

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KEYSIGHT TECHNOLOGIES, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, LLC,
Patent Owner.

IPR2023-00448
Patent 11,012,474 B2

Before KEVIN F. TURNER, AARON W. MOORE, and
STEVEN M. AMUNDSON, *Administrative Patent Judges*.

PETITIONER'S ORAL ARGUMENT DEMONSTRATIVES

April 22, 2024

Jonathan I. Detrixhe, Gerard M. Donovan

REED SMITH LLP

Grounds for Institution and Disputes

Institution Decision found that the grounds have a reasonable likelihood of prevailing in showing unpatentability of all claims:

- Claims 1–3, 5–7, 9–11, 13–15, 17–19, 21–23, 25–27, 29–31, 33 obvious over Law in view of Golnabi
- Claims 2, 10, 18, 26 obvious over Law, Golnabi, and Wood
- Claims 4, 12, 20, 28 obvious over Law, Golnabi, and Ke
- Claims 5, 13, 21, 29 obvious over Law, Golnabi, and Jungck
- Claims 7, 8, 15, 16, 23, 24, 31, 32 obvious over Law, Golnabi, and Johnson

(Paper 7 at 2, 11)

Grounds for Institution and Disputes

Institution Decision rejected Patent Owner's arguments from its Preliminary Response:

- Rejected Patent Owner's argument 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 because IT personnel purportedly would still be required to update rulesets (Paper 7 at 31-34)
- Rejected Patent Owner's argument 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" 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 (Paper 7 at 38-40)
- Rejected Patent Owner's argument that Law does not render obvious "wherein a first packet matching rule of the packet filtering rules comprises: ... an indication of a feed ..." 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 (Paper 7 at 44-48)

Grounds for Institution and Disputes

Patent Owner's Response consists of substantially the same arguments presented in Patent Owner's Preliminary Response:

- Repeats the argument 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” in view of assertion that IT personnel would still required to update the ruleset when new threats are discovered (Paper 12 at 11-19; Paper 6 at 11-17)
- Repeats the argument 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” 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 (Paper 12 at 19-28; Paper 7 at 17-25)
- Repeats the argument that Law does not render obvious “wherein a first packet matching rule of the packet filtering rules comprises: ... an indication of a feed ...” 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 (Paper 12 at 28-34; Paper 7 at 25-27)

Overview of asserted prior art - Law

(19) **United States**

(12) **Patent Application Publication**

Law et al.

(10) **Pub. No.: US 2011/0072506 A1**

(43) **Pub. Date: Mar. 24, 2011**

(54) **INTEGRATED UNIFIED THREAT
MANAGEMENT FOR A PROCESS CONTROL
SYSTEM**

Publication Classification

(51) **Int. Cl.**
G06F 21/00 (2006.01)

(52) **U.S. Cl.** **726/11; 726/3**

(57) **ABSTRACT**

(75) **Inventors:** **Gary K. Law**, Georgetown, TX (US); **Nate Kube**, Vancouver (CA); **Robert K. Huba**, Georgetown, TX (US); **Brandon Hieb**, Cedar Park, TX (US); **David R. Denison**, Austin, TX (US); **Cheyenne Hernandez**, Quezon City (PH)

(73) **Assignee:** **FISHER-ROSEMOUNT
SYSTEMS, INC.**, Austin, TX (US)

(21) **Appl. No.:** **12/889,235**

(22) **Filed:** **Sep. 23, 2010**

Related U.S. Application Data

(60) Provisional application No. 61/245,496, filed on Sep. 24, 2009.

A Unified Threat Management System (UTMS) for securing network traffic in a process control system may comprise network devices configured to receive network traffic related to the process control system and including a ruleset received from an external source. The ruleset may include one or more rules defining a condition to accept or deny the network traffic received at the network device. The state of the network device may be integrated into the process control system as a process control object or variable, thus allowing the state and other UTMS and component network device parameters and variables to be displayed to an operator at a workstation within a graphical process control system environment. The network devices may also communicate with a perpetual service that proactively supplies the devices with rulesets to meet the latest security threats, threat patterns, and control system vulnerabilities found or predicted to exist within the network.

(Ex. 1005, Abstract; Paper 2 at 12-13)

Overview of asserted prior art - Law

- Law discloses UTMS-configured firewalls 146a and 146b that implement one or more rulesets to inspect and drop malicious packets from the network

NIDS-configured UTMS-configured firewall 146a, 146b and/or UTMS-configured network access device 149a, 149b, 149c or other UTMS-configured elements within the process control system 100 may use one or more rulesets to inspect and drop malicious packets from the network before the malicious packets can reach their intended destination within the process control systems and cause a fault. Additionally or

(Ex. 1005 ¶ 52; Paper 2 at 12)

- Law's protected network 150 may include subnetworks 150a and 150b

other desired standard(s) or protocols, including any standards or protocols developed in the future. The network 150 and devices may also be standard Ethernet communications and network devices supporting any communications protocol (e.g., TCP/IP, ModbusIP, etc.). The field devices 130, 133,

(Ex. 1005 ¶ 55; Paper 2 at 12)

or any other desired communication network 150a, 150b. A network device 146 includes one or more of a network interface card, a network switch, a router, a firewall, a UTMS-configured firewall, a network access device, a UTMS-configured device, or any other component that facilitates data transmission over the network 150a, 150b without changing the underlying data communicated over any portion of a network, for example, the network 150a, 150b. The communication network 150a, 150b may be a local area network (LAN), a wide area network (WAN), a telecommunications network, etc. and may be implemented using hardwired or wireless technology, any portion of which may be implemented using an Internet connection. The controller 110 is

(Ex. 1005 ¶ 54; Paper 2 at 12)

Overview of asserted prior art - Law

- Law discloses a cyber security risk management firm 305 that generates rulesets using threat data and ruleset information provided by third party sources 315 and distributes the generated rulesets to Law's UTMS-configured firewalls 146a and 146b over the Internet

the process control system 100. The UTMS-configured device or entity may receive the ruleset data and the UTMS-configured process object 204e may be configured or programmed to access the ruleset data 147, 148, 151, 153, (FIG. 1a) and other update data on a periodic or non-periodic basis

via any desired communication link to the device or to a third party source (such as cyber security risk management firm 305 as described in relation to FIG. 3, below) via the network 150 or an Internet connection, via another UTMS-configured device that distributes ruleset data to the other UTMS-configured process objects within the process control system 100, or in any other desired manner. A data store 220c may

(Ex. 1005 ¶ 66; Paper 2 at 12)

[0088] As previously described, the various rulesets (e.g., rulesets 147, 148, 151, 153) associated with the UTMS configured network devices 146, 134, 149, 152 require updates to remain effective against network threats. With reference to FIG. 3, a third party, cyber security risk management firm 305 such as Wurdtech Security, Inc. of Vancouver, BC Canada, or other entity, 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,

(Ex. 1005 ¶ 88; Paper 2 at 12-13)

as described above. The sources 315 may create the threat data 310 by monitoring, defining, and analyzing potential and known threats to the security of the process control network (s) 150. For example, data from the Vulnerability Research Service (VRS) of Assurent Secure Technologies, the Computer Emergency Response Team (CERT) of Carnegie Mellon University, Secunia, end user research and monitoring, and data from Achilles™ certified product users (to name but a few of the sources for firewall ruleset data) may be aggregated.

(Ex. 1005 ¶ 92; Paper 2 at 12-13)

Overview of asserted prior art - Law

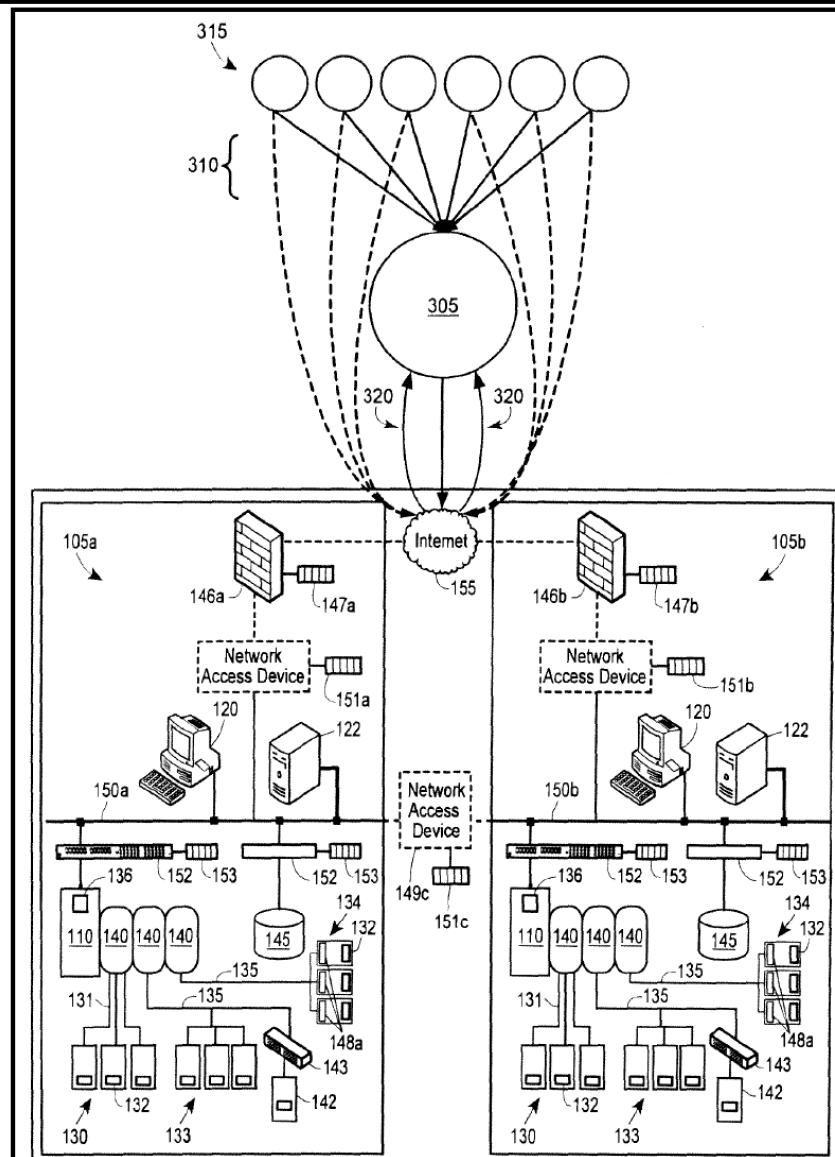
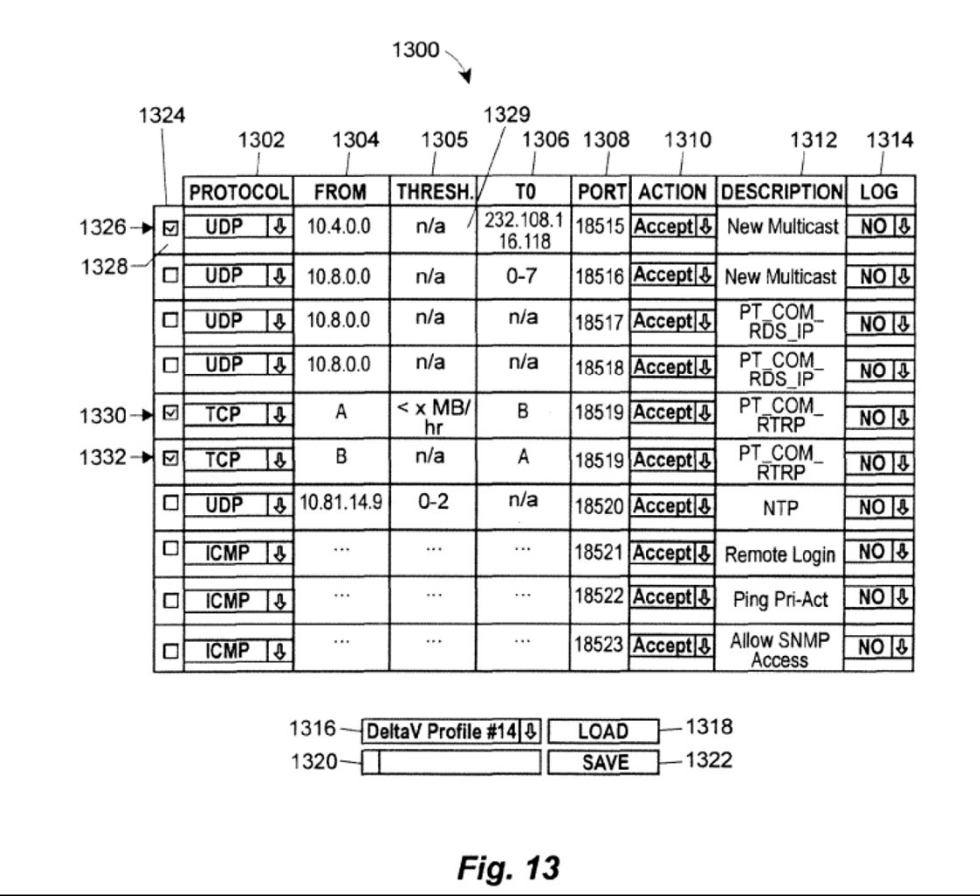


Fig. 3

(Ex. 1005 Fig. 3; Paper 2 at 13)

Overview of asserted prior art - Law

Fig. 13 illustrates a format of the rulesets implemented by Law's perimeter UTMS firewalls 146a and 146b:



a control system 100 from unwanted access and/or malicious attack. For example, a UTMS-configured process object 204e (FIG. 2) may allow a user to access one or more user interfaces to configure and control any of the rules within the rulesets 147, 148, 151, 152 and the network security in the process control system. As illustrated in FIG. 13, a ruleset user interface such as a protocol rule table 1300 may be accessed via the UTMS-configured process object 204e and includes a protocol type column 1302, a from-address column 1304, a threshold parameter column 1305, a to-address column 1306, a port number column 1308, an action column 1310, a description column 1312, and a log column 1314. Protocol types of the example protocol type column 1302 may include, but are not limited to, UDP, TCP, ICMP, HART, and/or SCPI. Addresses in the from-address column 1304

(Ex. 1005 ¶ 102; Paper 2 at 14)

(Ex. 1005 Fig. 13; Paper 2 at 14)

Overview of asserted prior art - Golnabi

Analysis of Firewall Policy Rules Using Data Mining Techniques

Korosh Golnabi, Richard K. Min, Latifur Khan
Department of Computer Science
The University of Texas at Dallas
Richardson, USA
(koroshg, rkm010300, lkhan)@utdallas.edu

Ehab Al-Shaer
School of Computer Science, Telecommunications
and Information Systems
DePaul University
Chicago, USA
ehab@cs.depaul.edu

Abstract— Firewall is the *de facto* core technology of today's network security and defense. However, the management of firewall rules has been proven to be complex, error-prone, costly and inefficient for many large-networked organizations. These firewall rules are mostly custom-designed and hand-written thus in constant need for tuning and validation, due to the dynamic nature of the traffic characteristics, ever-changing network environment and its market demands. One of the main problems that we address in this paper is that how much the firewall rules are useful, up-to-dated, well-organized or efficient to reflect the current characteristics of network traffics. In this paper, we present a set of techniques and algorithms to analysis and manage firewall policy rules: (1) Data Mining technique to deduce efficient firewall policy rules by mining its network traffic log based on its frequency, (2) Filtering-Rule Generalization (FRG) to reduce the number of policy rules by generalization, and (3) a technique to identify any decaying rule and a set of few dominant rules, to generate a new set of efficient firewall policy rules. The anomaly detection based on the mining exposes many hidden but not detectable by analyzing only the firewall policy rules, resulting in two new types of the anomalies. As a result of these mechanisms, network security administrators can automatically review and update the rules. We have developed a prototype system and demonstrated usefulness of our approaches.

Keywords- firewall; data mining; network security; policy

I. INTRODUCTION

In the global world of Internet, firewall is the *de facto* core technology of today's network security and first line of defense against external network attacks and threats. Firewall controls or governs network access by allowing or denying the incoming or outgoing network traffic according to firewall policy rules. These rules are explicitly written and managed to filter out any unwanted traffic coming into or going from the secure network. However, the management of firewall rules has been proven to be complex, error-prone, costly and inefficient for many large-networked organizations. These firewall rules are often custom-designed and hand-written by and for the human policy writer of an organization and tailored to accommodate ever-changing business and market demands of the global Internet. Therefore, these rules are in a constant need of updating, tuning and validating to optimize firewall security.

Although the deployment of firewall technology is the first important milestone toward securing networks, the effectiveness of firewall security may be limited or compromised by a poor management of firewall policy rules.

One of the interesting problems is on how much the rules are useful, up-to-dated, well-organized or efficient to reflect current characteristics and volume of network packets. For example, the network traffic trend may show that some rules are out-dated or not used recently. This may further lead one to consider removing, aggregating or reordering of the rules to optimize the firewall policy and efficiency. Also, server and network logs may validate or confirm that firewall policy rules are updated and consistent with the current network services.

More importantly, data mining over network traffic log may further reveal any violation against the current firewall policies such as transferring plain text over a secure IPsec/VPN link or allowing traffic which may not be permitted by the other downstream devices behind firewalls. Furthermore, the task of manually-managing firewall policy rules becomes very difficult and time-consuming, if not impossible, as the number of filtering rules increases drastically beyond the reasonable scope and scale of a manual process. This enormous task addresses the need for the effective management of firewall security with policy management techniques and tools that enable network administrators with ease to optimize and validate firewall rules automatically.

The first step to bridge the gap between what is written in the firewall policy rules and what is being observed in the network is to analyze traffic and log of the packets using data-mining techniques. Current research is extending the traditional and classical research in the analysis and management of the these policy rules, not only to minimize the number of rules but to generate an efficient rule-set, to reflect the up-to-dated traffic trend, and further to provide a real-time policy update capability from the application (for example, mail server detecting a massive incoming spam-mails from a host).

In this paper, we present a set of techniques and algorithms to analysis and manage firewall policy rules: (1) a data mining technique, Mining firewall Log using Frequency (MLF) to deduce efficient firewall policy rules by mining its network traffic log based on its frequency, (2) Filtering-Rule Generalization (FRG) to reduce the number of policy rules by

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.”); Ex. 1003 ¶ 53.

On the other hand, Golnabi teaches that “[i]t is always possible to split the filtering rule of a multivalued field into several rules.” Ex. 1009, 312. The split rules can then be prioritized “in order to optimize the filtering matching at real-time.” *Id.*, 313-314; Ex. 1003 ¶ 54. As Golnabi shows in Figure 14, example rules 5 and 10 are heavily used:

(Paper 2 at 15-16; Ex. 1009 at 308, 312)

(Ex. 1009 at 1; Paper 2 at 15-16)

Law 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”

- Law’s cyber security risk-management firm 305 necessarily comprises a security policy management server, which automatically creates or alters one or more rules within ruleset 147

because cyber security risk management firm 305 distributes ruleset 147 to perimeter UTMS firewalls 146a and 146b over the Internet 155 (Ex. 1005 ¶¶ 66, 88), a POSITA would have understood that cyber security risk management firm 305 necessarily comprises a server. Ex. 1003 ¶ 63. In addition, although Fig. 3

(Paper 2 at 26; Ex. 1005 ¶ 88; Ex. 1003 ¶ 63)

(Paper 2 at 29-30;
Ex. 1005 ¶ 88;
Ex. 1003 ¶ 70)

Law discloses or renders obvious that one or more rules in ruleset 147 were automatically created by cyber security risk management firm 305. For example, 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-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.” Ex. 1005 ¶ 88. A POSITA would have understood that ruleset constructing using “any type of information technology methods suitable for” ruleset constructing would have included methods of automatically constructing rules. Ex. 1003 ¶ 70.

Law 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”

- It would have been obvious that Law’s cyber security risk-management firm 305 automatically creates or alters one or more rules within ruleset 147

automatically, it would have been obvious to a POSITA for at least a portion of the constructed rules to have been constructed automatically. Ex. 1003 ¶ 71. For example, in addition to disclosing that cyber security risk management firm 305 may use “any type of information technology methods” for “[r]uleset collecting” and “constructing” (Ex. 1005 ¶ 88), 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.” Ex. 1005 ¶ 21. **It would have been obvious to a POSITA to incorporate such known techniques for automatically generating rules for at least some of the rules in ruleset 147 created by cyber security risk management firm 305.** Ex. 1003 ¶ 71.

(Paper 2 at 30; Ex. 1005 ¶¶ 21, 88; Ex. 1003 ¶ 71)

Law further discloses rules that were automatically altered by cyber security risk management firm 305. For example, Law expressly discloses automatically updating (i.e., altering) rulesets in response to detected conditions. Ex. 1005 ¶ 83 (“**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.”); *see also id.* ¶ 88 (“the various rulesets (e.g., rulesets 147, 148, 151, 153) associated with the UTMS configured network devices 146, 134, 149, 152 **require updates** to remain effective against network threats”); *id.* ¶ 89 (disclosing that cyber security risk management firm 305 “translate[s]” “known vulnerabilities” into “rules for the various rulesets 147, 148, 151, 153,” which “the firm 305 may provide” as part of “an ongoing remediation update service” to the system 100 in the form of UTMS-device **updates**); Ex. 1003 ¶ 72.

(Paper 2 at 31;
Ex. 1005 ¶ 83;
Ex. 1003 ¶ 72)

Law 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.

(Paper 16 at 2-3)

Law 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’s argument should continue to be rejected

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

(Paper 16 at 3-4; Ex. 1003 ¶ 61-64)

Law 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’s argument should continue to be rejected

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-**

(Paper 16 at 4-5; Ex. 1005 ¶ 88; Ex. 1017 ¶ 11)

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 ruleset constructing 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.*

(Paper 16 at 4-5; Ex. 1005 ¶ 88; Ex. 1017 ¶ 11)

Law 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’s argument should continue to be rejected

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 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.

(Paper 16 at 5-6; Ex. 1017 ¶ 12)

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.

(Paper 16 at 6-7; Ex. 1017 ¶ 13)

- Patent Owner’s reliance on the background of Law, describing problems in the prior art, should be rejected

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.”).

(Paper 16 at 7; Paper 12 at 13-15)

[0016] Some commercial off-the-shelf (COTS) firewall systems and other network devices are able to provide a partial solution to network security, but still must be managed outside of the operator environment. COTS firewalls are managed by IT personnel specifically trained to integrate the firewall into the needs of the process control system and configure the various rulesets as described above. Even so, COTS firewall systems have a number of disadvantages. For example, the “end of life” for the firewall is controlled by the manufacturer, not the user or by plant floor personnel, which may lead to an unexpected product replacement, lack of manufacturer support, and plant downtime. Further, IT personnel are still required to update the ruleset when new threats are discovered or upgrades to software components of the system are implemented. In a process control system, each ruleset is specific to the system it protects; changes to the system require changes to the rulesets. IT personnel, who are not typically trained to understand the process control system and its upgrades, may not understand how or why the rulesets must also be changed. If left solely as a stand-alone application managed by IT personnel, the rulesets may inadvertently provide less protection for the system than desired. For example, administration, configuration, and management of the firewall typically requires IT personnel to have detailed knowledge of the network architecture that is to be protected. IT personnel for process control networks typically need to understand the network topography, network business needs related to the network, permitted devices and services that the business requires within and between local networks, and the various external entities that should be permitted to access the local networks. Example internal entities may include mul-

(Ex. 1005 ¶ 16; Paper 16 at 7-8)

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”

- Patent Owner’s argument should continue to be rejected

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.

