No. 2021-1888

UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT

CENTRIPETAL NETWORKS, INC.,

Plaintiff-Appellee,

v.

CISCO SYSTEMS, INC.,

Defendant-Appellant.

On Appeal from the United States District Court for the Eastern District of Virginia in Case No. 2:18-cv-00094-HCM-LRL, Judge Henry C. Morgan, Jr.

NON-CONFIDENTIAL BRIEF FOR DEFENDANT-APPELLANT CISCO SYSTEMS, INC.

THOMAS G. SAUNDERS
HEATH A. BROOKS
WILMER CUTLER PICKERING
HALE AND DORR LLP
1875 Pennsylvania Avenue, NW
Washington, DC 20006
(202) 663-6000

THOMAS G. SPRANKLING
WILMER CUTLER PICKERING
HALE AND DORR LLP
2600 El Camino Real, Suite 400
Palo Alto, CA 94306
(650) 858-6000

WILLIAM F. LEE
MARK C. FLEMING
ANNALEIGH E. CURTIS
SOFIE C. BROOKS
COURTNEY C. MERRILL
WILMER CUTLER PICKERING
HALE AND DORR LLP
60 State Street
Boston, MA 02109
(617) 526-6000

L. NORWOOD JAMESON
MATTHEW C. GAUDET
DUANE MORRIS, LLP
1075 Peachtree Street, N.E., Suite 1700
Atlanta, Georgia 30309-3929
(404) 253-6900

August 27, 2021 *Attorneys for Defendant-Appellant Cisco Systems, Inc.*

REPRESENTATIVE PATENT CLAIMS

U.S. Patent No. 9,203,806 ("Rule Swap")

9. A system comprising:
a plurality of processors; and
a memory comprising instructions that when executed by at least one processor of the plurality of processors cause the system to:
receive a first rule set and a second rule set;
preprocess the first rule set and the second rule set to optimize performance of the system for processing packets in accordance with at least one of the first rule set or the second rule set;
configure at least two processors of the plurality of processors to process packets in accordance with the first rule set;
after preprocessing the first rule set and the second rule set and configuring the at least two processors to process packets in accordance with the first rule set, receive a plurality of packets;
process, in accordance with the first rule set, a portion of the plurality of packets;
signal, each processor of the at least two processors, to process packets in accordance with the second rule set; and
configure, each processor of the at least two processors to, responsive to being signaled to process packets in accordance with the second rule set:
cease processing of one or more packets;
cache the one or more packets;
reconfigure to process packets in accordance with the second rule set;
signal completion of reconfiguration to process packets in accordance with the second rule set; and
responsive to receiving signaling that each other processor of the at least two processors has completed reconfiguration to process packets in accordance with the second rule set, process, in accordance with the second rule set, the one or more packets.

U.S. Patent No. 9,917,856 ("Packet Filtering")

24. A packet-filtering system comprising:
at least one hardware processor; and
memory storing instructions that when executed by the at least one hardware processor cause the packet-filtering system to:

receive data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprise a domain name identified as a network threat:
identify packets comprising unencrypted data;
identify packets comprising encrypted data;
determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;
filter, based on at least one of a uniform resource identifier (URI) specified by a plurality of packet filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules:
packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators; and
the determined packets comprising the encrypted data that corresponds to the one or more network threat indicators; and
route, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.

U.S. Patent No. 9,560,176 ("Correlation")

11. A system comprising:
at least one processor; and
a memory storing instructions that when executed by the at least one processor cause the system to:
identify a plurality of packets received by a network device from a host located in a first network;
generate a plurality of log entries corresponding to the plurality of packets received by the network device;
identify a plurality of packets transmitted by the network device to a host located in a second network;

generate a plurality of log entries corresponding to the plurality of packets transmitted by the network device;
correlate, based on the plurality of log entries corresponding to the plurality of packets received by the network device and the plurality of log entries corresponding to the plurality of packets transmitted by the network device, the plurality of packets transmitted by the network device with the plurality of packets received by the network device; and
responsive to correlating the plurality of packets transmitted by the network device with the plurality of packets received by the network device:
generate, based on the correlating, one or more rules configured to identify packets received from the host located in the first network; and
provision a device located in the first network with the one or more rules configured to identify packets received from the host located in the first network.

U.S. Patent No. 9.686,193 ("Forward or Drop")

18. A system comprising:
at least one processor; and
a memory storing instructions that when executed by the at least one processor cause the system to:
receive, from a computing device located in a first network, a plurality of packets wherein the plurality of packets comprises a first portion of packets and a second portion of packets;
responsive to a determination that the first portion of packets comprises data corresponding to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network, wherein the data indicates that the first portion of packets is destined for the second network:
apply, to each packet in the first portion of packets, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and
drop each packet in the first portion of packets; and
responsive to a determination that the second portion of packets comprises data that does not correspond to the criteria. wherein the

data indicates that the second portion of packets is destined for a third network:

apply, to each packet in the second portion of packets, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, a second operator configured to forward packets not associated with the particular type of data transfer toward the third network; and

forward each packet in the second portion of packets toward the third network.

CERTIFICATE OF INTEREST

Counsel for Defendant-Appellant Cisco Systems, Inc. certifies the following:

1. Represented Entities. Fed. Cir. R. 47.4(a)(1). Provide the full names of all entities represented by undersigned counsel in this case.

Cisco Systems, Inc.

2. Real Party in Interest. Fed. Cir. R. 47.4(a)(2). Provide the full names of all real parties in interest for the entities. Do not list the real parties if they are the same as the entities.

Not applicable.

3. Parent Corporations and Stockholders. Fed. Cir. R. 47.4(a)(3). Provide the full names of all parent corporations for the entities and all publicly held companies that own 10% or more stock in the entities.

None.

4. Legal Representatives. List all law firms, partners, and associates that (a) appeared for the entities in the originating court or agency or (b) are expected to appear in this court for the entities. Do not include those who have already entered an appearance in this court. Fed. Cir. R. 47.4(a)(4).

DUANE MORRIS, LLP: Kevin P. Anderson, John M. Baird, Jennifer H. Forte, John R. Gibson, Nicole E. Johnson, Daniel T. McCloskey, Joseph A. Powers, Christopher J. Tyson

DAVIS POLK & WARDWELL LLP: Micah G. Block, Neil H. MacBride, James Y. Park

TROUTMAN PEPPER HAMILTON SANDERS LLP: Dabney J. Carr, IV

BENESCH, FRIEDLANDER, COPLAN & ARONOFF LLP: Joel E. Connolly, Christopher L. Letkewicz

ORRICK HERRINGTON & SUTCLIFFE LLP: Elizabeth Rose Moulton

5. Related Cases. Provide the case titles and numbers of any case known to be pending in this court or any other court or agency that will directly affect or be directly affected by this court's decision in the pending appeal. Do not include the originating case number(s) for this case. Fed. Cir. R. 47.4(a)(5). See also Fed. Cir. R. 47.5(b).

Reexamination No. 90/014,476 (USPTO)

6. Organizational Victims and Bankruptcy Cases. Provide any information required under Fed. R. App. P. 26.1(b) (organizational victims in criminal cases) and 26.1(c) (bankruptcy case debtors and trustees). Fed. Cir. R. 47.4(a)(6).

None.

Dated: August 27, 2021

/s/ William F. Lee
WILLIAM F. LEE
WILMER CUTLER PICKERING
HALE AND DORR LLP
60 State Street
Boston, MA 02109
(617) 526-6000

TABLE OF CONTENTS

Page

REPRESENTATIVE PATENT CLAIMS

CERTIFICATE OF INTEREST i

TABLE OF AUTHORITIES vi

STATEMENT OF RELATED CASES 1

INTRODUCTION 3

JURISDICTIONAL STATEMENT 4

STATEMENT OF ISSUES 5

STATEMENT OF THE CASE 5

A. Cisco's Core Networking Products: Switches, Routers, And Firewalls 5

B. Cisco's Network Security Products 6

C. Centripetal's RuleGATE And Its Failure In The Market 9

D. District Court Proceedings 11

SUMMARY OF ARGUMENT 14

ARGUMENT 16

I. STANDARD OF REVIEW 16

II. THE JUDGMENT CANNOT STAND BECAUSE THE DISTRICT COURT FOUND NO ACTS OF DIRECT INFRINGEMENT AND DID NOT LIMIT DAMAGES TO ANY DIRECT INFRINGEMENT 16

A. The District Court Legally Erred By Finding Direct Infringement Even Though Cisco Did Not Make, Use, Sell, Or Offer To Sell Any Product Practicing The Claims 16

B. At A Minimum, The Court Erred By Awarding Damages Based On Revenues From Every Sale Of The Accused Products, Rather Than Limiting The Award To The Specific Accused Combinations....21

III. THE INFRINGEMENT FINDINGS SHOULD BE REVERSED OR VACATED....23

A. '806 "Rule Swap" Patent....23

1. Background....23

2. The accused product combinations do not "cease processing" or "cache" packets "responsive to being signaled"....24

B. '856 "Packet Filtering" Patent....28

1. Background....28

2. The accused product combination does not "filter … the determined packets"....30

a. The court implicitly misconstrued "packets"....30

b. Stealthwatch does not "filter … the determined packets"....32

C. '176 "Correlation" Patent....37

1. Background....37

2. The accused product combination does not "correlate" transmitted packets with received packets....38

a. The accused combination does not "correlate" packets based on ingress and egress NetFlow records....38

b. The district court's sua sponte infringement theories are unsupported....41

D. '193 "Forward or Drop" Patent....43

Keysight, EX-1028
Page 9

1. Background 43

2. The accused product combination does not forward or drop packets depending on whether they are "associated with [a] particular type of data transfer" 45

IV. THE DAMAGES AWARD SHOULD BE VACATED 51

A. The Court Erred By Adopting Centripetal's Flawed Apportionment Analysis 51

B. The Royalty Rate Was Wrongly Drawn From A Single Non-Comparable License Centripetal Secured As A Settlement 56

C. A New Damages Trial (And Recalculation Of Other Monetary Awards) Is Required If This Court Sets Aside Any Of The Infringement Findings 57

V. THE DISTRICT COURT CLEARLY ERRED IN FINDING WILLFULNESS AND ABUSED ITS DISCRETION IN ENHANCING DAMAGES 58

A. Cisco Did Not Copy Centripetal 59

B. The Case Was Close 62

VI. THE JUDGMENT SHOULD BE VACATED BECAUSE THE DISTRICT JUDGE WAS STATUTORILY DISQUALIFIED 64

CONCLUSION 67

ADDENDUM

CERTIFICATE OF SERVICE

CERTIFICATE OF COMPLIANCE

CONFIDENTIAL MATERIAL OMITTED

The material omitted from pages 56 and 57 contains a description of a confidential license agreement between Centripetal and a third party that was sealed in the district court.

TABLE OF AUTHORITIES

CASES

Page(s)

01 Communique Laboratory, Inc. v. Citrix Systems, Inc.,
889 F.3d 735 (Fed. Cir. 2018) 63

Amazon.com, Inc. v. Barnesandnoble.com, Inc.,
239 F.3d 1343 (Fed. Cir. 2001) 51, 59

Amgen Inc. v. Sandoz Inc.,
923 F.3d 1023 (Fed. Cir. 2019) 16

Aro Manufacturing Co. v. Convertible Top Replacement Co.,
365 U.S. 336 (1961).....17

AstraZeneca AB v. Apotex Corp.,
782 F.3d 1324 (Fed. Cir. 2015) 21

Aylus Networks, Inc. v. Apple Inc.,
856 F.3d 1353 (Fed. Cir. 2017) 50

Cardiac Pacemakers, Inc. v. St. Jude Medical, Inc.,
576 F.3d 1348 (Fed. Cir. 2009) 22

Centripetal Networks, Inc. v. Cisco Systems, Inc.,
__ F. Supp. 3d __, 2021 WL 1030286 (E.D. Va. Mar. 17, 2021) 13

Centripetal Networks, Inc. v. Cisco Systems, Inc.,
492 F. Supp. 3d 495 (E.D. Va. Oct. 5, 2020) 13

Centripetal Networks, Inc. v. Cisco Systems, Inc.,
847 F. App'x 869 (Fed. Cir. 2021) (nonprecedential).....43

Chase Manhattan Bank v. Affiliated FM Insurance Co.,
343 F.3d 120 (2d Cir. 2003) 66

Commonwealth Scientific & Industrial Research Organisation v. Cisco Systems, Inc.,
809 F.3d 1295 (Fed. Cir. 2015) 51

Corning v. Fast Felt Corp.,
873 F.3d 896 (Fed. Cir. 2017) 31

DDR Holdings, LLC v. Hotels.com, L.P.,
773 F.3d 1245 (Fed. Cir. 2014) 57

Deepsouth Packing Co. v. Laitram Corp.,
406 U.S. 518 (1972).....17

E.I. du Pont de Nemours & Co. v. Unifrax I LLC,
921 F.3d 1060 (Fed. Cir. 2019) 24

Enplas Display Device Corp. v. Seoul Semiconductor Co.,
909 F.3d 398 (Fed. Cir. 2018) 21

Ericsson, Inc. v. D-Link Systems, Inc.,
773 F.3d 1201 (Fed. Cir. 2014) 55

Exmark Manufacturing Co. v. Briggs & Stratton Power Products Group, LLC,
879 F.3d 1332 (Fed. Cir. 2018) 51

Finjan Inc. v. Blue Coat Systems, Inc.,
879 F.3d 1299 (Fed. Cir. 2018) 54, 55

Finjan, Inc. v. SonicWall Inc.,
No. 5:17-cv-04467 (N.D. Cal. May 21, 2021), ECF No. 477 .....2, 55

Garretson v. Clark,
111 U.S. 120 (1884).....51

Halo Electronics, Inc. v. Pulse Electronics, Inc.,
136 S. Ct. 1923 (2016).....58

IGT v. Bally Gaming International Inc.,
610 F. Supp. 2d 288 (D. Del. 2009), *aff'd*, 659 F.3d 1109 (Fed. Cir. 2011) 26

Immunex Corp. v. Sandoz Inc.,
964 F.3d 1049 (Fed. Cir. 2020) 16

In re Cement Antitrust Litigation,
688 F.2d 1297 (9th Cir. 1982) 66

Intel Corp. v. Broadcom Corp.,
No. Civ.A. 00-796-SLR, 2003 WL 360256 (D. Del. Feb. 13, 2003) 26-27

LaserDynamics, Inc. v. Quanta Computer,
694 F.3d 51 (Fed. Cir. 2012) 56, 57

Liljeberg v. Health Services Acquisition Corp.,
486 U.S. 847 (1988).....66

Lucent Technologies, Inc. v. Gateway, Inc.,
580 F.3d 1301 (Fed. Cir. 2009) 22, 51

MAG Aerospace Industries v. B/E Aerospace, Inc.,
816 F.3d 1374 (Fed. Cir. 2016) 36

MLC Intellectual Property, LLC v. Micron Technology, Inc.,
No. 2020-1413, __ F.4th __, 2021 WL 3778405 (Fed. Cir. Aug.
26, 2021) 55, 57

Nease v. Ford Motor Co.,
848 F.3d 219 (4th Cir. 2017) 16

Newport News Holdings Corp. v. Virtual City Vision, Inc.,
650 F.3d 423 (4th Cir. 2011) 16

Omega Patents, LLC v. CalAmp Corp.,
920 F.3d 1337 (Fed. Cir. 2019) 23, 57

Paice LLC v. Toyota Motor Corp.,
504 F.3d 1293 (Fed. Cir. 2007) 58

Polara Engineering Inc. v. Campbell Co.,
894 F.3d 1339 (Fed. Cir. 2018) 62, 63

Regents of University of Minnesota v. AGA Medical Corp.,
717 F.3d 929 (Fed. Cir. 2013) 36

Rite-Hite Corp. v. Kelley Co.,
56 F.3d 1538 (Fed. Cir. 1995) 58

Rotec Industries, Inc. v. Mitsubishi Corp.,
215 F.3d 1246 (Fed. Cir. 2000) 17

Rude v. Westcott,
130 U.S. 152 (1889).....56

Shell Oil Co. v. United States,
672 F.3d 1283 (Fed. Cir. 2012) 64, 65, 66

TrafFix Devices, Inc. v. Marketing Displays, Inc.,
532 U.S. 23 (2001).....59

Twigg v. Norton Co.,
894 F.2d 672 (4th Cir. 1990) 42, 43

Verizon Services Corp. v. Vonage Holdings Corp.,
503 F.3d 1295 (Fed. Cir. 2007) 57

VirnetX, Inc. v. Cisco Systems, Inc.,
767 F.3d 1308 (Fed. Cir. 2014) 51, 56

Whitserve, LLC v. Computer Packages, Inc.,
694 F.3d 10 (Fed. Cir. 2012) 57

Wi-Lan, Inc. v. Apple, Inc.,
811 F.3d 455 (Fed. Cir. 2016) 34

Wordtech Systems, Inc. v. Integrated Networks Solutions, Inc.,
609 F.3d 1308 (Fed. Cir. 2010) 57

STATUTES AND REGULATIONS

28 U.S.C.
§ 455(b).....*passim*
§ 455(b)(4) 64, 65, 66, 67
§ 455(c) 66
§ 455(d)(4) 64
§ 455(f).....65
§ 1295(a)(1) 5
§ 1338(a) 4

35 U.S.C.
§ 271(a) 3, 17, 20
§ 271(b) 19
§ 271(c) 19
§ 283 58
§ 284 21

5 C.F.R. § 2634.403(a)(2) 66

LEGISLATIVE MATERIAL

H.R. Rep. No. 93-1453, 93d Cong., 2d Sess. 1974, *reprinted in* 1974 U.S.C.C.A.N. 6351 (Oct. 9, 1974) 66

OTHER AUTHORITIES

Judicial Conference of the United States, Committee on Codes of Conduct, Advisory Opinion No. 110 65

McKeown, Hon. M. Margaret, *To Judge or Not to Judge: Transparency and Recusal in the Federal System*, 30 Rev. Litig. 653 (2011) 65-66

STATEMENT OF RELATED CASES

No appeal in this case was previously before this Court or any other court.

Plaintiff-appellee Centripetal Networks, Inc. ("Centripetal") previously asserted in this case that defendant-appellant Cisco Systems, Inc. ("Cisco") infringed various patent claims that the Patent Trial and Appeal Board ("PTAB") later held unpatentable in *inter partes* review ("IPR"). Centripetal dropped those claims from the district court litigation and they are not at issue in this appeal. This Court has affirmed the PTAB's unpatentability decisions in the following judgments, all captioned *Centripetal Networks, Inc. v. Cisco Systems, Inc.*:

- Nos. 20-1634, 20-1829 (Fed. Cir. May 11, 2021) (Rule 36 affirmance) (Prost, C.J., Lourie & Reyna, JJ.) (U.S. Patent No. 9,565,213);
- No. 20-1768 (Fed. Cir. May 11, 2021) (Rule 36 affirmance) (Prost, C.J., Lourie & Reyna, JJ.) (U.S. Patent No. 9,674,148);
- Nos. 20-1713, 20-1714, 20-1885 (Fed. Cir. May 11, 2021) (Prost, C.J., Lourie & Reyna, JJ.) (Rule 36 affirmance) (U.S. Patent No. 9,137,205);
- Nos. 20-1635, 20-1636 (Fed. Cir. Mar. 10, 2021) (Taranto, J., joined by Moore & Schall, JJ.) (U.S. Patent Nos. 9,124,552 and 9,160,713), *pet. for cert. filed*, No. 21-193 (U.S. Aug. 11, 2021);

- No. 20-2057 (Fed. Cir. Mar. 10, 2021) (Taranto, J., joined by Moore & Schall, JJ.) (U.S. Patent No. 9,413,722), *pet. for cert. filed*, No. 21-193 (U.S. Aug. 11, 2021).

The following case may be affected by the Court's decision in this appeal: in *Finjan, Inc. v. SonicWall Inc.*, No. 5:17-cv-04467 (N.D. Cal. May 21, 2021), ECF No. 477, expert witness Dr. Aaron Striegel proffered a similar damages theory as he did for Centripetal in this case, and the district court excluded his testimony as unreliable. Dr. Striegel's damages theory is discussed below at pages 51-56.

Counsel for Cisco is aware of no other case pending in this Court or any other court that would directly affect or be directly affected by the Court's decision in this appeal.

Keysight, EX-1028
Page 17

INTRODUCTION

Following a remote bench trial, the district court found that Cisco infringed four Centripetal patents and entered a judgment that, with ongoing royalties, exceeds $2.75 billion. That judgment is the result of multiple misunderstandings of patent law. Even on their own terms, the district court's findings cannot support it.

First, although Centripetal's infringement theories each required combining multiple separately-sold Cisco products in specific ways, the court nowhere found that Cisco did that. Indeed, the district court made no finding that Cisco committed any act of direct infringement under 35 U.S.C. § 271(a), and Centripetal disavowed theories of induced and contributory infringement. The court's failure to find that Cisco made, used, offered for sale, or sold the patented inventions compels reversal as to infringement and, at a minimum, shows that the damages award rests on a grossly overstated royalty base.

Second, the court's comparison of the accused products to the asserted claims was fatally deficient. At Centripetal's invitation, the court repeatedly ignored critical elements in the lengthy claims, which arise in a crowded field of prior art, and improperly generalized the specific functions performed by Cisco's products. As a result, it identified no evidence that Cisco's products satisfied key claim limitations.

Third, the damages award rests on a royalty that was anything but reasonable. Rather than apportion the overstated royalty base to the claimed inventions, the district court relied on a collection of high-level product "functions," many of which were generic or not even accused of infringement. The court then applied an inflated royalty rate taken from an inapposite mid-trial litigation settlement.

Finally, after revealing a late-discovered disqualifying financial interest, the district judge nonetheless held onto the case for months, issuing two lengthy post-trial opinions and entering a blockbuster damages judgment—despite a bright-line statutory obligation to recuse himself. The court's opinions contained numerous sharp and unfounded accusations against Cisco, such as faulting Cisco for using trial demonstratives in this technically-complicated case, even though Centripetal did exactly the same thing and the court relied on demonstratives in its opinions. The court then enhanced damages 2.5-fold, accounting for over $1 billion of the judgment, even though Centripetal lost on seven out of eleven originally-asserted patents and there was no evidence that Cisco copied any claimed feature.

For any of these reasons, the judgment should be reversed or vacated.

JURISDICTIONAL STATEMENT

The district court had jurisdiction under 28 U.S.C. § 1338(a), entered final judgment on October 5, 2020 (Appx18380), and denied timely post-judgment

Keysight, EX-1028
Page 19

motions on March 17, 2021 (Appx222-271). Cisco timely appealed. Appx18563-18565. This Court has jurisdiction under 28 U.S.C. § 1295(a)(1).

STATEMENT OF ISSUES

1. Whether the infringement judgment and/or damages award should be reversed or vacated because Centripetal did not prove—and the district court did not find—that Cisco made, used, offered for sale, or sold any product practicing the asserted claims.

2. Whether the infringement findings are clearly erroneous and/or rest on legal errors.

3. Whether the damages award should be reversed or vacated for lack of apportionment or reliance on a noncomparable settlement license.

4. Whether the district court clearly erred in finding willful infringement and enhancing the damages award 2.5 times.

5. Whether the district judge should have recused himself under 28 U.S.C. § 455(b).

STATEMENT OF THE CASE

A. Cisco's Core Networking Products: Switches, Routers, And Firewalls

Founded in 1984 by two Stanford computer scientists, Cisco is a leader in networking technology. Cisco spends billions annually on research and development on computing technology. Appx1205(205:17-21).

Cisco's success dates back decades, based largely on three core networking products forming the modern Internet's backbone:

Switches: Cisco has sold switches since the 1980s. Appx4491(3480:14-17). Similar to a telephone switchboard operator, computer switches connect computing devices within a local network, such as two different computers or a computer and printer. Appx51-52.

Routers: Cisco invented routing technology in the mid-1980s. Appx1204-1205(204:22-205:13). Like a dispatcher sending vehicles to a specific location, a router determines the optimal path to send data traffic units ("packets") to their intended destination. While switches connect devices together in small networks, routers transmit data between those networks, thus forming larger networks. Appx52; Appx55.

Firewalls: Cisco has sold firewalls since the early 2000s. Appx3508-3509(2502:16-2503:3). Firewalls separate a network from potentially dangerous data outside the network. Appx52-53; Appx63.

B. Cisco's Network Security Products

Cisco also invests heavily in sophisticated network security products that protect data from theft or interference. Centripetal accused a subset of Cisco's many security products.

Keysight, EX-1028
Page 21

Stealthwatch: Stealthwatch is a hardware device that runs various software applications to detect threats in computer traffic. Appx62; Appx77-78(¶¶15-20); Appx1453(453:7-13). Stealthwatch detects threats by receiving so-called "NetFlow" information from routers and switches. Appx77-78(¶¶15-20); Appx113-114(¶15). Cisco invented NetFlow in 1996. Appx1136(136:5-10); Appx1214(214:6-10). NetFlow summarizes data about packets that have already passed through a given router or switch. Appx77(¶16); Appx113(¶¶12-13). Stealthwatch compares the NetFlow data to known information about potential security threats (often called "threat intelligence") to identify whether packets posing potential threats have infiltrated the network. Appx77-78(¶¶15-20).

Customers can add two other products to Stealthwatch to provide additional threat-detection capabilities:

1. ***Cognitive Threat Analytics ("CTA"):*** CTA is a Cisco-created software tool that interacts with Stealthwatch to compare NetFlow and other packet flow summaries to threat intelligence. Appx62; Appx113-114(¶¶15-16); Appx1155-1158(155:4-158:1). CTA runs separately in the cloud, not on the Stealthwatch device. Appx2698-2699(1695:6-1696:20). CTA enhances Stealthwatch's threat-detection capability by using more sophisticated algorithms, including machine learning and artificial intelligence ("AI"). Appx2690-2691(1687:20-1688:6).

2. Encrypted Traffic Analytics ("ETA"): ETA is another Cisco-created software tool that interacts with Stealthwatch to detect threats in encrypted computer traffic. Appx62-63; Appx75-78(¶¶10-20). ETA adds additional information fields to NetFlow records and includes additional algorithms using machine learning and AI. Appx76-77(¶12); Appx2695(1692:3-12); Appx5206.

Identity Services Engine ("ISE"): ISE is a management device for tracking user and computer identities on a network and for administering access to other network devices. Appx62; Appx1149(149:16-23). For example, ISE could prevent an employee in a company's shipping department from accessing computers in the payroll department. Appx79(¶22); Appx3205-3206(2202:5-2203:25).[1]

Digital Network Architecture ("DNA"): DNA is a network management device used to configure other network devices, troubleshoot, and interact with routers and switches on the network. Appx61-62. DNA is especially useful when configuring a new router/switch on a large network containing many

[1] The district court correctly identified ISE as a "device." Appx62. It later attempted to retreat from this finding, insisting that ISE was "part of Cisco's infringing software," but cited nothing. Appx257-258. The court was right the first time; ISE is a separate device. Appx2002(1002:24-25) (Centripetal's expert calling ISE a "device"); Appx2006-2007(1006:19-1007:5).

routers/switches, as it ensures that they operate properly. Appx1148-1149(148:22-149:6).

Firepower Management Center ("FMC"): FMC is a device used to configure and operate a network's firewall devices. Appx63.

Each of the above-described Cisco products—routers, switches, firewalls, Stealthwatch (optionally with CTA and/or ETA), ISE, DNA, and FMC—is a standalone product that a customer can purchase on its own or combine with innumerable other Cisco or third-party products.

C. Centripetal's RuleGATE And Its Failure In The Market

Centripetal, founded in 2009, does not compete with Cisco in the marketplace for routers, switches, and firewalls. In fact, Centripetal bought switches from Cisco. Appx5805-5806; Appx5934-5935(14:24-22:15). Instead, Centripetal set out to supplement (not replace) existing network security solutions like Cisco's. Appx1270-1273(270:4-273:1); Appx5458-5459. In 2014, Centripetal launched a hardware product called "RuleGATE." Like many prior art products Cisco and others sold, RuleGATE applied "rules" to identify and filter out suspicious data packets before they entered a network. Appx1268(268:1-11); Appx5875(47:4-9); Appx5876(66:4-7). RuleGATE's innovation was that, unlike prior products that applied only tens of thousands of rules at a time, RuleGATE

Keysight, EX-1028
Page 24

could apply ***millions*** of rules. Appx1277(277:1-8); Appx2263(1261:6-22). The patents-in-suit arose from this work.

In 2015 and 2016, Centripetal repeatedly solicited Cisco for investment. The companies signed a standard nondisclosure agreement and had meetings that were "high-level" and akin to a "marketing presentation," as meeting materials and attendee testimony confirmed. Appx3819-3820(2811:17-2812:19) (Cisco attendee); Appx5125-5131 (Centripetal presentation); Appx5876-5877(76:21-77:20) (Centripetal attendee); Appx5897-5898(34:2-34:12). No witness testified that Centripetal gave Cisco any source code or details of any specific algorithm. Appx2281-2283(1279:17-1281:16) (Centripetal founder); Appx5873(36:13-19) (Centripetal attendee); Appx5897-5898(33:4-34:25) (Centripetal attendee). Centripetal's presentations focused on RuleGATE's ability to apply millions of rules to incoming packets.

Cisco was not interested in Centripetal's technology. Cisco's products already applied tens of thousands of rules, which Cisco believed sufficiently balanced security with communication speed; millions of rules would unacceptably slow down network traffic. Appx1124(124:6-16); Appx2263(1261:6-22); Appx3475-3476(2470:20-2471:7); Appx3852-3853(2844:13-2845:16); Appx5053-5055. There is no evidence that anyone at Cisco "look[ed]" at any Centripetal algorithms or studied its patent claims. Appx3824-3825(2816:22-2817:25) (Cisco

employee). No evidence suggested that Cisco relied on anything from Centripetal in designing the accused products or features. And no evidence exists that Centripetal ever told Cisco, prior to filing suit, that Cisco needed to license its patents or that any Cisco product infringed.

Centripetal attempted to partner with other companies, even retaining a financial institution, Oppenheimer, to reach out to numerous potential investors. Appx1294-1296(294:5-296:3); Appx2292-2293(1290:1-5, 1290:19-1291:5). Nothing panned out. Its business failing to gain traction, Centripetal opted to sue.

D. District Court Proceedings

Centripetal asserted eleven patents against Cisco. The Patent Office invalidated six over the crowded field of prior art. The district court held a 23-day remote bench trial on the other five patents. Appx395-410(entries 430-550).

After trial but before issuing his opinion, the district judge disclosed that his wife bought Cisco stock nine months earlier and held it throughout the trial and the court's deliberation. Appx30. The judge refused to recuse himself. Appx41.

The court ultimately found that Cisco did not infringe one patent (the '205 patent), but directly infringed the remaining four. Importantly, the district court did not and could not find that the making, use, or sale of any one Cisco product ***by itself*** infringed any patent claim. Rather, the court's infringement findings required that separately-sold devices be ***combined*** in specific implementations:

Keysight, EX-1028
Page 26

Patent	Accused Product Combination
’806	Switches/routers combined with DNA Center Firewalls combined with FMC
’856	Switches/routers combined with Stealthwatch and ISE
’176	Switches/routers combined with Stealthwatch
’193	Switches/routers combined with ISE

See infra pp. 16-21. Centripetal did not assert, and the district court did not find, infringement by equivalents for any limitation relevant here.[2]

The court also held that Cisco’s infringement was willful due to supposed “copying” and because it believed Cisco “did not advance any objectively reasonable defenses.” Appx200; Appx203. Relatedly, the court leveled numerous sharp (and baseless) accusations against Cisco. For instance, the court faulted Cisco for using “animations prepared ex post facto for trial” in this complicated trial conducted remotely over videoconference (*e.g.*, Appx202), even though Centripetal used demonstratives too (*e.g.*, Appx1523(523:14-15); Appx1758-1759(758:24-759:12); Appx1911-1912(911:18-912:12); Appx1975-1976(975:22-976:9)); the court relied on demonstratives in its opinion (Appx63-64; Appx164);

[2] *See* Appx84; Appx115; Appx132-133; Appx150; Appx1549-1551(549:22-551:20); Appx1713-1714(713:1-714:18); Appx2087-2088(1087:13-1088:7); Appx17935-174936.

and Cisco called several knowledgeable technical witnesses (Appx48-50; *see also infra* pp. 62-64).

The court awarded damages of $755,808,545, which it enhanced 2.5 times to $1,889,521,362.50. The court denied Centripetal's requested injunction, but awarded a six-year ongoing royalty with a minimum value of $754,701,723.30. Appx209.

Cisco moved to amend the judgment and for a new trial. Cisco reiterated that Centripetal disavowed any indirect infringement theory and failed to prove direct infringement because Centripetal asserted only that separate Cisco devices, if combined together, would practice the claims—not that Cisco actually made, used, or sold such an infringing combination. Appx18433. Alternatively, Cisco explained that, at a minimum, the royalty should be confined to instances where Cisco actually sold products together in the accused combinations. Appx18429-18440. The district court denied Cisco's post-judgment motions.[3]

[3] The district court's merits opinion is published at 492 F. Supp. 3d 495, and the order denying post-judgment motions at __ F. Supp. 3d __, 2021 WL 1030286.

SUMMARY OF ARGUMENT

1. Centripetal asserted only that Cisco itself directly infringed the patents-in-suit, disavowing all indirect infringement theories. But Centripetal offered no evidence, and the court made no finding, that Cisco made, used, sold, or offered to sell any patented invention. Rather, the evidence shows only sales of separate devices that Centripetal said would infringe if combined together. Sale of separate components that *could* infringe if combined is not direct infringement. At a minimum, the royalty base should have been limited to sales of particular accused combinations, as opposed to sales of individual products that do not infringe on their own.

2. At Centripetal's invitation, the district court effectively read out key limitations, finding infringement without identifying any evidence that Cisco's products, even in combination, would practice them. The '806 patent requires taking actions "responsive to being signaled"; the court found infringement by actions taken irrespective of any signal. The '856 patent requires filtering "packets"; the court relied on analysis of NetFlow records, which are undisputedly not "packets." The '176 patent requires correlating transmitted packets to received packets; the court relied on correlations of NetFlow records to external threat intelligence, neither of which are packets. And the '193 patent requires filtering

packets depending on the "type of data transfer"; the court nowhere found that Cisco's products do that.

3. The damages award rested on an excessive royalty base that did not apportion the patented inventions' contribution, but rather claimed for Centripetal the value of "top-level functions" that were either generic or not accused of infringing, such as a "processor" or "Advanced Security." The royalty rate was also unjustified, as it rested on a single, inapposite settlement agreement between Centripetal and a third party.

4. The willfulness and enhancement findings are unwarranted. No evidence showed that Cisco copied Centripetal, Centripetal had not shared confidential information regarding the patented technology, and no witness identified anything in Cisco's products originating from Centripetal. The court's criticisms of Cisco's defenses were unfair and erroneous, and certainly did not warrant a 2.5-factor enhancement of over $1 billion.

5. The district judge was disqualified by his wife's financial interest in Cisco, which arose in the case's early stages and persisted through post-trial rulings. 28 U.S.C. § 455(b) required recusal or divestment upon discovery of the interest, yet the court did neither. Public confidence in the judiciary's compliance with its statutory obligations requires vacatur in this high-profile case.

Keysight, EX-1028
Page 30

ARGUMENT

I. STANDARD OF REVIEW

Claim construction is reviewed *de novo*. *Amgen Inc. v. Sandoz Inc.*, 923 F.3d 1023, 1027 (Fed. Cir. 2019). Factual findings are reviewed for clear error, legal conclusions *de novo*. *Immunex Corp. v. Sandoz Inc.*, 964 F.3d 1049, 1056 (Fed. Cir. 2020). This Court finds clear error when, "despite some supporting evidence, [it is] left with the definite and firm conviction that a mistake has been made." *Id.* (quotation marks omitted). Decisions regarding exclusion of expert testimony and recusal are reviewed for abuse of discretion, which includes an error of law or clearly erroneous factual finding. *Nease v. Ford Motor Co.*, 848 F.3d 219, 228 (4th Cir. 2017); *Newport News Holdings Corp. v. Virtual City Vision, Inc.*, 650 F.3d 423, 432 (4th Cir. 2011).

II. THE JUDGMENT CANNOT STAND BECAUSE THE DISTRICT COURT FOUND NO ACTS OF DIRECT INFRINGEMENT AND DID NOT LIMIT DAMAGES TO ANY DIRECT INFRINGEMENT

A. The District Court Legally Erred By Finding Direct Infringement Even Though Cisco Did Not Make, Use, Sell, Or Offer To Sell Any Product Practicing The Claims

Centripetal conceded that it relied exclusively on direct infringement and made no "assertions of contributory or inducing infringement." Appx18490. As relevant here, direct infringement occurs only if the defendant "without authority makes, uses, offers to sell, or sells any patented invention, within the United

States." 35 U.S.C. § 271(a). Because direct infringement requires a "patented invention," the manufacture or sale of ***components*** that could be ***combined*** into a patented invention is not direct infringement. *See Deepsouth Packing Co. v. Laitram Corp.*, 406 U.S. 518, 523-524, 528 (1972) (selling machine parts to customers who would assemble the complete machine did not directly infringe a patent on the machine, because § 271(a) "protects only against the operable assembly of the whole and not the manufacture of its parts"); *see also Aro Mfg. Co. v. Convertible Top Replacement Co.*, 365 U.S. 336, 344 (1961). "[A]s to claims brought under § 271(a), *Deepsouth* remains good law: one may not be held liable under § 271(a) for 'making' or 'selling' less than a complete invention." *Rotec Indus., Inc. v. Mitsubishi Corp.*, 215 F.3d 1246, 1252 n.2 (Fed. Cir. 2000).

That principle resolves this case, as the court's infringement findings depended on combinations of separately-sold Cisco products:

(1) The court found the '806 patent infringed by Cisco's routers and switches, but only "in combination with Cisco's Digital Network Architecture" device. Appx150; *see also* Appx143-144(¶¶12, 14). Similarly, the court found the '806 patent infringed by Cisco's firewall products, but only when used "with [the] Firepower Management Center" device. Appx150; *see also* Appx144(¶¶13, 15).

Keysight, EX-1028
Page 32

(2) The court found the '856 patent infringed by Cisco's routers and switches, but only "in combination with Cisco's Stealthwatch and [ISE]" devices. Appx75(¶9); Appx84.

(3) The court found the '176 patent infringed by Cisco's routers and switches, but only "in combination with Cisco's Stealthwatch" device. Appx112(¶8); Appx115.

(4) The court found the '193 patent infringed by Cisco's routers and switches, but only together with Cisco's ISE device. Appx133 (analyzing "switches and routers aided with Cisco's Identity Services Engine," and observing that "[t]he Cisco packet-filtering system operates by using the Identity Services Engine"); Appx258 (relying on "Stealthwatch forwarding data to ISE which in turn forwards data to the switches and routers"); Appx259 ("the infringing software embedded in Cisco's switches and routers processes the data sent to them by ISE and Stealthwatch").[4]

The court thus did not find, and could not have found, that Cisco's routers, switches, and firewalls infringe by themselves. Its infringement findings depended

[4] Although the post-judgment order sought to minimize ISE's involvement (Appx258), it confirms that the infringement finding requires that data be sent "by ISE and StealthWatch via a two stage process" (Appx259). The court also relied on ISE to distinguish the claims from the prior art for invalidity purposes. Appx140 (holding that "the Identity Services Engine packet filtering system" "contains the functionality taught by the claims of the '193 Patent").

Keysight, EX-1028
Page 33

on specific combinations with other devices—Stealthwatch, ISE, DNA, or FMC. Nor did the court find that Cisco made, used, offered to sell, or sold a product embodying any complete patented invention. On the contrary, the various Cisco products are undisputedly distinct devices sold separately. *See, e.g.*, Appx232; Appx1802-1803(802:25-803:2) (Centripetal's expert Mitzenmacher agreeing that "not everyone who buys a Cisco router or switch buys Stealthwatch or has Stealthwatch"); Appx2058(1058:3-9) (Centripetal's expert Cole admitting that ISE is "sold independently").

Accordingly, direct infringement would only occur, if at all, when a customer purchased separate Cisco products and combined them together into a single system. Even if that would support a direct infringement claim against a *customer*, or an inducement or contributory infringement claim against Cisco (if the requirements of § 271(b) or (c) were met), Centripetal expressly disavowed such theories. Appx18490.

Cisco repeatedly pointed out this glaring evidentiary hole. Appx17329-17330(¶¶263-264); Appx17368-17369(¶397); Appx17397-17398(¶¶497-498); Appx17475(¶¶785-786); Appx17852-17853(¶¶36-37); Appx17861(¶¶66-67); Appx4483(3472:13-20). The court's initial opinion ignored it. Although Cisco raised it again (Appx18433-18438), the court's post-judgment opinion did not cite, much less attempt to distinguish, *Deepsouth* and *Aro*. Instead, the court sought to

Keysight, EX-1028
Page 34

sidestep § 271(a)'s requirements through three assertions not made in its original opinion. None has merit.

First, the court emphasized that ETA software is "embedded" in Cisco's switches. Appx230. But the court nowhere found that switches alone—even accounting for "embedded" software like ETA—infringed any asserted claim. Rather, infringement required combining switches with separate devices like Stealthwatch and ISE. *See supra* pp. 17-19.

Second, the district court cited Cisco's witness Dr. Schmidt, who testified that "'customers'" might assemble a "'layered defense'" that could include firewalls and "'tools like StealthWatch.'" Appx232 (quoting Appx3133(2130:7-20)). As explained above (p. 19), such evidence might support a direct infringement claim against *customers*. But it does not show that Cisco made, used, offered to sell, or sold the complete patented invention—as direct infringement under § 271(a) requires—rather than separate component pieces.

Finally, the court suggested that Cisco's production during discovery of "sales data" regarding the "accused products" was an admission that each "accused product[] contained in the sales data infringed." Appx236. But providing discovery on sales data for "accused products" does not concede infringement; even Centripetal never made such an argument. Nor did Cisco "deny[] that any sales of accused products have been proven." Appx241. Of course Cisco sold

each of the accused products. The point is that selling those products separately does not directly infringe; holding otherwise is legal error.

As in *Deepsouth*, sale of an invention's components is not direct infringement. This Court should accordingly reverse.

B. At A Minimum, The Court Erred By Awarding Damages Based On Revenues From Every Sale Of The Accused Products, Rather Than Limiting The Award To The Specific Accused Combinations

The district court adopted the analysis of Centripetal's expert Lance Gunderson, who testified that the royalty base should include ***every*** sale of ***every*** accused component, totaling $7.5 billion. Appx192. That was legal error.

Even if *Deepsouth* permitted a finding of direct infringement for sales of components that would infringe *if combined* (it does not, *supra* pp. 16-21), the royalty base under such a theory would at most be the sales of particular infringing combinations. A reasonable royalty "cannot include activities that do not constitute patent infringement, as patent damages are limited to those 'adequate to compensate for the infringement.'" *AstraZeneca AB v. Apotex Corp.*, 782 F.3d 1324, 1343 (Fed. Cir. 2015) (quoting 35 U.S.C. § 284); *see also Enplas Display Device Corp. v. Seoul Semiconductor Co.*, 909 F.3d 398, 411 (Fed. Cir. 2018) (overturning verdict based "in part, on non-infringing sales"). Indeed, because infringement damages must be "correlated, in some respect, to the extent" that customers use the patented invention, and the record was "conspicuously devoid"

Keysight, EX-1028
Page 36

of data on that issue, Centripetal has not proven any damages at all. *Lucent Techs., Inc. v. Gateway, Inc.*, 580 F.3d 1301, 1334 (Fed. Cir. 2009); *see also Cardiac Pacemakers, Inc. v. St. Jude Med., Inc.*, 576 F.3d 1348, 1359 (Fed. Cir. 2009) ("Cardiac can only receive infringement damages on those devices that actually performed the patented method during the relevant infringement period.").

Mr. Gunderson based his calculation on every accused device sold; he did not consider whether anyone purchased—much less used—the specific devices together in an accused combination. Appx2530(1527:12-25); *see also* Appx2549-2550(1546:25-1547:3) (conceding he had "not undertaken an analysis as to how many customers have put into use [the] infringing combinations").

For example, the court found that the '856 patent was only infringed by (1) Catalyst Switches used in combination with (2) Stealthwatch and (3) ISE. *See supra* p. 18. Mr. Gunderson was asked, "using the '856 patent as an example," if Cisco sold (1) 1000 Catalyst Switches, (2) 250 versions of Stealthwatch, and (3) 100 ISEs, how many sales could be considered in the royalty base. Appx2553-2554(1550:3-1551:7). To correctly answer this question, Mr. Gunderson should have at least identified the number of potentially infringing combinations sold. *Cf.* Appx3885-3886(2887:5-2888:22) (Cisco's damages expert Dr. Becker performing this calculation). Instead, Mr. Gunderson erroneously asserted 1350 infringing sales—i.e., counting each individual product sale, even though no individual

Keysight, EX-1028
Page 37

product infringes by itself. Appx2554(1551:1-7); *see also* Appx3886(2878:6-17) (Dr. Becker pointing out this error).

Because Centripetal's "damages theory was premised on [the defendant's] total actual sales of its accused products" but—at best—only a subset of those sales could infringe, the damages award should be vacated. *Omega Patents, LLC v. CalAmp Corp.*, 920 F.3d 1337, 1350 (Fed. Cir. 2019).[5]

III. THE INFRINGEMENT FINDINGS SHOULD BE REVERSED OR VACATED

A. '806 "Rule Swap" Patent

1. Background

One way to secure a network is to prevent transmission of packets that violate network security rules derived from "threat intelligence" information. Because threat intelligence evolves quickly, these sets of rules must be replaced frequently. The '806 patent, informally called the "Rule Swap Patent" (Appx141), claims a particular system for updating or "swapping" rule sets.

Asserted claims 9 and 17 recite a system and computer-readable media that use a first rule set to process packets, receive a "signal" to use a second rule set to process packets, and then, "***responsive to being signaled***," configure processors to:

[5] As explained above (p. 18 n. 4), the district court was wrong to suggest that the '193 patent could have been infringed by use of a single accused product. In any event, the court did not suggest that the entire damages award could have rested on the '193 patent alone. *See* Appx192; *infra* pp. 51-58.

"***cease processing*** of one or more packets"; "***cache*** the one or more packets"; reconfigure to apply the second rule set; and ultimately "process, in accordance with the second rule set, the one or more packets." Appx288(11:40-54).[6]

Cisco demonstrated that its products do not update rule sets in this way. Cisco prioritized continuous processing of packets over processing packets only with a new rule set, and thus Cisco's products swap rule sets during an idle period that occurs in the normal course of packet processing; they do not "cease processing" or "cache" packets in response to a signal to swap rule sets. The district court erred in rejecting Cisco's argument.

2. The accused product combinations do not "cease processing" or "cache" packets "responsive to being signaled"

The district court identified no evidence that Cisco's products cease processing and cache packets "responsive to being signaled to process packets in accordance with the second rule set." That was legal error and effectively read out a key limitation. *E.I. du Pont de Nemours & Co. v. Unifrax I LLC*, 921 F.3d 1060, 1073 (Fed. Cir. 2019) ("[I]f even one limitation is not met, there is no literal infringement.").

In the first place, the district court made no finding that the accused ***firewall*** products cease processing or cache packets ***at all***, much less responsive to being

[6] Emphases are added unless otherwise noted.

signaled. *See generally* Appx141-150; Appx152 (concluding that "switches and routers" cease packet processing, but making no finding as to firewalls); Appx18392-18393; Appx18437. Nor would the evidence support such a finding, as Cisco's firewalls do not "cease" processing packets. *E.g.*, Appx3522-3524(2516:22-2518:3) (Cisco witness Hari Shankar testifying that "[w]e cannot stop processing packets [in the accused firewalls] just because we are trying to switch [rule sets]"). That complete failure compels judgment of noninfringement as to firewall products and their removal from any damages award, because they were not held to infringe any other patent.

As to Cisco's switches and routers,[7] the district court found that they process a packet "every two or four internal clock periods," which "operate in milliseconds." Appx146(¶25). The court determined that packet processing includes a short period "in the middle of the two to four clock cycles." Appx149(¶29). The court recognized that a rule set (known as an "access control list" or "ACL") swap "occurs in the middle of the two to four clock cycles, when the device is operating in idle." *Id.* The court relied on this period as the time

[7] The district court made several findings it asserts apply to "switches and routers" but that are based on operation of the Uniform Access Data Plane ("UADP") processor, which is present ***only*** in Cisco's switches. *See, e.g.*, Appx3568(2562:12-18) (Cisco engineer Peter Jones testifying that the UADP is present in the Catalyst 9000 switches).

when Cisco's routers and switches "cease processing" packets. Appx146(¶25); Appx149(¶29); Appx3578(2572:10-13). The district court also found the "cache" limitation satisfied because switches and routers store packet payloads in a buffer. Appx151-152.

But the claims are not satisfied merely because a device "cease[s] processing" or "cache[s]" packets; those actions must occur "responsive to being signaled to process packets in accordance with the second rule set." Importantly, the court made no finding that the normal idle period in the switches' and routers' ordinary processing was "responsive to being signaled." On the contrary, the court recognized that Cisco's switches and routers "cease processing packets during their ***normal packet processing operation***." Appx152. In other words, the idle period occurs regardless whether the device receives any "signal" that a second rule set is ready. The evidence did not support any other conclusion; Cisco engineer Peter Jones testified without contradiction that "***we don't stop processing the packets***, there's just an idle period between two packets." Appx3578(2572:10-13); Appx250 (finding Mr. Jones credible).

A device that takes an action regardless whether it receives a signal does not do so "responsive to being signaled." *See IGT v. Bally Gaming Int'l Inc*., 610 F. Supp. 2d 288, 332 (D. Del. 2009) ("'responsive to'" means "in reply or reaction to [an] occurrence"), *aff'd*, 659 F.3d 1109 (Fed. Cir. 2011); *Intel Corp. v. Broadcom*

Corp., No. Civ.A. 00-796-SLR, 2003 WL 360256, at *7-8 (D. Del. Feb. 13, 2003) (defining "responsive" as "to respond or react" in claim limitations reciting "responsive to a control signal").

Similarly, regarding the "cache" limitation, the evidence showed that every packet entering Cisco's switches is stored in the buffer during normal packet processing—not cached "***responsive to***" a signal to process packets under the second rule set. Appx3569(2563:14-15) (Mr. Jones testifying that ***all packets*** pass through the buffer). Likewise in Cisco's routers, buffering is part of normal packet processing, not responsive to any signal. Appx5867 (Hughes: "All routers have packet buffers where packets are stored before processing."). As with the ceasing of processing, this supposed "caching" likewise cannot satisfy the "***responsive to being signaled***" limitation.

The court's only factual finding relating to a "signal" was that, after compiling a new ACL, the switch or router "signals the processor to begin processing packets with the new updated ACL rule set." Appx149(¶28). But the court did not find that any Cisco device ceases packet processing or caches packets in response to a signal to process packets with an updated ACL rule set. Rather, as the court elsewhere acknowledged, the idle period and buffering happen "during their normal packet processing operation," not responsive to a signal. Appx152.

The court rationalized its disregard of the critical "responsive to" limitation by venturing that Cisco "greatly improve[d] the security functionality of its products without dropping packets." Appx153. That irrelevant generalization cannot relieve Centripetal's burden to prove every element. Centripetal did not, and could not, patent every system that improves security "without dropping packets." And the court did not, and could not, find that Cisco's products met the "responsive to being signaled" limitation. That compels a finding of noninfringement.

B. '856 "Packet Filtering" Patent

1. Background

Claims 24 and 25 of the '856 patent describe the "filtering" of packets in a network through a specific three-step process in the following order: (1) "***determine*** … ***packets*** comprising encrypted data that corresponds to the one or more network-threat indicators"; (2) "***filter*** … the ***determined packets*** comprising the encrypted data"; and (3) "***route*** … ***filtered packets*** to a proxy system." Appx357-358(28:59-30:31).

Centripetal alleged infringement by a Cisco router/switch in combination with Stealthwatch (including both ETA and CTA) and ISE. Appx75-79; Appx2057(1057:11-19). Centripetal's infringement allegations relied on Stealthwatch's analysis of NetFlow.

Keysight, EX-1028
Page 43

NetFlow, which Cisco invented in 1996, consists of periodic summaries of information about the flow of packets that passed through a router or switch. NetFlow records are not "packets"; the court and Centripetal called them "logs" or "logging" information, "summaries of information" from packets, or "representations of the unencrypted portion" of packets. Appx77-78(¶¶15-20); Appx99; Appx113(¶13); Appx1983-1984(983:18-984:24); Appx1986(986:2-8); Appx2675(1672:1-12); Appx2677(1674:12-19). There is no one-to-one correspondence between a NetFlow record and an individual packet; a single NetFlow record could summarize information from hundreds of thousands of packets. Appx2675(1672:13-18).

NetFlow records—not packets—are sent to Stealthwatch, while the packets summarized by the NetFlow records undisputedly continue to their intended destinations. *See* Appx2064-2066(1064:21-1066:6); Appx2079(1078:7-18); *see also* Appx1159(159:11-13); Appx2675-2679(1672:19-1676:2); Appx2688-2689(1685:24-1686:23); Appx2727-2728(1724:9-1725:1); Appx2747-2750(1744:6-1747:10); Appx2818(1815:10-18); Appx2909-2913(1906:5-1907:22, 1908:23-1910:24); Appx3130-3133(2127:8-2130:1); Appx3210(2207:5-24).

Stealthwatch cannot filter, re-route, or otherwise block packets it determines correspond to threat indicators. Stealthwatch is an "after-the-fact" system, also referred to as "out-of-band" or "allow-and-detect." Appx1153-1154(153:24-

Keysight, EX-1028
Page 44

154:23). Such a system allows packets to reach their destination, subsequently analyzes NetFlow data to determine whether the communication might be threatening, and if so, acts to prevent similar future threats. Appx1153-1158(153:24-158:1); Appx2677-2679(1674:20-1676:2). This approach is analogous to putting a hold on a credit card based on a suspicious transaction that has already occurred, rather than preventing the transaction from occurring at all. Appx1133(133:5-15); Appx1156(156:6-16).

Nevertheless, the court found that Stealthwatch supposedly "filter[s]" packets because it analyzes ***NetFlow***. Appx77-78(¶¶15-20); Appx99. In doing so, the court implicitly construed "packets" too broadly, and thus erred by finding the asserted claims infringed by analysis of something other than "packets."

2. The accused product combination does not "filter … the determined packets"

a. The court implicitly misconstrued "packets"

At *Markman*, the district court gave "packets" its plain and ordinary meaning (Appx82), which its merits opinion described as a unit of data containing "two different parts: the header and the payload," with the payload sometimes being encrypted (Appx56). That construction was correct, but the court abandoned it and implicitly adopted an erroneous construction when assessing infringement.

The court found that Stealthwatch "filter[s] … packets" when it analyzes NetFlow records. But NetFlow records are not packets; they are "summaries of

Keysight, EX-1028
Page 45

information" from packets that previously passed through a router or switch. Appx113(¶13); Appx1134-1135(134:10-11, 134:22-135:12); Appx2818-2819(1815:5-7, 1816:4-5); Appx5219. The court called NetFlow "***representations of information*** from the ***unencrypted portion*** of encrypted packets." Appx77(¶15); *see also* Appx78(¶20); Appx99. Thus, the court implicitly construed "packets" to include not the packets themselves, but mere "representations of information" from "the unencrypted portion" of packets.

Nothing in the '856 patent supports expanding the meaning of "packets" to include NetFlow, which is an industry standard that long predated and is unmentioned by the '856 patent. Appx1136(5-10); Appx1214(214:6-10). Instead, the patent teaches that a "packet" includes both (1) the actual header and payload, not merely "representations" of a portion thereof; and (2) the encrypted portion of the packet, not just "the unencrypted portion." Appx346(5:53) ("payload data" "in the packets"); Appx346(5:36-37, 46-47) ("header fields of the packets").

Accordingly, the court erred by implicitly construing "packets" to include "representations of information" from only the unencrypted portion of a packet. *See Corning v. Fast Felt Corp.*, 873 F.3d 896, 900-901 (Fed. Cir. 2017) (reversing patentability determination based on "implicit[]" claim construction).

Keysight, EX-1028
Page 46

b. Stealthwatch does not "filter … the determined packets"

When "packets" are properly understood to comprise both the header and the payload, the court's infringement finding cannot stand, because Stealthwatch indisputably does not "filter … the determined packets."

As the court acknowledged, Stealthwatch analyzes ***NetFlow***, which is merely a historical summary of information from the flow of packets through a router/switch. Appx77-78(¶¶17, 20); Appx113(¶13).[8] Under any of the court's characterizations of NetFlow—"logs," "summaries," or "representations" of information in a portion of a packet—NetFlow records are not "packets."

At one point, the court suggested that Stealthwatch "filter[s] … the determined packets" because filtering "the representation of packets" (i.e., NetFlow) equates to filtering "flows of packets." Appx99-100. The court cited two documents and corresponding expert testimony, but neither shows filtering "packets"; they at most show analyzing information about packets.

First, the court cited PTX-570, which describes a user's ability to perform a Cryptographic Audit via the Stealthwatch Management Console (SMC). Appx99;

[8] Centripetal acknowledged this when asserting the '176 patent claims, which require generating "a plurality of ***log entries*** corresponding to the plurality of ***packets*** received by the network device." Appx309-310(17:12-13, 19:1-2). For the '176 patent, Centripetal's witness asserted that NetFlow records are the claimed "log entries," not the claimed "packets." Appx1983-1984(983:18-984:24); Appx1986(986:2-8).

Appx5153-5161. A Cryptographic Audit verifies that the user's security technology is current, and is done by a human performing a database query that produces an Excel spreadsheet. Appx2921-2923(1918:6-1920:12); Appx5161. The court and Centripetal's expert claimed that this audit showed filtering packets based on the "protocol version"—information that is again part of NetFlow. Appx99; Appx1950-1951(950:1-951:20); *see also* Appx5206. Both the court and Centripetal's expert admitted that a Cryptographic Audit at most filters "***[i]nformation*** that came from a packet" (i.e., NetFlow), not the packets themselves. Appx2087-2088(1086:21-1087:10). Indeed, such an audit cannot "filter … the determined packets" because the packets ***reach their intended destination*** within milliseconds of passing through the router/switch, long before a human can perform a database query. Appx2818(1815:13-18); Appx2912(1909:3-10); Appx2921-2923(1918:6-1920:12).[9]

Second, the court cited a Stealthwatch configuration guide, and specifically a page discussing "ETA Flow Records"—i.e., NetFlow. Appx100; Appx1957(957:6-21); Appx5206. It found that this document shows packet-

[9] Even if PTX-570 could somehow show packet filtering during a Cryptographic Audit (which it cannot), neither Centripetal's expert nor the court attempted to show that such filtered packets would then be "route[d] … to a proxy system," as the claims also require. Appx78-79(¶¶21-23); Appx94-98; Appx358(29:29-30:31); Appx1958-1973(958:9-973:3).

filtering based on "Server Name Indication," which is also part of NetFlow. *Id.* But again, the document at most shows analyzing NetFlow, not filtering the packets themselves.

Indeed, even the court recognized that the above-described actions based on protocol version and server name were (at most) filtering only "representation[s]" of a portion of packets, not packets themselves: "The SMC allows for the ***representation*** of packets currently being processed within the network ***to be filtered*** and ordered ***by*** information within the unencrypted part of the packet such as ***protocol version***, ***server name*** or domain name." Appx99.

The undisputed evidence showed that Stealthwatch cannot "filter … the determined packets" or "route … filtered packets" to a proxy system. The plain meaning of "the determined packets" requires that the system "filter" the same packets previously "determined" to be potential threats. *See Wi-Lan, Inc. v. Apple, Inc.*, 811 F.3d 455, 462 (Fed. Cir. 2016) ("Subsequent use of the definite articles 'the' or 'said' in a claim refers back to the same term recited earlier in the claim."). But the packets for which NetFlow is generated are undisputedly delivered to their ultimate destination long before Stealthwatch even receives the corresponding NetFlow records. *See* Appx2064-2066(1064:21-1066:6); Appx2079(1078:7-18); *see also* Appx1133-1134(133:20-134:2); Appx1159(159:11-13); Appx2675-2679(1672:19-1676:2); Appx2688-2689(1685:24-1686:23); Appx2727-

2728(1724:9-1725:1); Appx2747-2750(1744:6-1747:10); Appx2818(1815:10-18); Appx2909-2913(1906:5-1907:22, 1908:23-1910:24); Appx3130-3133(2127:8-2130:1); Appx3210(2207:5-24). A packet is delivered to its ultimate destination in "milliseconds," while the corresponding NetFlow record does not reach Stealthwatch until thirty seconds to five minutes later. Appx2675-2676(1672:19-1673:5); Appx2688-2689(1685:24-1686:23); Appx2727-2728(1724:9-1725:1); Appx2818(1815:10-18); Appx3130-3133(2127:8-2130:1). Even Centripetal's expert admitted that the packets proceed to their ultimate destination before NetFlow records reach Stealthwatch. Appx2064-2066(1064:21-1066:6); Appx2079(1078:7-18). Thus, by the time Stealthwatch "determines" that any NetFlow records correspond to a threat, it is too late to "filter … the determined packets," which have already reached their destination. Similarly, Cisco's accused routers/switches do not and cannot perform the last step—"route … filtered packets to a proxy system"—because the relevant packets have already been delivered to their final destination before they could be "route[d]" elsewhere.

The district court wrongly believed that the claims' very specific limitations were satisfied by generic statements in marketing documents concerning, for example, the ability of Cisco products to "detect and stop threats," "detect and respond to threats in real time," "prevent high impact" threats, address threats "proactively," and address threats "before they are able to have a major impact."

Keysight, EX-1028
Page 50

Appx84-94 (citing Appx5112-5113, Appx5191, Appx5398). Such marketing statements cannot refute technical evidence of the products' actual operation. *MAG Aero. Indus. v. B/E Aero., Inc.*, 816 F.3d 1374, 1377 (Fed. Cir. 2016) ("promotional and non-technical documents" cannot overcome technical documents describing the products); *Regents of Univ. of Minn. v. AGA Med. Corp.*, 717 F.3d 929, 939 (Fed. Cir. 2013) ("[S]ales descriptions neither expand the [asserted] patent nor bring [the accused] device within its scope" in the face of undisputed technical evidence).

The asserted claims are narrowly drawn to a specific sequence of steps: "***determin[ing]*** … ***packets***" with encrypted data corresponding to a threat indicator; "filter[ing] … ***the determined packets***"; and "rout[ing] … ***filtered packets***." Nothing in the court's cited marketing documents, or the testimony the court quotes at length, suggests that Stealthwatch "filter[s]" packets previously "determine[d]" to be threats or "route[s]" them to a proxy system. Appx84-94.[10]

[10] The court's discussion of the '856 patent included several general criticisms of Cisco's evidence. Appx80(¶¶25-27). These criticisms are baseless but ultimately irrelevant to noninfringement. Cisco's argument on appeal rests on the court's own reasoning and the undisputed record.

C. '176 "Correlation" Patent

1. