

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KEYSIGHT TECHNOLOGIES, INC. and
PALO ALTO NETWORKS, INC.
Petitioner,

v.

CENTRIPETAL NETWORKS, INC.,
Patent Owner.

IPR2023-00445⁴
Patent 10,785,266 B2

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:

- All challenged claims -- claims 1-27 -- obvious over Law

of the challenged claims of the '266 Patent. Accordingly, we institute an *inter partes* review of claims 1–27 of the '266 Patent on the grounds of unpatentability raised in the Petition.

(Paper 10 at 2)

Having determined that Petitioner has demonstrated a reasonable likelihood of prevailing on the basis of the first ground applying Law alone, applicable to all challenged claims, we do not explicitly address the patentability challenges on the basis of the remaining grounds. We also note

(Paper 10 at 26)

Grounds for Institution and Disputes

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

- Rejected Patent Owner's argument that Law fails to teach or suggest that its firewalls 146a and 146b collectively provide an interface across a boundary of the protected network 150 (Paper 10 at 20-21)
 - Rejected Patent Owner's argument that Law does not teach or suggest that network access device 149c joins LANs 150a and 150b into a single network (Paper 10 at 21)
 - Institution Decision found that one of ordinary skill in the art would have regarded the paired LANs of Law as viewable as a single network, when compared to the Internet, and each firewall would provide protections to the single network. (Paper 10 at 20)
 - Institution Decision found that all network traffic between joined LANs 150a and 150b and the Internet must pass through either firewall 146a or 146b, and that Law's disclosure of an alternative "bypass" embodiments confirms that ordinarily skilled artisans would have viewed firewalls 146a and 146b as providing the entire interface across the boundary of the network. (Paper 10 at 20)
- Rejected Patent Owner's argument that Law's firewalls 146a and 146b would have necessarily applied different rulesets (Paper 10 at 22-23)
 - Institution Decision found that persons of ordinary skill in the art would have understood that perimeter UTMS firewalls 146a and 146b would have applied ruleset 147 to all network traffic passing therethrough. (Paper 10 at 23)

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 (Paper 10 at 24-25)
 - Rejected Patent Owner's argument that rules within the rulesets distributed by firm 305 are not automatically created or altered because IT personnel would still be required to update rulesets when new threats are detected. (Paper 10 at 24-25)
- Rejected Patent Owner's argument that receiving an updated set of rules from Law's firm 305 following an initial operator-created ruleset would not satisfy receiving the claimed "first set of packet filtering rules" (Paper 10 at 25)
 - Rejected Patent Owner's implicit claim construction. I.D. at 25 ("We do not agree with Patent Owner's arguments. We are not persuaded that the received packet filtering rules (limitation [1.1]) need be the first set of rules to be applied or modified by the PSGs."). (Paper 10 at 25)

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 “a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected” in view of Patent Owner's contention that a POSITA would not have understood Law's sub-networks 150a and 150b to have been combinable as a single network 150 (Paper 17 at 17-27; Paper 7 at 29-36)
- Repeats the argument that Law does not disclose or render obvious applying “a first set of filtering rules” to “all network traversing the boundary” in view of Patent Owner's contention that the ruleset 147 applied by Law's firewall 146a and would have been different than the ruleset 147 applied by Law's firewall 146b (Paper 17 at 27-33; Paper 7 at 36-38)
- 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 17 at 33-42; Paper 7 at 45-51)
- Repeats the argument that Law does not disclose or render obvious “receiving ... a dynamic security policy comprising a first set of packet filtering rules” in view of assertion that Law does not disclose receiving an initial ruleset and instead purportedly requires an operator to configure the initial ruleset (Paper 17 at 42-53; Paper 7 at 39-45)

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; Paper 10 at 16)

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; Paper 10 at 18)

- 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; Paper 10 at 18)

network management and maintenance. The process control system 100 may include one or more sub-systems 105a, 105b one or more process control networks 150a, 150b and one or more process controllers 110 communicatively connected to one or more host workstations or computers 120-122 (which may be any type of personal computers, workstations, etc.), at least one having a display screen, via one or more network devices 146 over a process control network 150. While the

(Ex. 1005 ¶ 53; Paper 2 at 13-14)

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; Paper 10 at 18)

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; Paper 10 at 18)

[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; Paper 10 at 18)

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 13; Paper 10 at 18)

