

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. 11,012,474

DECLARATION OF DOUG W. JACOBSON, PH.D

TABLE OF CONTENTS

I.	INTRODUCTION	5
A.	Engagement	5
B.	Compensation	6
C.	Qualifications and Experience	6
D.	Information Considered And Relied Upon	9
II.	LEGAL STANDARDS RELATED TO PATENTABILITY	10
A.	My Understanding of Claim Construction	10
B.	My Understanding of Obviousness	12
III.	LEVEL OF ORDINARY SKILL IN THE ART	17
IV.	The '474 Patent	18
A.	Summary of the '474 Patent	18
B.	Prosecution History	20
C.	Effective Filing Date	21
V.	CLAIM INTERPRETATION	21
VI.	SUMMARY OF UNPATENTABILITY ANALYSIS	23
VII.	GROUND 1: LAW IN VIEW OF GOLNABI RENDERS OBVIOUS CLAIMS 1-3, 5-7, 9-11, 13-15, 17-19, 21-23, 25-27, 29-31, 33	24
A.	Overview of Law	24
B.	Overview of Golnabi	28
C.	A POSITA would have considered Golnabi in conjunction with Law	30
D.	Independent Claims	31
1.	Claim 1	31
2.	Claim 9	59
3.	Claim 17	61
4.	Claim 25	63
E.	Dependent Claims	67
1.	Claims 2, 10, 18, 26	67
2.	Claims 3, 11, 19, and 27	68

3.	Claims 5, 13, 21, 29	69
4.	Claims 7, 15, 23, 31	70
VIII.	GROUND 2: LAW IN VIEW OF GOLNABI AND WOOD RENDERS OBVIOUS CLAIMS 2, 10, 18, 26.....	72
A.	Overview of Wood	72
B.	A POSITA Also Would Have Considered Wood In Conjunction With Law	74
C.	Claims 2, 10, 18, 26.....	76
IX.	GROUND 3: LAW IN VIEW OF GOLNABI AND KE RENDERS OBVIOUS CLAIMS 4, 12, 20, 28	77
A.	Overview of Ke	77
A.	A POSITA Also Would Have Considered Ke In Conjunction With Law	78
B.	Claims 4, 12, 20, 28.....	79
1.	[4.0], [12.0], [20.0], [28.0].....	79
2.	[4.1], [12.1], [20.1], [28.1].....	80
3.	[4.2], [12.2], [20.2], [28.2].....	80
X.	GROUND 4: LAW IN VIEW OF GOLNABI AND JUNGCK RENDERS OBVIOUS CLAIMS 5, 13, 21, 29	81
A.	Overview of Jungck.....	81
B.	A POSITA Also Would Have Considered Jungck In Conjunction With Law	81
C.	Claims 5, 13, 21, 29.....	82
XI.	GROUND 5: LAW IN VIEW OF GOLNABI AND JOHNSON RENDERS OBVIOUS CLAIMS 7-8, 15-16, 23-24, and 31-32.....	83
A.	Overview of Johnson.....	83
B.	A POSITA Also Would Have Considered Johnson In Conjunction With Law	83
C.	Claims 7, 15, 23, 31.....	84
D.	Claims 8, 16, 24, 32.....	84
1.	[8.0], [16.0], [24.0], [32.0].....	84
2.	[8.1], [16.1], [24.1], [32.1].....	85

3.	[8.2], [16.2], [24.2], [32.2]	86
4.	[8.3], [16.3], [24.3], [32.3]	86
XII.	CONCLUSION.....	87
	Appendix A – List of Exhibits	90

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

I. INTRODUCTION

A. Engagement

1. I have been retained by counsel for Petitioner Keysight Technologies, Inc. (“Keysight” or “Petitioner”) as an expert witness for the above-captioned *inter partes* review (IPR) proceeding. I have been asked to provide my opinions about the state of the art of the technology described in U.S. Patent No. 11,012,474 (“’474 Patent,” Ex. 1001). Specifically, I have been asked to consider the validity of claims 1-33 of the ’474 Patent (the “Challenged Claims”) in view of prior art, obviousness considerations, and the understanding of a person of ordinary skill in the art at the time of the invention as it relates to the ’474 Patent. I have personal knowledge of the facts and opinions set forth in this declaration and believe them to be true. If called upon to do so, I would testify competently thereto.

2. I understand that Centripetal Networks, Inc. (“Patent Owner” or “P.O.”) purports to own all substantial rights, title, and interest in the ’474 patent and is currently asserting the ’474 patent against Petitioner in concurrent litigation. In particular, I understand that on January 1, 2022, P.O. sued Petitioner in the U.S. District Court for the Eastern District of Virginia. I understand that P.O. alleged infringement of the ’474 patent.

B. Compensation

3. For my time working on this matter, I am being compensated at my standard hourly consulting rate. I do not have any personal or financial stake or interest in the outcome of the present proceeding, and the compensation is not dependent on the outcome of this IPR and in no way affects the substance of my statements in this Declaration. I do not have any expectation or promise of additional business with the Petitioner in exchange for the positions explained herein. My analysis here is based on my years of education, research and experience, as well as my investigation and study of relevant materials, including those cited herein.

C. Qualifications and Experience

4. My qualifications and professional experience are described in my *Curriculum Vitae*, which includes a complete list of my publications, a copy of which I understand is being submitted as Ex. 1004. A summary of my background and experience that qualifies me to offer the opinions offered in this Declaration set forth as an expert in the technical issues in this case are as follows.

5. I am a University Professor in the Department of Electrical and Computer Engineering at Iowa State University and currently hold the Sunil & Sujata Gaitonde Professorship in Cybersecurity. I joined the faculty in 1985 after receiving a PhD degree in Computer Engineering from Iowa State University in

1985. Since 1995 I have taught courses in network security and information warfare.

6. I created the first network security course and information warfare course at Iowa State University. Both courses have taught the concepts of intrusion detection since they were created. I have authored two text books in the area of computer and network security. Both of these courses taught the concepts of intrusion detection and I have been running various forms of intrusion detection systems in my teaching and research lab since 1995.

7. I am the founding director of the Iowa State University Center for Cybersecurity Innovation and Outreach (formally known as “Information Assurance Center”), which has been recognized by the National Security Agency as a charter Center of Academic Excellence for Information Assurance Education. I am also director of the Internet-Scale Event and Attack Generation Environment (ISEAGE) project. I also serve as the executive director of the Iowa Cyber Hub, which is dedicated to creating a statewide cybersecurity ecosystem.

8. My current funded research is targeted at developing robust countermeasures for network-based security exploits and large scale attack simulation environments. A few funded projects have led to patents. I have been PI or Co-PI on over 15 million dollars of security related funding.

9. I am also the founder of Palisade Systems, Inc., an Ames-based company marketing Internet management and security devices. The core technology for Palisade Systems was based on a patent I was co-inventor on.

10. I have given over 150 presentations in the area of computer security and I have testified in front of the U.S. Senate committee of the Judiciary on security issues associated with peer-to-peer networking.

11. I have advised 24 Ph.D. students since 1985, and over 50% had security related topics. I have advised over 300 master's students since 1985 and a majority of the project since 1995 have been security related.

12. Additional information on my qualifications and background is set forth in my curriculum vitae, which is provided in Ex. 1004. A list of publications that I have authored or co-authored is provided in Ex. 1004.

13. I have been retained as an expert witness 4 times in the past 15 years. One engagement (Recording Industry Association of America [RIAA]) was for 5 years. I have been deposed 4 times as an expert witness and have testified in court 4 times in connection with prior expert witness engagements. A listing of each case for which I have testified is provided in Ex. 1004.

14. I have been retained as an expert witness or technical consultant for the following companies: State of Iowa department of Human Services, State of

Iowa Department of Administrative Services, several cities in the state of Iowa,
Iowa Department of Transportation, Attorney General for the State of Iowa.

15. I hold a Secret Clearance through the United States Department of Homeland Security (“DHS”) in order to be able to help the State of Iowa recover from a large scale cyber attack.

D. Information Considered And Relied Upon

16. My opinions in this declaration are based on my years of education, training, research, knowledge, and experience, as well as my investigation and study of relevant materials. In forming my opinions, I have studied the materials listed in Appendix A. I have relied on these materials to varying degrees. Citations to these materials that appear below are meant to be exemplary but not exhaustive.

17. Each of these materials is a type of document that experts in my field would have reasonably relied upon when forming their opinions and would have had access to either through the applicable patent office and/or well-known libraries, conferences, publications, organizations and websites in the field as further discussed herein.

18. I may rely upon these materials, my knowledge and experience, and/or additional materials to respond to arguments raised by the Patent Owner. I may also consider additional documents and information in forming any necessary opinions — including documents that may not yet have been provided to me.

19. My analysis of the materials produced in this investigation is ongoing and I will continue to review any new material as it is provided. This report represents only those opinions I have formed to date. I reserve the right to revise, supplement, and/or amend my opinions stated herein based on new information and on my continuing analysis of the materials already provided.

II. LEGAL STANDARDS RELATED TO PATENTABILITY

20. I am not a lawyer. In preparing and expressing my opinions in this declaration, I have applied the legal standards described below, which were explained to me by counsel for Petitioner.

A. My Understanding of Claim Construction

21. I have been informed that for purposes of this *Inter Partes* Review, the standard for claim construction is the same as the standard used in federal district court litigation: claim terms should generally be given their ordinary and customary meaning as understood by one of ordinary skill in the art at the time of the invention and after reading the patent and its prosecution history.

