

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KEYSIGHT TECHNOLOGIES, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, INC.,
Patent Owner.

IPR2023-00448

Patent 11,012,474 B2

PETITIONER'S REPLY TO PATENT OWNER'S RESPONSE

Table of Contents

I. Introduction	1
II. Argument.....	2
A. Law discloses or renders obvious “one or more first packet filtering rules of the first set of packet filtering rules ... were automatically created or altered by the security policy management server”	2
B. Law in view of Golnabi renders obvious “wherein one or more of the packet filtering rules were added, removed, or altered by the security policy management server based on a correlation between portions of the malicious traffic information”	8
C. Law in view of Golnabi renders obvious “wherein a first packet matching rule of the packet filtering rules comprises: ... an indication of a feed managed by at least one of the plurality of malicious host tracker services”	15
III. Conclusion.....	23

PETITIONER'S EXHIBIT LIST

Exhibit No.	Description
Ex. 1001	U.S. Patent No. 11,012,474 (“’474 Patent”)
Ex. 1002	File History of U.S. Patent No. 11,012,474
Ex. 1003	Declaration of Dr. Doug Jacobson In Support for <i>Inter Partes</i> Review Petition for U.S. Pat. 11,012,474
Ex. 1004	<i>Curriculum Vitae</i> of Dr. Doug Jacobson
Ex. 1005	U.S. Patent Pub. 2011/0072506 (“Law”)
Ex. 1006	U.S. Patent Publication No. 2007/0097976 (“Wood”)
Ex. 1007	Declaration from Nathaniel E. Frank-White, attaching Feb. 2, 2007 Assurent website printout regarding its Vulnerability Research Service (VRS), <i>available at</i> https://web.archive.org/web/20070202094127/http://www.assurent.com:80/index.php?id=58 (“Assurent VRS”)
Ex. 1008	U.S. Patent Pub. 2009/0262741 (“Jungck”)
Ex. 1009	“Analysis of Firewall Policy Rules Using Data Mining Techniques,” authored by Golnabi et al, published by the IEEE in 2006 (“Golnabi”)
Ex. 1010	U.S. Patent 7,095,716 (“Ke”)
Ex. 1011	U.S. Patent Pub. No. 2004/0123220 (“Johnson”)
Ex. 1012	Listing of claims of the ’474 Patent
Ex. 1013	IEEE <i>Xplore</i> Digital Library record for Golnabi
Ex. 1014	Complaint filed in <i>Centripetal Networks, Inc. v. Keysight Technologies, Inc.</i> , Case No. 2:22-cv-00002

Exhibit No.	Description
Ex. 1015	Affidavit of service of complaint filed in <i>Centripetal Networks, Inc. v. Keysight Technologies, Inc.</i> , Case No. 2:22-cv-00002
Ex. 1016	INTERIM PROCEDURE FOR DISCRETIONARY DENIALS IN AIA POST-GRANT PROCEEDINGS WITH PARALLEL DISTRICT COURT LITIGATION (June 21, 2022)
Ex. 1017	Reply Declaration of Doug W. Jacobson, Ph.D.
Ex. 1018	Transcript of Jan. 12, 2024 Deposition of Dr. Michael Goodrich

I. INTRODUCTION

Petitioner submits this Reply to Patent Owner's Response, Paper 12 ("Response") in the *inter partes* review of U.S. Patent No. 11,012,474 B2 ("the '474 Patent"). The Response consists of substantially the same arguments presented in Patent Owner's Preliminary Response, Paper 6 ("Preliminary Response" or "POPR"), which the Board considered and rejected in its Decision Granting Institution of *Inter Partes* Review. See Paper 7 ("Institution Decision" or "I.D."). Specifically, as it did in its Preliminary Response, Patent Owner presents the same three arguments:

1) that Law does not disclose or render obvious "one or more first packet filtering rules" that "were automatically created or altered by the security policy management server" [1.2], [9.4], [17.2], and [25.5] in view of the background of Law disparaging "commercial off-the-shelf (COTS) firewall systems" that had the "disadvantage[]" of "IT personnel [being] still required to update the ruleset when new threats are discovered" (Response at 11-19; POPR at 11-17);

2) that Law in view of Golnabi does not render obvious "wherein one or more of the packet filtering rules were added, removed, or altered by the security policy management server based on a correlation between portions of the malicious traffic information" [1.4], [9.6], [17.4], and [25.7] because a POSITA purportedly would not have recognized that the problem of duplicate rules arising from Law's

aggregation of threat data, nor Golnabi's explicit solution to this problem (Response at 19-28; POPR at 17-25);

3) that Law does not render obvious "wherein a first packet matching rule of the packet filtering rules comprises: ... an indication of a feed ..." [1.5], [9.7], [17.5], and [25.6] because a POSITA purportedly would not have appreciated the desirability of displaying an identification of Law's sources of threat data in a table displaying rules to an operator based on that threat data (Response at 28-34; POPR at 25-27).

The Board was correct in rejecting the arguments presented in the POPR, and, for the reasons set forth in the Petition, the Institution Decision, and below, none of the additional argument or evidence presented in the Response change that. As a result, Petitioner respectfully requests that the Board find that Challenged Claims 1-33 of the '474 Patent are unpatentable on each of the grounds presented in the Petition and should be canceled.

II. ARGUMENT

A. Law discloses or renders obvious "one or more first packet filtering rules of the first set of packet filtering rules ... were automatically created or altered by the security policy management server"

Patent Owner argues that Law does not disclose or render obvious a security policy management server (SPMS) that automatically creates or alters any rules within the rulesets distributed by firm 305. Response at 11-19. Specifically, Patent

Owner contends that Law does not disclose or render obvious the firm 305 automatically generating rulesets because firm 305 would be a company that includes IT personnel. *See* Response at 12. Likewise, Patent Owner contends that “IT personnel ... are still required to manually update the rulesets of process control systems.” Response at 12.

The Institution Decision rejected these arguments. I.D. at 30-35; *id.* at 32 (“Because Petitioner identifies Law’s disclosure that prior-art techniques for creating firewall rulesets include ‘automatically locating devices and generating rules by passively analyzing traffic on the network,’ we disagree with Patent Owner that Petitioner’s assertions about ‘known techniques for automatically generating rules’ lack ‘evidentiary support.’”); *id.* at 34 (“[W]e also disagree with Patent Owner that (1) ‘operators create the rulesets’ in Law’s system and (2) updating the rulesets ‘requires the use of IT personnel.’”). The Board should continue to reject these arguments.

Initially, Patent Owner argues that “Law explicitly discloses firm 305 to be a commercial entity.” Response at 12. To the extent Patent Owner is arguing that firm 305 does not comprise a security policy management server, Patent Owner is wrong, for the same reasons as explained in the Petition. Pet at 23-26; Ex. 1003 ¶¶ 61-64. Moreover, to the extent Patent Owner is arguing that the claim language prohibits the “security policy management server” from being owned by a

commercial entity, Patent Owner is wrong, as no such requirement is recited by the claim language.¹

Furthermore, Patent Owner's argument regarding firm 305 being a company that includes IT personnel fails to rebut Law's relevant teachings regarding firm 305. For example, Patent Owner does not dispute that Law discloses that "third party, cyber security risk management firm 305 ... may collect threat data 310 from a plurality of various sources 315 to construct the various rulesets 147, 148, 151, 153, validate the rulesets, verify, and distribute the rulesets to the UTMS-configured firewalls 146a, 146b," and that such "[r]uleset **collecting, constructing, validating, and distributing may be performed using any type of information technology methods suitable for performing such actions using electronic data,**" including "collecting the threat data 310 from the World Wide Web using various data collection techniques (e.g., robots, crawling, data feeds, collaborative forums, etc.), constructing data files to convey the rulesets to their destination devices in a device-compatible manner, **executing a computer-**

¹ When asked whether the claim language included any requirement that prohibited the claimed "security policy management server" from being owned by a commercial entity, Dr. Goodrich was unable to provide an answer. Ex. 1018 at 64:17-68:25.

implemented algorithm to determine if the rulesets effectively secure the process control systems in a desirable manner (e.g., simulation or other testing method), and distributing the rulesets to the UTMS-configured entities via a secure Internet interface or other suitable method.” Pet. at 29-30 (citing Ex. 1005 ¶ 88 (emphasis added)). Nor does Patent Owner appear to meaningfully dispute that a POSITA would have understood that using “any type of information technology methods suitable for” ruleset constructing would have included methods of automatically constructing rules, but to the extent Patent Owner argues that IT personnel would have necessarily been involved in that process, Patent Owner is wrong. Ex. 1003 ¶ 70; Ex. 1017 ¶ 11. Furthermore, Patent Owner fails to explain what role IT personnel would have had, if any, in the constructing of rulesets by firm 305 using information technology methods and computer-implemented algorithms. *Id.*