Overview of asserted prior art - Law

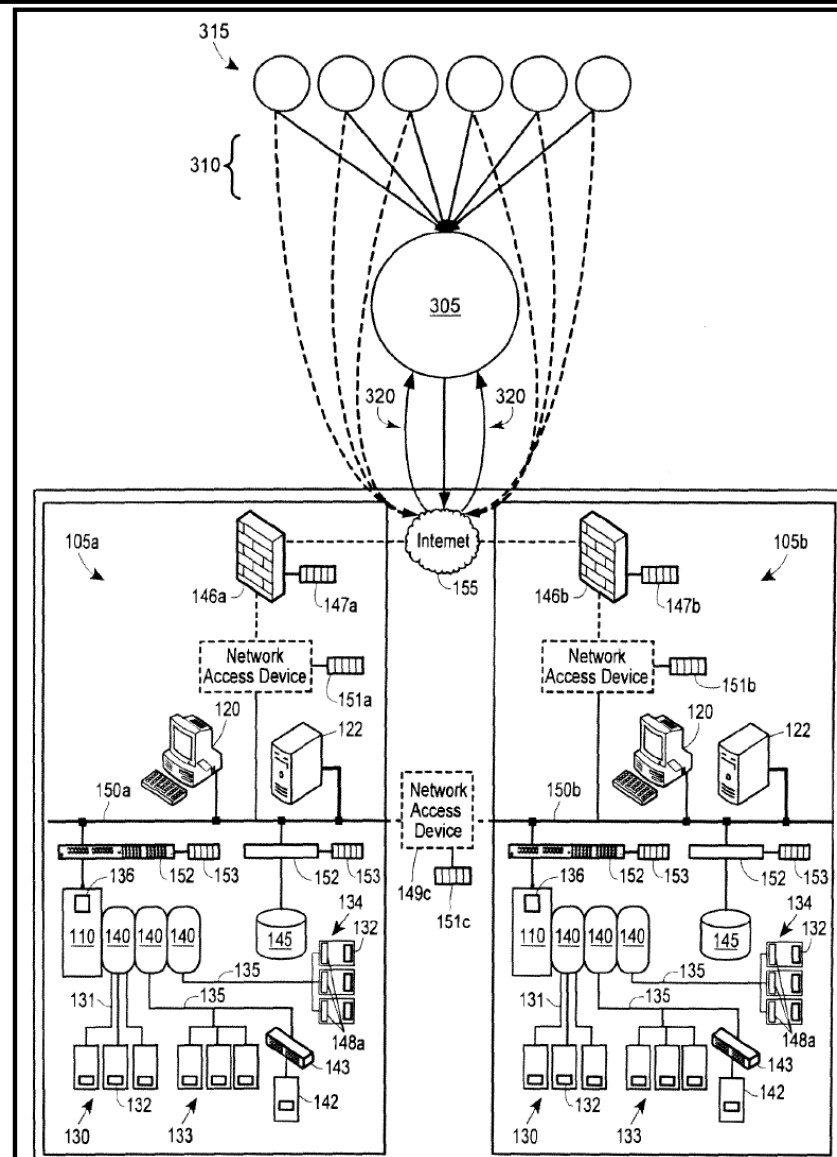


Fig. 3

(Ex. 1005 Fig. 3; Paper 2 at 12;
Paper 10 at 17)

Law renders obvious “a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected”

- Fig. 3 shows that network access device 149c may optionally be provided to join LANs 150a and 150b together into a single network 150:

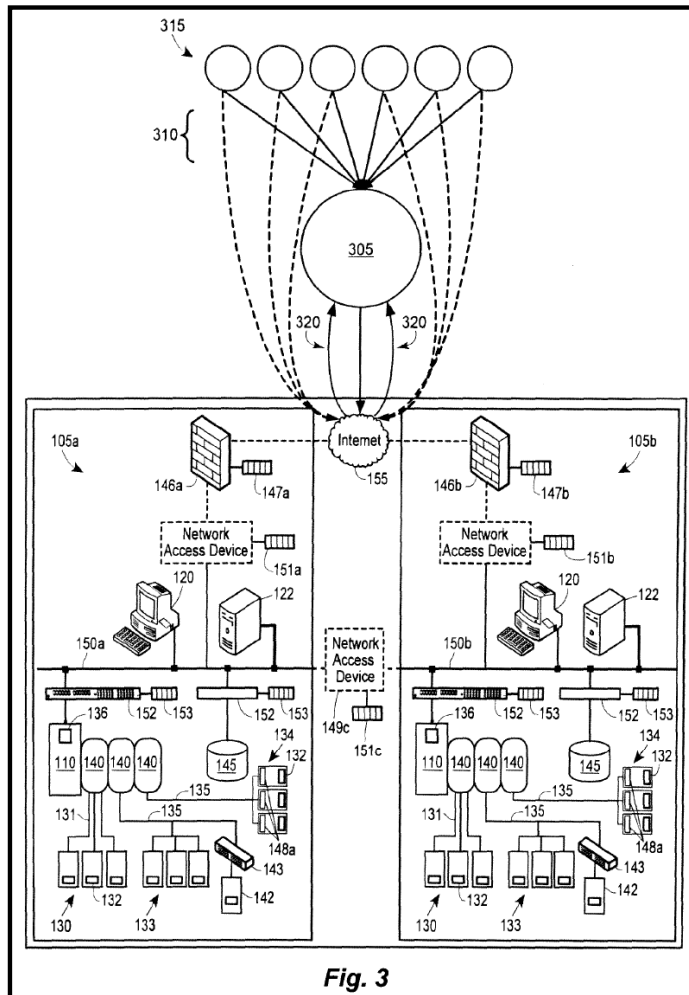


Fig. 3

149c joining LANs 150a and 150b); Ex. 1003 ¶ 64. Likewise, Law explains that network access device 149c can be used to join LANs 150a and 150b, which are part of subsystems 105a and 105b, respectively. Ex. 1005 ¶ 51 (describing an “alternative embodiment” that “include[s] a UTMS-configured network access device 149c that may or may not include a ruleset such as ruleset 151c” and that provides “a cross-system connection between the sub-systems 105a and 105b”); *see also id.* ¶ 55 (referring to a single “network 150” rather than separately specifying subnetworks 150a and 150b); Ex. 1003 ¶ 64. Furthermore, and consistent with Fig. 1A, Fig. 3 confirms that Law’s perimeter UTMS firewalls 146a and 146b collectively provide the entire interface across the boundary of the network protected by firewalls 146a and 146b (the network 150 formed by joining LANs 150a and 150b) and the Internet 155, as all network traffic between joined LANs 150a and 150b and the Internet must pass through either firewall 146a or 146b. Ex. 1003 ¶ 64.

(Paper 2 at 21; Ex. 1003 ¶ 64)

(Paper 2 at 19-21; Paper 21 at 4-5; Ex. 1003 ¶ 64)

Law renders obvious “a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected”

- Law’s disclosure of an alternative “bypass” embodiment further confirms that the non-bypass embodiments, such as illustrated in Fig. 3 necessarily provide the entire interface across the boundary of the network protected by firewalls 146a and 146b.

Furthermore, Law’s express disclosure of an alternative “bypass” embodiment further confirms that the non-bypass embodiments, such as those illustrated in Figs. 1A and 3 (which include perimeter UTMS firewalls 146a and 146b), necessarily provide the entire interface across the boundary of the network protected by firewalls 146a and 146b. Ex. 1003 ¶ 65. In particular, Law discloses

an “**alternative[]**” bypass embodiment that “**may** be implemented to provide a software method that selectively activates and deactivates communication between any of the process control system 100 entities.” Ex. 1005 ¶ 93. For example, Law explains that Figs. 4-12 disclose a bypass embodiment for that “**may** provide an operator a solution **for bypass control** to selectively turn off and turn on network connections to entities that are internal or external to the process control network **to re-route network traffic around a disabled, malfunctioning, or rigidly-configured network device.**” *Id.* Moreover, in addition to using different figures to describe the bypass embodiment (i.e., Figs. 4-12), in order to avoid any confusion between the perimeter UTMS firewalls 146a and 146b, such as those shown in Figs. 1A and 3—which do not support bypass functionality—and UTMS-configured devices that do support bypass functionality, Law uses a different numerical identifier (800) when referring to UTMS-configured devices that do support bypass functionality. *Id.* ¶ 102 (distinguishing “perimeter UTMS-configured devices 146” with “bypass UTMS-configured network access devices 800”). Accordingly, a POSITA would have understood that Law’s express

subnetworks 150a and 150b. Pet. 21 (citing Ex. 1005 ¶ 55). We also agree with Petitioner that all network traffic between joined LANs 150a and 150b and the Internet must pass through either firewall 146a or 146b, and that Law’s disclosure of an alternative “bypass” embodiments confirms that ordinarily skilled artisans would have viewed firewalls 146a and 146b as providing the entire interface across the boundary of the network. *Id.* (citing Ex. 1003 ¶¶ 64–65).

(Paper 10 at 21)

(Paper 2 at 21-22;
Ex. 1003 ¶ 65)

Law renders obvious “a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected”

- Patent Owner disputes that a POSITA would have understood that Law’s sub-networks 150a and 150b may be joined as a single network protected by firewalls 146a and 146b

Patent Owner disputes that a POSITA would have understood that Law’s sub-networks 150a and 150b may be joined as a single network protected by firewalls 146a and 146b. Response at 18. For example, Patent Owner argues that “Law never uses the term ‘network 150’ to refer to any combination of networks 150a and 150b” and instead “only uses that term when there is only one relevant network and/or it is not necessary to distinguish between networks 150a and 150b.” Response at 18. In addition, Patent Owner argues that “[w]hen discussing both process control networks, Law refers to ‘one or more process control networks 150a, 150b,’” and “[w]hen it is not necessary to differentiate between the two networks, Law refers to ‘a process control network 150.’” Response at 20-21. Lastly, Patent Owner argues that network access device 149c supports Patent Owner’s theory that sub-networks 150a and 150b may not be joined into a single network. Response at 25 n. 4 (arguing that “network access device 149c is a perimeter device that allows for communications between networks” and “appl[ies] ruleset 151c.”).

