

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KEYSIGHT TECHNOLOGIES, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, INC.,
Patent Owner.

Inter Partes Review No.: Unassigned

U.S. Patent No. 10,785,266

PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT 10,785,266

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	MANDATORY NOTICES	1
	A. Real Party-In-Interest	1
	B. Related Matters.....	1
	C. Lead and Back-Up Counsel and Service Information	1
III.	CERTIFICATION OF GROUNDS FOR STANDING	2
IV.	OVERVIEW OF CHALLENGE AND RELIEF REQUESTED.....	2
V.	BACKGROUND	3
	A. Summary of the '266 Patent.....	3
	B. Prosecution History	6
	C. Effective Filing Date	7
	D. Procedural History.....	7
	E. Level of Ordinary Skill in the Art	8
	F. Claim Construction	8
VI.	THE BOARD SHOULD NOT DENY INSTITUTION FOR DISCRETIONARY REASONS.....	11
	A. <i>Sotera</i> Stipulation	11
	B. The Board Should Not Exercise 325(d) Discretion	11
VII.	GROUND 1: LAW RENDERS OBVIOUS CLAIMS 1-27	12
	A. Overview of Law.....	12
	B. Independent Claims.....	14
	1. Claim 1	14
	2. Claim 8.....	52
	3. Claim 15.....	54
	4. Claim 21	56
	C. Dependent Claims	57
	1. Claims 2, 9, 16, 22	57
	2. Claims 3, 10, 17 and 23	58
	3. Claims 4, 11 and 24	60

4.	Claims 5, 12, 18 and 25	60
5.	Claims 6, 13, 19, and 26	61
6.	Claims 7, 14, 20 and 27	62
VIII.	GROUND 2: LAW IN VIEW OF WOOD RENDERS OBVIOUS CLAIMS 1-24	63
A.	Overview of Wood	63
B.	A POSITA Would Have Considered Wood In Conjunction With Law	65
C.	Claims 1-24	67
IX.	GROUND 3: LAW IN VIEW OF JUNGCK RENDER OBVIOUS CLAIMS 6, 13, 19 AND 26	68
A.	Overview of Jungck.....	68
B.	A POSITA Would Have Considered Jungck In Conjunction With Law	68
C.	Claims 6, 13, 19, and 26.....	69
X.	GROUND 4: LAW IN VIEW OF WOOD AND JUNGCK RENDERS OBVIOUS CLAIMS 6, 13, 19, AND 28	70
XI.	CONCLUSION.....	71

PETITIONER’S EXHIBIT LIST

Exhibit No.	Description
Ex. 1001	U.S. Patent No. 10,785,266 (“’266 Patent”)
Ex. 1002	File History of U.S. Patent No. 10,785,266
Ex. 1003	Declaration of Dr. Doug Jacobson In Support for <i>Inter Partes</i> Review Petition for U.S. Pat. 10,785,266
Ex. 1004	<i>Curriculum Vitae</i> of Dr. Doug Jacobson
Ex. 1005	U.S. Patent Pub. 2011/0072506 (“Law”)
Ex. 1006	U.S. Patent Publication No. 2007/0097976 (“Wood”)
Ex. 1007	Declaration from Nathaniel E. Frank-White, attaching Feb. 2, 2007 Assurent website printout regarding its Vulnerability Research Service (VRS), available at https://web.archive.org/web/20070202094127/http://www.assurent.com:80/index.php?id=58 (“Assurent VRS”)
Ex. 1008	U.S. Patent Pub. 2009/0262741 (“Jungck”)
Ex. 1009	Listing of claims of the ’266 Patent
Ex. 1010	Complaint filed in <i>Centripetal Networks, Inc. v. Keysight Technologies, Inc.</i> , Case No. 2:22-cv-00002
Ex. 1011	Affidavit of service of complaint filed in <i>Centripetal Networks, Inc. v. Keysight Technologies, Inc.</i> , Case No. 2:22-cv-00002
Ex. 1012	INTERIM PROCEDURE FOR DISCRETIONARY DENIALS IN AIA POST-GRANT PROCEEDINGS WITH PARALLEL DISTRICT COURT LITIGATION (June 21, 2022)

I. INTRODUCTION

Keysight Technologies, Inc. (“Petitioner”) petitions for *inter partes* review of claims 1-27 (hereinafter, the “Challenged Claims”) of U.S. Patent No. 10,785,266 (“’266 Patent,” Ex. 1001). The ’266 Patent is assigned to Centripetal Networks, Inc. (“Patent Owner”).

II. MANDATORY NOTICES

A. Real Party-In-Interest

Keysight Technologies, Inc. is the real party-in-interest. No other party had access to or control over this petition, and no other party funded or participated in preparation of this petition.

B. Related Matters

Patent Owner sued Petitioner in the U.S. District Court for the Eastern District of Virginia, alleging infringement of the ’266 Patent: *Centripetal Networks, Inc. v. Keysight Technologies, Inc.*, Civ. No. 2-22-cv-00002 (E.D. Va., filed Jan. 1, 2022) (the “Parallel Litigation”). Ex. 1010. Patent Owner served the complaint in the Parallel Litigation on January 6, 2021. Ex. 1011. The Parallel Litigation remains pending.

C. Lead and Back-Up Counsel and Service Information

Lead Counsel

Gerard M. Donovan, Reg. No. 67,771

GDonovan@ReedSmith.com

REED SMITH LLP, 1301 K Street N.W., Suite 1000, East Tower,
Washington, DC, 20005-3317

Telephone: +1 202 414 9200; Facsimile: +1 202 414 9299

Backup Counsel

Peter J. Chassman, Reg. No. 38,841

pchassman@reedsmith.com

REED SMITH LLP, 811 Main Street, Suite 1700, Houston, TX 77002-6110

Telephone: +1 713 469 3800; Facsimile: +1 713 469 3899

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

jdetrixhe@reedsmith.com

REED SMITH LLP, 101 Second Street, Suite 1800, San Francisco, CA 94105-3659

Telephone: +1 415 543 8700; Facsimile: +1 415 391 8269

Sidharth Kapoor, Reg. No. 68,159

skapoor@reedsmith.com

REED SMITH LLP, 101 Second Street, Suite 1800, San Francisco, CA 94105-3659

Telephone: +1 415 543 8700; Facsimile: +1 415 391 8269

Petitioner consents to electronic service of documents to the email addresses
of the counsel identified above.

III. CERTIFICATION OF GROUNDS FOR STANDING

Petitioner certifies that the '266 Patent is available for *inter partes* review
and that Petitioner is not barred or estopped from requesting an *inter partes* review
of the Challenged Claims on the grounds identified herein.

IV. OVERVIEW OF CHALLENGE AND RELIEF REQUESTED

Petitioner asserts that the Challenged Claims are unpatentable on the
following grounds:

Ground	Claims	35 U.S.C. §	References
1	1-27	103(a)	Law ¹
2	1-27	103(a)	Law, Wood ²
3	6, 13, 19, 26	103(a)	Law, Jungck ³
4	6, 13, 19, 26	103(a)	Law, Wood, Jungck

Law was published on Mar. 24, 2011. Ex. 1005, 1. Wood was published on May 3, 2007. Ex. 1006, 1. Jungck was published on Oct. 22, 2009. Ex. 1008, 1. Accordingly, each of these references is prior art under 35 U.S.C. §102(b).

This Petition is supported by the Declaration of Dr. Doug Jacobson. Ex. 1003.

V. BACKGROUND

A. Summary of the '266 Patent

The '266 Patent discloses methods and systems for protecting a secured network. Ex. 1001, 1. As shown in Fig. 1 below, a “network environment 100” is illustrated that includes a plurality of networks “A-E 102, 104, 106, 108, and 110;” “packet security gateways 112, 114, 116, and 118;” and a “security policy management server 120.” Ex. 1001, 4:40-60.

¹ U.S. Patent Publication No. 2011/0072506 (Ex. 1005, “Law”).

² U.S. Patent Publication No. 2007/0097976 (Ex. 1006, “Wood”).

³ U.S. Patent Publication No. 2009/0262741 (Ex. 1008, “Jungck”).

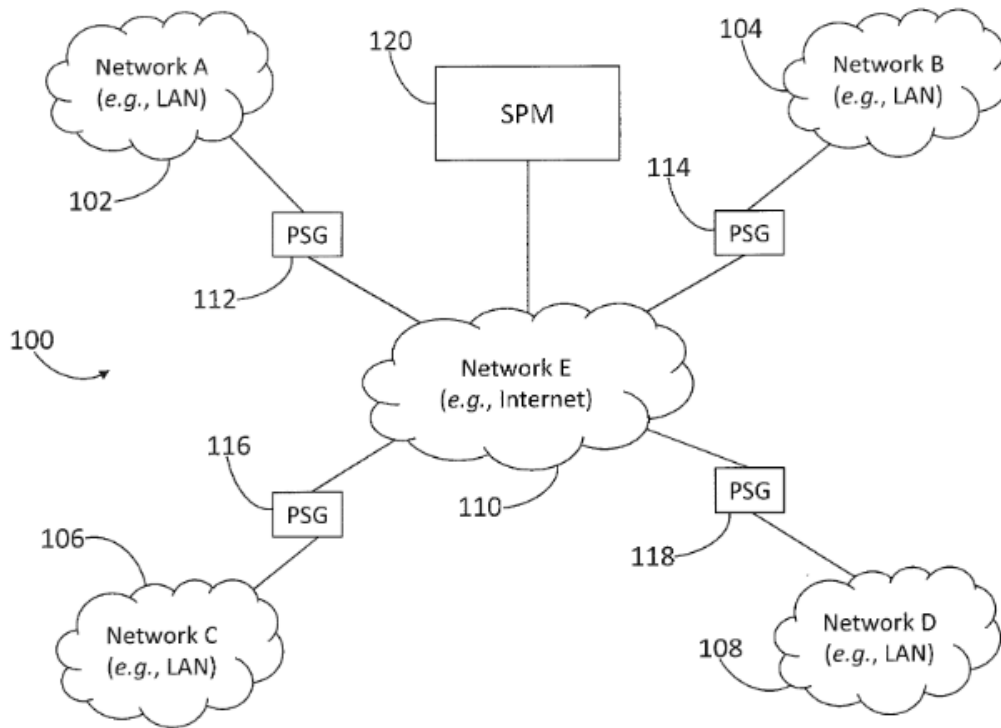


FIG. 1

The packet security gateways (PSGs) are situated at boundaries between networks (102, 104, 106, 108, and 110) and a security policy management server (SPMS) (120) that communicates dynamic security policies to the PSGs. Ex. 1001, 4:59-5:10.

The PSGs perform packet transformation functions (e.g., actions such as packet forwarding, dropping, or re-routing to a different destination address) on received packets according to rules in a dynamic security policy that specifies one or more actions that are performed on packets associated with specific criteria. Ex. 1001, 4:59-5:11; 6:24-28; 7:23-26.

The dynamic security policies can be added, removed, or altered by SPMS based on information received from third-party services, as illustrated in Fig. 5 below:

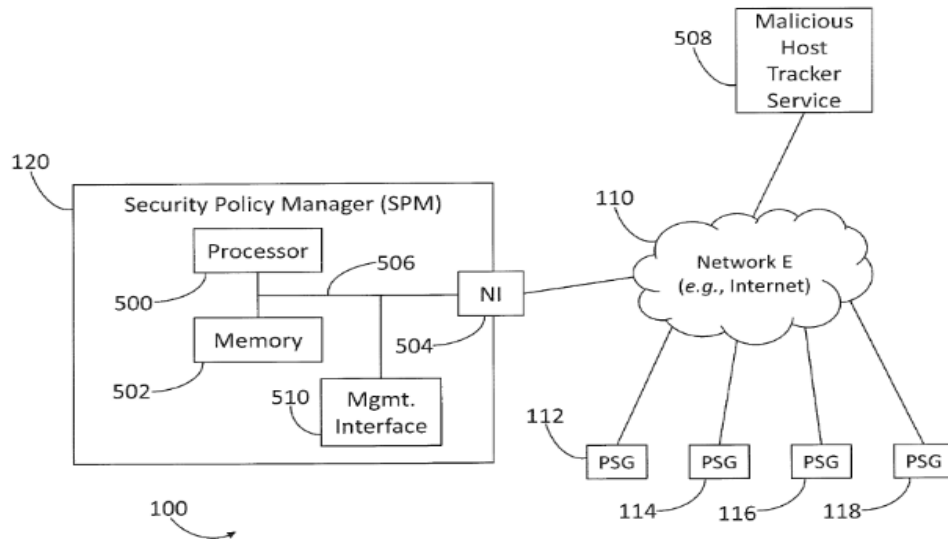


FIG. 5

Ex. 1001, 14-9:13; Fig. 5. For example, SPMS can provide a dynamic security policy including rules that specify a list of network addresses known to be associated with malicious network traffic and for which traffic should be blocked. Ex. 1001, 14:13-17. These addresses can be obtained from a third-party service provider (e.g., malicious host tracker service 508 and/or subscribing service), which may also provide updates (e.g., as part of a subscription) to the list of network addresses. Ex. 1001, 14:17-28. SPMS creates or alters one or more of the rules included in the dynamic security policy based on updates for new network addresses associated with malicious network traffic. Ex. 1001, 14:28-39.