Furthermore, Patent Owner’s argument the firm 305 could have included IT personnel overseeing the distributed rulesets does not negate Law’s teachings that rules within the constructed rulesets may have been created automatically. Ex. 1017 ¶ 12. In particular, the claim language does not require that every rule in the set of packet filtering rules have been automatically created or altered by the SPMS. Rather, the claim language only requires that “one or more” rules of the set of packet filtering rules have been automatically created or altered by the SPMS. *See* Ex. 1001 at claims 1, 9, 17, and 25; Ex. 1012 at [1.2], [9.4], [17.2], and [25.5].

Moreover, Dr. Goodrich admitted that so long as one or more rules in the rulesets distributed by firm 305 were automatically created or altered (as Law teaches and suggests), the claim language would be satisfied even if a security policy is subsequently modified by a person. Ex. 1018 at 75:14-76:16.

Patent Owner's arguments regarding firm 305 being a company that includes IT personnel also fails to rebut Law's teachings regarding techniques for automatically constructing rules being well known. For example, as the Petition explained, Law expressly recognizes prior art techniques for "creat[ing] firewall rules" by "**automatically** locating devices and **generating rules** by passively analyzing traffic on the network." Pet. at 30 (citing Ex. 1005 ¶ 21) (emphasis added). In addition, as the Petition explained, in view of Law's disclosure that cyber security risk management firm 305 may use "any type of information technology methods" for "[r]uleset collecting" and "constructing" (Ex. 1005 ¶ 88), it would have been obvious to a POSITA for firm 305 to have used these known techniques for creating firewall rules by automatically locating devices and generating rules by passively analyzing traffic on the network. Pet. at 30; Ex. 1003 ¶ 71. Patent Owner's allegation that firm 305 employs IT personnel for unspecified purposes does not negate the obviousness of incorporating Law's teachings with respect to the automatic generation of rules into the "any type of information

technology methods” used by firm 305 for ruleset constructing, for at least some of the rules in the constructed ruleset. Ex. 1014 ¶ 35.

Lastly, Patent Owner relies extensively on background paragraph 16 of Law for its assertions that firm 305 requires IT personnel to generate rulesets. *See* Response at 13 (arguing that “Law’s paragraph 16 expressly discloses that ‘specifically trained’ IT personnel are required to manage updates outside the operator environment when new threats are detected.”); Response at 14-15 (arguing that “firm 305 is a service that includes separately-trained IP personnel who ‘are still required to update the ruleset[s]’ when the updates occur outside the operator environment.”) (citing Ex. 1005 ¶ 16); Response at 18 (quoting from paragraph 16 in arguing that “[r]eading paragraph 21 in view of third-party firms, a skilled artisan would appreciate that ‘separately-trained IT personnel’ are still required to update rules to meet the needs of industrial environments they service.”).

Patent Owner is wrong. Nothing in Law’s paragraph 16 suggests that firm 305 would require separately-trained IT personnel to update rules. Ex. 1017 ¶ 15. To the contrary, Paragraph 16 of Law is in Law’s “DESCRIPTION OF THE RELATED ART” section, which describes problems faced in the prior art. In describing prior art, Law’s paragraph 16 explains that “commercial off-the-shelf (COTS) firewall systems ... have a number of disadvantages,” including that “IT

personnel are still required to update the ruleset when new threats are discovered or upgrades.” Ex. 1005 ¶ 16. Thus, Law describes that requiring IT personnel to update the ruleset is a disadvantage of the prior art to be avoided, which is the opposite of Patent Owner’s narrative. Instead of requiring IT personnel, Law endeavors to overcome the need for specifically trained IT personnel to create or update firewall rulesets by providing “a Unified Threat Management System (UTMS) including a UTMS-configured firewall, UTMS-configured network access device, and UTMS-configured field devices that are capable of defending against both known and ‘zero day’ vulnerabilities and threats to control systems for both embedded, proprietary devices, and standard, commonly-used devices.” Ex. 1005 ¶ 22.

Likewise, Law’s disclosure that “[d]etection 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” clarifies that updates can occur automatically, without being performed manually by IT personnel, and is consistent with Law’s objective of streamlining protection against known and ‘zero day’ vulnerabilities and threats to control systems without the need for specifically-trained IT personnel. Ex. 1017 ¶ 16; Ex. 1005 ¶ 83.