22. I have been informed that patent claims are construed from the viewpoint of a person of ordinary skill in the art of the patent at the time of the alleged invention. I have been informed that patent claims generally should be interpreted consistent with their plain and ordinary meaning as understood by a person of ordinary skill in the art in the relevant time period (*i.e.*, at the time of the

purported invention, or the so called “effective filing date” of the patent application), after reviewing the patent claim language, the specification and the prosecution history (*i.e.*, the intrinsic record).

23. I have further been informed that a person of ordinary skill in the art must read the claim terms in the context of the claim itself, as well as in the context of the entire patent specification. I understand that in the specification and prosecution history, the patentee may specifically define a claim term in a way that differs from the plain and ordinary meaning. I understand that the prosecution history of the patent is a record of the proceedings before the U.S. Patent and Trademark Office, and may contain explicit representations or definitions made during prosecution that affect the scope of the patent claims. I understand that an applicant may, during the course of prosecuting the patent application, limit the scope of the claims to overcome prior art or to overcome an examiner’s rejection, by clearly and unambiguously arguing to overcome or distinguish a prior art reference, or to clearly and unambiguously disavow claim coverage.

24. In interpreting the meaning of the claim language, I understand that a person of ordinary skill in the art may also consider “extrinsic” evidence, including expert testimony, inventor testimony, dictionaries, technical treatises, other patents, and scholarly publications. I understand this evidence is considered to ensure that a claim is construed in a way that is consistent with the understanding of those of

skill in the art at the time of the alleged invention. This can be useful for technical terms whose meaning may differ from its ordinary English meaning. I understand that extrinsic evidence may not be relied on if it contradicts or varies the meaning of claim language provided by the intrinsic evidence, particularly if the applicant has explicitly defined a term in the intrinsic record.

B. My Understanding of Obviousness

25. I have been informed that a claim may be unpatentable under (AIA) 35 U.S.C. § 103(a) if the subject matter described by the claim as a whole would have been obvious to a hypothetical person of ordinary skill in the art in view of a prior art reference or in view of a combination of references at the time the claimed invention was made. I have been informed that obviousness is determined from the perspective of a hypothetical person of ordinary skill in the art and that the asserted claims of the patent should be read from the point of view of such a person at the time the claimed invention was made. I have been informed that a hypothetical person of ordinary skill in the art is assumed to know and to have all relevant prior art in the field of endeavor covered by the patent in suit.

26. I have been informed that there are two criteria for determining whether prior art is analogous and thus can be considered prior art: (1) whether the art is from the same field of endeavor, regardless of the problem addressed, and (2) if the art is not within the field of the patentee's endeavor, whether the teachings of

the art are still reasonably pertinent to the particular problem with which the patentee is involved. I have also been informed that the field of endeavor of a patent is not limited to the specific point of novelty, the narrowest possible conception of the field, or the particular focus within a given field. I have also been informed that a prior art reference is reasonably pertinent if, even though it may be in a different field from that of the patentee's endeavor, it is one which, because of the matter with which it deals, logically would have commended itself to a patentee's attention in considering his problem.

27. I have also been informed that an analysis of whether a claimed invention would have been obvious should be considered in light of the scope and content of the prior art, the differences (if any) between the prior art and the claimed invention, and the level of ordinary skill in the pertinent art involved. I have been informed as well that a prior art reference should be viewed as a whole.

28. I have also been informed that in considering whether an invention for a claimed combination would have been obvious, I may assess whether there are apparent reasons to combine known elements in the prior art in the manner claimed in view of interrelated teachings of multiple prior art references, the effects of demands known to the design community or present in the market place, and/or the background knowledge possessed by a person having ordinary skill in the art. I have been informed that other principles may be relied on in evaluating whether a

claimed invention would have been obvious, and that these principles include the following:

- A combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results;
- When a device or technology is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or in a different one, so that if a person of ordinary skill can implement a predictable variation, the variation is likely obvious;
- If a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill;
- An explicit or implicit teaching, suggestion, or motivation to combine two prior art references to form the claimed combination may demonstrate obviousness, but proof of obviousness does not depend on or require showing a teaching, suggestion, or motivation to combine;

- Market demand, rather than scientific literature, can drive design trends and may show obviousness;
- In determining whether the subject matter of a patent claim would have been obvious, neither the particular motivation nor the avowed purpose of the named inventor controls;
- One of the ways in which a patent's subject can be proved obvious is by noting that there existed at the time of invention a known problem for which there was an obvious solution encompassed by the patent's claims;
- Any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed;
- "Common sense" teaches that familiar items may have obvious uses beyond their primary purposes, and in many cases a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of a puzzle;
- A person of ordinary skill in the art is also a person of ordinary creativity, and is not an automaton;
- A patent claim can be proved obvious by showing that the claimed combination of elements was "obvious to try," particularly when

there is a design need or market pressure to solve a problem and
there are a finite number of identified, predictable solutions such
that a person of ordinary skill in the art would have had good
reason to pursue the known options within his or her technical
grasp; and

- One should be cautious of using hindsight in evaluating whether a claimed invention would have been obvious.

29. I have further been informed that, in making a determination as to whether or not the claimed invention would have been obvious to a person of ordinary skill, the Board may consider certain objective factors if they are present, such as: commercial success of products practicing the claimed invention; long-felt but unsolved need; teaching away; unexpected results; copying; and praise by others in the field. These factors are generally referred to as “secondary considerations” or “objective indicia” of nonobviousness. I have been informed, however, that for such objective evidence to be relevant to the obviousness of a claim, there must be a causal relationship (called a “nexus”) between the claim and the evidence, and that this nexus must be based on what is claimed and novel in the claim rather than something in the prior art. I have also been informed that even when they are present, secondary considerations may be unable to overcome

primary evidence of obviousness (e.g., motivation to combine with predictable results) that is sufficiently strong.

III. LEVEL OF ORDINARY SKILL IN THE ART

30. I understand that the level of ordinary skill may be reflected by the prior art of record, and that a person of ordinary skill in the art (“POSITA”) to which the claimed subject matter pertains would have the capability of understanding the scientific and engineering principles applicable to the pertinent art.

31. I understand there are multiple factors relevant to determining the level of ordinary skill in the pertinent art, including (1) the levels of education and experience of persons working in the field at the time of the invention; (2) the sophistication of the technology; (3) the types of problems encountered in the field; and (4) the prior art solutions to those problems.

32. I am familiar with the network computing art that is pertinent to the ’474 Patent. I am also aware of the state of the art at the time the application resulting in the ’474 Patent was filed. I have been informed by counsel to assume that the priority date for the ’474 Patent is April 16, 2014.

33. I understand that in prior IPRs on patents related to the ’474 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. I agree with this determination, and I believe that the same level of ordinary skill in the art should apply in this proceeding. I believe that I possessed at least such experience and knowledge as of the priority date of the '474 Patent, and that I am qualified to opine on the subject matter in the '474 Patent.

34. For purposes of this Declaration, in general, and unless otherwise noted, my statements and opinions, such as those regarding my experience and the understanding of a POSITA generally (and specifically related to the references I consulted herein), reflect the knowledge that existed in the field before the earliest priority date of the '474 Patent.

IV. The '474 Patent

A. Summary of the '474 Patent

35. The '474 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, 4:46-67.

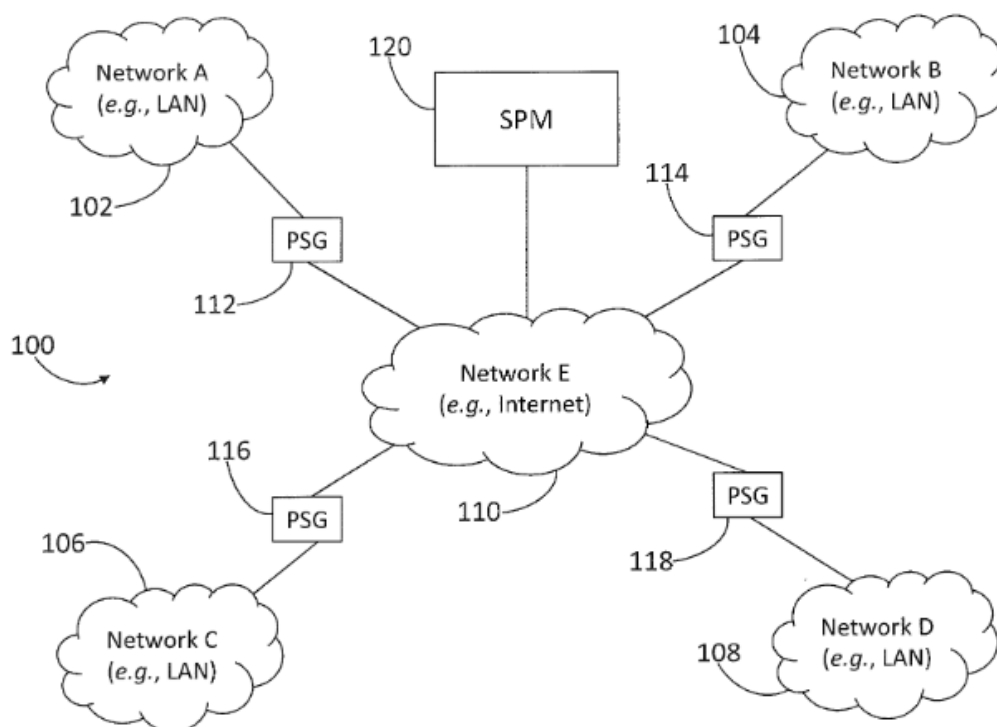


FIG. 1

36. 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, 1:66-2:3, 8:23-34.

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

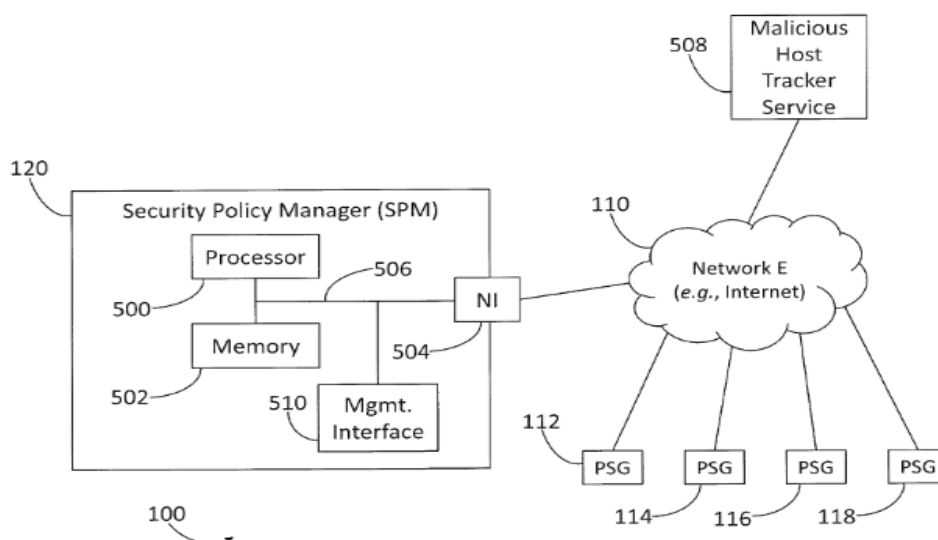


FIG. 5

Ex. 1001, 15:7-55; Fig. 5.

38. The '474 Patent also discloses receiving information from a plurality of such third party services. *Id.*, 15:7-55. In that case, given that there may be “duplicate[s]” in the network address information received between two services, the '474 Patent discloses correlating the network address information received from the two services (e.g., comparing to determine duplicates), and removing the duplicates. *Id.*

B. Prosecution History

39. I understand that during prosecution of the application that led to the '474 Patent, the Patent Office rejected the claims as unpatentable over a combination of references. Ex. 1002, 128-149. I further understand that, following amendments in a response and a subsequent examiner interview, Patent Owner had

amended the independent claims to recite, *inter alia*, “wherein a first packet matching rule of the packet filtering rules comprises: at least one packet matching criterion, a corresponding packet transformation function, and an indication of a feed managed by at least one of the plurality of malicious host tracker services,” a “plurality of” malicious host tracker services, and “wherein at least two of the plurality of malicious host tracker services are managed by different organizations, wherein one or more of the packet filtering rules were added, removed, or altered by the security policy management server based on a correlation between portions of the malicious traffic information.” *Id.*, 63-72, 85, 100-111. I understand that, following these amendments, the Examiner allowed the application. *Id.*, 38-54.

C. Effective Filing Date

40. I have been asked to assume that the effective filing date for the ’474 Patent is April 16, 2014. *See, e.g.*, Ex. 1001, 1-2.

V. CLAIM INTERPRETATION

41. I have been informed that only terms necessary to resolve the controversy need to be construed. For the purposes of the present declaration, I have applied the legal principles outlined above in Section II.A.

42. I understand that various claim terms construed in IPR2018-01836 (’213 Patent), IPR2018-01512 (’213 Patent), IPR2021-01157 (’906 Patent), IPR2018-01443 (’205 Patent), IPR2018-01444 (’205 Patent), and IPR2018-01513

(’077 Patent) also appear in the Challenged Claims. I understand that the Board may adopt those same constructions here. 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> IPR2021-01157, Paper 10 (ID); IPR2018-01443, Paper 25 (FWD); IPR2018-01444, Paper 32 (FWD); IPR2021-01157, Paper 10 (ID)
packet transformation function	[one or more] operations performed on a packet <i>See</i> IPR2021-01157, Paper 10 (ID); 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).
dynamic security policy ¹	any rule, message, instruction, file, data structure, or the like that specifies criteria corresponding to one or more packets and

¹ 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

Term	PTAB Constructions
	identifies a packet transformation function to be performed on packets corresponding to the specified criteria <i>See</i> IPR2021-01157, Paper 10 (ID); IPR2018-01836, Paper 31 (FWD), 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> IPR2018-01836, Paper 31 (FWD), IPR2018-01443, Paper 25 (FWD); IPR2018-01444, Paper 32 (FWD); IPR2021-01157, Paper 10 (ID)

VI. SUMMARY OF UNPATENTABILITY ANALYSIS

43. I have been asked to provide my opinion as to whether claims 1-33 (“the Challenged Claims”) of the ’474 Patent would have been obvious in view of the prior art. The discussion below provides a detailed analysis of how the prior art references I reviewed teach the limitations of the Challenged Claims of the ’474 Patent.

44. As part of my analysis, I have considered the scope and content of the prior art and any potential differences between the claimed subject matter and the

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.

prior art. I conducted my analysis as of the priority date of the '474 Patent: April 16, 2014. I have also considered the level of ordinary skill in the pertinent art as of that date.

45. I describe in detail below the scope and content of the prior art, as well as any differences between the claimed subject matter and the prior art, on an element-by-element basis for each Challenged Claim of the '474 Patent. This analysis supports my finding that the differences between the claims of the '474 Patent and the prior art discussed herein are such that the subject matter as a whole would have been obvious at the time of the filing of the '474 Patent to a person having ordinary skill in the art to which the subject matter pertains.

46. As described in detail below, the claimed subject matter of the Challenged Claims would have been obvious in view of the teachings of the identified prior art references as well as the knowledge of a POSITA.

47. Unless otherwise noted, all **bold** and **bold underline** emphasis in any quoted material has been added.

VII. GROUND 1: LAW IN VIEW OF GOLNABI RENDERS OBVIOUS CLAIMS 1-3, 5-7, 9-11, 13-15, 17-19, 21-23, 25-27, 29-31, 33

A. Overview of Law

48. 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.

49. Law discloses that a cyber security risk management firm 305 may distribute rulesets to Law’s firewalls over the Internet. *Id.* ¶¶ 66, 88. 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, threat patterns, and control system vulnerabilities found to exist within the network.” *Id.* ¶ 22; *id.*, Abstract; *id.* ¶ 88 (disclosing that “the various rulesets ... require updates to remain effective against network threats”).

50. Fig. 3 illustrates an embodiment that shows Law’s perimeter UTMS firewalls 146a and 146b protecting LANs 150a/150b while connected to cyber security risk management firm 305 over the Internet 155 for receiving updated rulesets, which obtains aggregated threat data 310 from sources 315:

1300

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

1316

DeltaV Profile #14 ↓

LOAD

1318

1320

SAVE

1322

Fig. 13

Ex. 1005, Fig. 13. Rulesets include “from” and “to” fields 1304 and 1306 for specifying IP addresses of packets on which to perform an action 1310, such as blocking. *Id.* ¶¶ 102-103.

52. 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. 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 (“The network 150 and devices may also be standard Ethernet communications and network devices 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.)”).

B. Overview of Golnabi

53. Golnabi discloses generating policy rules for firewalls designed to “filter out any unwanted traffic coming into or going from the secure network.” Ex. 1009, 305-306. In this context, Golnabi recognizes that it is important “to generate a minimum number of firewall policy rules for efficiency.” *Id.*, 308. To achieve a minimum number of policy rules, Golnabi merges rules that have similar characteristics. *Id.* (“For example, let’s consider to have a few rules of all matching

fields with an exception of source port field. In this case, these rules are then aggregated by combining all the matching fields...to get one generalized rule.”).