B. Prosecution History

The '266 Patent issued from U.S. Application 16/728,766 (“the ‘766 application”), which was filed on December 27, 2019. The ‘266 Patent claims priority to a series of continuation applications with an earliest priority date of October 22, 2012, corresponding to U.S. Application 13/657,010 (now U.S. Pat. 9,137,205). Ex. 1001, 1-2.

The Patent Office rejected the claims as unpatentable over a combination of references. Ex. 1002, 168-214. In response, Patent Owner amended the independent claims to recite, *inter alia*, “at least one third party malicious host tracker service located in the one or more networks other than the network protected by the packet security gateway, that comprises network addresses that have been determined, by the at least one third party malicious host tracker service, to be associated with malicious network traffic” and argued that this limitation is not disclosed in the prior art. *Id.*, 138-150.

Following this amendment, the Examiner allowed the '766 Application, indicating that the added features of the independent claims were purportedly novel. *Id.*, 65-66.

C. Effective Filing Date

The '266 Patent is a continuation that claims priority back to an application filed on Oct. 22, 2012,⁴ which Petitioner assumes is the priority date for purposes of this Petition. Ex. 1001, 1.

D. Procedural History

The '266 Patent is a continuation of U.S. Pat. 10,567,437 ("437 Patent"), which is a continuation of U.S. Pat. 10,091,246 ("246 Patent"), which is a continuation of U.S. Pat. 9,560,077 ("077 Patent"), and which is a continuation of U.S. Pat. 9,137,205 ("205 Patent"). Ex. 1001, 1-2. Each of these patents in the '266 Patent family has been subject to one or more IPR proceedings before the Board.⁵

The IPRs on the '205 and '077 Patents resulted in the cancellation of the claims of those patents. *See* IPR2018-01443, Paper 25 (PTAB Feb. 11, 2020) ('205 Patent); IPR2018-01444, Paper 32 (PTAB Feb. 11, 2020) ('205 Patent); and IPR2018-01513, Paper 26 (PTAB Mar. 31, 2020) ('077 Patent). Each of those IPRs applied Jungck (Ex. 1008) as the primary reference. The Federal Circuit affirmed

⁴ The '266 Patent is therefore subject to pre-AIA law.

⁵ *See* IPR2018-01443, IPR2018-01444, IPR2018-01506, and IPR2018-01505 for '205 Patent; IPR2018-01513 for '077 Patent; IPR2021-01152 for '246 Patent; IPR2021-01153 for '437 Patent; and IPR2021-01154 for '266 Patent.

those decisions. *See, e.g., Centripetal Networks, Inc. v. Cisco Sys., Inc.*, 847 F.App'x 929 (CAFC May 11, 2021).

The '266 Patent also was previously challenged by a different petitioner, Palo Alto Networks (PAN), in IPR2021-01154, which relied on Jungck (Ex. 1008) as the primary reference. The Board denied institution, finding that PAN had failed to carry its burden to show that Jungck discloses or renders obvious the “an entire interface across a boundary of a network” and “all network traffic traversing the boundary” limitations. *See* IPR2021-01154, Paper 11 at 13-15 (PTAB Jan. 24, 2022).

E. Level of Ordinary Skill in the Art

In prior IPRs on the patents related to the '266 Patent, the Board determined that a POSITA “would have had a bachelor’s degree in computer science, computer engineering, or an equivalent, four years of professional experience, and a working knowledge of packet-switched networking, firewalls, security policies, communication protocols and layers, and the use of customized rules to address cyber-attack.” *See, e.g.,* IPR2018-01443, Paper 7 at 6 (PTAB Feb. 12, 2019). The same level of ordinary skill in the art should apply in this proceeding. Ex. 1003 ¶ 33.

F. Claim Construction

Claims subject to IPR are to be construed using the *Phillips* standard. §42.100(b); *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005). Only terms necessary to resolve the controversy need to be construed. *See Nidec Motor*

Corp. v. Zhongshan Broad Ocean Motor Co., 868 F.3d 1013, 1017 (Fed. Cir. 2017).

Various claim terms construed in IPR2018-01443 ('205 Patent), IPR2018-01444 ('205 Patent), and IPR2018-01513 ('077 Patent) also appear in the Challenged Claims. To the extent necessary to resolve any controversy, Petitioner requests that the Board adopt those same constructions here. Indeed, the '266, '077, and '205 Patents share the same specification. The table below shows the proposed constructions for each such term, including support for such constructions in prior IPRs:

Term	PTAB Constructions
packet security gateway	a gateway computer configured to receive packets and perform a packet transformation function on the packets <i>See</i> IPR2018-01443, Paper 25 (FWD); IPR2018-01444, Paper 32 (FWD).
packet transformation function	[one or more] operations performed on a packet <i>See</i> IPR2018-01443, Paper 25 (FWD); IPR2018-01444, Paper 32 (FWD); IPR2018-01513, Paper 26 (FWD); <i>see also</i> IPR2021-01152, Paper 9 at 12 (PTAB Jan. 26, 2022) (ID); IPR2021-01157, Paper 10 at 22 (PTAB Mar. 15, 2022) (ID).
rule(s)	a condition or set of conditions that when satisfied causes a specific function to occur <i>See</i> IPR2018-01443, Paper 25 (FWD); IPR2018-01444, Paper 32 (FWD); IPR2018-01513, Paper 26 (FWD).

Term	PTAB Constructions
dynamic security policy ⁶	any rule, message, instruction, file, data structure, or the like that specifies criteria corresponding to one or more packets and identifies a packet transformation function to be performed on packets corresponding to the specified criteria <i>See</i> IPR2018-01443, Paper 25 (FWD); IPR2018-01444, Paper 32 (FWD)
security policy management server	a server configured to communicate a dynamic security policy to a packet gateway <i>See</i> IPR2018-01443, Paper 25 (FWD); IPR2018-01444, Paper 32 (FWD)
network layer address	an address that identifies a device for communication on the network layer, such as an IP address <i>See</i> IPR2018-01513, Paper 26 (FWD).

⁶ In a previous district court proceeding on a related patent, a district court construed this term to mean “a changeable set of one or more rules, messages, instructions, files, or data structures, or any combination thereof, associated with one or more packets.” *Centripetal Networks, Inc. v. Keysight Techs., Inc.*, 2:17-cv-383, Dkt. 484 (E.D.V.A. Sep. 17, 2018). The art discloses this limitation under either construction.

**VI. THE BOARD SHOULD NOT DENY INSTITUTION FOR
DISCRETIONARY REASONS**

A. *Sotera* Stipulation

Petitioner stipulates that if the Board institutes *inter partes* review, Petitioner will not pursue in the Parallel Litigation any ground that was raised or reasonably could have been raised in this IPR petition. Accordingly, the Parallel Litigation does not provide a basis for discretionary denial. *See* Ex. 1012.

B. The Board Should Not Exercise 325(d) Discretion

The Board should not exercise discretion to deny institution under §325(d) because the same or substantially the same art and arguments were not previously presented to the Office.

As discussed above, Law was not considered by the Examiner during the prosecution history of the '266 Patent. *See, e.g.*, Ex. 1001, 1-6). In addition, Law has not been at issue in the prior IPRs of related patents. Accordingly, the art and arguments in this Petition, which rely on Law as the primary reference for all grounds, were not previously presented to the Office.

Both the substantive rationale behind the obviousness grounds, as well as the underlying evidence, have not previously been presented or considered by the Patent Office or the Board. As such, step one of *Advanced Bionics* favors institution of this Petition. *See Comcast Cable Comms, LLC, v. Rovi Guides, Inc.*, IPR2019-01434, Paper 14 at 13-14 (PTAB Feb. 12, 2020) (declining to exercise discretion to deny

institution where “combination of prior art is not the same or substantially the same as that previously presented to the Office”).

Because step one is not met, the Board therefore need not proceed to step two. *Advanced Bionics*, IPR2019-01469, Paper 6 at 7; *Bowtech, Inc. v. MCP IP, LLC*, IPR2019-00379, Paper 14 at 20 (PTAB July 3, 2019).

VII. GROUND 1: LAW RENDERS OBVIOUS CLAIMS 1-27

A. Overview of Law

Law is a patent application that published on Mar. 24, 2011. Ex. 1005, 1. Accordingly, Law is prior art at least under 35 U.S.C. § 102(b) (pre-AIA).

Law is directed to “[a] Unified Threat Management System (UTMS) for securing network traffic in a process control system.” Ex. 1005, Abstract. In particular, Law discloses UTMS-configured network devices, such as firewalls 146a and 146b, that implement “one or more rulesets to inspect and drop malicious packets from the network before the malicious packets can reach their intended destination.” *Id.* ¶ 52. The firewalls 146a and 146b protect a network 150, which may include subnetworks 150a and 150b. *Id.* ¶¶ 54-55.

Law discloses that a cyber security risk management firm 305 may distribute rulesets to Law’s firewalls over the Internet. *Id.* ¶¶ 66, 88; *id.*, Fig. 3. In turn, the cyber security risk management firm 305 may formulate rulesets based on aggregated threat data 310 from various third party sources 315, which include

cyber-security threat intelligence providers such as “the Vulnerability Research Service (VRS) of Assurent Secure Technologies.” *Id.* ¶ 92. The cyber security risk management firm 305 is a “perpetual service that proactively supplies the UTMS-configured firewalls ... with” updated “rulesets to meet the latest security threats.” *Id.* ¶ 22; *id.*, Abstract; *id.* ¶ 88 (disclosing that “the various rulesets ... require updates to remain effective against network threats”).

Although Law discloses its unified threat management system in the context of protecting a “process control network,” such as a communication network implemented in the context of “process control systems like those used in power generation, chemical, petroleum, or other processes” (*id.* ¶ 3), a POSITA would have understood the applicability of Law’s unified threat management system to protecting any network. Ex. 1003 ¶ 58. For example, Law implements its communication network using standard networking protocols, and the devices within Law’s network include ordinary personal computers. Ex. 1005 ¶ 54 (“The communication network 150a, 150b may be a local area network (LAN) ... and may be implemented using hardwired or wireless technology” including “standard protocols such as Ethernet”); *id.* ¶ 55 (“supporting any communications protocol,” including “TCP/IP”); *id.* ¶ 53 (“process control networks 150a, 150b” are “communicatively connected to one or more host workstations or computers 120-

122 (which may be any type of personal computers, workstations, etc.)”). Ex. 1003 ¶ 58.

B. Independent Claims

1. Claim 1

(A) [1.0]⁷ “*A method of filtering packets ...*”

Law is directed to a method of filtering packets at a packet security gateway. In particular, Law’s perimeter UTMS firewalls 146a and 146b each correspond to the claimed “packet security gateways.” Ex. 1003 ¶ 59. For example, Law discloses that the security of “networks may be enhanced by providing a Unified Threat Management System (UTMS) including a UTMS-configured firewall.” Ex. 1005 ¶ 22. The UTMS-configured firewalls may be located at the perimeter of a network. *Id.* (“The UTMS-configured firewall ... devices may include stand-alone network devices located at the perimeter of the ... network.”). For example, Fig. 1A of Law illustrates UTMS-configured firewalls 146a and 146b at a perimeter of a network, each providing a boundary that separates local area networks—LANs 150a and 150b—from the Internet 155:

⁷ The numerical identification of the claim limitations of the ’266 Patent correspond to that provided in the exhibit providing a claim listing. Ex. 1009.

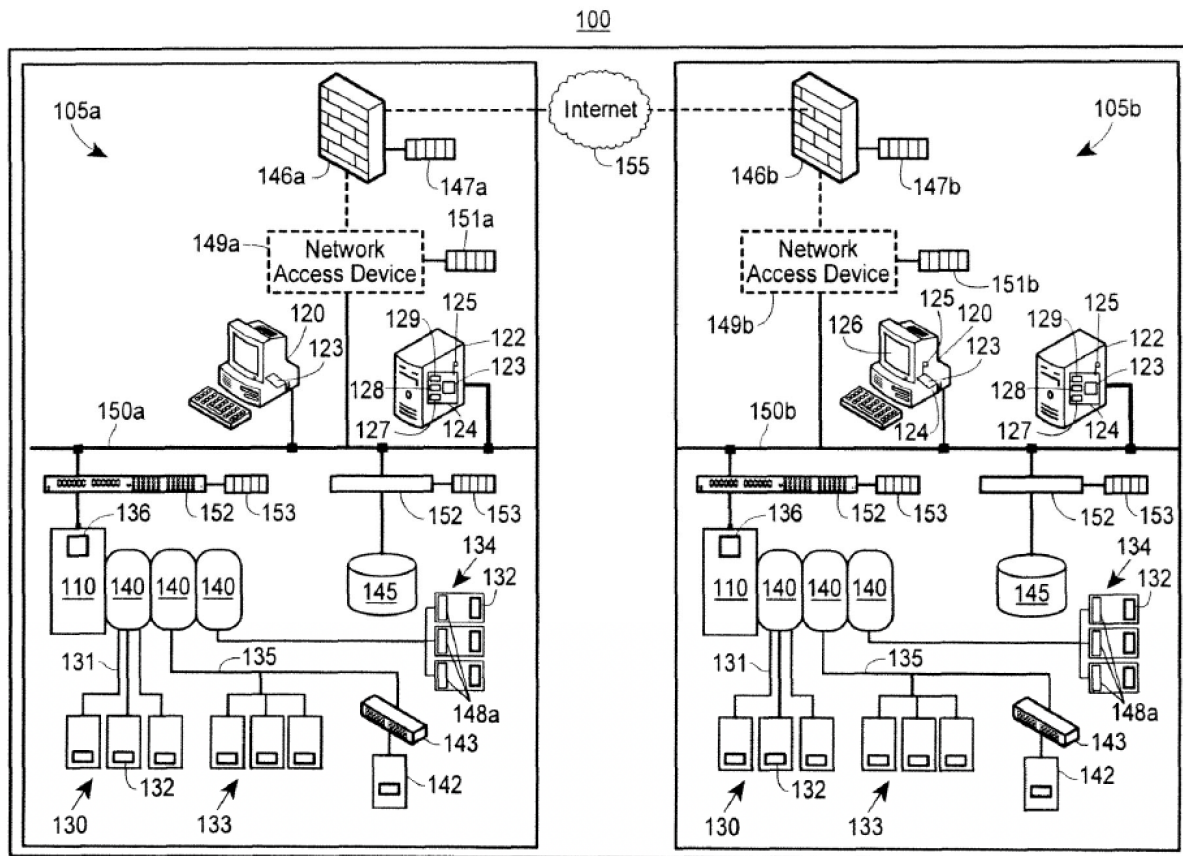


Fig. 1A

Id., Fig. 1A; *id.* ¶ 51 (“FIG. 1a is a schematic representation ... in which external communication between, for example, each subsystem via the Internet or other external source may be secured by a ‘Unified Threat Management System’ (UTMS) including one or more UTMS-configured network devices (e.g., firewalls) 146a, 146b”); *id.* ¶ 54 (“The communication network 150a, 150b may be a local area network (LAN) ... and may be implemented using hardwired or wireless technology” including “standard protocols such as Ethernet”); *id.* ¶ 55 (“The network 150 and devices may also be standard Ethernet communications and

network devices supporting any communications protocol,” including “TCP/IP”); *see also id.*, Fig. 3; Ex. 1003 ¶ 59.

In addition, and as further described below with respect to element [1.4], UTMS-configured firewalls, including firewalls 146a and 146b, perform packet filtering. *See, e.g., id.* ¶ 52 (“UTMS-configured firewall 146a, 146b ... may use one or more rulesets to inspect and drop malicious packets from the network before the malicious packets can reach their intended destination.”). For example, firewalls 146a and 146b implement rulesets, including rulesets 147a and 147b. *Id.* ¶ 51 (“Each firewall 146 ... may include a ruleset, for example, rulesets 147a ... 147b”); *id.*, Fig. 1A (showing rulesets 147a and 147b corresponding to firewalls 146a and 146b, respectively). The firewalls 146a and 146b use these rulesets to determine whether to filter (i.e., block) packets. *Id.* ¶ 91 (“Each 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”).

As explained above, “packet security gateway” has been construed to mean “a gateway computer configured to receive packets and perform a packet transformation function on the packets.” In turn, “packet transformation function” has been construed to mean “[one or more] operations performed on a packet.” In addition to being packet security gateways under the plain meaning of these terms,

Law's firewalls 146a and 146b are packet security gateways under these constructions. Ex. 1003 ¶ 61. In particular, a POSITA would have understood that Law's perimeter UTMS firewalls 146a and 146b are gateways, as they are firewalls that separate a LAN (e.g., LANs 150a and 150b) from the Internet. *Id.* Furthermore, Law describes that its "UTMS devices ... are preferably implemented in software" and executed using "a standard multi purpose CPU," though they may also "may be implemented in hardware, firmware, etc., and may be executed by any other processor." Ex. 1005 ¶ 117. As such, a POSITA would have understood that Law's UTMS firewalls 146a and 146b correspond to gateway computers. Ex. 1003 ¶ 61. In addition, Law's UTMS firewalls 146a and 146b are configured to perform one or more operations on a packet. *Id.* For example, in addition to being configured to perform blocking operations on a packet, Law's UTMS firewalls 146a and 146b may be configured to implement other actions specified by rules, including accept (forward to destination), notify, and re-route actions. Ex. 1005 ¶ 103 ("While the example first rule 1326 identifies an action of 'accept,' other actions may include, but are not limited to, block, notify, and/or re-route."); Ex. 1003 ¶ 61. Accordingly, Law's perimeter UTMS firewalls 146a and 146b are packet security gateways that are configured to filter packets. *Id.*

In addition, Law's perimeter UTMS firewalls 146a and 146b correspond to 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. In particular, as shown above in Fig. 1A, firewall 146a provides the entire interface across a boundary of a network protected by the firewall 146a (LAN 150a) and one or more networks other than the network protected by firewall 146a (Internet 155). Ex. 1005, Fig. 1A; Ex. 1003 ¶ 62. For example, as shown in Fig. 1A by the single line connecting LAN 150a through firewall 146a to Internet 155, all network traffic between a device on LAN 150a—e.g., from “one or more host workstations or computers 120-122 (which may be any type of personal computers, workstations, etc.)” (Ex. 1005 ¶ 53)—and the Internet 155, must first pass through firewall 146a. Ex. 1003 ¶ 62. Likewise, firewall 146b provides the entire interface across a boundary of a network protected by the firewall 146b (LAN 150b) and one or more networks other than the network protected by firewall 146b (Internet 155). Ex. 1005, Fig. 1A; Ex. 1003 ¶ 62. As shown in Fig. 1A by the single line connecting LAN 150b through firewall 146b to Internet 155, all network traffic between a device on LAN 150b—e.g., from “one or more host workstations or computers 120-122 (which may be any type of personal computers, workstations, etc.)” (Ex. 1005 ¶ 53)—and the Internet 155 must first pass through firewall 146b. Ex. 1003 ¶ 62. Moreover, Law’s description of UTMS firewalls 146a and 146b as “perimeter” devices further confirms to a POSITA that they serve as the entire interface

between the Internet 155 and the network(s) 150 protected by firewalls 146a and 146b. *Id.*

In addition to Law's figures illustrating that firewalls 146a and 146b provide the entire interface between the protected network(s) and the Internet, a POSITA would have understood the necessity of that requirement from the description of Law. Ex. 1003 ¶ 63. For example, Law describes that “[a]ny external connection into a process control system network presents a possible point of attack into the system,” and that “[n]etwork devices such as firewalls ... mitigate the risk of network attacks” by “block[ing] network traffic that is not authorized to access one or more portions of the network.” Ex. 1005 ¶¶ 10-11 (emphasis added)⁸; *see also id.* ¶ 59 (“The UTMS-configured firewalls 146 ... and associated rulesets 147 ... are configured to protect the process control system 100 from internal and external network threats such as viruses, worms, or any other attack”); *id.* ¶ 15 (recognizing that “particularly high-risk” systems use “restrictive connection policies” that “demand[s] that **all** external network connections be completely secure”).

To the extent that the preamble is construed to require that a plurality of packet security gateways collectively protect a single network, Law discloses an embodiment in which LANs 150a and 150b are optionally joined together to form

⁸ Unless indicated otherwise, all bold emphasis in any quoted material has been added.

a single network protected by perimeter UTMS firewalls 146a and 146b. Ex. 1003

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

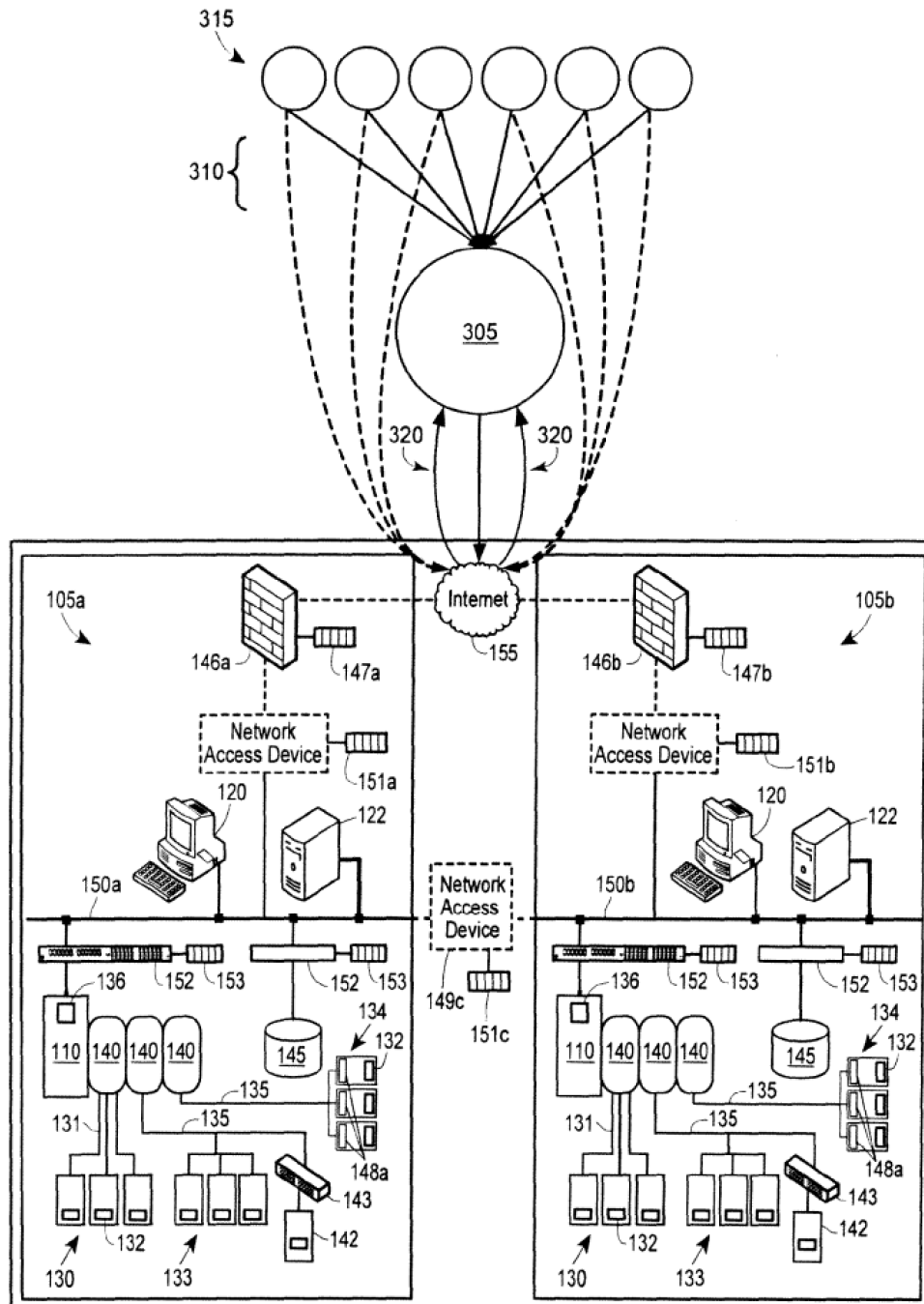


Fig. 3

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

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 disclosure of this alternative bypass embodiment, which provides the ability to turn on or off re-routing of network traffic around a malfunctioning device, does not describe the perimeter UTMS firewalls 146a and 146b illustrated in Figs. 1A and 3, and, in fact, further confirms that perimeter UTMS firewalls 146a and 146b lack

bypass functionality. Ex. 1003 ¶ 65. As such, the perimeter UTMS firewalls 146a and 146b necessarily provide the entire interface across the boundary of the network protected by firewalls 146a and 146b. *Id.*

Lastly, although the preamble’s requirement of “a plurality packet security gateways” is satisfied by Law’s express disclosure of two packet security gateways (firewalls 146a and 146b), it would have been obvious to a POSITA to expand Law’s disclosure to any number of packet security gateways. Ex. 1005 ¶ 53 (“While the process control system 100 of FIG. 1a shows only two process control sub-systems 105a and 105b ..., a process control system 100 may include any number of sub-systems as well as devices, modules, and components that are communicatively connected to each other through any type of connection including Internet, LAN, wireless”); Ex. 1003 ¶ 66.

