

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KEYSIGHT TECHNOLOGIES, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, LLC,
Patent Owner.

Case IPR2023-00448
Patent No. 11,012,474

PATENT OWNER'S SUR-REPLY

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. THE CHALLENGED CLAIMS ARE PATENTABLE	3
A. Law’s Firm 305 is Not a “Security Policy Management Server” That “Automatically” Updates Rulesets	3
1. Firm 305 is Not a “Security Policy Management Server” But a Commercial Entity	3
2. Firm 305 Does Not Automatically Update Rulesets as IT Personnel Are Required in the Updates	5
B. Law Alone or in View of Golnabi Does Not Render Obvious Adding, Removing, or Altering Rules in a Dynamic Security Policy Based on Correlation Between Portions of Malicious Traffic Information, Knowledge of a Problem Does Not Provide the Motivation to Reach the Particular Claimed Invention.....	8
1. Law Alone Does Not Render Obvious Adding, Removing, or Altering Rules in a Dynamic Security Policy Based on Correlation	10
2. Law in View of Golnabi Does Not Render Obvious Adding, Removing, or Altering Rules in a Dynamic Security Policy Based on Correlation.....	12
C. Neither of Petitioner’s Theories Support a Finding That Law Teaches or Suggests “an Indication of a Feed”	14
III. CONCLUSION.....	22

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Ariosa Diagnostics v. Verinata Health, Inc.</i> , 805 F.3d 1359 (Fed. Cir. 2015)	7, 8
<i>Becton, Dickinson & Co. v. Tyco Healthcare Grp., LP</i> , 616 F.3d 1249 (Fed. Cir. 2010)	14
<i>Belden Inc. v. Berk-Tek LLC</i> , 805 F.3d 1064 (Fed. Cir. 2015)	10, 11
<i>Cisco Sys., Inc. v. Egenera, Inc.</i> , No. IPR2017-01341, Paper 10 (P.T.A.B. Nov. 13, 2017).....	14, 15
<i>Comcast Cable Comm'ns, LLC v. Promptu Sys. Corp.</i> , 838 F. App'x 551 (Fed. Cir. 2021)	15
<i>Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.</i> , 800 F.3d 1375 (Fed. Cir. 2015)	6
<i>Engel Indus., Inc. v. Lockformer Co.</i> , 96 F.3d 1398 (Fed. Cir. 1996)	14
<i>In re Gorman</i> , 933 F.2d 982 (Fed. Cir. 1991)	8
<i>Henny Penny Corp. v. Frymaster LLC</i> , 938 F.3d 1324 (Fed. Cir. 2019)	7
<i>Innogenetics, N.V. v. Abbott Lab'ys</i> , 512 F.3d 1363 (Fed. Cir. 2008)	9, 12
<i>Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.</i> , 821 F.3d 1359 (Fed. Cir. 2016)	4, 20, 21
<i>Platinum Optics Tech. Inc. v. Viavi Solutions Inc.</i> , No. IPR2021-00432, Paper 8 (P.T.A.B. Aug. 17, 2021).....	11
<i>Samsung Elecs. Co. v. Netlist, Inc.</i> , No. IPR2022-00063, Paper 53 (P.T.A.B. May 3, 2023)	18

<i>SIBIA Neurosciences, Inc. v. Cadus Pharm. Corp.</i> , 225 F.3d 1349 (Fed. Cir. 2000)	9
<i>TQ Delta, LLC v. CISCO Sys., Inc.</i> , 942 F.3d 1352 (Fed. Cir. 2019)	9
<i>Xerox Corp. v. Bytemark, Inc.</i> , No. IPR2022-00624, Paper 9 (P.T.A.B. Aug. 24, 2022).....	16
Statutes	
35 U.S.C. § 312(a)(3).....	4
35 U.S.C. § 316(e)	6

