

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KEYSIGHT TECHNOLOGIES, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, INC.,
Patent Owner.

IPR2023-00445

Patent 10,785,266 B2

REPLY DECLARATION OF DOUG W. JACOBSON, PH.D

TABLE OF CONTENTS

I.	Introduction.....	3
II.	Response to Centripetal’s and Dr. Goodrich’s Unpatentability Analysis	4
A.	Law discloses or renders obvious “a packet security gateway, of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway and one or more networks other than the network protected by the packet security gateway”	4
B.	Law discloses or renders obvious “a first set of packet filtering rules to be applied to all network traffic traversing the boundary”	12
C.	Law discloses or renders obvious “one or more first packet filtering rules of the first set of packet filtering rules ... were automatically created or altered by the security policy management server”	16
D.	Law discloses or renders obvious “receiving, by the packet security gateway and from a security policy management server external from the network protected by the packet security gateway, a dynamic security policy comprising a first set of packet filtering rules”	24
III.	Conclusion	27

I, Dr. Doug W. Jacobson, declare as follows:

I. INTRODUCTION

1. I previously submitted a Declaration (Ex. 1003) in this proceeding (IPR2023-00445) that set forth my opinions regarding U.S. Patent No. 10,785,266 B2 (“266 Patent,” Ex. 1001).

2. I submit this Reply Declaration to respond to Patent Owner’s Response and the Declaration of Dr. Goodrich submitted with Patent Owner’s Response (Ex. 2012).

3. In preparing this Reply Declaration, in addition to the materials identified in my first declaration (Ex. 1003), I have considered:

- The Board’s Institution Decision (Paper 10)
- Patent Owner’s Response (Paper 17) (“Response”)
- Declaration of Dr. Goodrich (Ex. 2012)
- Deposition Transcript of Dr. Goodrich (Ex. 1015)
- The exhibits submitted by Patent Owner (*see* Ex. 2001-2015, 2017); and
- Any other document referenced herein.

4. My qualifications can be found in my first Declaration (Ex. 1003 ¶¶ 4-15) and in my CV, Ex. 1004. The discussion of the level of ordinary skill in the art and relevant legal standards are also the same as my first Declaration. In forming

the opinions expressed below, I have considered the documents list above (and any additional documents discussed below) along with my own knowledge and experience based upon my work in the field of network security systems.

II. RESPONSE TO CENTRIPETAL’S AND DR. GOODRICH’S UNPATENTABILITY ANALYSIS

A. Law discloses or renders obvious “a packet security gateway, of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway and one or more networks other than the network protected by the packet security gateway”

5. I understand that elements [1.0], [8.0], and [15.0] of the ’266 patent recite, among other things: “a packet security gateway, of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway and one or more networks other than the network protected by the packet security gateway.”

6. In my first Declaration, I explained how Law discloses or renders obvious this claim language. *See* Ex. 1003 ¶¶ 59-67.

7. I understand that 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, I understand that 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, I understand that 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, I understand that Patent Owner argues that network access device 149c being used to join sub-networks 150a and 150b 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.”).

8. I disagree. None of Patent Owner’s arguments changes my opinion that Law explicitly discloses, and at the very least renders obvious, that one of ordinary skill in the art would understand that LANs 150a and 150b are joined together to form a single network 150 protected by perimeter UTMS firewalls 146a and 146b, as shown in Fig. 3.