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

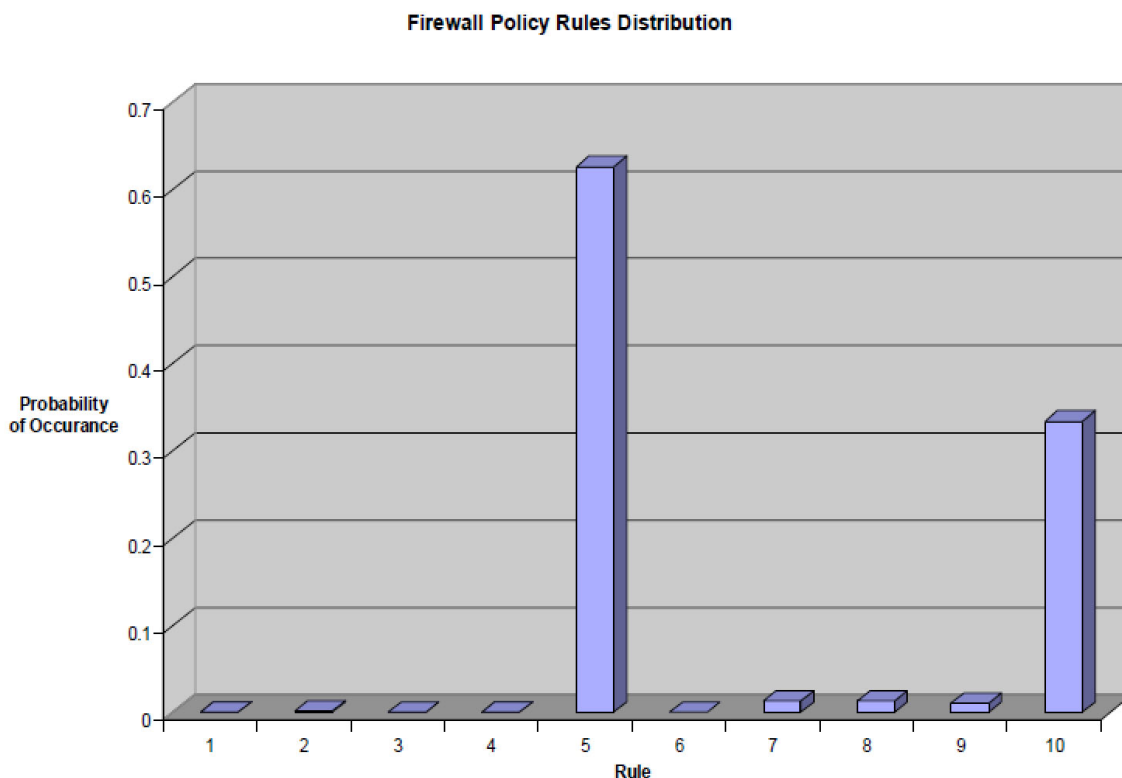


Figure 14. Distribution of Packets Over Initial Filtering Rules

Ex. 1009, Fig. 14. Because Rules 5 and 10 are heavily used, Golnabi explains that “**reordering** or prioritizing”² of the rules may provide “a tremendous performance gain as a result.” *Id.*, 314. A POSITA would have understood that by evaluating the more-heavily used rules earlier, the firewall may obviate the need to evaluate other, less commonly matched rules.

C. A POSITA would have considered Golnabi in conjunction with Law

55. A POSITA would have been motivated to combine the teachings of Law and Golnabi to produce the obvious, beneficial, and predictable result of implementing Law’s rulesets by merging, separating, and ordering as taught by Golnabi so as to avoid inefficient ruleset processing by Law’s perimeter UTMS firewalls 146a and 146b.

56. Law and Golnabi are analogous prior art, as they both pertain to the same field of endeavor of network protection systems, including network devices (such as firewalls) that implement rules. Ex. 1005, Abstract, ¶ 52; Ex. 1009, 305.

57. A POSITA would have combined the teachings of Golnabi with Law’s teachings, to obtain predictable and beneficial results. Law teaches constructing rulesets using threat information received from a plurality of sources, and installing the generated rulesets into network firewalls. Ex. 1005 ¶¶ 66, 88, 92.

² All emphasis added unless otherwise indicated.

Given Law's disclosure of receiving threat information from numerous independent third-party sources (*id.* ¶ 92), a POSITA would have recognized the likelihood for duplication and overlap in the threat information received by cyber security risk management firm 305. For example, if one source is aware of a threat, there is a reasonable likelihood that another source may be aware of the same threat. *Id.* Given the likelihood of duplication and overlap in the received threat information that is used in constructed Law's rulesets, a POSITA would have recognized that it is desirable to process the rule sets, by merging, separating, and ordering rules of the rule sets such that they provide optimized performance during operational processing. As Golnabi contemplates combining, separating, and ordering of rules in rulesets in order to optimize performance, a POSITA would have been motivated to implement those processes in Law to achieve optimized performance and would have had success doing so. Ex. 1005 ¶¶ 52, 88; Ex. 1009, 305.

D. Independent Claims

1. Claim 1

- (A) [1.0]³ *“A method of filtering packets at a packet security gateway configured for protection of a network, wherein the packet security gateway is capable of receiving a plurality of dynamic security policies and is*

³ I understand that the numerical identification of the claim limitations of the '474 Patent correspond to that provided in the exhibit providing a claim listing. Ex. 1012.

***associated with a security policy management server
external from the network, the method comprising:***

58. Law is directed to a method of filtering packets at a packet security gateway configured for protection of a network. In particular, Law's perimeter UTMS firewalls 146a and 146b each correspond to the claimed "packet security gateways." 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:

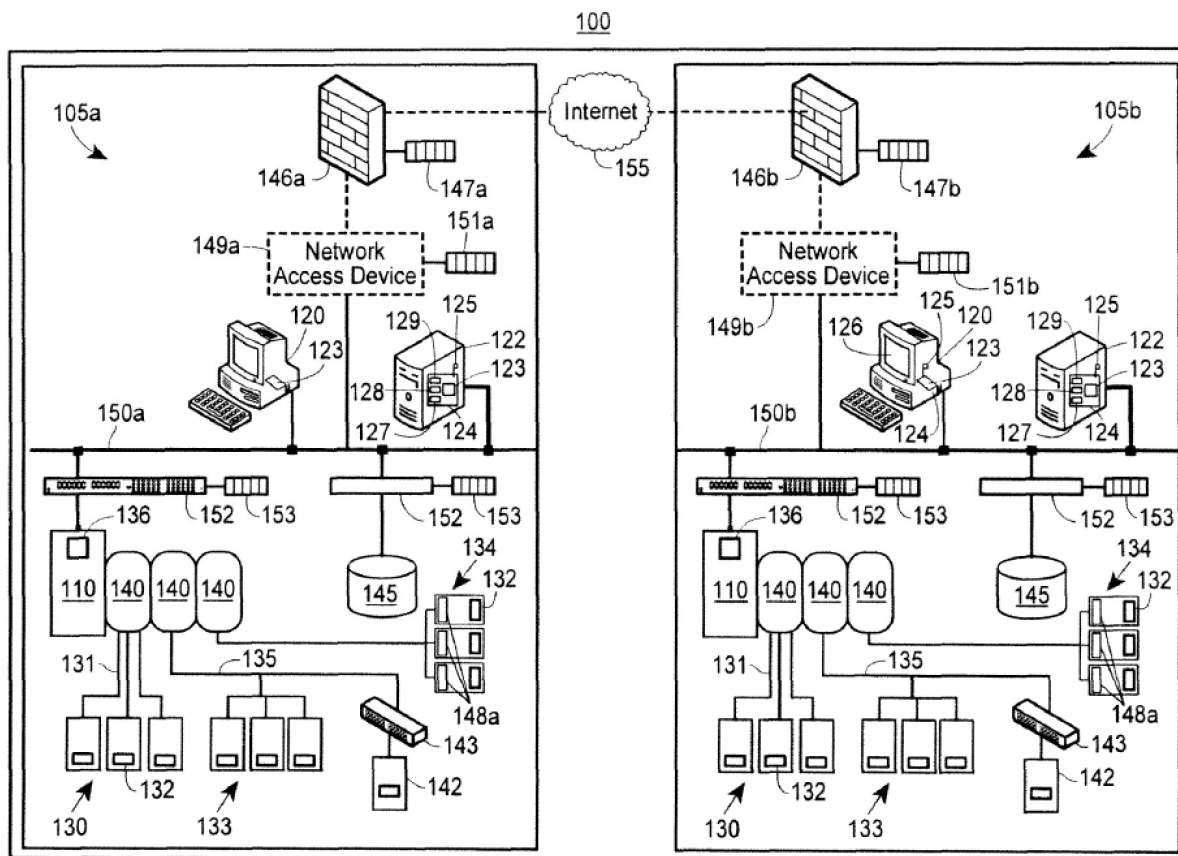


Fig. 1A

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.

59. In addition, 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”).

60. 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. 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. 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. 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."); Accordingly, Law's perimeter UTMS firewalls 146a and 146b are packet security gateways that are configured to filter packets.

61. Law's perimeter UTMS firewalls 146a and 146b are associated with a security policy management server external from the network. For example, perimeter UTMS firewalls 146a and 146b receive rulesets from cyber security risk

management firm 305, which corresponds to the claimed security policy management server.

62. 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**”).

63. 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:

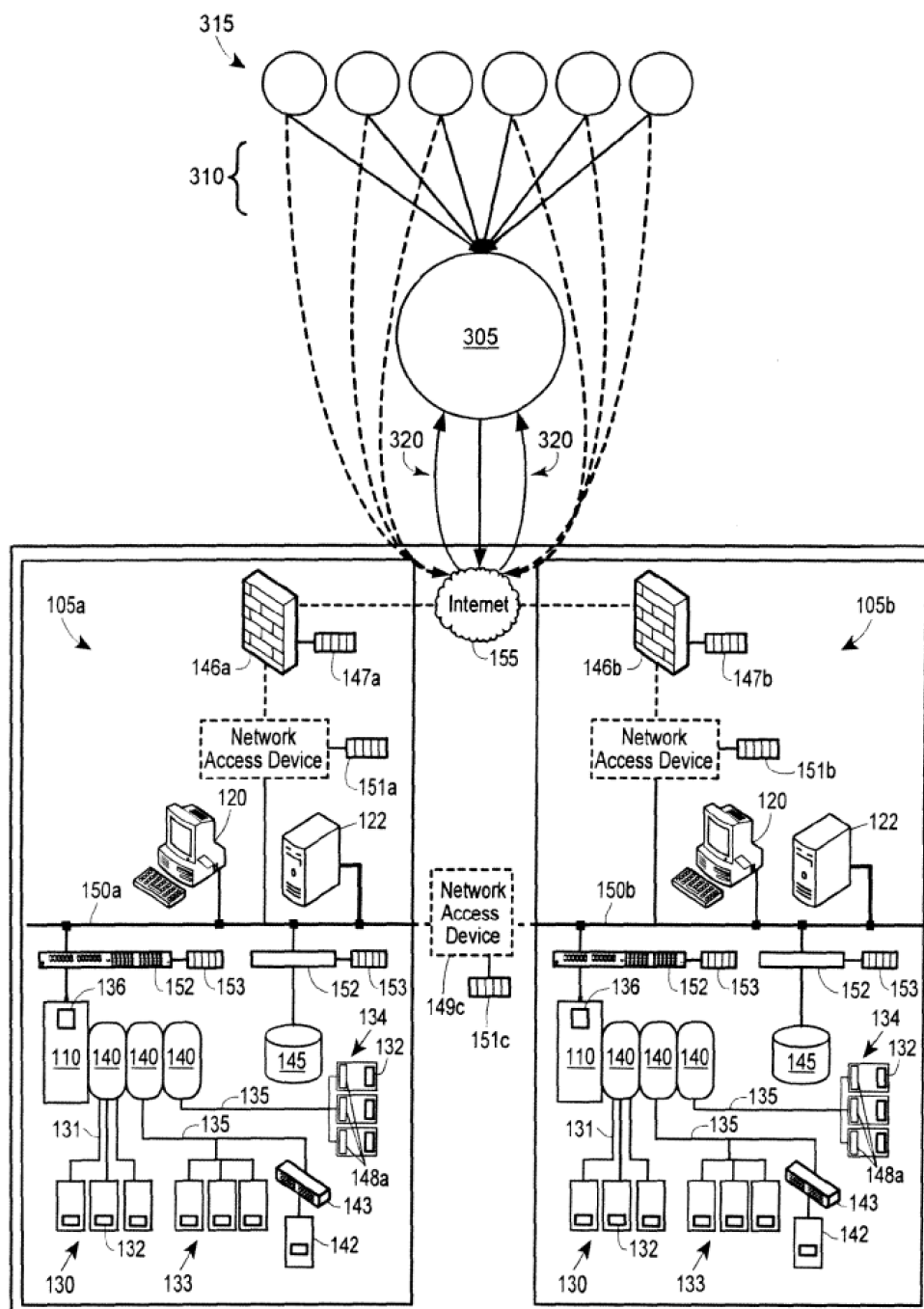


Fig. 3

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

64. 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. 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”).

65. 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).

66. 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.

67. Law discloses that UTMS firewalls 146a and 146b are capable of receiving a plurality of dynamic security policies. Law expressly discloses that ruleset 147 is 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”); *see also, e.g., id.* ¶ 92.

68. Accordingly, Law discloses or renders obvious the preamble.

(B) [1.1] *“receiving, by the packet security gateway and from the security policy management server, a dynamic security policy comprising packet filtering rules,”*

69. For the same reasons as explained above in [1.0], Law discloses that UTMS firewalls 146a and 146b receive from cyber security risk management firm 305 a dynamic security policy (e.g., rulesets 147) comprising packet filtering rules. *See, e.g.,* Ex. 1005 ¶ 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”); *see also id.* ¶ 52, 59; *id.*, Fig. 3. The received rulesets comprise packet filtering rules. *See id.* ¶¶ 102-103.

(C) [1.2] *“wherein one or both of the dynamic security policy or one or more of the packet filtering rules of the dynamic security policy were automatically created or altered, by the security policy management server, based on malicious traffic information received from a plurality of malicious host tracker services,”*

70. Law discloses or renders obvious that one or more rules in ruleset 147 were automatically created by cyber security risk management firm 305. For example, Law discloses that “third party, cyber security risk management firm 305 ... may collect threat data 310 from a plurality of various sources 315 to construct the various rulesets 147, 148, 151, 153, validate the rulesets, verify, and distribute the rulesets to the UTMS-configured firewalls 146a, 146b,” and that such **“[r]uleset collecting, constructing, validating, and distributing may be performed using any type of information technology methods suitable for performing such actions using electronic data,”** including “collecting the threat data 310 from the World Wide Web using various data collection techniques (e.g., robots, crawling, data feeds, collaborative forums, etc.), constructing data files to convey the rulesets to their destination devices in a device-compatible manner,

executing a computer-implemented algorithm to determine if the rulesets effectively secure the process control systems in a desirable manner (e.g., simulation or other testing method), and distributing the rulesets to the UTMS-configured entities via a secure Internet interface or other suitable method.” Ex.

1005 ¶ 88. A POSITA would have understood that ruleset constructing using “any type of information technology methods suitable for” ruleset constructing would have included methods of automatically constructing rules.

71. 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. 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.

72. 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**).

73. 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.

74. 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 a plurality of third party malicious host tracker services (“plurality of various sources 315”). Ex. 1005 ¶¶ 88, 91-92, 102-103; *id.*, Fig. 13.

75. 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:

76. The various sources 315 that provide threat data 310 correspond to a plurality of third party malicious host tracker services. *Id.* ¶ CITE. 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 party providers of malicious traffic information. For example, a POSITA would have recognized that Assurent Secure Technologies and Secunia were cybersecurity firms, and that Carnegie Mellon University is a university. 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. 1007,⁴ 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

⁴ 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. 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.

security 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.

(A) [1.3] “*wherein at least two of the plurality of malicious host tracker services are managed by different organizations*”

77. For the same reasons as explained above in [1.2], Law discloses or renders obvious that the plurality of malicious host tracker services (e.g., various sources 315) are managed by different organizations. Ex. 1005 ¶ 92 (identifying Assurent, Secunia, and Carnegie Mellon, each of which are managed by different organizations). A POSITA would have understood each of the exemplary identified sources 315 of threat data 310 to be third party providers of malicious traffic information managed by different organizations.

(B) [1.4] “*wherein one or more of the packet filtering rules were added, removed, or altered by the security policy management server based on a correlation between portions of the malicious traffic information, and*”

78. The ’474 Patent explains that when receiving malicious traffic information from a plurality of third party services, there may be “duplicate[s]” in

the malicious traffic information received between the plurality of services. Ex.

1001, 15:7-55. The '474 Patent explains that “correlation” refers to comparing the received malicious traffic information to find the duplicates, and the ruleset altered by removing the duplicates. *Id.*

79. Law renders obvious that the cyber security risk management firm 305 alters or removes one or more rules in ruleset 147 based on a correlation between portions of the malicious traffic information. In particular, as explained above in [1.2], Law discloses receiving malicious traffic information (threat data 310) from several different third-party sources 315. *See* Ex. 1005 ¶ 92 (describing at least three different sources of threat data, Assurent, Secunia, and Carnegie Mellon); *id.*, Fig. 3 (illustrating six different sources 315 of threat data 310 being provided to cyber security risk management firm 305). It would have been obvious to a POSITA that there would have been a high likelihood of duplicates in the received threat data 310. For example, it would have been common for different sources 315 to have been aware of some of the same threats. *Id.* Rather than simply aggregate the received threat data 310 with no processing, which would be very inefficient in that it would cause firewalls 146 to process the duplicated rules multiple times on the same packets, it would have been obvious to a POSITA to analyze the received threat data 310 to remove duplicate rules in order to avoid the

inefficiency, wasted processing power, and slower execution speed of not doing so.

Id.

80. To the extent not obvious in view of Law alone, processing the received threat data 310 to remove duplicate rules would have been obvious over Law in view of Golnabi. Golnabi teaches merging a plurality of rules using “an aggregation algorithm to generate a minimum number of firewall policy rules for efficiency” and that “these **rules are then aggregated by combining...to get one generalized rule.**” Ex. 1009, 308 (“combining a group of similar rules”); *see also id.*, 312. It would have been obvious to a POSITA to combine rules as Golnabi teaches, when constructing rulesets as Law teaches using threat data 310 from a plurality of sources 315, because the appropriate combining of rules can minimize total rules thereby providing processing efficiency.

81. Therefore, Law in combination with Golnabi renders obvious element [1.4].

(C) [1.5] “*wherein a first packet matching rule of the packet filtering rules comprises: at least one packet matching criterion, a corresponding packet transformation function, and an indication of a feed*

managed by at least one of the plurality of malicious host tracker services; and”

82. Law discloses that a first packet matching rule of the packet filtering rules comprises at least one packet matching criterion and a corresponding packet transformation function. Ex. 1005 ¶¶ 52, 91, 102-103; *id.*, Fig. 13.

83. 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.”).

84. 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. These generally correspond to the same rule conditions in the exemplary rule table provided by the '474 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. 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.”).

85. 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.”). 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.*

86. In addition, Law discloses or renders obvious that a packet matching rule of the packet filtering rules would include an indication of a feed managed by at least one of the plurality of malicious host tracker services. For example, Law describes rules with widely varying attributes. In particular, Law explains that “Protocol types of the example protocol type column 1302 may include, but are not limited to, UDP, TCP, ICMP, HART, and/or SCPI.” Ex. 1005 ¶ 102. A POSITA would have understood that any of Law’s feeds of threat data 310 from sources

315 may have been uniquely associated with a particular combination of rule parameters. For example, one feed may have specialized in the SCPI protocol. *Id.* Accordingly, under such a scenario, a POSITA would have understood a rule featuring SCPI in the protocol type column 1302 to have provided an indication of that particular feed.