PATENT OWNER'S EXHIBIT LIST

Exhibit	Description
2001	Excerpts from The American Heritage Dictionary - "Firm" (4th ed. 2001)
2002	Declaration of Dr. Michael T. Goodrich in Support of Patent Owner's Response
2003	RESERVED
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	IBM Webpage – Centripetal Networks X-Force Security, available from https://www.ibm.com/case-studies/centripetal-networks-x-force-security , dated April 12, 2022
2006	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
2007	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 Board should hold patentable the Challenged Claims because Petitioner fails to show that Law teaches or suggests a “security policy management server” (“SPMS”) that “automatically create[s] or alter[s]” “one or more of the packet filtering rules.” ’474 Patent at Claims 1, 9, 17, 25. Petitioner’s reliance on Law’s cyber security risk management firm 305 (“firm 305”) as corresponding to the claimed SPMS introduces several errors into Petitioner’s obviousness analysis.

First, firm 305 is not itself a server but rather a commercial entity consisting of IT personnel and various infrastructure components. Petitioner also does not identify with any particularity a server within the commercial entity that performs the claimed automatically generating and distributing dynamic security policy functionality. Thus, for this basis alone, Law’s firm 305 does not satisfy the claimed SPMS. *Second*, firm 305 does not automatically update rulesets because it leverages IT personnel to perform such updates. Significantly, Law makes clear that IT personnel of third party firms, such as firm 305, are “still required to update the ruleset[s] when new threats are discovered” to ensure that the updates provide the desired process control system protection. Law (Ex. 1005) at ¶¶ 16; *see also id.* at ¶ 88.

Petitioner also fails to show that Law taken alone or in view of Golnabi teaches or suggests adding, removing, or altering rules in a dynamic security policy,

as in the Challenged Claims. '474 Patent at Claims 1, 9, 17, 25. In reply, Petitioner contends that Law identifies the duplicate rule problem that would have motivated a POSITA to make the modification to Law alone or in combination with Golnabi. See Paper 16 ("Reply") at 10-12. But nowhere does Law disclose or even suggest such a problem nor a solution. Even if it had, identifying a known problem does not provide the motivation to modify the art in such a way to arrive at the claimed invention. In fact, Petitioner's obviousness theory does not even facially arrive at the claimed invention. Petitioner's allegations, which have no support in Law, show the removal of duplicate data from the received threat data itself. Accordingly, even if Petitioner's fabrication found a basis in Law, this theory does not meet the claims because there is no alteration to the "dynamic security policy" as the Challenged Claims require. See '474 Patent at Claims 25 (adding, removing or altering the "one or more rules of the dynamic security policy" based on the correlation); see also *id.* at Claims 1, 9, 17. Thus, assuming *arguendo* a motivation to modify Law alone or in view of Golnabi absent hindsight (there is none), a POSITA would not have reached the claimed invention.

Finally, Petitioner fails to show that Law teaches or suggests "a first packet filtering rule of the packet filtering rules" including "an indication of a feed." Petitioner presents two theories for this limitation: one based on disclosure and the

other based on obviousness. Both of which fail as they are legally and factually unsound.

II. THE CHALLENGED CLAIMS ARE PATENTABLE¹

A. Law's Firm 305 is Not a "Security Policy Management Server" That "Automatically" Updates Rulesets

The Challenged Claims are 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.

1. 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." Paper 2 ("Pet.") at 23; Ex. 2007 at 38:2-39:1. 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. Paper at 12 ("POR") at 12-13 (citing Ex. 2001 at 3). On cross-examination, Dr. Jacobson acknowledged that firm 305 operates as a service comprising various IT

¹ Grounds 2-5 challenge the dependent claims, accordingly, Centripetal's arguments concerning the independent claims in Ground 1 also apply to Grounds 2-5.

infrastructure and staff. Ex. 2006 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 system.” Law at ¶ 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 3-4. 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 Keysight 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 Keysight 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, or one of its IT infrastructure components, satisfies the claimed SPMS.

2. 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[]" the "one or more packet filtering rules," as required by the Challenged Claims. See '474 Patent at Claims 1, 9, 17, 25. 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 2-7.

First, Law does not disclose automatically creating or altering rulesets. See *id.* at 4-5,6, 7 (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 5, 6 (citing Law ¶ 88)), it does not disclose any methods would or even could forego the required manual input of IT personnel. Law at ¶ 88. On the contrary, Law is clear that IT personnel are "still required to update the ruleset when new threats are discovered." Law at ¶ 16, *see also id.* at ¶ 88; POR at 9-10, 16-18.

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 5. 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 updating rulesets, *i.e.* constructing the 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. 2006 at 38:1-10; POR at 13, 18-19.

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 14-15. 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. 2006 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, Keysight's reliance on alleged state-of-the-art techniques is unavailing. Reply at 6-7. Keysight 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 18-19 (citing Law at ¶ 21 (“‘[S]eparately-trained IT personnel’ are required to ‘quickly and accurately manage’ the industrial environment”)). In this manner, IT personnel are involved in configuring ruleset updates so as to “account for the unique needs of the control system,” not a server as claimed. Law at ¶ 20.

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 16-17 (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 8-10 (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” to argue that this would have *suggested* to a POSITA to use automatic techniques (see Reply at 6) to the exclusion of Law’s full disclosure explaining 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.”) (citation 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 6) 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 at ¶¶ 16, 88; *Ariosa Diagnostics*, 805 F.3d at 1366. As such, there is no support for Petitioner's argument and it should be rejected.

B. Law Alone or in View of Golnabi Does Not Render Obvious Adding, Removing, or Altering Rules in a Dynamic Security Policy Based on Correlation Between Portions of Malicious Traffic Information, Knowledge of a Problem Does Not Provide the Motivation to Reach the Particular Claimed Invention

There is no dispute that Law does not disclose nor otherwise suggest the limitation at issue. The Petition therefore gleans from the '474 Patent itself why it would have been obvious in Law, taken alone or in combination with Golnabi, to correlate threat data to remove duplicates. See POR at 20-27; Pet. at 36-37 (relying on the '474 Patent to identify the problem in Law). It is black letter law that using the claimed invention to fill in the gaps in the prior art is impermissible, and serves as an additional reason why the claims are patentable. See *In re Gorman*, 933 F.2d 982, 987 (Fed. Cir. 1991) (expressing that it is “impermissible . . . to engage in a

hindsight reconstruction of the claimed invention, using [its] structure as a template and selecting elements from the references to fill the gaps”) (citation omitted); *TQ Delta, LLC v. CISCO Sys., Inc.*, 942 F.3d 1352, 1361 (Fed. Cir. 2019) (a patent challenger cannot “use the challenged patent as a roadmap to reconstruct the claimed invention . . . i.e., the impermissible *ex post* reasoning and hindsight bias that *KSR* warned against.”) (citations omitted).

Petitioner's Reply compounds its hindsight error by alleging that a POSITA would have been motivated to correlate threat data in Law alone or in combination with Golnabi because of Law's alleged *duplicate rules problem*. See Reply at 10-12, 13. But Law does not describe such a problem, and even if it had, knowledge of a problem and motivation to solve it does not provide the motivation to modify Law alone or with Golnabi to reach the particular claimed invention. See *Innogenetics, N.V. v. Abbott Lab'ys*, 512 F.3d 1363, 1373 (Fed. Cir. 2008) (“[K]nowledge of a problem and motivation to solve it are entirely different from motivation to combine particular references to reach the particular claimed method.”) (citation omitted); *SIBIA Neurosciences, Inc. v. Cadus Pharm. Corp.*, 225 F.3d 1349, 1356 (Fed. Cir. 2000) (for single reference obviousness, “there must be a showing of a suggestion or motivation to modify the teachings of that reference to the claimed invention in order to support the obviousness conclusion.”) (citation omitted). Indeed, Petitioner's obviousness theories do not even reach the particular claimed invention.

1. Law Alone Does Not Render Obvious Adding, Removing, or Altering Rules in a Dynamic Security Policy Based on Correlation

Petitioner contends that it would have been obvious in Law to correlate threat data because of the data potentially including duplicate rules from which a duplicates rules problem arises. Reply at 11-12 (stating that threat data includes rules, and therefore “the problem of duplicate rules arising from Law’s aggregation of threat data follows directly from the text of Law.”). However, just because threat data potentially includes duplicate rules, does not mean that there exists a known problem in Law. Indeed, nowhere does Law expressly disclose or otherwise suggest a problem in receiving threat data with duplicate rules nor a solution needed based on correlation. Rather, Law simply discloses collecting and aggregating the threat data, nothing more. *See, e.g.*, Law at ¶ 89. As such, Petitioner’s duplicate rules problem argument is reliant upon *ex post* reasoning fashioned from the ’474 Patent. *See* POR at 22 (“Dr. Jacobson’s opinion [is] given from the opinion of one already imbued with the ’474 Patent’s **recognition of** and **solution to** the problem of duplicate information coming from multiple malicious host tracker services.”)

Even if duplicate rules were a known problem, the problem does not provide a sufficient reason for why a POSITA would have been motivated to correlate the threat data and remove packet filtering rules from the dynamic security policy based on the correlated information, as required by the Challenged Claims. *See Belden*

Inc. v. Berk-Tek LLC, 805 F.3d 1064, 1073 (Fed. Cir. 2015) (“[O]bviousness concerns whether a skilled artisan not only *could have made* but *would have been motivated to make* the combinations or modifications of prior art to arrive at the claimed invention.”) (citation omitted); *see also Platinum Optics Tech. Inc. v. Viavi Solutions Inc.*, No. IPR2021-00432, Paper 8 at 46-47 (P.T.A.B. Aug. 17, 2021) (finding that even if a problem was known, it does not provide the reasoning for why a POSITA would have looked to a reference to obtain the claimed invention).

Assuming *arguendo* that a POSITA would have been motivated to correlate the threat data in Law, they would have removed the duplicate data from the analyzed threat data itself, not the dynamic security policy, as recited in the Challenged Claims. *See* '474 Patent at Claims 1, 9, 17 (“wherein one or more of the packet filtering rules [***of the dynamic security policy***] were added, removed, or altered”), Claim 25; *see also* POR at 24-25 (asserting that a POSITA would have analyzed the received threat data and removed duplicate data before constructing updates to the rulesets). Petitioner does deny this. Reply at 11-12 (alleging that the threat data includes the duplicate rules); *see also id.* at 13; Ex. 2007 at 48:11-22. In fact, Petitioner does not dispute that Law’s operator-creator rulesets (e.g., ruleset 147) do not include any duplicate rules. *See* POR at 23-24. As such, there is no update to the dynamic security policy as claimed because Law is completely silent

as to removing any data, much less from a dynamic security policy. See POR at 24 (citing Law at ¶¶ 21, 23, 81, 90).

2. Law in View of Golnabi Does Not Render Obvious Adding, Removing, or Altering Rules in a Dynamic Security Policy Based on Correlation

Law in view of Golnabi does not resolve the above deficiencies for the reasons as follows. *First*, Petitioner's allegation that Golnabi "solve[s] the same problem" (Reply at 12) does not supply the motivation to combine the references to reach the particular claimed invention for the reasons discussed above. *Innogenetics*, 512 F.3d at 1373.

Second, assuming *arguendo* that a POSITA would have modified Law with Golnabi's technique, the resulting system would have removed the duplicate data from the threat data. Just as would be done in Law alone. See § II.B.1, *supra*. Petitioner appears to misapprehend that Centripetal's argument is based on the threat data including duplicate rules, because any duplicates would be included in the received threat data, not the operator-created rulesets. See Reply at 13; POR at 23-24 (citing Institution Decision at 40). Thus, Petitioner's reply argument of the threat data including the duplicate rules proves Centripetal's point. Reply at 13-14. Because it is undisputed that Law's operator-created rulesets do not include duplicate rules, Golnabi's technique would at most be performed on the threat data having the duplicate data, not the rulesets. See POR at 23-24.