- B. Law in view of Golnabi renders obvious “wherein one or more of the packet filtering rules were added, removed, or altered by the security policy management server based on a correlation between portions of the malicious traffic information”**

As set forth in the Petition, Law discloses receiving malicious traffic information (threat data 310, including firewall ruleset data) from several different third-party sources 315. *See* Pet. at 36-38; Ex. 1005 ¶ 92 (describing at least three different sources of threat data, Assurent, Secunia, and Carnegie Mellon); *id.*, Fig. 3 (illustrating six different sources 315 of threat data 310 being provided to cyber security risk management firm 305); Ex. 1005 ¶ 92 (disclosing that sources 315 include “sources for firewall ruleset data”). The Petition explained that it would have been obvious to a POSITA that there would have been a high likelihood of duplicates in the received threat data 310. Pet. at 37; Ex. 1003 ¶ 79. For example, it would have been common for different sources 315 to have been aware of some of the same threats. Ex. 1003 ¶ 79; Ex. 1005 ¶ 92.

The Petition explained that processing the received threat data 310 to remove duplicate rules would have been obvious over Law in view of Golnabi, given that Golnabi teaches merging a plurality of rules using “an aggregation algorithm to generate a minimum number of firewall policy rules for efficiency” and that “these **rules are then aggregated by combining...to get one generalized rule.**” Pet. at 38; Ex. 1009, 308 (“combining a group of similar rules”); *see also id.*, 312. It would have been obvious to a POSITA to combine rules as Golnabi teaches, when constructing rulesets as Law teaches using threat data 310 from a

plurality of sources 315, because the appropriate combining of rules can minimize total rules thereby providing processing efficiency. Pet. at 38; Ex. 1003 ¶ 80.

As it did in its Preliminary Response, Patent Owner disputes that a POSITA would have recognized that Law's aggregation of threat data from multiple sources 315 would have given rise to the problem of duplicate rules, and instead asserts that Dr. Jacobson's analysis was tainted by hindsight. Response at 22; POPR at 18-20.

Patent Owner is wrong. As explained in detail in the Petition, a POSITA's awareness that Law's system of aggregating threat data and ruleset data from multiple independent sources would have given rise to duplicate rules is based exclusively on the teachings of Law and a POSITA's understanding of those teachings, not hindsight. For example, Law discloses "aggregat[ing] threat data 310," which includes "firewall ruleset data," from numerous sources 315. Ex. 1005 ¶ 92. The sources 315 include at least three named sources 315—Assurent, Secunia, and Carnegie Mellon—as well as at least three additional unnamed sources. *See* Ex. 1005 ¶ 92 (describing at least three different sources of threat data, Assurent, Secunia, and Carnegie Mellon); *id.*, Fig. 3 (illustrating six different sources 315 of threat data 310 being provided to cyber security risk management firm 305). Accordingly, a POSITA would have understood from the text of Law alone, rather than hindsight, the likelihood of duplicate threat data existing across

the threat data aggregated from the numerous independent sources. Ex. 1017 ¶ 20.

Patent Owner's expert, Dr. Goodrich, agrees:

Q. So in this figure, there is at least six sources 315, correct?

A. I do not dispute that.

Q. As I understand your position that the data provided by the sources 315 includes only threat data, but not rules based on the threat data. Would a person of ordinary skill in the art understand there to be potential overlap in the threat data provided by sources 315?

A. Yes.

Q. In other words, some sources may identify the same threats, correct?

A. Yes, I think that's true.

Ex. 1018 at 83:11-23. However, Dr. Goodrich's contention that threat data provided by sources 315 would not include rules is contradicted by Law, which describes the sources 315 of threat data 310 to be "sources for firewall ruleset data." Ex. 1005 ¶ 92; Ex. 1017 ¶ 20. A POSITA would have understood that "firewall ruleset data" may have included rules. Ex. 1017 ¶ 20. Accordingly, given Law's disclosure of the likelihood of duplicate threat data existing across the threat data aggregated from the numerous independent sources, and given Law's disclosure that the threat data includes firewall ruleset data, the problem of

duplicate rules arising from Law's aggregation of threat data follows directly from the text of Law. Ex. 1017 ¶ 20.