Accordingly, Law discloses or renders obvious the preamble.

(B) [1.1] “*receiving, ...*”

As explained above in [1.0], Law’s perimeter UTMS firewalls 146a and 146b are packet security gateways.

As explained below, Law’s cyber security risk management firm 305 corresponds to the claimed “security policy management server,” is located on an external network (i.e., the Internet 155), and distributes to Law’s perimeter UTMS firewalls 146a and 146b a dynamic security policy comprising a first set of packet

filtering rules to be applied to all network traffic traversing the boundary between the protected network 150 and the Internet 155. *See* Ex. 1005 ¶¶ 22, 66, 88, 92; *id.*, Fig. 3; Ex. 1003 ¶ 69.

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**”).

Fig. 3 confirms that cyber security risk management firm 305 is external from network 150 (including subnetworks 150a and 150b) protected by perimeter UTMS firewalls 146a and 146b:

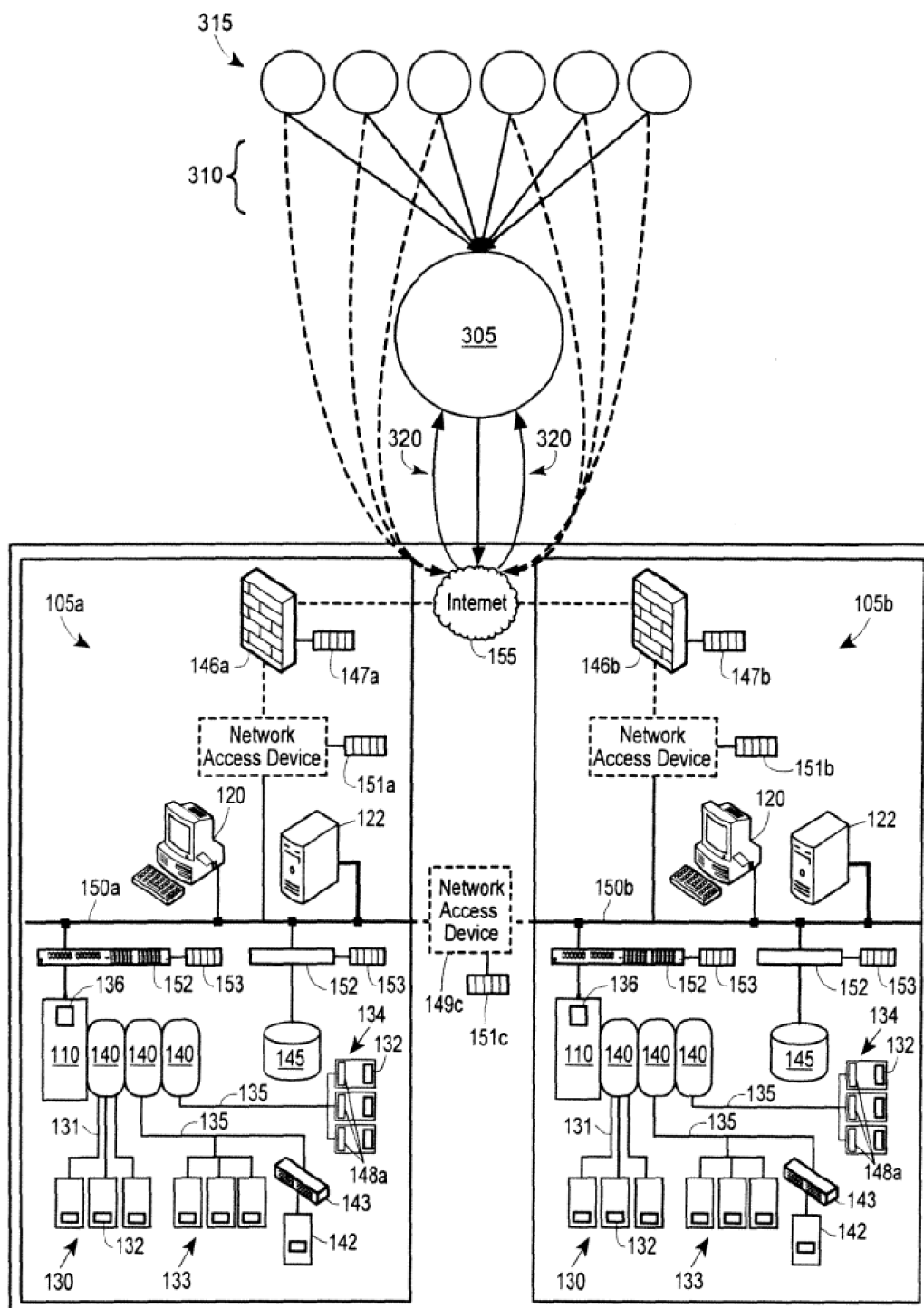


Fig. 3

Ex. 1005, Fig. 3; *see also id.* ¶ 26 (disclosing “receiv[ing] a ruleset from a source that is external to the process control system”); Ex. 1003 ¶ 71. In addition,

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 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.

The ruleset 147 distributed by cyber security risk management firm 305 to perimeter UTMS firewalls 146a and 146b comprises a first set of packet filtering rules, as further described below with respect to elements [1.2]-[1.4]. Ex. 1003 ¶ 72. For example, Law explains that “UTMS-configured firewall 146a, 146b ... may use [its] rulesets to inspect and drop malicious packets from the network before the malicious packets can reach their intended destination.” Ex. 1005 ¶ 52; *see also id.* ¶ 59 (“The UTMS-configured firewalls 146 ... and associated rulesets 147 ... are configured to protect the process control system 100 from internal and external network threats such as viruses, worms, or any other attack”).

As explained above, “rule” has been construed to mean “a condition or set of conditions that when satisfied causes a specific function to occur.” The ruleset 147 received by UTMS firewalls 146a and 146b includes rules that satisfy this

construction. In particular, 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.” Ex. 1005 ¶ 91; *see also id.*, Fig. 13 (illustrating detection conditions such as the “PROTOCOL,” “FROM,” “TO,” and “PORT” fields as well as a specific “ACTION” that occurs upon satisfaction of the conditions); *id.* ¶ 103 (describing that actions that may be performed on packets include, but are not limited to, accept, block, notify, re-route, and logging); Ex. 1003 ¶ 73.

Furthermore, the ruleset 147 distributed by cyber security risk management firm 305 to perimeter UTMS firewalls 146a and 146b comprises a dynamic security policy. As explained above, “dynamic security policy” has been construed to mean “any rule, message, instruction, file, data structure, or the like that specifies criteria corresponding to one or more packets and identifies a packet transformation function to be performed on packets corresponding to the specified criteria.” First, ruleset 147 may be distributed via a data file. Ex. 1005 ¶ 90 (“**Each ruleset may be a data file** that includes known signature, policy, or other rules describing characteristics of network-based threats”). Second, as explained above, and as further explained below with respect to element [1.2], ruleset 147 specifies criteria corresponding to one or more packets (the “define[d] conditions” that identify packets, such as the “PROTOCOL,” “FROM,” “TO,” and “PORT” fields)

and identifies a packet transformation function to be performed on packets corresponding to the specified criteria (actions including accept, block, notify, re-route, and logging). Ex. 1005 ¶¶ 102-103, Fig. 13; Ex. 1003 ¶ 74.

To the extent a “dynamic security policy” requires the ability to change over time, Law expressly discloses that ruleset 147 is dynamic and may be updated whenever needed, including automatically. 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.”); *id.* ¶ 89 (describing updating rulesets 147, 148, 151, 153 to address “known vulnerabilities,” which “the firm 305 may provide an ongoing remediation update service to the system 100 in the form of UTMS-device updates”). Ex. 1003 ¶ 75.

As explained above, “security policy management server” has been construed to mean “a server configured to communicate a dynamic security policy to a packet gateway.” As explained above, cyber security risk management firm 305 is a server that communicates a dynamic security policy (ruleset 147) to a packet gateway (perimeter UTMS firewalls 146a and 146b). Ex. 1003 ¶ 76.

Lastly, a POSITA would have understood that perimeter UTMS firewalls 146a and 146b apply the received ruleset 147 to all network traversing the boundary between network 150 (including LANs 150a and 150b) and Internet 155.

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 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”); *id.* ¶ 102 (“The perimeter UTMS-configured devices 146 ... may include any number of additional rule tables to monitor and/or protect a control system 100 from unwanted access and/or malicious attack”); *id.* ¶ 103 (“**In operation, each row of the example table 1300 enforces a rule** if a corresponding row selector is active, as shown by an example row selection column 1324”).

In addition, Law’s disclosure of an alternative embodiment to “bypass” and “selectively turn off” the rules applied by UTMS firewalls 146a and 146b (*id.* ¶ 93)

makes clear that in the standard, non-bypass embodiment, firewalls 146a and 146b apply its rulesets to all network traffic, without exception. Ex. 1003 ¶ 78; *see also* Ex. 1005 ¶ 94 (explaining that the bypass embodiment is used “to temporarily bypass firewalls 146 ... to allow less secure access (i.e., technical support, maintenance, etc.) without having to modify the firewall rules 147”). Law’s disclosure of an alternative embodiment that permits bypassing firewalls 146 without having to modify the firewall rules 147 informs a POSITA that in the standard, non-bypass embodiment, network traffic would not be able to bypass the firewall rules 147 applied by firewalls 146 without modifying the rules. Ex. 1003 ¶ 78.

Lastly, to the extent that Law does not explicitly disclose that perimeter UTMS firewalls 146a and 146b apply ruleset 147 to all network traffic passing therethrough, doing so would have been obvious to a POSITA in order to further Law’s objective of mitigating the risk of network attacks. Ex. 1003 ¶ 79; *see* Ex. 1005 ¶¶ 10-11 (describing that “[a]ny external connection into a process control system network presents a possible point of attack into the system,” and that “[n]etwork devices such as firewalls ... mitigate the risk of network attacks” by “block[ing] network traffic that is not authorized to access one or more portions of the network”); *see also id.* ¶ 59 (“The UTMS-configured firewalls 146 ... and associated rulesets 147 ... are configured to protect the process control system 100

from internal and external network threats such as viruses, worms, or any other attack”); *id.* ¶ 15 (recognizing that “particularly high-risk” systems use “restrictive connection policies” that “demand[s] that **all** external network connections be completely secure”).

According, Law discloses or renders obvious element [1.1].

(A) [1.2] “*each packet filtering rule ...*”

As explained above in [1.1], each packet filtering rule in ruleset 147 applied by the perimeter UTMS firewalls 146a and 146b comprises at least one packet matching criterion and a corresponding packet transformation function. Ex. 1005 ¶¶ 52, 91, 102-103; *id.*, Fig. 13; Ex. 1003 ¶ 81.