In fact, Petitioner's focus on Golnabi's technique occurring *at any time* reinforces just that. Reply at 14-15 (contending that "Golnabi's teachings are applicable rule optimization *at any time*" such that "a POSITA would have understood the applicability in Law.") (emphasis added). Based on Petitioner's contention, Golnabi's applicability in Law would be for removing the duplicate data from the threat data *at any time before* the rulesets are updated based on the analyzed and processed threat data (having any duplicates removed). That is, a POSITA would have, granting a motivation to modify Law with Golnabi, used Golnabi's technique to remove duplicate data from the threat data itself, which facially does not satisfy the Challenged Claims requirement of adding, removing, or altering rules *from* the dynamic security policy. See '474 Patent at Claims 1, 9, 17, 25.

* * *

At bottom, on the full record Petitioner fails to show by a preponderance of the evidence that Law alone or in view of Golnabi renders obvious "one or more of the packet filtering rules [of the dynamic security policy] were added, removed, or altered by the security policy management server based on a correlation between portions of the malicious traffic information." '474 Patent at Claims 1, 9, 17; see *also id.* at Claim 25.

C. Neither of Petitioner's Theories Support a Finding That Law Teaches or Suggests "an Indication of a Feed"

The Challenged Claims require that "a first packet filtering rule of the packet filtering rules" includes "an indication of a feed managed by at least one of the plurality of malicious host tracker services." Neither of Petitioner's two theories supports a finding that Law renders obvious this claim limitation. See POR at 28-34.

Petitioner's first theory is legally and factually unsound because it depends on Law's protocol 1302 of its rule table (the "protocol") for both the claimed "packet matching criterion" and "an indication of a feed." See Pet. at 38-39, 42-43; Reply at 17; see also POR at 28-29; see also '474 Patent at Claims 1, 9, 17, 25. Where a claim provides for two separate elements, these two elements "logically cannot be one and the same." *Engel Indus., Inc. v. Lockformer Co.*, 96 F.3d 1398, 1404-05 (Fed. Cir. 1996) (concluding that where a claim provides for two separate elements, a "second portion" and a "return portion," these two elements "logically cannot be one and the same"). Based on this legal principle, the Board in *Cisco Sys., Inc. v. Egenera, Inc.*, No. IPR2017-01341 rejected petitioner's theory as being improper because it relied on the same prior art component for multiple claim elements. *Cisco Sys.*, Paper 10 at 13-15 (P.T.A.B. Nov. 13, 2017) (finding that "reliance on the same component for multiple claim elements is improper.") (citing *Becton, Dickinson & Co. v. Tyco Healthcare Grp., LP*, 616 F.3d 1249, 1254 (Fed. Cir. 2010) ("Where a

claim lists elements separately, ‘the clear implication of the claim language’ is that those elements are ‘distinct component[s]’ of the patented invention.”)).

So too here, Petitioner’s first theory is improper because, as the Board correctly recognized at institution, Petitioner identifies Law’s protocol for both the claimed “packet matching criterion” and “indication of a feed.” See Paper 7, Institution Decision at 45-46. Specifically, for the “packet matching criterion” limitation, Petitioner asserts that the protocol (the SCPI protocol, for example) provides the “packet matching criterion.” See Pet. at 38-40 (asserting that the protocol in each row is part of a “single packet matching criterion”); Ex. 2007 at 39:21-40:17. Petitioner then asserts that the protocol also provides an “indication of [a] particular feed.” Pet. at 41-42; *see also* Reply at 18-19. Accordingly, Petitioner’s mapping of Law’s protocol to two distinct claim elements should be rejected for the reasons noted in *Cisco* as improper and consistent with the Federal Circuit’s affirmances. See *Cisco Sys., Inc.*, Paper 10 at 15; *Comcast Cable Comm’ns, LLC v. Promptu Sys. Corp.*, 838 F. App’x 551, 553-54 (Fed. Cir. 2021) (affirming the PTAB’s determination that a petitioner failed to demonstrate unpatentability when it mapped two distinct limitations to the same element in the prior art).

Petitioner’s first theory also fails because it lacks any evidentiary support for how Law’s protocol identifies a particular feed. See Reply at 18-19. Specifically, in reply, Petitioner asserts that if a source supplies a “less-common protocol, such as

the SCPI protocol,” then presumably “a rule featuring that protocol in the protocol type column 1302 would have identified [a] particular feed.” *Id.* at 18. For support, Petitioner relies on Dr. Jacobson’s reply declaration, which merely parrots the Reply’s conclusory argument without any supporting explanation or citation to corroborating evidence. *Id.* (citing Ex. 1017 at ¶ 29); *Xerox Corp. v. Bytemark, Inc.*, No. IPR2022-00624, Paper 9 at 15 (P.T.A.B. Aug. 24, 2022) (precedential) (“the cited declaration testimony is conclusory and unsupported, adds little to the conclusory assertion for which it is offered to support, and is entitled to little weight.”) (citations omitted). Significantly, during cross-examination, Dr. Jacobson admitted that he did not even know what the SCPI protocol is used for, let alone how it is less common so as to identify a particular feed. Ex. 2007 at 43:9-22. Accordingly, Petitioner’s presumption is grounded in no concrete evidence showing that a protocol, such as SCPI, is “less common protocol” than others, nor any explanation on how a POSITA would know that the protocol is unique to and identifies one particular feed.

Petitioner’s conclusory, unsupported presumption is contradicted by its own admissions as well as those from Dr. Jacobson. For example, Petitioner admits that different sources provide rules with the same protocol, such as SCPI. See Reply at 18 (recognizing that it is “not always . . . the case that one of the sources 315 of a plurality of sources would have been the only source providing rules under a

particular protocol (such as SCPI)”), *id.* at 19 (conceding that rules are attributable to several sources). Similarly, Dr. Jacobson admits that there is a “high likelihood” that various sources provide rules including the same protocol, such as SCPI. Ex. 2006 at 20:5-22, 22:17-24:23 (testifying that there is a “high likelihood” that various sources provide duplicate rules with the same protocol, including SCPI); Ex. 2007 at 48:11-24; *see also id.* at 43:23-45:9. Because of the “high likelihood” that a number of sources provide duplicate rules under a particular protocol type, there is no factual basis for Petitioner’s assumption that Law’s protocol would, or even could, identify a particular feed from one source. *See* Reply at 18-19.

Petitioner’s second theory is equally deficient. As a preliminary matter, in reply, Petitioner confuses Centripetal’s responsive arguments concerning Petitioner’s first theory (premised on “a combination of rule parameters” (*i.e.* protocols)) with the Petition’s second theory. *Compare* POR at 29 (addressing Petitioner’s first theory on “a combination of rule parameters”), Pet. at 42 (under Petitioner’s first theory a “combination of rule parameters” allegedly “provide an indication of [a] particular feed” because a source may be associated with the combination) *with* Reply at 19-20 (conflating the Petition’s “combination of rule parameters” of the first theory with the Petition’s second theory). Accordingly, Petitioner’s reply arguments are unconnected to its first theory’s combination of rule parameter and Centripetal’s responsive arguments.

Petitioner's second theory is premised on Law allegedly rendering obvious "an indication of a feed" that explicitly refers to "identifying the feed," *i.e.* indicating the source. Pet. at 42-43. For this explicit identification, the theory would require modification to both the process control system's rule table 1300 to include an identifying source column and third-party firm 305's updated rulesets to include the indication of the source. But Petitioner's alleged rationale focuses only on the modification of the rule table, not the updated rulesets themselves that are distributed by firm 305. *Id.* (providing alleged rationale for the modification of the rule table to communicate information to an operator). Without firm 305's rules identifying the sources, there is no information that could be used to modify the process control system's rule table. See POR at 31-33.

Grounding the modification of firm 305's rules on the process control system is circular, and based on hindsight. See POR at 32-33; Reply at 20-21 (relying on Law's process control system's rule table for modifying firm 305's rules). Simply because Law discloses a rule table does not demonstrate that a POSITA, with no knowledge of the claimed invention, would modify the rulesets of firm 305 to include indication of the sources and then distribute the modified rules to the rule table that also requires modification to include an indication of the source column to store the identifying data. POR at 32-33 (citing *Samsung Elecs. Co. v. Netlist, Inc.*, No. IPR2022-00063, Paper 53 (P.T.A.B. May 3, 2023)).

