pet. at 29), does not acknowledge or otherwise engage with Law’s teachings that the rulesets are specific to the particular process control systems that they are intended to protect. Law at ¶ 16; *see also* Pet. at 29-30. Petitioner does not explain, for example, why a POSITA would have understood that one of Law’s firewalls protecting a subsystem having certain vulnerabilities would

have included the same ruleset as another one of Law's firewalls protecting a different subsystem having different vulnerabilities. The unique threats and vulnerabilities of Law's separate sub-systems (105a, 105b) undermine any argument that their respective firewalls necessarily would have applied the same rulesets. Traffic received at one of Law's firewalls (e.g., 146a) would not have been subject to the same rules as traffic received at another one of its firewalls (e.g., 146b) having a ruleset (e.g., 147b) configured to account for the unique threats and vulnerabilities of its corresponding sub-system (e.g., 105b). The rulesets (147a, 147b) at Law's firewalls (146a, 146b) thus do not constitute the claimed "packet filtering rules" that are "applied to **all network traffic**" traversing the boundary of Law's networks (150a, 150b).

3. Petitioner Fails to Demonstrate that Law Teaches or Suggests "Receiving a First Set of Packet Filtering Rules by the PSG" in which "the First Set of Packet Filtering Rules is Automatically Created or Altered by the SPMS" Limitations

Petitioner fails to demonstrate that Law teaches or suggests "receiving a first set of packet filtering rules by the" PSG in which "the first set of packet filtering rules is automatically created or altered by the SPMS." '266 Patent, Claims 1, 8, 15, and 21. Law's rulesets are created in the first instance by operators within the process control environment.

Petitioner alleges that Law satisfies these limitations because firm 305 allegedly creates ruleset 147 (allegedly a first set of rules) and distributes that ruleset

to firewalls 146a and 146b. *See* Pet. at 39 (alleging that “Law discloses that cyber security risk firm 305 generates its rulesets, including ruleset 147”), *id.* at 27 (alleging that the generated ruleset 147 comprises a first set of rules that is distributed to the UTMS-configured firewall devices), *id.* at 24.

Petitioner's theory is flawed because the UTMS-configured firewall devices do not receive newly created rulesets from firm 305. The initial ruleset 147 is created by operators within the process control system. And while firm 305 provides updates to these operator-created rulesets 147 it does not do so *automatically* because IT personnel are still required to update rulesets when new threats are detected.

a. Law does not teach or suggest the “receiving a first set of packet filtering rules by the PSG” limitation

The Challenged Claims require “receiving a first set of packet filtering rules by the PSG” with the first set “automatically created or altered by the SPMS.” Petitioner's theory is predicated upon firm 305 creating ruleset 147 which comprises a first set of rules that is then distributed to the UTMS-configured firewall devices. *See* Pet. at 36 (alleging that “Law further discloses rules that were automatically created by the security policy management server”), *id.* at 37 (alleging that firm 305 creates ruleset 147), *id.* at 27 (alleging that “[t]he ruleset 147 distributed by cyber security risk management firm 305 to perimeter UTMS firewalls 146a and 146b comprises a first set of packet filtering rules”), *id.* at 24 (alleging that “the service

[firm 305] supplies and distributes the rulesets . . . including rulesets 147”). This theory fails because the UTMS-configured firewalls do not receive ruleset 147 along with a first set given that ruleset 147 is an operator-created ruleset.

In Law's system, ruleset 147 (and a first set of rules) is created by operators within the process control system to ensure that the rulesets are specific to the system it protects. Law at ¶¶ 16, 23, 81, 90. Firm 305 is simply leveraged as a remediation service that provides updates to ruleset 147 when new threats are detected. *Id.* at ¶¶ 30, 88-89 (describing firm 305 as a remediation update service that provides updates to the operator-created ruleset 147). Accordingly, because the process control system already includes the operator-created ruleset 147 with a first set of rules, the UTMS-configured firewall devices receive only updates to ruleset 147, not a first set.

i. Law's operators within the process control system create ruleset 147 and a first set of rules

With process control systems “each ruleset is specific to the system it protects.” *Id.* 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.

Critical to Law's invention is graphical display applications that allow operators to create rulesets specific to the process control system. *Id.* at Abstract (operators utilize “a workstation within a graphical process control system

environment.”). Thus, 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).

Specifically, Law's graphic display application allows an operator to configure ruleset 147 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 10.

Id. 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 ruleset 147, the system already includes a first set of rules in the operator-created ruleset 147. 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 UTMS-configured firewall devices. Law at ¶¶ 23, 81, 90, 102.

Contrary to Petitioner's argument, firm 305 acts as a remediation service to update rules in ruleset 147 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. Specifically, 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 migrations or rules for ruleset 147. *See id.* at ¶ 89 (“Each of these known vulnerabilities may then be translated into migrations 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.*

By leveraging firm 305 as a remediation service to update the operator-created ruleset 147, the process control system's UTMS-configured firewall devices can either access the operator-created ruleset 147 data (e.g., including a first set of rules) as in figure 1A or receive updates to ruleset 147 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.”).

In view of the foregoing, operators within the process control system create ruleset 147 and its first set of rules with firm 305 simply providing updates to the operator-created ruleset 147.

**ii. Petitioner's Only Evidence Is Directed to Law's
UTMS-configured firewall devices receiving
updates to ruleset 147**

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 id.* 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). With this understanding, Petitioner acknowledges that figure 3 of Law is directed to firm 305 and its remediation service of updating rulesets. *Id.* 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., id.* 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 can construct rule and rulesets in figure 3, those rules and rulesets only update operator-created ruleset 147

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; *id.* at ¶¶ 20, 66, 88.

Thus, Petitioner's only record evidence shows that the UTMS-configured firewall devices receive updates to the operator-created ruleset 147 (having a first set of rules) from firm 305, it does not generate ruleset 147 with a first set of rules which is received by the UTMS-configured firewall devices.

* * *

For at least the foregoing reasons, Petitioner's theory of firm 305 creating and distributing ruleset 147 (including a first set of rules) to the UTMS-configured firewall devices fails because the UTMS-configured firewall devices, at best, receive updates to the operator-created ruleset 147 from firm 305. Petitioner, therefore, fails to demonstrate that Law teaches or suggests the “receiving a first set of packet filtering rules by the PSG” limitation.

b. Law does not teach or suggest “the first set of packet filtering rules is automatically created or altered by the SPMS” limitation

Under the construction adopted by the Board in previous IPRs, the claimed SPMS means “a server configured to communicate a dynamic security policy to a packet gateway.” *See* § V.B, *supra*. In addition to this requirement, the Challenged Claims also require that the claimed SPMS automatically creates or alters a first set

of packet filtering rules. *See* '266 Patent at Claim 1 (“the one or more first packet filtering rules of the first set of packet filtering rules . . . [are] automatically created or altered by the security policy management server”); *see also id.* at Claims 8, 15, 21. Petitioner fails to show that Law’s firm 305 discloses or renders obvious the claimed SPMS and required functionality of automatically creating or altering the first set of packet filtering rules.

i. Law’s firm 305 does not disclose the claimed SPMS that automatically creates or alters a first set of packet filtering rules

Petitioner alleges that firm 305 is itself a server that automatically constructs and distributes ruleset 147. But Law defines firm 305 as a commercial company such as Wurldtech Security, Inc. 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.”).