In particular, each packet filtering rule in ruleset 147 applied by the perimeter UTMS firewalls 146a and 146b comprises at least one packet matching criterion. For example, 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.” Ex. 1005 ¶ 91. Those conditions are specified in Fig. 13, which includes condition fields including PROTOCOL 1302, FROM 1304, TO 1306, and PORT 1308:

1300

	1324	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 ↓	LOAD	1318
1320		SAVE	1322

Fig. 13

Ex. 1005, Fig. 13; *id.* ¶ 102 (“The perimeter UTMS-configured devices 146 ... may include any number of additional rule tables to monitor and/or protect a control system 100 from unwanted access and/or malicious attack.”); *id.* (“As illustrated in FIG. 13 ... protocol rule table 1300 ... 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.”).

As Law explains, the protocol type column 1302, from-address column 1304, to-address column 1306, and port number column 1308 are conditions that determine whether the action 1310 is performed on a packet. Ex. 1005 ¶¶ 102-103; Ex. 1003 ¶ 83. These generally correspond to the same rule conditions in the exemplary rule table provided by the '266 patent. *See* Ex. 1001, Fig. 3 (identifying protocol, source address, destination address, and source and destination ports). In addition, given that Law explains that “each row of the example table 1300 enforces a rule if a corresponding row selector is active” (Ex. 1005 ¶ 103), a POSITA would have understood that each row of a ruleset table corresponds to a single packet matching criterion for a single packet filtering rule within ruleset 147. Ex. 1003 ¶ 83. Law further provides a concrete example of such a packet matching criterion for a single packet filtering rule. Ex. 1005 ¶ 103 (“A first example row 1326 ... results in the enforcement of a rule that monitors UDP protocol packets from a device associated with address 10.4.0.0 to a device associated with address 232.108.116.118, which includes port number 18515.”).

Each packet filtering rule in ruleset 147 applied by the perimeter UTMS firewalls 146a and 146b also comprises a corresponding packet transformation function. As explained above, “packet transformation function” has been construed to mean “[one or more] operations performed on a packet.” Law explains that one such operation performed on a packet includes blocking, or dropping, the packet.

Ex. 1005 ¶ 52 (“UTMS-configured firewall 146a, 146b ... may use one or more rulesets to inspect and drop malicious packets from the network before the malicious packets can reach their intended destination”). Law discloses other operations that each rule may perform on a packet in the action column 1310 of the exemplary protocol rule table 1300 of Fig. 13. *Id.*, Fig. 13. For example, in addition to blocking, Law discloses that other operations that may be performed on a packet include actions of “accept,” “notify,” and “re-route.” *Id.* ¶ 103 (“While the example first rule 1326 identifies an action of ‘accept,’ other actions may include, but are not limited to, block, notify, and/or re-route.”); Ex. 1003 ¶ 84. A POSITA would have understood that an “accept” action refers to forwarding a packet to its intended destination. *Id.* In addition, a POSITA would have understood that a “re-route” action refers to forwarding a packet to a different location than the destination location specified by the packet header. *Id.*

Accordingly, Law discloses or renders obvious element [1.2].

(B) [1.3] “*one or more first packet filtering rules ...*”

As explained above in [1.2], Law discloses that one or more first packet filtering rules of the first set of packet filtering rules comprise packet matching criteria. In particular, each packet filtering rule in ruleset 147 applied by the perimeter UTMS firewalls 146a and 146b comprises packet matching criteria,

including the protocol type column 1302, from-address column 1304, to-address column 1306, and port number column 1308. Ex. 1005 ¶¶ 102-103; Ex. 1003 ¶ 86.

Law further discloses that the one or more first packet filtering rules of the first set of packet filtering rules comprise packet matching criteria corresponding to one or more network addresses. For example, the packet matching criteria includes from-address column 1304 and to-address column 1306, which “correspond to one or more addresses associated with a given protocol type,” such as “IP addresses” that are “typically employ[ed]” by the “TCP, UDP, and ICMP protocols.” Ex. 1005 ¶ 102. A POSITA would have understood that an IP address is a network address. Ex. 1003 ¶ 87. In addition, Law explains that setting any packet-filtering criteria to “N/A” will not impose any constraints by the criteria set to “N/A.” Ex. 1005 ¶ 104. Accordingly, for a rule to comprise packet matching criteria based only on one or more network addresses, a POSITA would have understood to include one or more IP addresses in the from-address column 1304 and/or to-address column 1306 while setting the other packet matching criteria to “N/A.” Ex. 1003 ¶ 87; Ex. 1005 ¶ 104 (“In the illustrated example of FIG. 13, the first row 1326 permits communications between the from-address and the to-address with no limitation imposed by the threshold column 1305”).

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.

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. 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.

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.

Accordingly, because Law discloses or renders obvious both automatically creating rules and automatically altering / updating rules by cyber security risk management firm 305, Law discloses or renders obvious that the ruleset distributed to firewalls 146 would have been “automatically created **or** altered” by the firm 305. Ex. 1003 ¶ 91.

In addition, Law discloses or renders obvious that the security policy management server (cyber security risk management firm 305) generates rulesets based on aggregated malicious traffic information received from at least one third party malicious host tracker service (“plurality of various sources 315”) located in the one or more networks other than the network protected by the packet security gateway (Internet 155), that comprises network addresses that have been determined, by the at least one third party malicious host tracker service, to be associated with malicious network traffic. Ex. 1005 ¶¶ 88, 91-92, 102-103; *id.*, Fig. 13; Ex. 1003 ¶ 92.

In particular, Law discloses that cyber security risk management firm 305 generates its rulesets, including ruleset 147, by aggregating threat data and other malicious traffic information received from a plurality of various sources 315,

which include third-party sources. Ex. 1005 ¶ 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**”). Fig. 3 illustrates the connection between cyber security risk management firm 305 and the connections to sources 315 that provide the threat data 310:

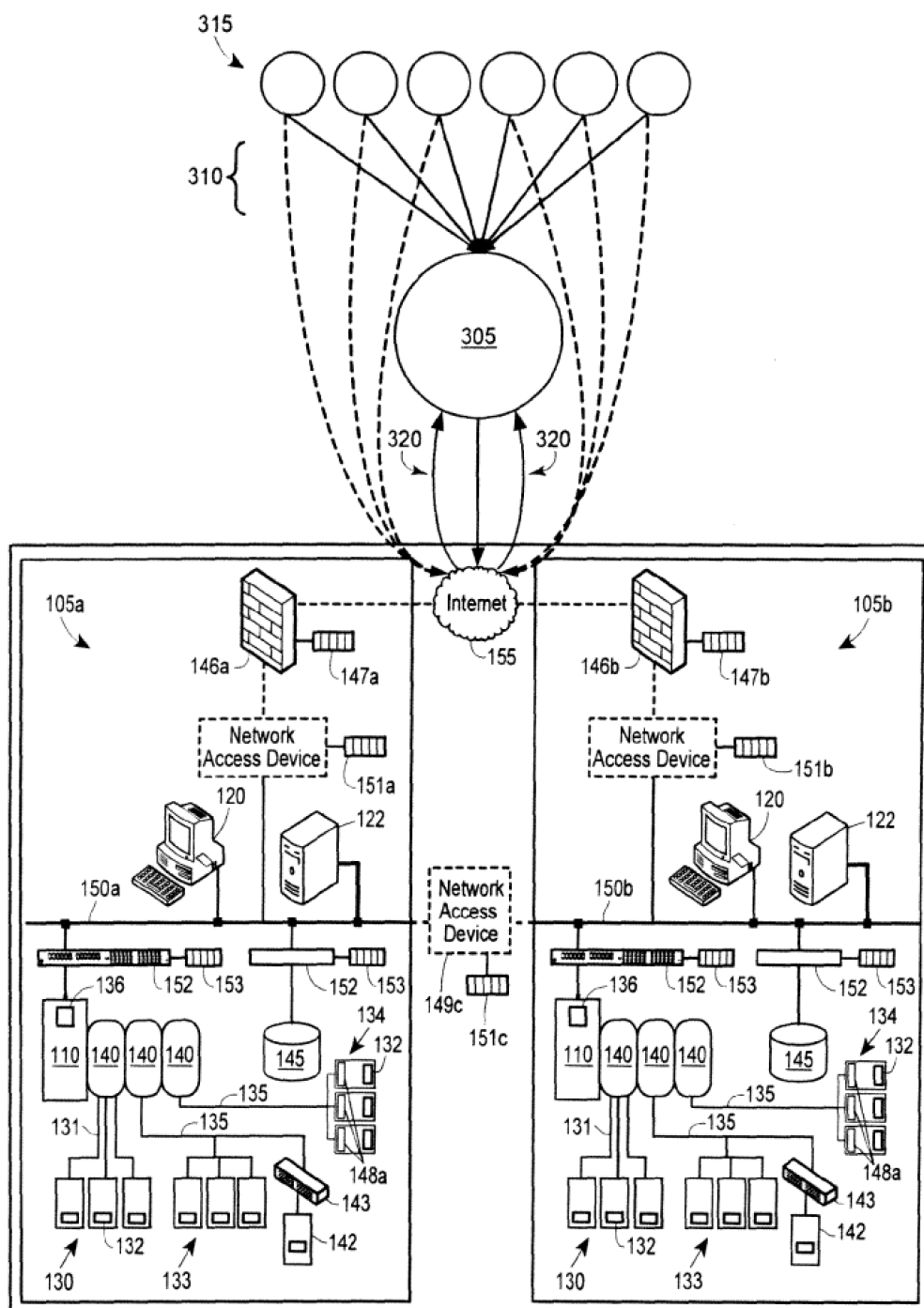


Fig. 3

Ex. 1005, Fig. 3. As shown in Fig. 3, both the cyber security risk management firm 305 and sources 315 that provide threat data 310 are separated from the protected

network 150 by the Internet 155, and thus are located in a network other than the network protected by firewalls 146. Ex. 1003 ¶ 93.

The various sources 315 that provide threat data 310 correspond to third party malicious host tracker services. *Id.* ¶ 94. For example, Law discloses:

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.TM. certified product users (to name but a few of the sources for firewall ruleset data) may be aggregated.

Ex. 1005 ¶ 92. A POSITA would have understood each of the exemplary identified sources 315 of threat data 310 to be third parties. Ex. 1003 ¶ 94. For example, a POSITA would have recognized that Assurent Secure Technologies and Secunia were cybersecurity firms, and that Carnegie Mellon University is a university. *Id.* Moreover, a POSITA would have known that Assurent's "Vulnerability Research Service (VRS)" is a service that provides rapid updates to rulesets to help its subscribers (security product vendors) help their customers stay protected against

emerging and changing network security threats. *Id.*; Ex. 1007,⁹ at 5 (“Assurent’s Vulnerability Research Services provide a range of services focused on security vulnerability research,” including “provid[ing] the industry’s best respons [sic] time for early warning of emerging threats” and providing “**vulnerability data** [that] enables security product vendors to deliver product **updates** (signatures, **filters**, scripts) without the need for additional research,” and which are provided as part of a “Vulnerability Research Subscription feed[] for security product vendors, for managed service providers, and for enterprise security teams,” including “provid[ing] near real-time coverage for the most severe security

⁹ Ex. 1007 is a declaration from Nathaniel E. Frank-White of the Internet Archive attaching a Feb. 2, 2007 capture of Assurent’s website that describes its Vulnerability Research Service (VRS) (“Assurent VRS”). Ex. 1007 is evidence of how a POSITA would have understood Law’s disclosure that Assurent’s VRS service should be used as a source 315 and therefore is properly considered with respect to ground 1. To the extent that consideration of Ex. 1007 would require combining Law with Assurent VRS as a separate obvious ground, it would have been obvious to a POSITA to combine Law with Assurent VRS in view of Law’s explicit directive to use Assurent’s Vulnerability Research Service (VRS) as a source 315. Ex. 1005 ¶ 92; Ex. 1003 ¶ 94 n. 4. In addition, based on the horizontal layout of the headers “HOME,” “COMPANY,” “SOLUTIONS,” “SERVICES,” “RESEARCH,” and “PRODUCTS,” and the left-side layout of categories of “Products” including “Web Application Firewall,” “Secure Software Development Model,” “Vulnerability Data,” and “Spyware Data,” with an arrow indicating that the “Vulnerability Data” product category had been selected, a POSITA would have understood that the website capture shown in Ex. 1007 would have been easily accessible to a POSITA by navigating to www.assurent.com in a web browser, selecting the “PRODUCT” heading to bring up the product categories sidebar, and then selecting the “Vulnerability Data” product category. Ex. 1007, 5. Ex. 1003 ¶ 94 n. 4.

vulnerabilities in products and networking devices”). It would have been obvious to a POSITA that the threat data 310 provided by Assurent’s VRS service, which provides “[s]ubscription feeds for security product vendors ... which provide near real-time coverage for the most severe security vulnerabilities in ... networking devices,” would have included one or more network addresses, such as IP addresses, associated with malicious network traffic. Ex. 1007, 5. Ex. 1003 ¶ 94.