There is no teaching or otherwise suggestion for modifying Law's rule table, let alone firm 305's updated rulesets. See POR at 33-34. Although Petitioner relies on an embodiment in which Law's process control system receives threat data directly from the sources, that reliance is unavailing and wrong. See Reply at 21 (citing Law at ¶ 92). Specifically, Petitioner alleges that because in this embodiment Law's system receives threat data directly from the sources, it would also identify the source. *Id.* This embodiment, however, does nothing to show that the updated rulesets would include the source information nor that the rule table would include a column to display such information, which is ultimately required for Petitioner's theory. See Pet. at 42-43 (the theory premised upon the rule table modified with an indication of a feed column to communicate the information from the rules). In fact, the embodiment shows just the opposite. See POR at 33-34.

Because the process control system receives threat data directly from the sources for ruleset updates, Law would have described the rule table as including an identifying sources column *if* the updated rulesets themselves included such information. Law at ¶ 92. It does not. See *id.*, Fig. 13 (no sources column indicated in the rule table); POR at 33-34. Considering that the updated rulesets derived from threat data received directly from the sources do not include information identifying sources, a POSITA would **not** "have included that same information indirectly through the rulesets distributed by firm 305." Reply at 21.

Petitioner's rationale also does not supply the motivation for modifying the rule table or firm 305's rules. In the Petition and Reply, Petitioner relies on reliability and trustworthiness as the reason to modify the rule table. *See* Pet. at 42-43; Reply at 20, 22. However, this rationale would not have prompted a POSITA to make any modification to the rule table, much less firm 305's rules, because, as Dr. Goodrich testified, "a threat is a threat" an operator of the process control system would not care what source the threat originated from and whether it is reliable or trustworthy. Ex 1018 ("Goodrich Tr.") at 84:12-20 (testifying that reliability does not matter "[b]ecause a threat is a threat" and "[h]ow many people say it as a threat doesn't make it worse or better"). Further, on cross-examination, Dr. Jacobson testified that because "everything is built on trust" the process control system would "trust [] [firm] 305" and therefore accept firm 305's assessment of source trustworthiness. Ex. 2007 at 51:5-52:22. In this regard, Dr. Jacobson also admits that operators would not care where the threat originated from because trustworthiness of the sources has been accepted.

Petitioner's rationale based on the "possibility of errors" is new and improper and likewise fails to supply a reason that would have prompted a POSITA to make any modifications to the rule table or the rules. *See* Reply at 20, 22. This possibility of errors argument was not advanced in the Petition, and therefore the Board should not considered this new rationale raised for the first time in reply. *Intelligent Bio-*

Sys., 821 F.3d at 1369-70 (the Board is not permitted to entertain an “entirely new rationale” in reply).

Regardless of whether considered, this rationale shows at most ***firm 305*** using such source information when constructing updates to the operator-created rulesets, not operators of the process control system. Goodrich Tr. at 84:21-85:11 (testifying that because threat data is not necessarily always correct it is “aggregated and possessed [sic] by the Firm 305”); Law at ¶¶ 88, 92, FIG. 3. Dr. Jacobson also agreed that firm 305 considers errors when assigning a level of trust to the sources. Ex. 2007 at 49:12-51:4. Having addressed the errors at firm 305, there is no reason to modify the updated rulesets to include the source information nor the rule table to display such information to operators.

Because Law itself does not teach or otherwise contemplate an indication of a feed in its rules and there is no rationale prompting such modifications to both firm 305's rules and the rule table of the process control system to support Petitioner's theory, Petitioner fails to show why a POSITA would have modified Law's rule table and third-party firm 305's rules to arrive at the claimed invention, absent hindsight. See POR at 34. Therefore, on the full record, Petitioner fails to show by a preponderance of the evidence that Law renders obvious “a first packet filtering rule of the packet filtering rules” including “an indication of a feed.”

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 5,141 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

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