(Paper 2 at 36-38; Paper 16 at 9;
Ex. 1005 ¶ 92; Ex. 1003 ¶ 79)

as described above. The sources 315 may create the threat data 310 by monitoring, defining, and analyzing potential and known threats to the security of the process control network (s) 150. For example, data from the Vulnerability Research Service (VRS) of Assurent Secure Technologies, the Computer Emergency Response Team (CERT) of Carnegie Mellon University, Secunia, end user research and monitoring, and data from Achilles™ certified product users (to name but a few of the sources for firewall ruleset data) may be aggregated.

(Ex. 1005 ¶ 92; Paper 2 at 36-38)

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”

- Patent Owner’s argument should continue to be rejected

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.

(Paper 2 at 38; Paper 16 at 9-10;
Ex. 1009 at 308, 312; Ex. 1003 ¶ 80)

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”

- Patent Owner’s argument should continue to be rejected

As it did in its Preliminary Response, Patent Owner’s Response 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

(Paper 16 at 10; Ex. 1003 ¶ 92, Fig. 3)

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

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 – Law also describes the sources 315 of threat data 310 to be “sources for firewall ruleset data.” Ex. 1005 ¶ 92; Ex. 1017 ¶ 20. As the text suggests, a POSITA would have understood that “firewall ruleset data” may have included rules. Ex. 1017 ¶ 20.

(Paper 16 at 11; Ex. 1005 ¶ 92;
Ex. 1018 at 83:11-23; Ex. 1017 ¶ 20)

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”

- Patent Owner’s argument should continue to be rejected

In addition to disputing that a POSITA would have appreciated Law’s duplicate rule problem, Patent Owner also 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.

(Paper 16 at 12; Paper 12 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.

(Paper 16 at 12-14)

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”

- Patent Owner’s argument should continue to be rejected

Next, Patent Owner also 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.

(Paper 16 at 13; Paper 12 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 duplicate rules would have been more than outweighed by the tremendous performance gains achieved using Golnabi’s technique. Ex. 1017 ¶ 24.

(Paper 16 at 13-14; Ex. 1017 ¶ 24)

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”

- Patent Owner’s argument should continue to be rejected**

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.

(Paper 16 at 14; Paper 12 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) (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,

(Paper 16 at 14-15; Ex. 1017 ¶ 26)

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”

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’s Response does not appear to have included the requested briefing on the meaning of this term. Response at 28-34. Nevertheless, Patent Owner’s Response 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 Petitioner believes that Law renders obvious a rule comprising an identification of a feed under both of its obviousness theories, and Patent Owner’s concession that identification of a feed satisfies the claim scope, Petitioner submits that further briefing is not necessary to resolve the patentability issues.

(Paper 16 at 16; Paper 7 at 45; Paper 12 at 30)

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”

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:

(Paper 16 at 17; Paper 12 at 46)

	1302	1304	1305	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 1318 LOAD 1318
1320 1322 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,

(Paper 16 at 18;
Ex. 1017 ¶ 29)

(Ex. 1005 Fig. 13;
Paper 16 at 17-18)

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”

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))).

(Paper 16 at 19;
Ex. 1017 ¶ 29)

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”

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.*

(Paper 2 at 42; Paper 16 at 19-20; Ex. 1003 ¶ 87)

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”

- Patent Owner’s argument should continue to be rejected

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, I understand that 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.*

(Paper 16 at 20; Paper 12 at 29)

(Paper 16 at 20-21; Ex. 1017 ¶ 32; Ex. 1018 at 84:21-24)

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 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.

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”

- Patent Owner’s argument should continue to be rejected

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.

(Paper 16 at 21-22; Ex. 1017 ¶ 34;
Ex. 1005 ¶ 92)

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”

- Patent Owner’s argument should continue to be rejected

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.

(Paper 16 at 22-23; Ex. 1017 ¶ 36; Ex. 1005 ¶ 92, Fig. 3)