(Paper 17 at 18; Paper 21 at 3)

Law renders obvious “a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected”

- Patent Owner’s assertion that Law never uses the term network 150 to refer to any combination of networks 150a and 150b and instead only uses that term when there is only one relevant network and/or it is not necessary to distinguish between networks 150a and 150b is incorrect

Patent Owner’s contention that Law never uses the term network 150 to refer to any combination of networks 150a and 150b and instead only uses that term when there is only one relevant network and/or it is not necessary to distinguish between networks 150a and 150b is demonstrably wrong. Ex. 1014 ¶ 10. For example, in paragraph 53, Law states that “[t]he process control system 100 may include one or more sub-systems 105a, 105b one or more process control networks 150a, 150b and one or more process controllers 110 communicatively connected to one or more host workstations or computers 120-122 ... over a process control network 150.” Ex. 1005 ¶ 53. Here, Law uses the terms “networks 150a and 150b” and “network 150” in the same sentence, and the context makes clear that “network 150” refers to the single network formed from the combination of sub-networks 150a and 150b. Ex. 1014 ¶ 10.

(Paper 21 at 6-7)

network management and maintenance. The process control system 100 may include one or more sub-systems 105a, 105b one or more process control networks 150a, 150b and one or more process controllers 110 communicatively connected to one or more host workstations or computers 120-122 (which may be any type of personal computers, workstations, etc.), at least one having a display screen, via one or more network devices 146 over a process control network 150. While the

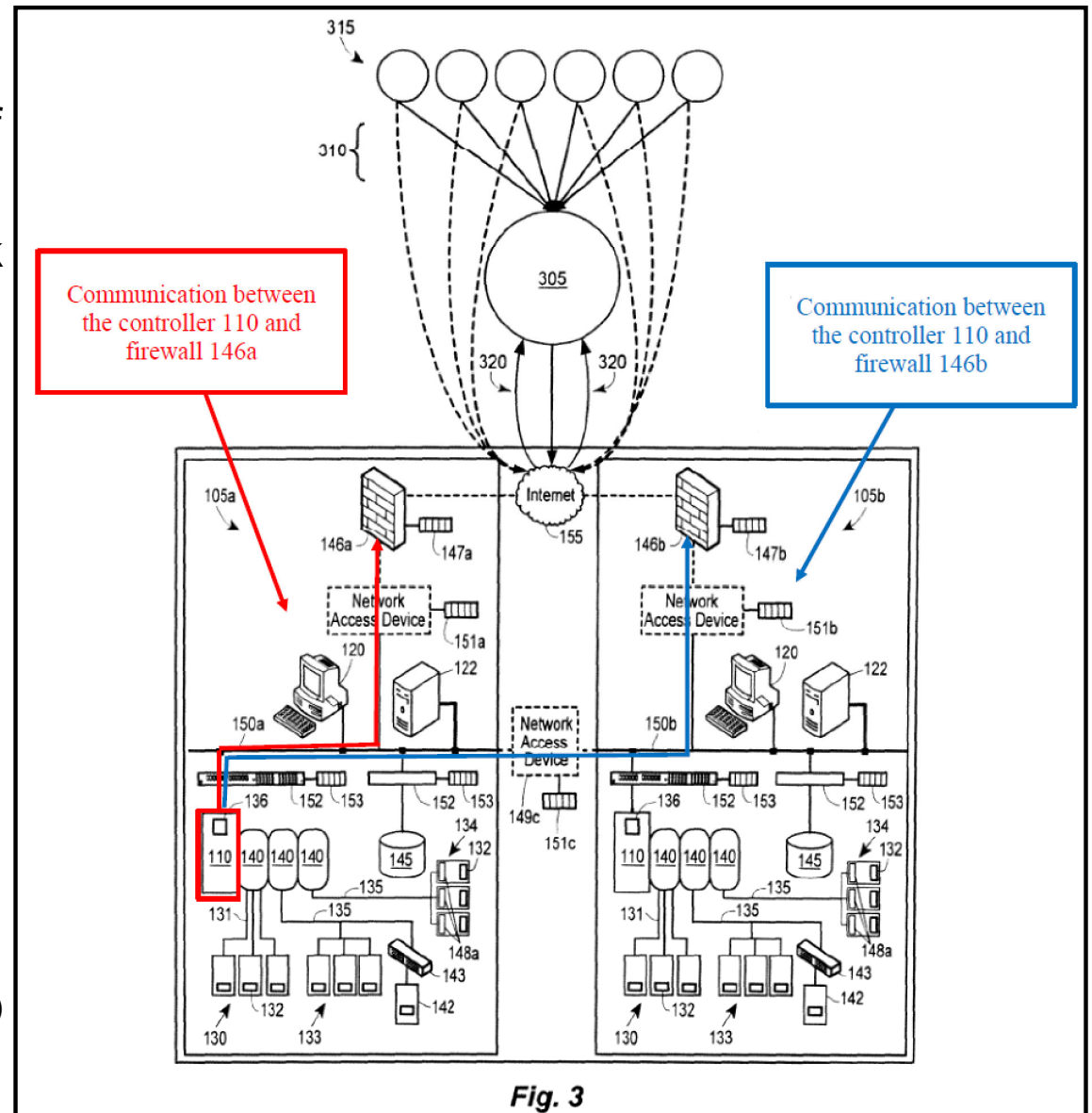
(Ex. 1005 ¶ 53; Paper 21 at 6-7)