In addition to disputing that a POSITA would have appreciated Law's duplicate rule problem, Patent Owner disputes that a POSITA would have been motivated to consider the express solution to this problem provided by Golnabi. Response at 23. For example, Patent Owner asserts that "there is no record evidence that a POSITA would have considered solving this problem by correlating malicious traffic information at an SPMS and then adding, removing, or altering rules based on that correlation." Response at 23.

Patent Owner is wrong. As explained in the Petition, Golnabi is directed to solving the same problem of removing duplicate rules. Pet. at 15-17, 38. In particular, Golnabi discloses generating policy rules for firewalls designed to "filter out any unwanted traffic coming into or going from the secure network." Ex. 1009, 305-306. In this context, Golnabi recognizes that it is important "to generate a minimum number of firewall policy rules for efficiency." *Id.*, 308. To achieve a minimum number of policy rules, Golnabi merges rules that have similar characteristics. *Id.* ("For example, let's consider to have a few rules of all matching fields with an exception of source port field. In this case, these rules are then aggregated by combining all the matching fields...to get one generalized rule."). Golnabi teaches merging a plurality of rules using "an aggregation algorithm to

generate a minimum number of firewall policy rules for efficiency” and that “these **rules are then aggregated by combining...to get one generalized rule.**” Ex. 1009, 308 (“combining a group of similar rules”); *see also id.*, 312. It would have been obvious to a POSITA to combine rules as Golnabi teaches, when constructing rulesets as Law teaches using threat data 310 from a plurality of sources 315, because the appropriate combining of rules can minimize total rules thereby providing processing efficiency. Ex. 1003 ¶ 80; Ex. 1017 ¶ 22.

Next, Patent Owner asserts that even if a POSITA would have been motivated to analyze Law’s threat data, a POSITA would have found it more efficient to remove duplicate information in the threat data provided by sources 315 rather than use Golnabi’s technique to remove duplicate rules. Response at 24.

Patent Owner is wrong. First, Patent Owner’s argument appears to be based on a misunderstanding that the “threat data” provided by Law’s sources does not include rules, which is contrary to Law’s teaching. Ex. 1017 ¶ 24; Ex. 1005 ¶ 92 (describing the sources 315 of threat data 310 to be “sources for firewall ruleset data.”). Second, in any event, a POSITA would have appreciated that Golnabi’s technique, which may provide “a tremendous performance gain as a result” (Ex. 1009, 314), operates on rules, as explained above. Ex. 1017 ¶ 24. Accordingly, a POSITA would have understood that any inefficiencies from having aggregated

duplicate rules would have been more than outweighed by the tremendous performance gains achieved using Golnabi's technique. Ex. 1017 ¶ 24.

Lastly, Patent Owner argues that a POSITA setting out to improve Law's system with Golnabi's teachings would not have reached the claimed invention. Response at 25. In particular, Patent Owner argues that Golnabi's teachings would have required implementing a ruleset on a protected network, running traffic through the ruleset to create firewall log data, and processing the firewall log data to find and combine similar rules. Response at 25.

Patent Owner is wrong. Patent Owner made a similar argument regarding the purported limits of Golnabi's teachings in another IPR proceeding that addressed Golnabi, which was rejected. *See Cisco Systems, Inc. v. Centripetal Networks, Inc.*, IPR2018-01454, Paper 33 at 16-17 (PTAB Mar. 5, 2020) (FWD rejecting Patent Owner's argument that "Golnabi does not disclose preprocessing because it, instead, discloses 'data mining' a 'firewall log file' to extract characteristics of traffic after that traffic was already received, and does not disclose the processing of rule sets at all" because "a person of ordinary skill would have considered optimizing operations prior to packet processing, although Golnabi addresses managing of rules during packet processing.").

Patent Owner's argument should be rejected for the same reasons here. A POSITA would have understood that Golnabi's teachings are applicable rule

optimization at any time. Ex. 1017 ¶ 26; Ex. 1009, 305, 313-14. Likewise, a POSITA would have been motivated to implement Golnabi's processes for "combining, separating, and ordering of rules" in Law. Ex. 1003 ¶ 57; Ex. 1017 ¶ 26. A POSITA would have recognized that it is desirable to process the rule sets, as Golnabi teaches, by merging, separating, and ordering rules of the rule sets such that they provide optimized performance during operational processing. Ex. 1009, 305; Ex. 1003 ¶ 57; Ex. 1017 ¶ 26. As Golnabi contemplates combining, separating, and ordering of rules in rulesets in order to optimize performance, a POSITA would have been motivated to implement those processes in Law to achieve optimized performance and would have had success doing so. Ex. 1005 ¶¶ 52, 88; Ex. 1009, 305. For example, a POSITA would have understood the applicability in Law by implementing Golnabi's process for combining rules, e.g., by "combining all the source ports as a range" or by aggregating the IP addresses. Ex. 1009, 308. Ex. 1017 ¶ 26.

C. Law in view of Golnabi renders obvious "wherein a first packet matching rule of the packet filtering rules comprises: ... an indication of a feed managed by at least one of the plurality of malicious host tracker services"

The Petition presented two theories for how Law rendered obvious the limitation of the '474 patent that recites that "a first packet matching rule of the packet filtering rules comprises: ... an indication of a feed managed by at least one of the plurality of malicious host tracker services." Pet. at 41-43. The first theory

explained how a POSITA may have been able to ascertain an indication of a feed by inspection of the protocol-type field of Law's rule table, whereas the second theory explained why it would have been obvious to a POSITA to add a column of information to Law's rule table identifying the source[s] on which any particular rule was based. *Id.*

At the outset, the Institution Decision invited the parties to provide briefing in the post-institution papers about the meaning of "an indication of a feed managed by at least one of the plurality of malicious host tracker services." Institution Decision at 45. Patent Owner has not directly briefed the meaning of this term. Response at 28-34. Nevertheless, Patent Owner appears to have acknowledged that whatever the outer bounds of the claim scope, identification of a feed managed by at least one of the plurality of malicious host tracker services is included within the scope of the claimed "indication" of that feed. Response at 30. Because Law renders obvious a rule comprising an identification of a feed under both of Petitioner's obviousness theories, and Patent Owner appears to concede that identification of a feed satisfies the claim scope, Petitioner submits that further briefing is not necessary to resolve the patentability issues.

Starting with respect to the first theory, the Institution Decision determined that "based on the current record, Petitioner does not explain adequately how 'a rule featuring' SCPI as the protocol type may satisfy limitation 1.5's distinct

requirements for a ‘packet matching criterion’ and ‘an indication of a feed.’”

Institution Decision at 46.

As explained in the Petition, with respect to the packet matching criterion, Law explains that “[e]ach of the rulesets 147, 148, 151, 153 may define conditions that, if detected, implement some combination of blocking suspected malicious communications or alerting an operator.” Pet. at 39; Ex. 1005 ¶ 91. Those conditions are specified in the rule table of Fig. 13, which includes condition fields including PROTOCOL 1302, FROM 1304, TO 1306, and PORT 1308:

1300

	1324	1302	1304	1305	1329	1306	1308	1310	1312	1314
		PROTOCOL	FROM	THRESH.	TO	PORT	ACTION	DESCRIPTION	LOG	
1326 →	☒	UDP ↓	10.4.0.0	n/a	232.108.1 16.118	18515	Accept ↓	New Multicast	NO ↓	
1328 →	☐	UDP ↓	10.8.0.0	n/a	0-7	18516	Accept ↓	New Multicast	NO ↓	
	☐	UDP ↓	10.8.0.0	n/a	n/a	18517	Accept ↓	PT_COM_ RDS_IP	NO ↓	
	☐	UDP ↓	10.8.0.0	n/a	n/a	18518	Accept ↓	PT_COM_ RDS_IP	NO ↓	
1330 →	☒	TCP ↓	A	< x MB/ hr	B	18519	Accept ↓	PT_COM_ RTRP	NO ↓	
1332 →	☒	TCP ↓	B	n/a	A	18519	Accept ↓	PT_COM_ RTRP	NO ↓	
	☐	UDP ↓	10.81.14.9	0-2	n/a	18520	Accept ↓	NTP	NO ↓	
	☐	ICMP ↓	...	...	...	18521	Accept ↓	Remote Login	NO ↓	
	☐	ICMP ↓	...	...	...	18522	Accept ↓	Ping Pri-Act	NO ↓	
	☐	ICMP ↓	...	...	...	18523	Accept ↓	Allow SNMP Access	NO ↓	

1316	DeltaV Profile #14 ↓	LOAD	1318
1320		SAVE	1322

Fig. 13

Pet. at 39; Ex. 1005, Fig. 13; *id.* ¶ 102. Although the protocol 1302 is part of Law's packet matching criterion, the packet matching criterion also includes the from-address column 1304, a to-address column 1306, and a port number column 1308. Pet. at 40; Ex. 1005 ¶ 102. Accordingly, under the first obviousness theory, if one of Law's sources 315 was known to be the only source of a set of sources that provided rules with a less-common protocol, such as the SCPI protocol, a POSITA would have understood that a rule featuring that protocol in the protocol type column 1302 would have identified that particular feed. Ex. 1017 ¶ 29. In addition, Law's from-address column 1304, to-address column 1306, and port number column 1308 still would have satisfied limitation [1.5]'s distinct requirement for the packet matching criterion. *Id.*

Although a POSITA implementing Law's system would have understood that it would not always have been 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), on the occasions where that would have been the case, the unusual protocol in the protocol type column 1302 would have been sufficient to identify that particular feed to a POSITA. Ex. 1017 ¶ 29. *See Hewlett-Packard Co. v. Mustek Sys., Inc.*, 340 F.3d 1314, 1326 (Fed. Cir. 2003) ("Just as 'an accused product that sometimes, but not always, embodies a claimed method nonetheless infringes,' a prior art product that sometimes, but not always,

embodies a claimed method nonetheless teaches that aspect of the invention.”
(quoting *Bell Commc’ns Research, Inc. v. Vitalink Commc’ns Corp.*, 55 F.3d 615, 622–623 (Fed. Cir. 1995))).

With respect to the second obviousness theory, the Petition explained that Fig. 13 of Law illustrates a “a ruleset user interface such as a protocol rule table 1300” that “may allow a user to access one or more user interfaces to configure and control any of the rules within the rulesets 147, 148, 151, 152.” Pet. at 42; Ex. 1005 ¶ 102. Given Law’s disclosure of receiving threat data 310 from several sources 315, it would have been obvious to a POSITA that information regarding the source 315 of each rule may be helpful to a user when using the ruleset interface to configure and control any of the rules within rulesets. Ex. 1003 ¶ 87. For example, a POSITA would have understood that some sources 315 may be more trustworthy or reliable than others, and therefore it would have been obvious to communicate that information to a user, such as by adding a column to the rule table 1300 shown in Fig. 13 to indicate, for each rule, the source[s] 315 upon which the rule is based. *Id.*

Patent Owner argues that “Petitioner fails to reconcile with how a ‘combination of rule parameters’ could even identify a particular source when various sources 315 provide the same rules and rule parameters.” Response at 29. In particular, Patent Owner argues that “[b]ecause of the high likelihood that the

various sources provide the same rules, a POSITA would understand that a ‘combination of rule parameters’ in the rules would not and could not identify particular feeds the rules come from.” *Id.*

Patent Owner is wrong. As explained by the Petition, some sources 315 may be more trustworthy or reliable than others, and therefore it would have been obvious to communicate that information to a user, such as by adding a column to the rule table 1300 shown in Fig. 13 to indicate, for each rule, the source[s] 315 upon which the rule is based. Ex. 1003 ¶ 87. When adding such a “column to the rule table 1300 to indicate the source[s] 315 upon which the rule is based” (Ex. 1003 ¶ 87), a POSITA would have understood that it would have been as easy to have identified multiple sources 315 in that column as it would have been to have identified a single source. Ex. 1017 ¶ 32. Accordingly, Patent Owner’s argument regarding certain rules being attributable to multiple sources 315 would not have provided a reason to not identify those sources in table 1300 to provide information to Law’s ruleset operator. *Id.*

To the contrary, even Patent Owner’s expert Dr. Goodrich acknowledges that there may be errors in the ruleset information provided by Law’s sources 315. *See* Ex. 1018 at 84:21-24 (Dr. Goodrich’s agreement that the threat data provided by any source is not necessarily correct). Given the possibility of errors in the ruleset information provided by sources, a POSITA would have understood that

identifying multiple sources for a particular rule in a column added to the rule table 1300 would have given an operator viewing the rule table even greater confidence in the accuracy of a given rule. Ex. 1017 ¶ 32.

Next, Patent Owner also asserts that a POSITA would not have been motivated to modify firm 305 to update rulesets with information indicating the sources 315 the updates are from. Response at 32. However, Law already discloses an embodiment in which sources deliver threat data directly to firewalls, thereby identifying the source of the threat data to Law's firewalls. Ex. 1017 ¶ 34. For example, Law discloses that firewalls 146a and 146b may "collect and aggregate threat data 310 directly from the firm 305 or plurality of sources 315 to construct, validate, and verify the various rulesets." Ex. 1005 ¶ 92. Likewise, Law's Figure 3 depicts "dotted communication lines to deliver" threat data 310 from sources 315 to firewalls 146a and 146b without going through firm 305. *Id.* ¶ 92, Fig. 3. If a firewall collected threat data 310 directly from one of the sources 315, a POSITA would have understood that the firewall would have received an identification of that feed directly from that source. Ex. 1017 ¶ 34; Ex. 1005 ¶ 92. Given that Law discloses providing identifying information of a feed directly to the firewalls 146a and 146b, it would have been obvious to a POSITA to have included that same information indirectly through the rulesets distributed by firm 305, given that firm

305 receives the same source feed information. *See* Ex. 1017 ¶ 34; Ex. 1005, Fig. 3, ¶ 92.

Lastly, Patent Owner appears to dispute that a POSITA would have understood that some sources 315 are more trustworthy or reliable than others. Response at 33. To the extent that Patent Owner is arguing that a POSITA would have understood all of Law’s sources 315—both named and unnamed—to necessarily be equally trustworthy and reliable, Patent Owner is wrong. Ex. 1017 ¶ 36. For example, given that Law names exemplary sources—Assurent, Secunia, and Carnegie Mellon—as well as disclosing additional unnamed sources, a POSITA would have understood that it is impossible to say that the unnamed sources are equally as reliable and trustworthy as the three named sources. Ex. 1017 ¶ 36; Ex. 1005 ¶ 92; *id.*, Fig. 3. Moreover, a POSITA would have understood the possibility of errors in the ruleset information provided by sources. *See* Ex. 1017 ¶ 36; *see also* Ex. 1018 at 84:21-24 (Dr. Goodrich’s agreement that the threat data provided by any source is not necessarily correct). Given the possibility for errors in the information provided by the sources, a POSITA would have understood that all possible sources 315 are not necessarily equally trustworthy, reliable, or error prone. Ex. 1017 ¶ 36. Accordingly, Patent Owner’s stated reasons for disputing the obviousness of the “indication of a feed” limitation have no merit.

III. CONCLUSION

For the reasons set forth in the Petition, and given above, Petitioner has established that the Challenged Claims 1-33 of the '474 Patent are unpatentable. Petitioner respectfully requests that the Board cancel each Challenged Claim.

Dated: January 24, 2024

Respectfully submitted,

/s/ Jonathan I. Detrixhe

Jonathan I. Detrixhe (Reg. No. 68,556)

Reed Smith LLP

101 Second Street

Suite 1800

San Francisco, CA 94105

Tel: 415.543.8700

Fax: 415.391.8269

jdetruxe@reedsmith.com

Counsel for Petitioner

CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. § 42.24 et seq., the undersigned certifies that this document complies with the type-volume limitations. This document contains 5,128 words as calculated by the “Word Count” feature of Microsoft Word for Microsoft 365 MSO (Version 2208), the word processing program used to create it.

Dated: January 24, 2024

Respectfully submitted,

/ Jonathan I. Detrixhe /

Jonathan I. Detrixhe (Reg. No. 68,556)

Reed Smith LLP

101 Second Street

Suite 1800

San Francisco, CA 94105

Tel: 415.543.8700

Fax: 415.391.8269

jdetrixe@reedsmith.com

Counsel for Petitioner

CERTIFICATE OF SERVICE

In accordance with 37 C.F.R. § 42.6(e), and pursuant to an agreement by the parties that filing with the Board through P-TACTS constitutes electronic service, the undersigned certifies that service is being made upon the Patent Owner's representatives identified below via the filing of this document.

James Hannah (jhannah@kramerlevin.com)
Jenna Fuller (jfuller@kramerlevin.com)
Jeffrey H. Price (jprice@kramerlevin.com)
Scott M. Kelly (skelly@bannerwitcoff.com)
Bradley C. Wright (bwright@bannerwitcoff.com)

Dated: January 24, 2024

Respectfully submitted,

/ Jonathan I. Detrixhe /
Jonathan I. Detrixhe (Reg. No. 68,556)
Reed Smith LLP
101 Second Street
Suite 1800
San Francisco, CA 94105
Tel: 415.543.8700
Fax: 415.391.8269
jdetrixhe@reedsmith.com

Counsel for Petitioner