87. To the extent that “an indication of a feed” is construed to refer to explicitly identifying the feed, providing such information would have been obvious in view of Law. In particular, Fig. 13 illustrates a “a ruleset user interface such as a protocol rule table 1300” that “may allow a user to access one or more user interfaces to configure and control any of the rules within the rulesets 147, 148, 151, 152.” Ex. 1005 ¶ 102. Given Law’s disclosure of receiving threat data 310 from several sources 315, it would have been obvious to a POSITA that information regarding the source 315 of each rule may be helpful to a user when using the ruleset interface to configure and control any of the rules within rulesets. For example, some sources 315 may be more trustworthy or reliable than others, and therefore it would have been obvious to communicate that information to a user, such as by adding a column to the rule table 1300 shown in Fig. 13 to indicate, for each rule, the source[s] 315 upon which the rule is based. *Id.*

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

(D) [1.6] ***“performing, based on the packet filtering rules, packet filtering on individual packets of a plurality of packets associated with the network protected by the packet security gateway,”***

89. Law discloses that perimeter UTMS firewalls 146a and 146b perform, based on packet filtering rules, packet filtering on individual packets of a plurality of packets associated with the network 150 protected by firewalls 146a and 146b. *See, e.g.*, Ex. 1005 ¶¶ 52, 59, 91, 102-103; *id.* Figs. 1A, 3, 13.

90. 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.”).

(E) [1.7] ***“wherein the packet filtering comprises:
inspecting individual packets; and”***

91. Law discloses inspecting individual packets to determine whether conditions of any rule are 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”); *id.*, Fig. 13. A POSITA would have understood that determining whether the conditions of any rule are satisfied would have necessarily required inspecting individual packets.

(F) [1.8] ***“filtering each packet based on content
determined from the inspection of that individual
packet.”***

92. Law discloses filtering each packet based on content determined from the inspection of that individual packet – namely, whether the condition for a particular rule was 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.”).

2. Claim 9

(A) [9.0] *“A packet security gateway configured for protection of a network, capable of receiving a plurality of dynamic security policies and associated with a security policy management server external from the network, the packet security gateway comprising:”*

93. See analysis at [1.0].

(B) [9.1] *“at least one processor; and”*

94. 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) [9.2] *“memory comprising instructions that, when executed by the last least one processor, cause the packet security gateway to:”*

95. 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. 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.

(D) [9.3] *“receive, from the security policy management server, a dynamic security policy comprising packet filtering rules,”*

96. See analysis at [1.1].

(E) [9.4] *“wherein one or both of the dynamic security policy or one or more of the packet filtering rules of the dynamic security policy were automatically created or altered, by the security policy management server, based on malicious traffic information received from a plurality of malicious host tracker services,”*

97. See analysis at [1.2].

(F) [9.5] *“wherein at least two of the plurality of malicious host tracker services are managed by different organizations,”*

98. See analysis at [1.3].

(G) [9.6] *“wherein one or more of the packet filtering rules were added, removed, or altered by the security policy management server based on a correlation between portions of the malicious traffic information, and”*

99. See analysis at [1.4].

(H) [9.7] *“wherein a first packet matching rule of the packet filtering rules comprises: at least one packet*

matching criterion, a corresponding packet transformation function, and an indication of a feed managed by at least one of the plurality of malicious host tracker services; and”

100. See analysis at [1.5].

(I) [9.8] *“perform, based on the packet filtering rules, packet filtering on individual packets of a plurality of packets associated with the network protected by the packet security gateway,”*

101. See analysis at [1.6].

(J) [9.9] *“wherein the packet filtering comprises: inspecting individual packets; and”*

102. See analysis at [1.7].

(K) [9.10] *“filtering each packet based on content determined from the inspection of that individual packet.”*

103. See analysis at [1.8].

3. Claim 17

(A) [17.0] *“One or more non-transitory computer-readable media comprising instructions that, when executed by one or more processors of a packet security gateway configured to protect a network, cause the packet security gateway to:”*

104. See analysis at [1.0].

105. 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. 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. *Id.*

- (B) [17.1] “*receive, from a security policy management server, a dynamic security policy comprising packet filtering rules,*”

106. See analysis at [1.1].

- (C) [17.2] “*wherein one or both of the dynamic security policy or one or more of the packet filtering rules of the dynamic security policy were automatically created or altered, by the security policy management server, based on malicious traffic information received from a plurality of malicious host tracker services,*”

107. See analysis at [1.2].

- (D) [17.3] “*wherein at least two of the plurality of malicious host tracker services are managed by different organizations,*”

108. See analysis at [1.3].

- (E) [17.4] “*wherein one or more of the packet filtering rules were added, removed, or altered by the security policy management server based on a correlation between portions of the malicious traffic information, and*”

109. See analysis at [1.4].

- (F) [17.5] “*wherein a first packet matching rule of the packet filtering rules comprises: at least one packet matching criterion, a corresponding packet transformation function, and an indication of a feed*

managed by at least one of the plurality of malicious host tracker services; and”

110. See analysis at [1.5].

(G) [17.6] *“perform, based on the packet filtering rules, packet filtering on individual packets of a plurality of packets associated with the network protected by the packet security gateway,”*

111. See analysis at [1.6].

(H) [17.7] *“wherein the packet filtering comprises: inspecting individual packets; and”*

112. See analysis at [1.7].

(I) [17.8] *“filtering each packet based on content determined from the inspection of that individual packet.”*

113. See analysis at [1.8].

4. Claim 25

(A) [25.0] *“A system comprising:”*

114. Law discloses a system. *See, e.g.*, Ex. 1005, Figs. 1A, 3; *id.* ¶¶ 51-52.

(B) [25.1] *“a security policy management server external from a network associated with a packet security gateway, wherein the security policy management server comprises:”*

115. For the same reasons as explained in [1.1], Law discloses a security policy management server (cyber security risk management firm 305), which is external from network 150 protected by UTMS firewalls 146a and 146b. *See* 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. 1005 ¶¶ 66, 88 (disclosing that cyber security risk management firm 305 distributes ruleset 147 to perimeter UTMS firewalls 146a and 146b over the Internet 155).

(C) [25.2] *“one or more first processors; and”*

116. As cyber security risk management firm 305 is capable of “executing a computer-implemented algorithm to determine if the rulesets effectively secure the process control systems in a desirable manner,” it necessarily includes one or more processors. Ex. 1005 ¶ 88.

(D) [25.3] *“first memory storing first instructions that, when executed by one or more first processors, cause the security policy management server to:”*

117. As cyber security risk management firm 305 is capable of “executing a computer-implemented algorithm to determine if the rulesets effectively secure the process control systems in a desirable manner,” it necessarily includes a first memory storing instructions that, when executed, perform the described functionality. Ex. 1005 ¶ 88.

(E) [25.4] *“receive, from a plurality of malicious host tracker services, first malicious traffic information, wherein at least two of the plurality of malicious host tracker services are managed by different organizations;”*

118. See analysis at [1.2]-[1.3].

- (F) **[25.5] “*automatically create, based on the first malicious traffic information, a dynamic security policy or packet filtering rules of the dynamic security policy,*”**

119. See analysis at [1.2].

- (G) **[25.6] “*wherein a first packet filtering rule of the packet filtering rules comprise: one or more packet matching criteria comprising a corresponding network addresses, one or more corresponding packet transformation functions, and an indication of a feed managed by at least one of the plurality of malicious host tracker services; and*”**

120. See analysis at [1.5].

121. In addition, Law discloses or renders obvious that a first packet filtering rule of the packet filtering rules includes one or more packet matching criteria comprising a corresponding network address. 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. 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. 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”).

(H) [25.7] *“add, remove, or alter the one or more rules of the dynamic security policy based, at least in part, on making a correlation between portions of the first malicious traffic information;”*

122. See analysis at [1.4].

(I) [25.8] *“the packet security gateway, wherein the packet security gateway is configured for protection of a network and associated with the security policy management server external from the network, the packet security gateway comprising:”*

123. See analysis at [1.0].

124. In addition, Law discloses that UTMS firewalls 146a and 146b are configured for protection of network 150. Ex. 1005 ¶ 59 (“The UTMS-configured firewalls 146 ... 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”).

(J) [25.9] *“one or more second processors; and”*

125. See analysis at [9.1].

- (K) [25.10] *“second memory storing second instructions that, when executed by one or more second processors, cause the packet security gateway to:”*

126. See analysis at [9.2].

- (L) [25.11] *“receive, from the security policy management server, the dynamic security policy comprising the packet filtering rules; and”*

127. See analysis at [1.1].

- (M) [25.12] *“perform, based on the packet filtering rules, packet filtering on individual packets of a plurality of packets associated with the network protected by the packet security gateway, wherein the packet filtering comprises:”*

128. See analysis at [1.6].

- (N) [25.13] *“inspecting individual packets; and”*

129. See analysis at [1.7].

- (O) [25.14] *“filtering each packet based on content determined from the inspection of that individual packet.”*

130. See analysis at [1.8].

E. Dependent Claims

1. Claims 2, 10, 18, 26

131. Claims 2, 10, 18, and 26, which depend from claims 1, 9, 17, and 25, respectively, recite: “wherein the at least one packet matching criterion comprises at least one network address associated with an indication of malicious network traffic.”

132. For the same reasons as explained above in [1.2], 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.

133. In addition, as explained above, Law 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; *id.*, Fig. 13. A POSITA would have understood that an IP address is a network address. Moreover, given the purpose of rules in “protect the process control system 100 from internal and external network threats such as viruses, worms, or any other attack,” it would have been obvious to a POSITA that the address columns of rules would have include IP addresses associated with malicious traffic to be blocked. *Id.*

2. Claims 3, 11, 19, and 27

134. Claims 3, 11, 19, and 27, which depend from claims 1, 9, 17, and 25, respectively, recite: “wherein at least one packet transformation function comprises a network protection action.”

135. As explained above, 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 147, 148, 151, 153 may define conditions that, if detected, ... 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.”).

3. Claims 5, 13, 21, 29

(A) [5.0], [13.0], [21.0], [29.0]

136. Law discloses or renders obvious receiving packets at firewalls 146a and 146b using an interface that is not addressed at the network layer, in a network layer transparent manner. 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. 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)**”).

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) [5.1], [13.1], [21.1], [29.1]

137. As explained above with respect to [5.0], Law discloses support for any communication protocol and any addressing scheme. Ex. 1005 ¶¶ 55, 103. As explained above at [1.6], 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, including at the network layer. *See, e.g.*, Ex. 1005 ¶¶ 52, 59, 91, 102-103; *id.* Figs. 1A, 3, 13.

4. Claims 7, 15, 23, 31

138. Law discloses or renders obvious filtering each packet one at a time. 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”); 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”).

139. Law discloses or renders obvious performing a packet digest logging function with respect to each filtered packet. For example, each rule includes a log column 1314, as shown in Fig. 13:

1300

	1302	1304	1305	1329	1306	1308	1310	1312	1314
	PROTOCOL	FROM	THRESH.	T0	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; Ex. 1005 ¶ 102 (“protocol rule table 1300 ... includes ... a log column 1314”). In addition, Law explains that certain conditions can cause a log to be generated. Ex. 1005 ¶ 104. Moreover, Law discloses a user interface in which log information may be included (status 1518) or other information. Ex. 1005 ¶ 108. Accordingly, Law discloses or renders obvious performing a packet digest logging function with respect to each filtered packet.

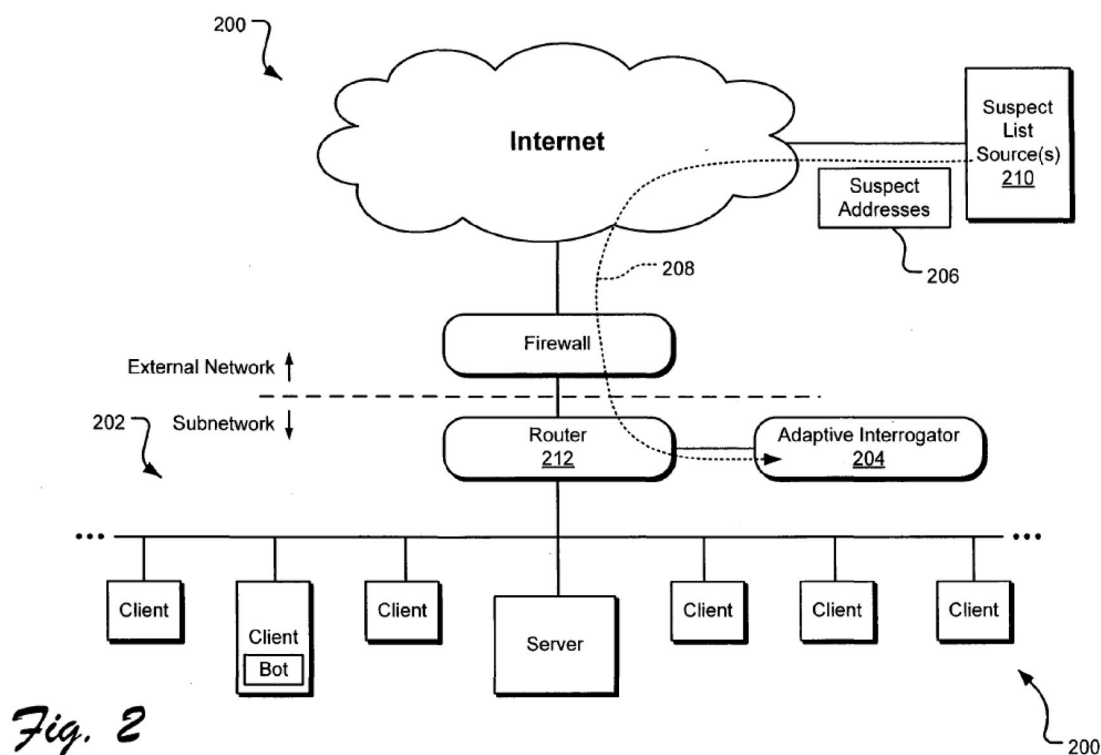
VIII. GROUND 2: LAW IN VIEW OF GOLNABI AND WOOD RENDERS OBVIOUS CLAIMS 2, 10, 18, 26

A. Overview of Wood

140. 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.*

141. 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.

142. 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 (e.g., a new IP address block is legitimately allocated by IANA or a new hacker site is identified). By quickly updating the suspect addresses 206, the suspect address sources 210 can provide the most up-to-date notice of possible threats.”). Wood 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 Also Would Have Considered Wood In Conjunction With Law

143. 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.

144. Both Law and Wood are in the same field of endeavor and analogous art to the ’474 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.

145. 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. 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. 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. 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. 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.

C. Claims 2, 10, 18, 26

146. To the extent not explicitly disclosed or rendered obvious in view of Law alone, the combined system of Law and Golnabi with Woods renders obvious claims 2, 10, 18, 26. 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. Upon receipt of an updated suspect address list by Law’s firm 305, it would have been obvious to a POSITA that the

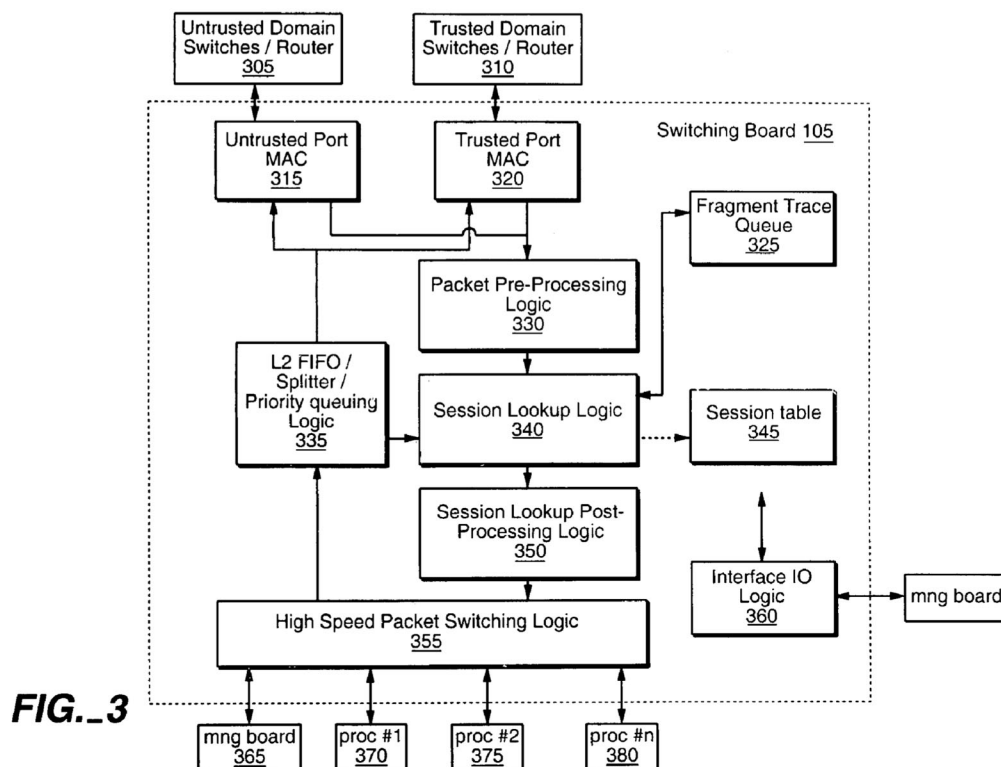
firm 305 would have created updated rulesets to reflect the information in the suspect address list, including adding blocking rules for packets matching IP addresses in the updated suspect address list. Ex. 1005 ¶ 88.

IX. GROUND 3: LAW IN VIEW OF GOLNABI AND KE RENDERS OBVIOUS CLAIMS 4, 12, 20, 28

A. Overview of Ke

147. Ke discloses an internet security device 200 that implements dynamic security policies for detecting, intercepting, and dropping unwanted packets. Ex. 1010, 4:10-16. Such policies “typically contain rules about what kinds of traffic should be allowed and how the traffic should be managed.” *Id.*, 8:18-24.

148. Ke teaches that a priority queuing logic unit 335, as shown in Fig. 3, is “used to buffer packets, determine if a packet is a session control packet, and queue packets in a priority queue so that certain packets get priority over others”; thus, the “priority queuing mechanism ensures quality of service and high throughput”:



Ex. 1001, Fig. 3; *id.*, 4:50-57.

A. A POSITA Also Would Have Considered Ke In Conjunction With Law

149. A POSITA would have been motivated to apply Ke’s teachings directed to queuing to Law’s system. For example, given the application of Law’s system to industrial process control systems, a POSITA would have appreciated that the traffic traversing network 150 would have vastly different priority levels. *Id.* In particular, Law discloses that networked devices include “field devices 130, 133, 134” that “may be any type of hardware component such as sensors, valves, transmitters, positioners, etc.” Ex. 1005 ¶ 55. A POSITA would have appreciated that the information from some sensors may have been critical to the functioning of

the process control system, whereas others may not have been important at all.

Furthermore, a POSITA would have appreciated that if a network bottleneck were to occur that disrupted network traffic from a critical sensor, it could mean disaster.

Id.