More specifically, Law explains that firm 305 is a “third party, cyber security risk management firm [] such as Wurldtech Security, Inc” that, as a company, provides a remediation update service to the process control system. Law at ¶ 88; *id.* at ¶ 89 (indicating that “firm 305 may provide an ongoing remediation update service to the system 100 in the form of UTMS-device updates” to rules in ruleset 147); *see also id.* at ¶¶ 22, 30. To provide this remediation update service firm 305 necessarily employs IT personnel and uses multiple components to update rulesets

specific to the process control system they protect. *See, e.g., id.* at ¶ 16 (explaining that because process control systems are unique, third-party management still requires “IT personnel . . . to update the ruleset when new threats are discovered”). Thus, firm 305 (external to the process control system) requires the involvement of IT personnel to ensure that updated rulesets provide the requisite protection. *Id.*

Petitioner's citation to paragraph 83 does not show otherwise. *See* Pet. at 38. Petitioner cites paragraph 83's passage of “automatic update of the ruleset 147” to allege that firm 305 automatically updates rulesets. *Id.* (quoting Law at ¶ 83). It does not. By reading Law's passage in isolation, Petitioner mistakenly conflates the process control system that performs automatic updates with that of external firm 305. *Id.* Specifically, paragraph 83 is directed to the process control system, not firm 305:

Generally speaking, a set of predefined graphic elements may be provided in the configuration application to enable a user to construct ***process graphic displays that reflect the process plant and the process control system 100*** in general and include visual representations of the UTMS-configured devices as described above Detection of certain network conditions may also trigger an automatic update of the rulesets 147, 148, 151, 153 or an alarm to prompt a user to perform a manual update of the rulesets or another action to fully secure the system 100.

Law at ¶ 83 (emphasis added); *see also id.* at ¶¶ 81, 82 (describing access to the user interfaces located within the process control system to allow for ruleset configuration, updates, and accepting ruleset updates).

As Law discloses that within the process control system, predefined graphic elements are provided “to enable a user to construct process graphic displays that reflect the process plant and process control system.” *Id.* at ¶ 83; *see also id.* Fig. 2 (showing user-defined profiles 232). In this way, graphic displays allow operators within the process control system to either “perform a manual update of the rulesets” or set “an automatic update” upon “[d]etection of certain network conditions.” *Id.* at ¶ 83. Accordingly, while the process control system manages updates to ruleset 147 either manually or automatically, there is no disclosure or contemplation that external firm 305 automatically updates ruleset 147. Nor could there be because, as explained above, IT personnel outside the system are still required to update rulesets when new threats are detected. *Id.* at ¶ 16.

Petitioner, therefore, makes an insufficient showing that Law discloses that firm 305 performs automatic updates to ruleset 147 to satisfy the claimed SPMS that automatically created or altered the first set of packet filtering rules.

ii. Law's firm 305 does not render obvious the claimed SPMS that automatically creates or alters a first set of packet filtering rules

Petitioner also argues in the alternative that Law renders obvious automatically creating or altering rules by firm 305. Pet. at 37-38. Petitioner's obviousness argument lacks substantiated evidence in view of Law's disclosure which shows involvement by third-party IT personnel.

As established above, Law explains that process control systems greatly differ from that of typical IT environments and require uniquely trained third-party IT personnel to update operator-created rulesets specific to the process control systems they protect. See § VI.A, *supra*. Therefore, in constructing updates to rulesets, IT personnel of firm 305 are instrumental in the updates when new threats are discovered to ensure that the updated rulesets provide the necessary protection. Law at ¶ 88; see also *id.* at ¶ 16 (“IT personnel are still required to update the ruleset when new threats are discovered” and must understand how and why the rulesets need to be changed to protect the specific process control system). Accordingly, third-party IT personnel may construct the updated rulesets and run tests to ensure that the “rulesets effectively secure the process control systems in a desirable manner,” all of which can be performed offline, *i.e.* not on a server. *Id.* at ¶ 88. In this manner, IT personnel and offline computing components are necessarily involved in the updating process.