In addition, as further explained below, it would have been obvious to a POSITA that the “threat data 310” created by “monitoring, defining, and analyzing potential and known threats to the security of the process control network(s) 150” would have included threats such as network addresses (e.g., IP addresses) that the sources 315, such as Assurent’s VRS service, Secunia, and Carnegie Mellon, determined to be associated with malicious traffic. *Id.* ¶ 95. Accordingly, any of the sources 315, including the identified threat-provider services from Assurent, Secunia, and Carnegie Mellon, correspond to a third party malicious host tracker service. *Id.*

As explained above, Law discloses that cyber security risk management firm 305 generates its rulesets, including ruleset 147, by aggregating threat data and other malicious traffic information received from the sources 315. Ex. 1005 ¶ 88 (“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”); *id.* ¶ 92 (explaining that the “threat data 310” from the sources 315 “**may be aggregated**”). In addition, a POSITA would have understood that threat data 310, which includes information on potential and known threats, would have included malicious traffic information. *Id.*; *see also id.* ¶ 52 (the “rulesets,” which Law explains are created using the threat data 310, includes rules that “inspect and drop **malicious packets** from the network before the malicious packets can reach their intended destination”); *id.* ¶ 91 (“Each of the rulesets 147, 148, 151, 153 may define conditions that, if detected, ... block[] suspected **malicious communications**”); Ex. 1003 ¶ 96. Accordingly, Law discloses that cyber security risk management firm 305 creates or alters its rulesets based on aggregated malicious traffic information.

To the extent that the claim language is interpreted to require that the malicious traffic information must be aggregated by one of the third party malicious host tracker services, Law discloses that subject matter or renders it obvious. *Id.* ¶ 97. In particular, a POSITA would have understood that Law’s disclosure that sources 315 create the “threat data 310” by “monitoring, defining, and analyzing potential and known threats” refers to the sources 315 aggregating the analyzed information on the potential and known threats. Ex. 1005 ¶ 92; Ex. 1003 ¶ 97. In addition, in view of Law’s disclosure that the threat data from sources 315 “may be aggregated,” it would have been obvious to a POSITA that

such aggregation also may have been performed by the sources 315. *Id.* Moreover, a POSITA would have understood that Assurent’s “Vulnerability Research Service (VRS),” which Law identifies as a source of threat data 310, was a service that aggregates information associated with malicious network traffic. *Id.*

Lastly, a POSITA would have understood that the “threat data 310” created by “monitoring, defining, and **analyzing potential and known threats to the security of** the process control **network(s) 150**” would have included network addresses (e.g., IP addresses) that the sources 315 such as Assurent, Secunia, and Carnegie Mellon determined to be associated with malicious traffic, as a POSITA would have understood malicious IP addresses to be a primary potential and known threat to the security of any network. Ex. 1005 ¶ 92; Ex. 1003 ¶ 98. To the extent not explicitly disclosed by Law, it would have been obvious to a POSITA in view of Law’s disclosure to include IP addresses determined to be associated with malicious traffic among the potential and known network security threats provided by sources 315, for several reasons. Ex. 1003 ¶ 98. First, Law discloses that the created rulesets are intended to block malicious traffic, including based on IP address. Ex. 1005 ¶ 52 (the “rulesets,” which Law explains are created using the threat data 310, includes rules that “inspect and drop **malicious packets** from the network before the malicious packets can reach their intended destination”); *id.* ¶ 91 (“Each of the rulesets 147, 148, 151, 153 may define conditions that, if

detected, ... block[] suspected **malicious communications**”); *id.* ¶ 11 (explaining generally that “rulesets define various restrictions on network communication based on IP addresses”). Given Law’s intention to block malicious traffic, and recognition of the need for rules to restrict network communication based on IP addresses, it would have been obvious to a POSITA that threat data 310 should include IP addresses determined to be associated with malicious traffic. Ex. 1003 ¶ 98. Second, as explained above in [1.2], Law discloses that the created rulesets include “from-address column 1304” for specifying “one or more ... IP addresses,” which, if satisfied, cause an action 1310 to be performed on a packet, including blocking the packet, and that the created rulesets are intended to “monitor and/or protect ... from unwanted access and/or malicious attack.” Ex. 1005 ¶¶ 102-103; *id.*, Fig. 13; Ex. 1003 ¶ 98. Accordingly, it would have been obvious to a POSITA that the ruleset 147 created by cyber security risk management firm 305 using aggregated threat data 310 from sources 315 would have included rules that utilize the functionality provided by Law’s rule tables to block packets based on IP addresses in order to protect the network 150 from malicious communications. Ex. 1003 ¶ 98.

Accordingly, Law discloses or renders obvious element [1.3].

(C) [1.4] “*performing ... packet filtering on a first portion of packets ...*”

As explained above in [1.0]-[1.2], Law discloses that perimeter UTMS firewalls 146a and 146b perform, on a packet by packet basis, packet filtering on a first portion of packets corresponding to network traffic traversing the boundary via UTMS firewalls 146a and 146b based on a first set of packet filtering rules (ruleset 147) by performing at least one packet transformation specified by at least one of the packet filtering rules in ruleset 147 (action column 1310, including actions such as block, accept, re-route, and notify) on the first portion of packets. *See, e.g.*, Ex. 1005 ¶¶ 52, 59, 91, 102-103; *id.* Figs. 1A, 3, 13; Ex. 1003 ¶ 100.

For example, Law discloses that perimeter UTMS firewalls 146a and 146b enforce rulesets, such as ruleset 147, to perform the packet transformation function (e.g., blocking packets) when the packet-matching criteria is satisfied. Ex. 1005 ¶ 52 (“UTMS-configured firewall 146a, 146b ... use one or more rulesets to inspect and drop malicious packets from the network before the malicious packets can reach their intended destination”); Ex. 1005 ¶ 91 (“Each 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”); Ex. 1005 ¶ 103 (“[E]ach row of the example table 1300 enforces a rule if a corresponding row selector is active, as shown by an example row selection column 1324”); *id.*

(“While the example first rule 1326 identifies an action of ‘accept,’ other actions may include, but are not limited to, block, notify, and/or re-route.”).

As explained above in [1.2], a POSITA would have understood that perimeter UTMS firewalls 146a and 146b apply ruleset 147 to all network traversing the boundary between network 150 (including LANs 150a and 150b) and Internet 155 via firewalls 146a and/or 146b, and hence necessarily would have applied ruleset 147 on a packet-by-packet basis. Ex. 1005, Figs. 1A, 3; *id.* ¶¶ 51, 59, 102-103; Ex. 1003 ¶ 102.

Accordingly, Law discloses or renders obvious element [1.4].

(D) [1.5] “*receiving, ... an updated second set of packet filtering rules ...*”

As explained above at [1.1], Law discloses that perimeter UTMS firewalls 146a and 146b receive from cyber security risk management firm 305 a dynamic security policy comprising a first set of packet filtering rules, ruleset 147. *See* Ex. 1005 ¶¶ 22, 51-52, 59, 66, 88, 91-92, 102-103; *id.*, Figs. 1A, 3, 13; Ex. 1003 ¶ 104. In addition, as explained above at [1.3], the ruleset 147 includes one or more rules created or altered by cyber security risk management firm 305 based on aggregated malicious traffic information (threat data 310) received from at least one third party malicious host tracker service (sources 315, including threat-provider services from Assurent, Secunia, and Carnegie Mellon). *See* Ex. 1005 ¶¶ 52, 83, 88-89, 91-92, Figs. 1A, 3, 13; Ex. 1003 ¶ 104.

Law discloses or renders obvious that perimeter UTMS firewalls 146a and 146b receive a second, updated ruleset from cyber security risk management firm 305 that comprises an update to the one or more packet filtering rules in first ruleset 147 created or altered by the cyber security risk management firm 305 based on updated malicious traffic information received from at least one of the sources 315, including threat-provider services from Assurent, Secunia, and Carnegie Mellon. Ex. 1003 ¶ 105.

For example, Law discloses that the UTMS firewalls continue to communicate with “a perpetual service” (cyber security risk management firm 305) in order to receive “updates” to the “rulesets” in order “to meet the latest security threats, threat patterns, and control system vulnerabilities found to exist within the network.” *Id.*; Ex. 1005 ¶ 22; *id.*, Abstract. Similarly, Law describes Fig. 3, which illustrates firewalls 146a and 146b in communication with cyber security risk management firm 305 over Internet 155, as disclosing a “block diagram of a method to **update rulesets** of the UTMS.” *Id.* ¶ 30. Law discloses updating ruleset 147 both “automatically” as well as by alerting an operator to perform a “manual update.” *Id.* ¶ 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.”). Likewise, Law discloses that the “update[s]” to ruleset 147

provided by cyber security risk management firm 305 to UTMS-configured

firewalls 146a and 146b may be provided “on a periodic or non-periodic basis via any desired communication link to ... cyber security risk management firm 305.”

Id. ¶ 66. Furthermore, in connection with cyber security risk management firm 305’s construction of rulesets 147, validation of the rulesets, and verification and distribution of the rulesets, Law discloses that “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.* ¶ 88; *see also id.* ¶ 89 (“Each of these known vulnerabilities may then be translated” by cyber security risk management firm 305 “into mitigations or rules for the various rulesets 147, 148, 151, 153, and **the firm 305 may provide an ongoing remediation update service to the system 100 in the form of UTMS-device updates.**”).

Accordingly, Law discloses or renders obvious element [1.5].

(E) [1.6] “*performing, ... packet filtering on a second portion of the packets ...*”

As explained above in [1.5], Law discloses receiving an updated second set of packet filtering rules. Ex. 1005 ¶¶ 66, 83, and 88-89.

For the same reasons as explained above in [1.4], Law discloses or renders obvious that firewalls 146a and 146b would continue to perform packet filtering on a second portion of the packets corresponding to network traffic traversing the

boundary via firewalls 146a/146b based on the updated second set of packet filtering rules (updated ruleset 147) by continuing to perform at least one packet transformation specified by at least one of the packet filtering rules in updated ruleset 147 (action column 1310, including actions such as block, accept, re-route, and notify) on the second portion of packets. *See, e.g.*, Ex. 1005 ¶¶ 52, 59, 66, 83, 88-89, 91, 102-103; *id.* Figs. 1A, 3, 13; Ex. 1003 ¶ 109.

In particular, Law discloses that “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.**” Ex. 1005 ¶ 88. Because the updates to rulesets 147 are required to remain effective against network threats, a POSITA would have understood that Law would have continued to enforce and perform packet filtering using the updated rulesets 147 in the same way that Law would have enforced and performed packet filtering using rulesets 147 prior to any updated, as described above in [1.4], as doing so would have been necessary to protect the network against threats. Ex. 1003 ¶ 110; Ex. 1005 ¶ 103; *id.* ¶ 52.

Accordingly, Law discloses or renders obvious element [1.6].

2. Claim 8

(A) [8.0] “*A packet security gateway ...*”

See analysis at [1.0].

(B) [8.1] “*one or more processors; and*”

As explained above in [1.0], perimeter UTMS firewalls 146a and 146b correspond to “packet security gateways.” Law discloses that UTMS firewalls 146a and 146b may comprise one or more processors. Ex. 1005 ¶ 117 (“[T]he UTMS devices and routines described herein are preferably implemented in software ... Thus, the methods described herein may be implemented in a standard multi purpose CPU”).

(C) [8.2] “*memory ...*”

Law discloses that “[w]hen implemented in software, the software” that is “implemented in a standard multi purpose CPU” on perimeter UTMS firewalls 146a and 146b “may be stored in any computer readable memory.” Ex. 1005 ¶ 117; Ex. 1003 ¶ 114. A POSITA would have understood that the software that implements the functionality of perimeter UTMS firewalls 146a and 146b described by Law necessarily would have included instructions that, when executed by the “standard multi purpose CPU,” causes the perimeter UTMS firewalls 146a and 146b to perform the functionality described by Law. *Id.*

(D) [8.3] “*receive ...*”

See analysis at [1.1].

(E) [8.4] “*each packet filtering rule ...*”

See analysis at [1.2].

(F) [8.5] “*one or more first packet filtering rules ...*”

See analysis at [1.3].

(G) [8.6] “*perform ... packet filtering on a first portion of packets*”

See analysis at [1.4].

(H) [8.7] “*receive ... an updated second set of packet filtering rules*”

See analysis at [1.5].

(I) [8.8] “*perform ... packet filtering on a second portion of the packets*”

See analysis at [1.6].

3. Claim 15

(A) [15.0] “*One or more non-transitory computer readable media ...*”

See analysis at [1.0].

In addition, Law discloses that “[w]hen implemented in software, the software” that is “implemented in a standard multi purpose CPU” on perimeter UTMS firewalls 146a and 146b “may be stored in any computer readable memory.” Ex. 1005 ¶ 117; Ex. 1003 ¶ 122. A POSITA would have understood that the software that implements the functionality of perimeter UTMS firewalls 146a and 146b described by Law necessarily would have included instructions stored with the software in the computer readable memory. *Id.* In addition, a POSITA

would have understood that those instructions, when executed by the “standard multi purpose CPU,” would have caused the perimeter UTMS firewalls 146a and 146b to perform the functionality described by Law. *Id.*

(B) [15.1] “*receiving ...*”

See analysis at [1.1].

(C) [15.2] “*each packet filtering rule ...*

See analysis at [1.2].

(D) [15.3] “*one or more first packet filtering rules ...*”

See analysis at [1.3].

(E) [15.4] “*performing ... packet filtering on a first portion of packets*”

See analysis at [1.4].

(F) [15.5] “*receiving ... an updated second set of packet filtering rules*”

See analysis at [1.5].

(G) [15.6] “*performing ... packet filtering on a second portion of the packets*”

See analysis at [1.6].

4. Claim 21

(A) [21.0] “*A method of filtering packets ...*”

For the reasons described above at [1.0] and [1.1], Law discloses or renders obvious the preamble of claim 21, which recites a subset of the subject matter recited by elements [1.0] and [1.1]. Ex. 1005 ¶¶ 10-11, 22, 51, 55, 88, 91-92; *id.*, Figs. 1A, 3; Ex. 1003 ¶ 129.

(B) [21.1] “*receiving ...*”

See analysis at [1.1].

(C) [21.2] “*wherein each ...*”

See analysis at [1.2].

(D) [21.3] “*wherein one or more first packet filtering rules ...;*”

See analysis at [1.3].

(E) [21.4] “*performing ... packet filtering on a first portion of packets*”

See analysis at [1.4].

(F) [21.5] “*receiving ... an updated second set of packet filtering rules*”

See analysis at [1.5].

(G) [21.6] “*performing ... packet filtering on a second portion of the packets*”

See analysis at [1.6].

C. Dependent Claims

1. Claims 2, 9, 16, 22

As explained above in [1.2], Law discloses or renders obvious that each packet filtering rule in ruleset 147 includes packet matching criteria that includes a from-address column 1304 and to-address column 1306, each of which may identify one or more network addresses, such as IP addresses. Ex. 1005 ¶¶ 102-103; *id.*, Fig. 13; Ex. 1003 ¶ 137.

In addition, for the same reasons as explained above in [1.3], Law discloses or renders obvious that one or more packet filtering rules in ruleset 147 that was automatically created or altered by cyber security risk management firm 305 would have comprised packet matching criteria corresponding to the one or more network addresses, including network addresses determined by at least one of the sources 315 (such as Assurent, Secunia, and/or Carnegie Mellon) to be associated with malicious traffic. Ex. 1005 ¶¶ 88, 91-92, 102-104; *id.*, Figs. 3, 13; Ex. 1003 ¶ 138.

For example, in order to block communications with one or more IP addresses determined to be associated with malicious network traffic, a POSITA would have known to include those IP addresses in the from-address column 1304 and/or to-address column 1306 of any rule, with the action column 1310 set to “block.” Ex. 1003 ¶ 139; *see also id.* ¶ 52 (the “rulesets,” which Law explains are created using the threat data 310, includes rules that “**inspect and drop malicious**

packets from the network before the malicious packets can reach their intended destination”); *id.* ¶ 91 (“Each of the rulesets 147, 148, 151, 153 may **define conditions** that, if detected, ... **block[] suspected malicious communications**”).

2. Claims 3, 10, 17 and 23

Law discloses or renders obvious the subject matter of claims 3, 10, and 23 for the same reasons as presented in [1.3]. For example, as explained in [1.3], any of the sources 315, which provide threat data 310, and including Assurent, Secunia, and Carnegie Mellon, correspond to a third party malicious host tracker service. *See, e.g.*, Ex. 1005 ¶¶ 88, 92. It would have been obvious to a POSITA that the services in providing threat data 310 offered by these third parties may have been offered as a subscription service. Ex. 1003 ¶ 141. For example, as explained above at [1.5], Law discloses that the rulesets “require updates to remain effective against network threats,” and that the firm 305 may provide such updates as part of “an ongoing remediation update service.” Ex. 1005 ¶¶ 88-89. In addition, a POSITA would have recognized that Assurent Secure Technologies and Secunia were cybersecurity firms, and it would have been obvious to a POSITA that the threat data 310 provided by these cybersecurity firms would have been offered as a subscription service. *Id.* Furthermore, with respect to Assurent, Law provides an example of such a subscription service—“the **Vulnerability Research Service (VRS)** of Assurent Secure Technologies.” Ex. 1005 ¶ 92. A POSITA would have

understood that the Vulnerability Research Service (VRS) provided by Assurent is a subscription service. Ex. 1003 ¶ 141; Ex. 1007, 5 (“Assurent’s principal Vulnerability Research offerings include: **Vulnerability Research Subscription feeds for security product vendors ... provide near real-time coverage for the most severe security vulnerabilities in software products and networking devices**”).

In addition, for the same reasons as explained in [1.3], it would have been obvious to a POSITA that any of the sources 315 that provide threat data 310 would have generated that threat data 310 by aggregating information associated with malicious network traffic. *Id.* ¶ 142. In particular, a POSITA would have understood that Law’s disclosure that sources 315 create the “threat data 310” by “monitoring, defining, and analyzing potential and known threats” refers to the sources 315 aggregating the analyzed information on the potential and known threats. Ex. 1005 ¶ 92; Ex. 1003 ¶ 142. In addition, in view of Law’s disclosure that the threat data from sources 315 “may be aggregated,” it would have been obvious to a POSITA that such aggregation may have been performed by the sources 315. *Id.* In addition, a POSITA would have understood that Assurent’s “Vulnerability Research Service (VRS)” was a service that aggregates information associated with malicious network traffic. *Id.*; Ex. 1007, 5 (“Assurent’s principal Vulnerability Research offerings include: **Vulnerability Research Subscription**

feeds for security product vendors, for managed service providers, and for enterprise security teams, which provide **near real-time coverage for the most severe security vulnerabilities in** software products and **networking devices**”).

3. Claims 4, 11 and 24

For the same reasons as explained above in [1.3], Law discloses or renders obvious that sources 315 provide threat data 310 that would have included one or more network addresses, such as IP addresses, associated with malicious network traffic. As explained above with respect to claims 3, 10, 17, and 23, Law discloses or renders obvious that sources 315 may correspond to a subscription service.

Accordingly, Law discloses or renders obvious the subject matter of claims 4, 11, and 24. Ex. 1005 ¶ 92; Ex. 1003 ¶¶ 143-145.

4. Claims 5, 12, 18 and 25

As explained above in [1.2] and [1.4], Law discloses a packet transformation function that includes a blocking action, which comprises a network protective action. *See, e.g.*, Ex. 1005 ¶ 91 (“Each of the rulesets ... may ... **block**[] suspected malicious communications”); *id.* ¶ 102 (“The perimeter UTMS-configured devices 146 ... may include any number of additional rule tables to monitor and/or **protect** a control system 100 from unwanted access and/or malicious attack.”); Ex. 1003 ¶ 147.

5. Claims 6, 13, 19, and 26

(A) [6.1], [13.1], [19.1], and [26.1]

Law discloses or renders obvious receiving packets at firewalls 146a and 146b using an interface that is not addressed at the network layer. For example, Law discloses that “[t]he network 150 and devices may also ... support[] **any communications protocol**,” which a POSITA would have understood includes communication protocols using an interface that is not addressed at the network layer. Ex. 1005 ¶ 55; Ex. 1003 ¶ 148. In addition, while Law discloses addressing schemes at the network layer (e.g., by using IP addresses), Law also discloses other addressing schemes, such as hardware-specific addressing, which a POSITA would have understood may not have been at the network layer. Ex. 1005 ¶ 103 (“While the example rule in the first row 1326 employs IP version 4 addresses, **any addressing scheme may be employed including**, but not limited to, IP version 6, **hardware specific addressing (e.g., GPIB device addresses)**”); Ex. 1003 ¶ 148. Accordingly, it would have been obvious to a POSITA that firewalls 146a and 146b may have received packets using an interface addressed using hardware-specific addressing. *Id.*

(B) [6.2], [13.2], [19.2], and [26.2]

As explained above with respect to [6.1], Law discloses support for any communication protocol and any addressing scheme. Ex. 1005 ¶¶ 55, 103. As explained above at [1.4], Law discloses or renders obvious that perimeter UTMS

firewalls 146a and 146b perform packet filtering on a first portion of packets based on a first set of packet filtering rules (ruleset 147) by performing at least one packet transformation specified by at least one of the packet filtering rules in ruleset 147 (action column 1310, including actions such as block, accept, re-route, and notify) on the first portion of packets. *See, e.g.*, Ex. 1005 ¶¶ 52, 59, 91, 102-103; *id.* Figs. 1A, 3, 13; Ex. 1003 ¶ 150.

For the same reasons as explained above at [1.4], a POSITA would have understood that Law discloses performing blocking actions on packets at the network layer. *Id.* For example, Law discloses that the conditions used to identify packets to block include “from-address column 1304” and “to-address column 1306,” which may include “IP Addresses,” which a POSITA would have recognized as identifying packets at the network layer. Ex. 1005 ¶¶ 102-103, Fig. 13; *id.*, ¶ 104 (providing example of applying rules to packets matching IP-address conditions); Ex. 1003 ¶ 151.

6. Claims 7, 14, 20 and 27

For the same reasons as described above in [1.2], Law discloses the subject matter of claims 7, 14, 20, and 27. For example, Law discloses that operations performed on packets include, in addition to forwarding and blocking, other operations that “notify” and “re-route.” Ex. 1005 ¶ 103. A POSITA would have understood that an “accept” action refers to forwarding a packet to its intended

destination. *Id.* In addition, a POSITA would have understood that a “re-route” action refers to forwarding a packet to a different location than the destination location specified by the packet header. Ex. 1003 ¶ 153.

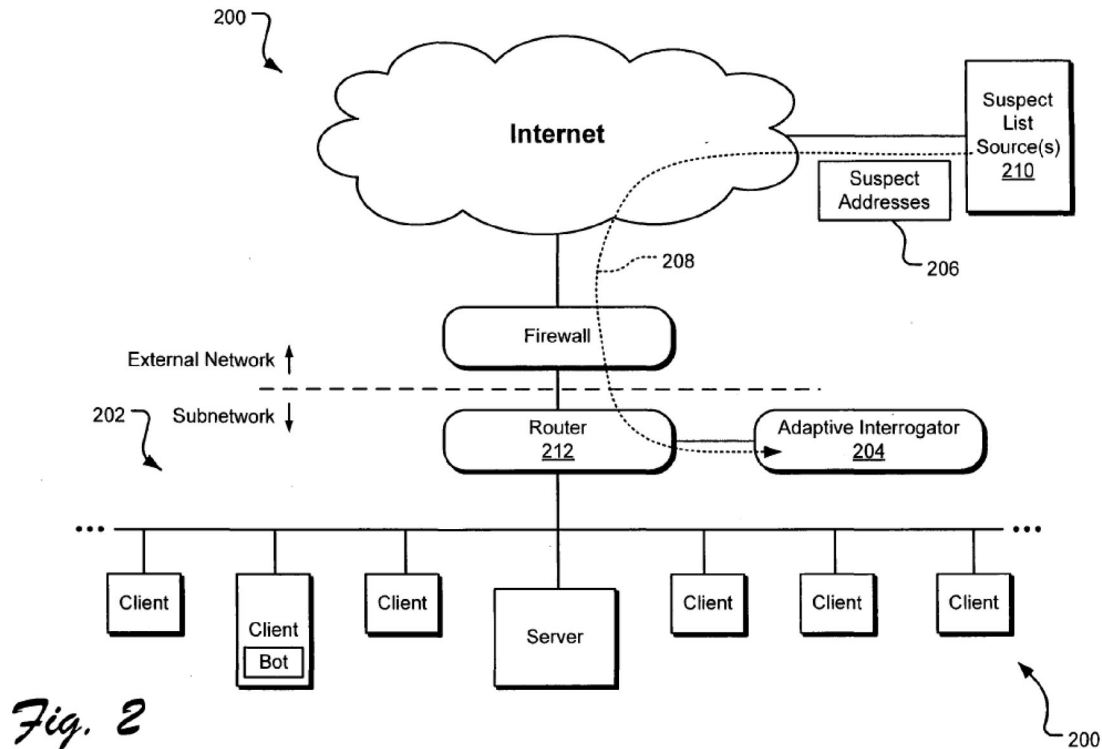
VIII. GROUND 2: LAW IN VIEW OF WOOD RENDERS OBVIOUS CLAIMS 1-24

A. Overview of Wood

Recognizing that “[m]odern computer systems are under constant threat of security breaches,” Wood discloses an “adaptive system” that “receives suspect traffic information pertaining to possible network threats.” Ex. 1006 ¶¶ 3, 7. In particular, Wood recognizes that “a great number of [] external network addresses ... fall into a category of suspect addresses” and discloses maintaining a “suspect address list” of such suspect network addresses. *Id.* ¶ 29. For example, Wood discloses that “**IP addresses of known threats** (e.g., a known hacker, a known phisher, a known pharmer, a known command and control node, etc.) **can be added to the suspect address list.**” *Id.*

Wood discloses that “[a] router can ... be configured to handle specific network packets in a predefined way. For example, incoming packets from certain addresses can be redirected to a null address, effectively blocking the packet traffic.” *Id.* ¶ 21. In addition, Wood discloses an “adaptive interrogation module” that “**may receive a feed of suspect addresses from one or more sources on the external network.**” *Id.* ¶ 21. For example, as shown below in Fig. 2, “an

exemplary adaptive interrogation module 204 ... receiv[es] suspect addresses 206 over communications 208,” “[t]he suspect addresses 206 [being] received from one or more suspect address sources 210”:



Ex. 1006, Fig. 2; *id.* ¶ 32. Using the suspect addresses 206, the adaptive interrogation module 204 configures or reconfigures a router 212 to redirect potentially malicious traffic associated with the suspect addresses, for example, to a null address to effectively block the traffic. Ex. 1006 ¶¶ 21, 32, 34; Ex. 1003 ¶ 155.

In addition, Wood recognizes that the suspect address list should be updated to quickly provide notice of possible threats. Ex. 1006 ¶ 34 (“[T]he suspect addresses 206 are updated as any one of the suspect address sources 210 receives a

change to its suspect address data By quickly updating the suspect addresses 206, the suspect address sources 210 can provide the most up-to-date notice of possible threats.”). Law discloses reconfiguring the router with each updated suspect address list. *Id.* ¶ 36 (“With each suspect address update (or some frequency), the adaptive interrogation module 304 reconfigures the router 306 with a new set of suspect addresses,” thereby “adapt[ing] to the changes in threats from the external network 300”).

B. A POSITA Would Have Considered Wood In Conjunction With Law

In view of Law’s disclosure that “**cyber security risk management firm 305 ... collect[s] 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; *id.*, Fig. 3), and in view of Wood’s disclosure of “one or more suspect address sources 210” providing a “a feed of suspect addresses from one or more sources on the external network” for configuring a router to drop potentially malicious traffic associated with the suspect addresses (Ex. 1006 ¶¶ 21, 32, 34; *id.*, Fig. 2), a POSITA would have been motivated to use Wood’s feed of suspect addresses as another source 315 among the plurality of sources 315 that provide threat data 310 used construct the rulesets 147 distributed to the UTMS-configured firewalls 146a, 146b. Ex. 1003 ¶ 157.

Both Law and Wood are in the same field of endeavor and analogous art to the '266 Patent, namely, network security and protection from malicious traffic.

Ex. 1005 ¶¶ 52, 88, 91, 102; Ex. 1006 ¶¶ 2, 30-34; Ex. 1001, 1:59-2:34; Ex. 1003 ¶ 158.

A POSITA would have been motivated to combine the teachings of Law and Wood because doing so would have produced predictable beneficial results, including enhancing threat protection. Ex. 1003 ¶ 159. Specifically, Law discloses that cyber security risk management firm 305 collects threat data 310 from a plurality of various sources for constructing rulesets. Ex. 1005 ¶ 88. Law provides three examples of such sources 315 of threat data 310 (*id.* ¶ 92), though a POSITA would have recognized that it would have been desirable to obtain threat data from additional sources to obtain even broader coverage of threat data, as shown by Fig. 3, which shows six sources 315 providing threat data 310 to firm 305. *Id.*, Fig. 3; Ex. 1003 ¶ 159. A POSITA would have recognized the suitability of Wood's "suspect address sources 210" as another such source among Law's plurality of various sources 315. Ex. 1006 ¶ 32; Ex. 1003 ¶ 159. For example, a POSITA would have recognized that Wood's feed of suspect addresses 206 provided by suspect address source 210 corresponds to an example of Law's threat data 310. *Id.* In addition, Wood discloses communicating its feed of suspect addresses 206 over the Internet, as shown in Fig. 2, so a POSITA would have understood that the

system of Law would not have required any modification for Law's security risk management firm 305 to also receive threat data over the Internet from Wood's suspect address source 210. *Id.*

C. Claims 1-24

As explained above in VII.B.1.B regarding element [1.3], Law discloses or renders obvious that aggregated malicious traffic information received from at least one third party malicious host tracker service comprises network addresses that the at least one third party malicious host tracker service determined to be associated with malicious network traffic.

To the extent this element is not disclosed or rendered obvious in view of Law alone, the combined system of Law and Woods renders obvious this element. Ex. 1003 ¶ 161. For example, Wood's "one or more suspect address sources 210" that provide a list of suspect addresses 206 corresponds to the at least one third party malicious host tracker service. Ex. 1006 ¶ 32; *id.*, Fig. 2. Furthermore, given Wood's disclosure of "one or more suspect address sources 210," a POSITA would have understood that the provided list of suspect addresses 206 includes aggregated malicious traffic information that includes several network addresses determined by the one or more suspect address sources 210 to be associated with malicious network traffic. *Id.* ¶¶ 21, 39 32. Accordingly, the combined system of Law and Wood also renders obvious the subject matter of claims 3-4, 10-11, 17, and 23-24.

In addition, Wood recognizes that the suspect address list should be updated to quickly to provide notice of possible threats. Ex. 1006 ¶¶ 34, 36. Upon receipt of an updated suspect address list by Law's firm 305, it would have been obvious to a POSITA that the firm 305 would have created updated rulesets to reflect the information in the suspect address list, including adding blocking rules for packets matching IP addresses in the updated suspect address list. Ex. 1005 ¶ 88; Ex. 1003 ¶ 162. Accordingly, the combined system of Law and Woods also renders obvious claims 2, 9, 16, and 23.

IX. GROUND 3: LAW IN VIEW OF JUNGCK RENDER OBVIOUS CLAIMS 6, 13, 19 AND 26

A. Overview of Jungck

Jungck was published on October 22, 2009, and thus constitutes prior art to the claims of the '266 Patent under 35 U.S.C. § 102(b).

Like Law, Jungck is directed to filtering packets at a network interface. For example, Jungck discloses that edge servers intercept "all network traffic" including "packets 704," via "network interface 710" and "packet analyzer 712" before the packets are "sent along to their intended destination." Ex. 1008 ¶¶ 107, 130, 152.

B. A POSITA Would Have Considered Jungck In Conjunction With Law

A POSITA would also have been motivated to combine Law's and Jungck's teachings. EX1003 ¶ 165. Law and Jungck are analogous prior art in the same field

of endeavor. Both references are directed to packet filtering techniques to prevent attacks in a network environment. Ex. 1005 ¶¶ 11, 59, 90-92, 102; Ex. 1008 ¶¶ 25, 111, 182-183, and 282.

Jungck teaches using “a list of blocked IP addresses” for addressing attacks. Ex. 1008 ¶ 176. Law teaches aggregating threat information 310 from a plurality of various sources 315. Ex. 1005 ¶¶ 88, 92. Thus, as a matter of design choice, a POSITA would have been motivated to combine Law’s and Jungck’s teachings, including incorporating Jungck’s list of blocked IP addresses as another source into received threat data 310 used to construct Law’s rulesets, because doing so would have produced predictable beneficial results, including enhancing threat protection, with predictable success. Ex. 1003 ¶ 166.

C. Claims 6, 13, 19, and 26

The combined system of Law and Jungck renders obvious receiving packets at Law’s perimeter UTMS firewalls 146a and 146b in a network layer transparent manner using an interface that is not addressed at the network layer. For example, Jungck discloses receiving, by a packet security gateway (e.g., “edge server”), packets in a network layer transparent manner (e.g., “selectively transparent to the network”) using an interface (e.g., “network interface 710”) that is not addressed at the network layer (e.g., “edge server...needs no address”). *See, e.g.*, Ex. 1008 ¶¶ 98, 126, 130.

Given Law's disclosure of supporting any communications protocol and any addressing scheme, a POSITA would have understood how to modify Law's perimeter UTMS firewalls 146a and 146b to support Jungck's communications protocol of communication in a manner selectively transparent to the network using a network interface that needs no address. Ex. 1003 ¶ 168.

X. GROUND 4: LAW IN VIEW OF WOOD AND JUNGCK RENDERS OBVIOUS CLAIMS 6, 13, 19, AND 28

A POSITA would have been motivated to combine Wood with Law and Jungck with Law for the reasons explained above in VIII.B and IX.B, respectively. For the same reasons, a POSITA would have been motivated to combine both Wood and Jungck with Law, including for the reason that both Wood and Jungck disclose providing threat information 310, and Law discloses receiving threat information 310 from a plurality of various sources 315. Ex. 1003 ¶ 169.

As explained above in VIII.C, to the extent element [1.3] is not disclosed or rendered obvious in view of Law alone, the combined system of Law and Woods renders obvious this element. *Id.* ¶ 170.

Likewise, as explained above in IX.C, to the extent claims 6, 13, 19, and 26 are not disclosed or rendered obvious in view of Law alone, the combined system of Law and Jungck renders obvious these claims. *Id.* ¶ 171.

Accordingly, the combined system of Law, Woods, and Jungck also renders obvious claims 6, 13, 19, and 26. *Id.* ¶ 172.

XI. CONCLUSION

Petitioner respectfully requests that a Trial be instituted and that the Challenged Claims of the '266 Patent be canceled as unpatentable.

Attached hereto or included herewith are Powers of Attorney, an Exhibit List, and copies of the references per 37 C.F.R. §§ 42.10(b), 42.63(e), and 42.6(c). Petitioner paid the requisite fee via Deposit Account. The Office is authorized to charge fee deficiencies and credit overpayments to Deposit Account No. 18-0586.

Respectfully submitted,

Date: January 6, 2023

/s/ Jonathan I. Detrixhe
Jonathan I. Detrixhe
Reg. No. 68,556
Counsel for Petitioner

CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. § 42.24(a) and (d), Petitioner hereby certifies, in accordance with and reliance on the word count provided by the word-processing system used to prepare this Petition, that the number of words in this paper is 13,983. Pursuant to 37 C.F.R. §42.24(a), this word count excludes the table of contents, table of authorities, mandatory notices under §42.8, certificate of service, certificate of word count, appendix of exhibits, and any claim listing.

Respectfully submitted,

Date: January 6, 2023

/s/ Jonathan I. Detrixhe
Jonathan I. Detrixhe
Reg. No. 68,556
Counsel for Petitioner

CERTIFICATE OF SERVICE

In accordance with 37 C.F.R. §§ 42.6(e) and 42.105, the undersigned certifies that the foregoing PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 10,785,266, including its supporting exhibits and Power of Attorney, were served on January 6, 2023 via Priority Mail Express, or by means at least as fast and reliable as Priority Mail Express, upon the following correspondence address of record for the subject patent:

BANNER & WITCOFF, LTD.
1100 13TH Street, N.W.
Suite 1200
Washington, D.C., 20005-4051

Date: January 6, 2023

/s/ Jonathan I. Detrixhe
Jonathan I. Detrixhe
Reg. No. 68,556
Counsel for Petitioner