Law renders obvious “a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected”

- Patent Owner’s assertion that Law never uses the term network 150 to refer to any combination of networks 150a and 150b and instead only uses that term when there is only one relevant network and/or it is not necessary to distinguish between networks 150a and 150b is incorrect

[0057] The controller 110, which may be one of many distributed controllers within the plant having one or more processors therein, implements or oversees one or more process control routines or modules 136. The routines may include one or more control loops that are stored in or associated with the controller. The controller 110 also communicates with the field devices 130, 133, 134, 142 the host computers 120-122, firewall(s) 146a, 146b and the data historian(s) 145 through the network 150 and other network devices to control a process in any desired manner. It should be noted that any control modules or routines 136 or elements described herein may have parts thereof implemented or executed by different controllers or other devices if so desired.

(Ex. 1005 ¶ 57; Paper 21 at 7-9)



(Fig. 3 (annotated); Paper 21 at 7-9; Ex. 1014 ¶ 11)

Law renders obvious “a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected”

- The network access device 149c does not support Patent Owner’s assertion that a POSITA would not consider sub-networks 150a and 150b to be joined into a single network

Patent Owner also is wrong on its argument that embodiments of Law in which network access device 149c is described as a “perimeter device” that “appl[ies] ruleset 151c” supports its theory that a POSITA would not consider sub-networks 150a and 150b to be joined into a single network. Response at 25 n. 4. As explained by the Petition, Fig. 3 of Law shows that network access device 149c directly connects sub-networks 150a and 150b to provide communications between them. Pet. at 20-21; Ex. 1003 ¶ 64; *see also* Ex. 1005 ¶ 51 (describing that “UTMS-configured network access device 149c” provides “a cross-system connection between the sub-systems 105a and 105b”).

(Paper 21 at 9; Ex. 1005 ¶ 51)

threats. FIG. 1b is an alternative embodiment illustrating a cross-system connection between the sub-systems 105a and 105b including a UTMS-configured network access device 149c that may or may not include a ruleset such as ruleset 151c as herein described and may control different types of process control network connections as described below.

(Ex. 1005 ¶ 51; Paper 21 at 9-10)

Lastly, Fig. 3 shows that network access device 149c provides a direct connection, without traversing the Internet or other network, joining together sub-networks 150a and 150b. Ex. 1014 ¶ 13. Patent Owner’s own expert, Dr. Goodrich, agreed. Ex. 1015 at 48:8-49:10. Accordingly, a POSITA would have understood that the network access device 149c shown in Fig. 3 is not a perimeter device but rather a device that is internal to network 150. Ex. 1014 ¶ 13. This is further confirmed by Law’s explicit teaching that network access device 149c can join sub-networks 150a and 150b without implementing any ruleset, including ruleset

151c. Ex. 1005 ¶ 51 (“UTMS-configured network access device 149c [] may *or may not* include a ruleset such as ruleset 151c.”) (emphasis added); Ex. 1014 ¶¶ 14-15.

(Paper 21 at 9-10; Ex. 1014 ¶ 13)

Law renders obvious “a first set of packet filtering rules to be applied to all network traffic traversing the boundary”

- A POSITA would have understood that firewalls 146a and 147b may apply the same ruleset 147

305 necessarily comprises a server. Ex. 1003 ¶ 71. In addition, although Fig. 3 identifies ruleset 147a corresponding to firewall 146a and ruleset 147b corresponding to firewall 146b, a POSITA would have understood that firewalls 146a and 146b may apply the same ruleset, which Law also identifies as “ruleset 147.” Ex. 1005 ¶ 88; Ex. 1003 ¶ 71.

(Paper 2 at 27; Ex. 1003 ¶ 71)

1005 ¶ 22. Law explains that the service that supplies and distributes the rulesets over the Internet to firewalls 146a and 146b, including rulesets 147, is a “third party source” that Law refers to as “cyber security risk management firm 305.” *Id.* ¶ 66 (“The UTMS-configured device or entity may receive the ruleset data ... 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 ... an Internet connection”); *id.* ¶ 88 (“With reference to FIG. 3, a third party, cyber security risk management firm 305 such as Wurldtech 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”).

(Paper 2 at 24; Ex. 1005 ¶¶ 66, 88)

Id. ¶ 77. As explained above with respect to element [1.0], the perimeter UTMS firewalls 146a and 146b provide the entire interface across the boundary of the network protected by firewalls 146a and 146b (i.e., the boundary between the protected network 150 and the Internet 155). Ex. 1003 ¶ 77. A POSITA would have understood that perimeter UTMS firewalls 146a and 146b would have applied ruleset 147 to all network traffic passing therethrough. *Id.* ¶ 77. For example, Law discloses that “[w]here the UTMS-configured device is a perimeter device,” such as perimeter UTMS firewalls 146a and 146b, “the rulesets 147 and 151 may include a global set of rules for access to any device within the subsystems 105a, 105b.” Ex. 1005 ¶ 51; *id.* ¶ 59 (“The UTMS-configured firewalls 146 ... and

(Paper 2 at 30; Ex. 1003 ¶ 77; Ex. 1005 ¶¶ 51, 59)

subsystems 105a, 105b.” Pet. 30 (quoting Ex. 1005 ¶ 51). Based on this, we agree with Petitioner that persons of ordinary skill in the art would have understood that perimeter UTMS firewalls 146a and 146b would have applied ruleset 147 to all network traffic passing therethrough. *Id.* (citing Ex. 1003 ¶ 77). Additionally, if ordinarily skilled artisans would have viewed subsystems 105a, 105b as a single network, per Petitioner’s assertions, they also would have been motivated to have Law’s firewalls protect against threats common thereto, and would have applied, at least partially, a common ruleset to both firewalls.

(Paper 10 at 23)

Law renders obvious “a first set of packet filtering rules to be applied to all network traffic traversing the boundary”

- Patent Owner still disputes that it would have been obvious that the ruleset 147 distributed to firewalls 146a and 146b could be the same ruleset

Patent Owner argues that Law does not disclose or render obvious that the ruleset 147 distributed to firewalls 146a and 146b could be the same ruleset. Response at 27-33. In particular, Patent Owner contends that Law’s “global” ruleset is not one that is applied to all traffic traversing the boundaries of a protected network, but rather, firewall 146a would apply one set of global rules for access to devices in subsystem 105a, and firewall 146b would apply a different set of global rules for access to devices in subsystem 105b. Response at 28. Furthermore, Patent Owner contends that because each of these global rulesets is unique to the particular devices in the subsystem, the “global” ruleset for subsystem 105a would be different from the “global” ruleset for subsystem 105b. *Id.*

(Paper 21 at 10; Paper 17 at 27-33)

Law renders obvious “a first set of packet filtering rules to be applied to all network traffic traversing the boundary”

- Patent Owner’s argument should continue to be rejected for several reasons

First, Patent Owner’s suggestion that ruleset 147a implemented by firewall 146a is necessarily different than the ruleset 147b implemented by firewall 146b is unsupported by Law and contrary to Law’s description of the ruleset implemented by both firewalls as “ruleset[] 147.” Ex. 1014 ¶ 21; Ex. 1005 ¶¶ 51, 88.

(Paper 21 at 11; Ex. 1014 ¶ 21; Ex. 1005 ¶¶ 51, 88)

Third, Patent Owner’s argument that the global ruleset is unique to the particular devices protected by the ruleset does not suggest that the ruleset for subsystem 105a would have been different than the ruleset for subsystem 105b. Ex. 1014 ¶ 23. Rather, a POSITA would have understood that the single global ruleset applied by both firewalls would have been tailored to protect all of the devices in both subsystems 105a and 105b. *Id.*; Ex. 1005 ¶ 51.

(Paper 21 at 11-12; Ex. 1014 ¶ 23; Ex. 1005 ¶ 51)

Second, Patent Owner misinterprets Law’s disclosure that “[w]here the UTMS-configured device is a perimeter device,” such as perimeter UTMS firewalls 146a and 146b, “the rulesets 147 and 151 may include a global set of rules for access to any device within the subsystems 105a, 105b.” Ex. 1005 ¶ 51 (emphasis added). In contrast to suggesting separate “global” rules for subsystems 105a and 105b, Law discloses a single set of global rules for both subsystems. Ex. 1014 ¶ 22. Patent Owner’s suggestion of a separate set of rules for subsystems 105a and 105b is further contradicted by Law’s disclosure that network access device 149c may provide cross-communication between subsystems 105a and 105b without implementing any rulesets. Ex. 1005 ¶ 51. Because Law permits cross-communication between subsystems 105a and 105b without implementing any rulesets, a POSITA would have understood that the ruleset 147 implemented by firewalls 146a and 146b would have needed to protect all of the devices in both subsystems. Ex. 1014 ¶ 22.

(Paper 21 at 11; Ex. 1014 ¶ 22; Ex. 1005 ¶ 51)

Law renders obvious “a first set of packet filtering rules to be applied to all network traffic traversing the boundary”

- Patent Owner’s argument should continue to be rejected for several reasons

Fourth, even if one were to incorrectly assume, as Patent Owner contends, that ruleset 147a is tailored only to the devices in subsystem 105a and that ruleset 147b is tailored only to the devices in subsystem 105b, it still would not follow that ruleset 147a would necessarily be different than ruleset 147b. Ex. 1014 ¶ 24. In particular, a POSITA would have understood that the devices in subsystem 105a may have been identical to the devices in subsystem 105b. *Id.* For example, Fig. 3 of Law illustrates subsystem 105a as including the same devices, arranged in the same configuration, as subsystem 105b. *Id.*

(Paper 21 at 12; Ex. 1014 ¶ 24; Ex. 1005 Fig. 3)

Fifth, to the extent Patent Owner’s argument that firewall 146a would implement a different ruleset than firewall 146b is predicated on Patent Owner’s argument that subnetworks 150a and 150b are not joined together as a single network, for the reasons explained above in II.A, Patent Owner is wrong.

(Paper 21 at 12)

Lastly, Patent Owner appears to argue that network access device 149c’s implementation of ruleset 151c suggests that firewall 146a would implement a different ruleset than firewall 146b. Response at 31-33. Patent Owner is wrong. This argument is based on the mistaken belief that network access device 149c necessarily implements ruleset 151c, which, as explained above, directly contradicts Law’s teachings. Ex. 1005 ¶ 51 (“UTMS-configured network access device 149c [] may *or may not* include a ruleset such as ruleset 151c.”) (emphasis added).

(Paper 21 at 12-13; Ex. 1005 ¶ 51)

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 ¶ 71. In addition, although Fig. 3

(Paper 2 at 27; Ex. 1005 ¶ 88)

(Paper 2 at 36-37;
Ex. 1005 ¶ 88;
Ex. 1003 ¶ 88)

Law further discloses rules that were automatically created by the security policy management server, which, as explained above in [1.1], corresponds to 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 ¶ 88.

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 ¶ 89. 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 ¶ 89.

(Paper 2 at 38; Ex. 1005 ¶¶ 21, 88; Ex. 1003 ¶ 89)

update to that initial ruleset, received from firm 305. We are persuaded by Petitioner that Law expressly discloses automatically updating (i.e., altering) rulesets in response to detected conditions, and that those updated rulesets would have been distributed for use. See Pet. 36–39 (citing Ex. 1005 ¶¶ 21, 83, 88–89).

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 ¶ 90.

(Paper 2 at 38-39;
Ex. 1005 ¶ 83;
Ex. 1003 ¶ 90)

(Paper 10 at 25)

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 33-42. 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 33-34. Likewise, Patent Owner contends that “IT personnel ... are still required to manually update the rulesets of process control systems.” Response at 34.

(Paper 21 at 13; Paper 17 at 33-34)

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 34. 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 23-27; Ex. 1003 ¶¶ 69-71. 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 21 at 14; Paper 2 at 23-27; Ex. 1003 ¶¶ 69-71)

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-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 37 (citing Ex. 1005 ¶ 88 (emphasis

(Paper 21 at 15; Ex. 1005 ¶ 88)

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 ¶ 88; Ex. 1014 ¶ 33. 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 21 at 16; Ex. 1005 ¶ 88; Ex. 1014 ¶ 33)

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. 1014 ¶ 34. 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, 8, 15, and 23; Ex. 1009 at elements [1.3], [8.5], [15.3], and [21.3]. 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. 1015 at 75:14-76:16.

(Paper 21 at 16; Ex. 1014 ¶ 34)

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 38 (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 38; Ex. 1003 ¶ 89. Patent Owner’s allegation that firm 305 employs IT personnel does not

(Paper 21 at 16-17; Ex. 1014 ¶ 35)

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 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 35 (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 37 (arguing that firm 305’s disclosure of continuously identifying network vulnerabilities and updating rulesets does not mean that it does so automatically because “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 41 (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 21 at 17-18; Paper 17 at 35, 37)

[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 21 at 18-19)

- Patent Owner’s argument should continue to be rejected

Patent Owner has argued that “the term ‘receiving, by the packet security gateway and from a security policy management server . . . a dynamic security policy comprising a first set of packet filtering rules’ ... means an initial dynamic security policy, including a first set of rules, that is received by the PSG from the SPMS.” Response at 8. Based on this proposed construction, Patent Owner has

argued that Law requires that “operators within the process control system create initial rulesets (ruleset 147),” not firm 305. Response at 47. Patent Owner is wrong on both accounts.

(Paper 21 at 19-20)

Law discloses or renders obvious “receiving ... from a security policy management server ... a dynamic policy comprising a first set of packet filtering rules”

- The claimed “first set of packet filtering rules” is not limited to a first set of rules in an initial dynamic security policy

The Institution Decision rejected Patent Owner’s implicit construction that “first set of packet filtering rules” be limited to an initial dynamic security policy. I.D. at 25 (“We do not agree with Patent Owner’s arguments. We are not persuaded that the received packet filtering rules (limitation [1.1]) need be the first set of rules to be applied or modified by the PSGs.”).

(Paper 21 at 20; Paper 10 at 25)

The Board should continue to reject Patent Owner’s claim construction position. In particular, Patent Owner’s proposed construction seeks to deviate from the plain and ordinary meaning of the claim terms by adding in a limitation that the “first set of packet filtering rules” be limited to an initial dynamic security policy. **Such an added limitation does not find support in the claim language.** For example, limitation [1.1] recites “receiving ... a dynamic security policy comprising a **first set of packet filtering rules**,” without any restriction that the “first set of packet filtering rules” be limited to an initial dynamic security policy, and limitation [1.5] recites “receiving ... an updated **second set of packet filtering rules** for the dynamic security policy” Ex. 1009 at [1.1], [1.5] (emphasis added).

(Paper 21 at 20)

(Paper 21 at 21-22)

Patent Owner’s attempt to import undue meaning into the word “first” has been rejected by numerous courts. **Contrary to Patent Owner’s argument, “[t]he use of the terms ‘first’ and ‘second’ is a common patent-law convention to distinguish between repeated instances of an element or limitation.”** *3M Innovative Props. Co. v. Avery Dennison Corp.*, 350 F.3d 1365, 1371 (Fed. Cir. 2003). Likewise, the use of the terms “first” and “second” in the ’266 claims utilizes this common patent-law convention to distinguish between repeated instances of “set[s] of packet filtering rules.” *See id.* Accordingly, the Board should reject Patent Owner’s attempt to construe “first set of packet filtering rules” as limited to an initial dynamic security policy. *See NNPT LLC v. Huawei Inv. & Holding Co.*, No. 2:14-CV-677-JRG-RSP, 2015 U.S. Dist. LEXIS 107584, *20-26 (E.D. Tex. Aug. 17, 2015) (“**Defendants have not adequately justified introducing an ‘initial’ or ‘first in time’ limitation,** particularly as to Claim 10 of the ’325 Patent, which recites only a ‘first indication’ and not any other indication.”) (citing *3M Innovative*, 350 F.3d at 1371); *Apple Inc. v. INVT SPE LLC*, IPR2018-01475, Paper 28, 2020 Pat. App. LEXIS 12868, *9-10 (PTAB Mar. 25, 2020) (“[W]e are not persuaded by Patent Owner’s contention that the broadest reasonable claim construction for ‘first information sequence’ should be ‘important information.’ ... [T]he claims are not specific as to what ‘first information’ is other than ‘**first**’ is merely used to ‘differentiate’ it from ‘second’ information, ‘a very common thing when it comes to patent claim drafting.’”) (citing *3M Innovative*, 350 F.3d at 1371).

Law discloses or renders obvious “receiving ... from a security policy management server ... a dynamic policy comprising a first set of packet filtering rules”

construction is adopted. Response at 42-53. But even if Patent Owner’s construction were to be adopted, Law renders obvious “receiving ... a first set of packet filtering rules,” including an initial dynamic security policy.

Patent Owner argues that Law requires that operators within the process control system create initial rulesets (ruleset 147), not firm 305. Response at 47. Patent Owner is wrong.

As set forth in the Petition, Law consistently describes the rulesets 147 as being constructed and distributed by the firm 305. Pet. at 23-24, 49-51; Ex. 1005 ¶¶ 22, 66, 88. In particular, Law discloses that “[t]he UTMS firewalls and devices may communicate with a **perpetual service** that proactively supplies the UTMS-configured firewalls ... with rulesets to meet the latest security threats, threat patterns, and control system vulnerabilities found to exist within the network.” Ex. 1005 ¶ 22. Law explains that the service that supplies and distributes the rulesets over the Internet to firewalls 146a and 146b, including rulesets 147, is a “third

(Paper 21 at 22)

party source” that Law refers to as “cyber security risk management firm 305.” *Id.* ¶ 66 (“The UTMS-configured device or entity **may receive the ruleset data** ... 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 ... an Internet connection”); *id.* ¶ 88 (“With reference to FIG. 3, **a third party, cyber security risk management firm 305** such as Wurldtech 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**”).

Patent Owner argues that Law discloses that “the rulesets 148, 147, 151, 153 may be configurable by an operator or other personnel from a graphic display 129 at a workstation 120.” Response at 44 (citing Ex. 1005 ¶ 90). While Law discloses an embodiment in which the rulesets may be configurable by an operator, this embodiment does not suggest that the rulesets that the operator may configure are necessarily created by an operator, rather than received by firm 305. Ex. 1014 ¶ 43.

(Paper 21 at 23; Ex. 1014 ¶ 43)