9. As I explained in my first Declaration, Fig. 3 of Law shows an embodiment in which LANs 150a and 150b are optionally joined together to form a single network protected by perimeter UTMS firewalls 146a and 146b. Ex. 1003

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

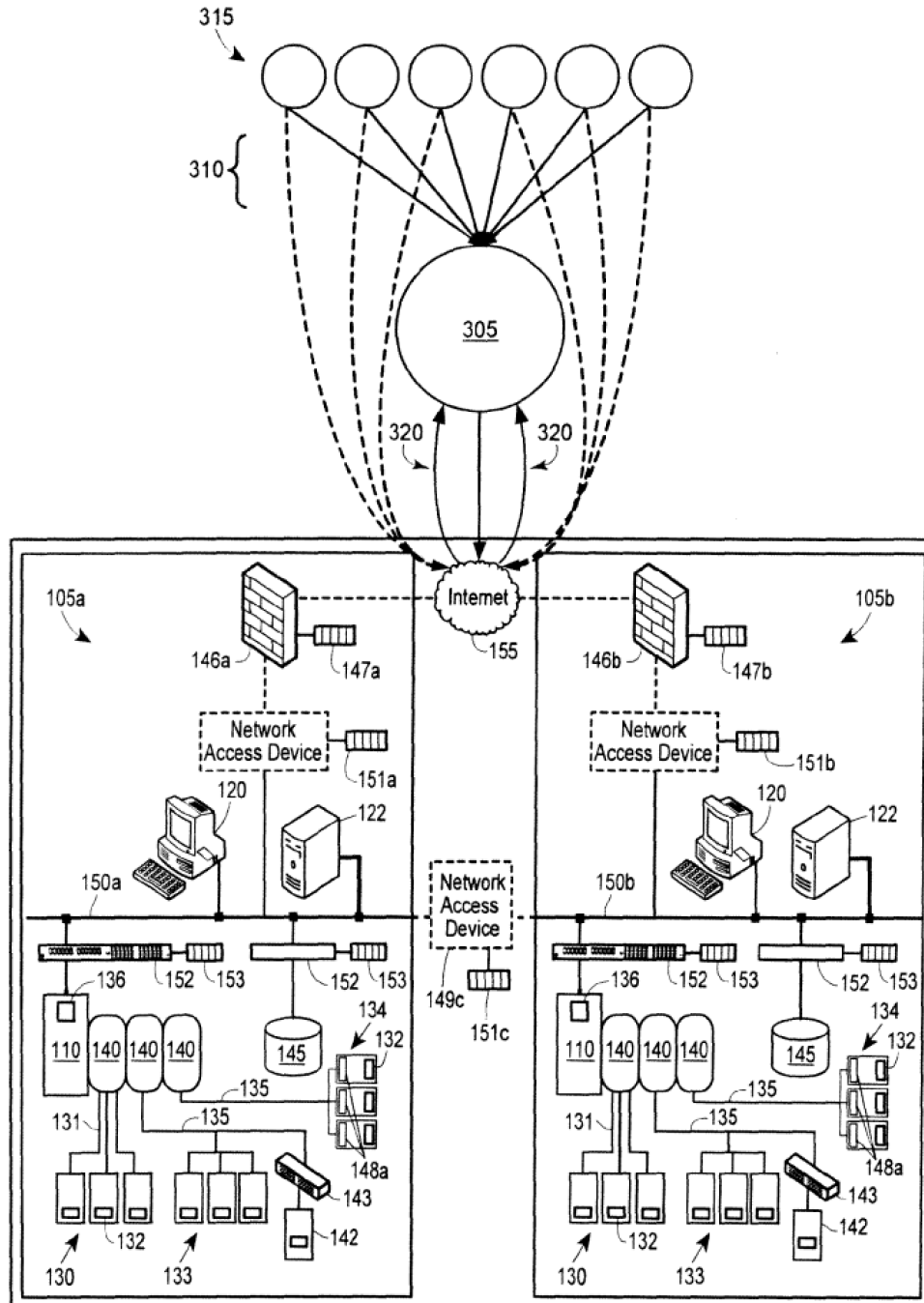


Fig. 3

Ex. 1005, Fig. 3; *see also id.*, Fig. 1B (similarly illustrating network access device 149c joining LANs 150a and 150b). 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). 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.