Critically, Petitioner ignores these unique and necessary third-party IT personnel requirements in referencing alleged “known techniques for automatically generating rules” and asserting “[i]t would have been obvious to a POSITA to incorporate [in firm 305].” Pet. at 38. Petitioner’s assertion is conclusory and lacks evidentiary support from Law itself. *See In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016) (a petitioner’s burden of proving obviousness cannot be satisfied by employing “mere conclusory statements”); *see also Google Inc. v. Koninklijke Philips N.V.*, No. IPR2017-00409, Paper 10 at 13-14 (P.T.A.B. Jun. 5, 2017) (denying institution based in part on petitioner’s conclusory statements that lacked reasoned analysis and evidentiary support.). In fact, Petitioner’s only support for this assertion is from Dr. Jacobson who merely repeats, verbatim the assertion for which it is offered for support. *See, e.g., Ex. 1003, Jacobson Decl.*, ¶ 89; *Xerox Corp. v. Bytemark, Inc.*, No. IPR2022-00624, Paper 9 at 15-16 (P.T.A.B. Aug. 24, 2022) (precedential).

Equally problematic is that Petitioner dispensed with “provid[ing] adequately developed explanations” when relying on the alleged techniques for automatically generating rules. *See Pet. at 37-38; Ariosa Diagnostics v. Verinata Health, Inc.*, 805 F.3d 1359, 1366 (Fed. Cir. 2015) (case law has “not dispense[d] with the need for parties to provide adequately developed explanations when relying on background knowledge based on cited art.”). Other than ostensibly saying that automatic

generation was allegedly known, Petitioner does not provide an adequate explanation for *why* a POSITA would have incorporated such an alleged technique in firm 305, nor *how* such incorporation would have ensured that each ruleset update is specific to the particular process control system and its particular security needs without the involvement of IT personnel that are “still required to update the ruleset when new threats are discovered.” Law at ¶¶ 16, 88; *see also* § VI.A, *supra*. Law’s firm 305 is not one that automatically updates rulesets, but instead, one that relies on the expertise and knowledge of the firm’s IT personnel to construct rules based on their understanding of the network topography of Law’s process control system and the particular needs of the devices it contains. *See* Law at ¶¶ 16, 88.

* * *

In view of the foregoing, Petitioner fails to show that Law teaches or suggests “the first set of packet filtering rules is automatically created or altered by the SPMS” limitation.

B. Ground 2: Claims 1-27 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 [] ‘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 § VII.A, *supra*. Accordingly, Ground 2 fails for the same reasons Ground 1 fails.

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

Petitioner has not demonstrated a reasonable likelihood 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 § VII.A, *supra*. Accordingly, Petitioner fails to demonstrate a reasonable likelihood that Claims 6, 13, 19, and 26, which depend from the independent claims, are unpatentable over Law in view of Jungck.

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

Petitioner has not demonstrated a reasonable likelihood 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 §§ VII.A-VII.C, *supra*. Accordingly, Petitioner fails to demonstrate a reasonable likelihood that Claims 6, 13, 19, and 26, which depend from the independent claims, are unpatentable over Law in view of Jungck.

VIII. CONCLUSION

For the foregoing reasons, institution should be denied.

Patent Owner's Preliminary Response
IPR2023-00445 (U.S. Patent No. 10,785,266)

Respectfully submitted,

Dated: April 26, 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 PRELIMINARY RESPONSE** specified in 37 C.F.R. § 42.24 has 11,378 words in compliance with the 14,000-word limit set forth in C.F.R. § 42.24(b)(1). This word count was prepared using the Microsoft Word word-processing system used to prepare this paper.

Dated: April 26, 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>	April 26, 2023
<i>Manner of service</i>	Electronic Filing with the Board
<i>Documents served</i>	PATENT OWNER'S PRELIMINARY RESPONSE
<i>Persons served</i>	Gerard M. Donovan Peter J. Chassman Jonathan I. Detrixhe Sidharth Kapoor REED SMITH LLP gdonovan@reedsmith.com pchassman@reedsmith.com jdetrixhe@reedsmith.com skapoor@reedsmith.com

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