150. Accordingly, a POSITA would have readily recognized the benefit and applicability of Ke to this bottleneck problem. Ke teaches queuing features that are intended to resolve issues relating to network traffic bottlenecks. Ex. 1010, 1:43-54. Ke also describes several advantages of queueing. *Id.*, 3:14-32. A POSITA would have been motivated to incorporate the queueing of Ke into the teachings of Law to obtain those advantages and prevent a disaster that could occur if a critical sensor was unable to communicate due to a network bottleneck. Indeed, Ke suggests combinations with other systems, stating that the “systems can be easily integrated into various types of environments with different requirements.” *Id.*, 3:30-32.

B. Claims 4, 12, 20, 28

1. [4.0], [12.0], [20.0], [28.0]

151. The combined system of Law and Golnabi with Ke renders obvious elements [4.0], [12.0], [20.0], [28.0]. For example, Ke discloses that a first set of the packets (e.g., “session control packet[s]”) should be placed in a first forwarding queue (e.g., “priority queue”) for “high throughput” and a second set of the packets

(e.g., “normal packets”) should be placed in a second forwarding queue (e.g., a non-priority “queue”). Ex. 1010, 4:50-57, Fig. 3. It would have been obvious to a POSITA to implement such first and second forwarding queues in Law’s network 150 in order to provide critical sensors with more reliable network communication.

2. [4.1], [12.1], [20.1], [28.1]

152. The combined system of Law and Golnabi with Ke renders obvious elements [4.1], [12.1], [20.1], [28.1]. For example, Ke discloses that the first forwarding queue has a higher forwarding rate than the second forwarding queue (e.g., implementation of “priority mechanisms” through “priority queueing logic (335)”). Ex. 1010, 4:50-57, Fig. 3.

3. [4.2], [12.2], [20.2], [28.2]

153. The combined system of Law and Golnabi with Ke renders obvious elements [4.2], [12.2], [20.2], [28.2]. For example, Ke discloses actually sending packets based on the forwarding queue, the first forwarding queue having a higher forwarding rate than the second forwarding queue (e.g., implementation of “priority mechanisms” through “priority queueing logic (335)”). Ex. 1010, 4:50-57, Fig. 3.

**X. GROUND 4: LAW IN VIEW OF GOLNABI AND JUNGCK
RENDERS OBVIOUS CLAIMS 5, 13, 21, 29**

A. Overview of Jungck

154. 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 Also Would Have Considered Jungck In Conjunction
With Law**

155. A POSITA would also have been motivated to combine Law’s and Jungck’s teachings. 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.

156. Jungck teaches using “a list of blocked IP addresses” for addressing attacks. Ex. 1008 ¶ 176. Law teachings 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 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.

C. Claims 5, 13, 21, 29

(A) [5.0], [13.0], [21.0], [29.0]

157. The combined system of Law, Golabi, 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.

158. 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.

(B) [5.1], [13.1], [21.1], [29.1]

159. Jungck discloses performing the at least one of the multiple packet transformation functions at the network layer. For example, Jungck discloses that

in the case of a match, the edge server “modif[ies] the IP address and payload of the captured packet 704 and releas[es] the modified packet 704 to the routing logic 730 of the router 702.” Ex. 1008 ¶¶ 153, 180. It would have been obvious to a POSITA to modify Law’s firewalls 146 to incorporate this functionality of Jungck’s edge servers.

XI. GROUND 5: LAW IN VIEW OF GOLNABI AND JOHNSON RENDERS OBVIOUS CLAIMS 7-8, 15-16, 23-24, and 31-32

A. Overview of Johnson

160. Johnson is entitled “Framer,” and relates to “extract[ing] packets from within a received frame and generat[ing] digests of the extracted packets.” Ex. 1011, Abstract. Johnson teaches identifying and extracting data from the network and application layers of packets, generating a packet-digest from such information, and logging such information. *Id.* ¶¶ 14, 21.

B. A POSITA Also Would Have Considered Johnson In Conjunction With Law

161. A POSITA would have been motivated to consider Johnson in conjunction with Law.

162. Law and Johnson are in the same field of endeavor (network security based on packet inspection). *See, e.g.*, Ex. 1005 ¶ 59; Ex. 1011 ¶¶ 1-4. Furthermore, Law and Johnson represent the application of known techniques (packet inspection and filtering and creating packet digest, respectively) to improve

a similar devices or method, by combination with the other. For example, Johnson teaches a specific implementation of a known technique (packet digesting) that Law refers to, generally. Ex. 1005 ¶¶ 102, 104, 108; *id.*, Fig. 13. Thus, a POSITA would have been motivated to combine the teachings of Law and Johnson.

C. Claims 7, 15, 23, 31

163. To the extent that not rendered obvious in view of the combination of Law and Golnabi, the combination of Law, Golnabi, and Johnson renders obvious claims 7, 15, 23, 31. For example, Johnson also teaches a packet digest logging function performed on packets. Ex. 1011 ¶¶ 182-183. Johnson discloses that such packet digests for logging may be created using a variety of types of information, including a packet's source IP address, destination IP address, transport protocol, source port or destination port (the "five-tuple"). Ex. 1011 ¶ 14. Moreover, the packet digest log may be created using application-layer packet-header information, such as an HTTP (application layer) packet header: "For example, a digest may be formed from bytes of a Universal Resource Locator (URL) included within a packet's payload." Ex. 1011 ¶ 14.

D. Claims 8, 16, 24, 32

1. [8.0], [16.0], [24.0], [32.0]

164. Johnson teaches including specified packet information in a digest. Ex. 1011 ¶ 14 ("As shown, the framer 102 generates 108 a digest from the packet.

The digest may vary based on a packet classification scheme being used...the digest may feature the IP source and destination address, transport protocol, and security parameter. Additionally, the digest may include packet data other than data from the packet's header. For example, a digest may be formed from bytes of a Universal Resource Locator (URL) included within a packet's payload. Such a digest may be useful in a scheme that handles packets based on requested web-content. Further, a digest may include information not included within the packet (e.g., data from one or more previous packets, network status information, and so forth).”).

165. A POSITA would have combined Law and Johnson as claimed here because Johnson provides specific implementation examples of the suggestions of Law. The teachings of Johnson represent an obvious extension of Law’s disclosure.

2. [8.1], [16.1], [24.1], [32.1]

166. Johnson teaches generating a record containing a subset of information identified for each packet. Ex. 1011 ¶ 14 (“As shown, the framer 102 generates 108 a digest from the packet. The digest may vary based on a packet classification scheme being used...the digest may feature the IP source and destination address, transport protocol, and security parameter. Additionally, the digest may include packet data other than data from the packet's header. For

example, a digest may be formed from bytes of a Universal Resource Locator (URL) included within a packet's payload. Such a digest may be useful in a scheme that handles packets based on requested web- content. Further, a digest may include information not included within the packet (e.g., data from one or more previous packets, network status information, and so forth).”).

3. [8.2], [16.2], [24.2], [32.2]

167. It would have been obvious to a POSITA in view of Law and Johnson to reformat, for each packet, the subset of information according to a logging system standard. For example, a POSITA would have understood that it would have been obvious to reformat log data into a standard log format, such as “syslog,” which was well known prior to 2014. *Id.* Furthermore, it would have been obvious to a POSITA that the packet digest created in Johnson “by selectively shifting bits of the packet into a register as the packet bits are output by the framer” could have been reformatted into a standard format such as Syslog. Ex. 1001 ¶ 15.

4. [8.3], [16.3], [24.3], [32.3]

168. It would have been obvious to a POSITA in view of Law and Johnson to route, based on the subset of information in the identified packet, each packet to a monitoring device. In particular, Law indicates that an action performed on a logged packet may be “re-route.” Ex. 1005 ¶ 103 (“[O]ther actions may include, but are not limited to, block, notify, and/or **re-route**.”). In view of Law’s express

disclosure of re-routing a packet based on the packet identification criteria of a corresponding rule, Law renders obvious routing such packets to a monitoring device.

XII. CONCLUSION

169. In summary, I have concluded that each of the Challenged Claims is unpatentable as obvious under 35 U.S.C. § 103 in light of the Law, Golnabi, Wood, Ke, Jungck, and/or Johnson prior art references as discussed above and the knowledge of one of ordinary skill in the art, as described in this declaration.

Specifically, in my opinion, for at least the above reasons:

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

170. I currently hold the opinions expressed in this declaration. But my analysis may continue, and I reserve the right to supplement my opinions in the future to respond to any arguments that Patent Owner or its expert(s) may raise and to take into account new information as it becomes available to me. In signing this declaration, I understand that the declaration will be filed as evidence in an inter partes review proceeding before the Patent Trial and Appeal Board of the U.S. Patent and Trademark Office. I acknowledge that I may be subject to cross examination in the case and that cross examination will take place within the United States. If cross examination is required of me, I will appear for cross examination within the United States during the time allotted for cross examination.

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

Declaration of Doug Jacobson, Ph.D
Inter Partes Review of U.S. 11,012,474

Executed on January 6, 2022 in Ames, Iowa.


Doug W. Jacobson, Ph.D

Appendix A – List of Exhibits

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

Declaration of Doug Jacobson, Ph.D
Inter Partes Review of U.S. 11,012,474

Ex. 1014	Complaint filed in <i>Centripetal Networks, Inc. v. Keysight Technologies, Inc.</i> , Case No. 2:22-cv-00002
Ex. 1015	Affidavit of service of complaint filed in <i>Centripetal Networks, Inc. v. Keysight Technologies, Inc.</i> , Case No. 2:22-cv-00002
Ex. 1016	INTERIM PROCEDURE FOR DISCRETIONARY DENIALS IN AIA POST-GRANT PROCEEDINGS WITH PARALLEL DISTRICT COURT LITIGATION (June 21, 2022)