10. Furthermore, I disagree with 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. 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, with the context making clear that “network 150” refers to the single network formed from the combination of sub-networks 150a and 150b. Moreover, Law further confirms that “network 150” may refer to a single local-area network by describing the two process control sub-systems 105a and 105b of Fig. 1b as communicating over a single local-area network. Ex. 1005 ¶ 53 (“[T]he process control system 100 of FIG. 1b shows only two process control sub-systems 105a and 105b communicating over a LAN ...”).

11. Patent Owner’s argument that Law only uses the term “network 150” when there is only one relevant network or it is not necessary to distinguish between networks 150a and 150b is further refuted by paragraph 57 of Law. In particular, Law describes that “[t]he 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.**” Ex. 1005 ¶ 57 (emphasis added). As shown in Fig. 3, communications between the controller 110 and firewall 146a occur through sub-network 150a, whereas communications between the controller 110 and firewall 146b occur through both sub-network 150a and sub-network 150b:

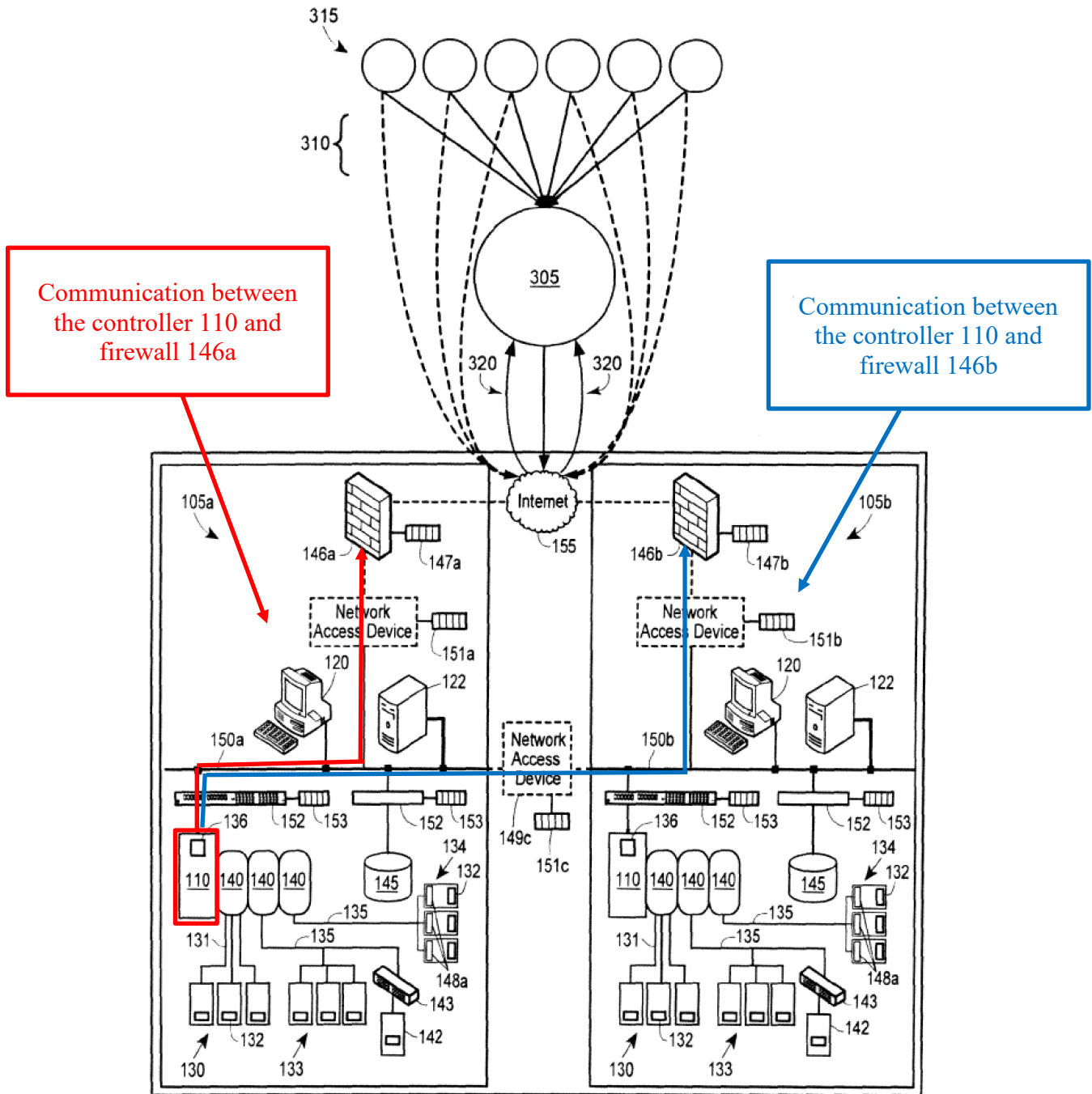


Fig. 3

Rather than describing the communications between the controller 110, firewall 146a, and firewall 146b as occurring across separate networks, which would be

necessary under Patent Owner's interpretation of Law, Law's description of both of these communications as occurring over "through the network 150" explicitly confirms that Law regarded the joined sub-networks 150a and 150b as a single network 150.

12. I also disagree with Patent Owner's argument that that network access device 149c being used to join sub-networks 150a and 150b supports Patent Owner's theory that a POSITA would not consider sub-networks 150a and 150b to 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."). As I explained in my first Declaration, Fig. 3 of Law shows that network access device 149c directly connects sub-network 150a and 150b to provide communications between them. Ex. 1003 ¶ 64; *see also* 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") (emphasis added).

13. It is clear from Fig. 3 that network access device 149c provides a direct connection, without traversing the Internet or other network, joining together subnetworks 150a and 150b. I understand that Dr. Goodrich agreed. Ex. 1015 at 48:8-49:10. Accordingly, as shown in Fig. 3, a POSITA would have understood

network access device 149c not to be a perimeter device in that embodiment but rather a device that is internal to network 150.

14. Nonetheless, despite the network access device 149c directly joining sub-networks 150a and 150b, I understand that Patent Owner has argued that sub-networks 150a and 150b should still be considered separate networks based on the capability of network access device 149c to implement a ruleset. Response at 25 n. 4; Ex. 1015 at 55:22-56:12. This argument neglects 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).

15. Apart from Patent Owner's and Dr. Goodrich's mistaken view that network access device 149c would necessarily implement a ruleset, the only other reason provided by Dr. Goodrich for not considering joined sub-networks (such as sub-networks 150a and 150b) to be a single network would be if the joined sub-networks implemented incompatible addressing schemes. Ex. 1015 at 55:22-56:12. However, a POSITA would have understood that Law's joined sub-networks 150a and 150b would have used compatible addressing schemes, and Patent Owner does not appear to contend otherwise. For example, using compatible addressing schemes would have furthered Law's goal of facilitating communication. *See, e.g.,*

Ex. 1005 ¶ 57 (describing communication between “[t]he controller 110” and “firewall(s) 146a, 146b ... through the network 150”).

16. Accordingly, for all of the above reasons, it remains my opinion that Law discloses or renders obvious “a packet security gateway, of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway and one or more networks other than the network protected by the packet security gateway,” as recited by elements [1.0], [8.0], and [15.0] of the ’266 patent.

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

17. I understand that elements [1.1], [8.3], and [15.1] of the ’266 patent recite, among other things: “a dynamic security policy comprising a first set of packet filtering rules to be applied to all network traffic traversing the boundary.”

18. In my first Declaration, I explained how Law discloses or renders obvious this claim language. *See* Ex. 1003 ¶¶ 68-80. For example, I explained that cyber security risk management firm 305 distributes ruleset 147 to perimeter UTMS firewalls 146a and 146b over the Internet 155 (Ex. 1005 ¶¶ 66, 88), and a POSITA would have understood that cyber security risk management firm 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, I explained that a POSITA would have understood that firewalls 146a and 146b may apply the same ruleset, which Law also identifies as “ruleset[] 147.” Ex. 1003 ¶ 71; Ex. 1005 ¶ 88. Likewise, I explained that a POSITA would have understood that perimeter UTMS firewalls 146a and 146b would have applied ruleset 147 to all network traffic passing therethrough. Ex. 1003 ¶ 77. For example, I explained that 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 associated rulesets 147, 148, 151, 153, are configured to protect the process control system 100 from internal and external network threats such as viruses, worms, or any other attack”).

19. I understand that Patent Owner disagrees that Law discloses or renders obvious that the ruleset 147 distributed to firewalls 146a and 146b could be the same ruleset. Response at 27-33.

20. In particular, I understand that 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, Patent Owner contends that firewall 146a would apply a one set of global set of rules for access to devices in subsystem 105a, and that firewall 146b would apply a different set of global rules for access to devices

in subsystem 105b. Response at 28. Furthermore, I understand that 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.*

21. I disagree with Patent Owner’s arguments for a number of 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 the teachings of Law and contrary to Law’s description of the ruleset implemented by both firewalls as “ruleset[] 147.” *See, e.g.,* Ex. 1005 ¶¶ 51, 88.

22. 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. *Id.* 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.

23. 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 be different from the ruleset for subsystem 105b. 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. Ex. 1005 ¶ 51.

24. Fourth, even if one were to incorrectly assume, as Patent Owner has done, 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 does not follow that ruleset 147a would necessarily be different than ruleset 147b. In particular, a POSITA would have understood that the devices in subsystem 105a may have been identical to the devices in subsystem 105b. For example, Fig. 3 of Law illustrates subsystem 105a as including the same devices, arranged in the same configuration, as subsystem 105b.

25. 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 (*see* Response at 30), I disagree for the same reasons I explained above.

26. 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. I disagree. This argument is based on the mistaken belief that network access device 149c necessarily implements ruleset 151c, which, as I explained above, directly contradict's 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).

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

27. I understand that elements [1.3], [8.5], [15.3], and [21.3] of the '266 patent recite, among other things: "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."

28. In my first Declaration, I explained how Law discloses or renders obvious this claim language. *See* Ex. 1003 ¶¶ 88-91. For example, I explained that Law discloses rules that were automatically created by cyber security risk

management firm 305. *See* Ex. 1003 ¶ 88; Ex. 1005 ¶ 88 (disclosing 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.”). 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.

29. Moreover, in my first Declaration, I explained that to the extent Law does not expressly disclose that at least a portion of the rules constructed by cyber

security risk management firm 305 were constructed 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 (emphasis added). 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.

30. Moreover, in my first Declaration, I explained that Law further discloses rules that were automatically altered by cyber security risk management firm 305. Ex. 1003 ¶ 90. 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).

31. 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, I disagree, for the reasons expressed in my first Declaration. Ex. 1003 ¶¶ 69-71. Moreover, the claim language does not prohibit the “security policy management server” from being owned by a commercial entity.

32. I also understand that Patent Owner argues that Law does not disclose or render obvious an SPMS that automatically generates rulesets. Response at 33-42. Specifically, I understand that 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, I understand that Patent Owner contends that “IT personnel ... are still required to manually update the rulesets of process control systems.” Response at 34. I disagree.

33. Patent Owner's arguments regarding firm 305 being a company that includes IT personnel fails to rebut Law's 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." Ex. 1005 ¶ 88 (emphasis added). As I explained in my first Declaration, 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, and I disagree that IT

personnel would have necessarily been involved in that process. Ex. 1003 ¶ 88.

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.

34. Furthermore, Patent Owner's argument that personnel would have been involved with running the service provided by firm 305, even if the firm 305 included IT personnel overseeing the distributed rulesets, does not negate Law's teachings that rules within the constructed rulesets may have been created automatically. 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, I understand that 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, the claim language would be satisfied even if a security policy is subsequently modified by a person. Ex. 1015 at 75:14-76:16.

35. 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, in my first

Declaration, I explained that 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 (emphasis added). I further 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. Patent Owner’s allegation that firm 305 employs IT personnel 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.

36. Lastly, I understand that Patent Owner relies on 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.”).

37. I disagree with Patent Owner. Law’s paragraph 16 does not suggest that firm 305 would require separately-trained IT personnel to update rules. To the contrary, Paragraph 16 of Law is in Law’s “DESCRIPTION OF THE RELATED ART” section, not Law’s “SUMMARY OF THE DISCLOSURE” section, and describes problems faced in the prior art. In particular, in describing prior art, Law’s paragraph 16 explains that some “commercial off-the-shelf (COTS) firewall systems” may “provide a partial solution to network security” for a process control system but “still must be managed outside of the operator environment” by “IT personnel specifically trained to integrate the firewall into the needs of the process control system and configure the various rulesets.” Ex. 1005 ¶ 16. Paragraph 16 also explains that “IT personnel are still required to update the ruleset when new threats are discovered or upgrades to software components of the system are implemented.” *Id.*

38. Law endeavors to overcome the need for specifically trained IT personnel to create or update firewall rulesets by providing an operator environment implementing “a Unified Threat Management System (UTMS) including a UTMS-configured firewall, UTMS-configured network access device, and UTMS-configured field devices that are capable of defending against both known and ‘zero day’ vulnerabilities and threats to control systems for both embedded, proprietary devices, and standard, commonly-used devices.” Ex. 1005 ¶ 22. Likewise, Law’s disclosure that “[d]etection of certain network conditions may also trigger an automatic update of the rulesets 147, 148, 151, 153 or an alarm to prompt a user to perform a manual update of the rulesets” clarifies that updates can occur automatically, without being performed manually by IT personnel, and is consistent with Law’s objective of streamlining protection against known and ‘zero day’ vulnerabilities and threats to control systems without the need for specifically-trained IT personnel. Ex. 1005 ¶ 83.

D. Law discloses or renders obvious “receiving, by the packet security gateway and from a security policy management server external from the network protected by the packet security gateway, a dynamic security policy comprising a first set of packet filtering rules”

39. I understand that element [1.1] of the ’266 patent recites, among other things: “receiving, by the packet security gateway and from a security policy management server external from the network protected by the packet security

gateway, a dynamic security policy comprising a first set of packet filtering rules.”

See also [8.3], [15.1], and [21.1]

40. In my first Declaration, I explained how Law discloses or renders obvious this claim language. *See* Ex. 1003 ¶¶ 68-80.

41. I understand that 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, I understand that 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.

42. I disagree on both accounts. First, I disagree that a POSITA would have understood the plain and ordinary meaning of the claim language to have required that the “first set of rules” be an initial dynamic security policy. Rather, the claim language simply recites “receiving . . . a dynamic security policy comprising a first set of packet filtering rules” [1.1] and later recites “receiving . . . an updated second set of packet filtering rules for the dynamic security policy” [1.5].

43. Second, I disagree that Law requires that “operators within the process control system create initial rulesets (ruleset 147),” not firm 305. To the contrary, Law consistently describes the rulesets 147 as being distributed by the firm 305. 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 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**”). While Law discloses an embodiment in which

“the rulesets 148, 147, 151, 153 may be configurable by an operator or other personnel from a graphic display 129 at a workstation 120,” this embodiment does not suggest that the rulesets that the operator may configure are created by an operator rather than received by firm 305.

III. CONCLUSION

44. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of the Title 18 of the United States Code and that such willful false statements may jeopardize the results of these proceedings.

Executed on January 24, 2024 in Ames, Iowa.



Doug W. Jacobson, Ph.D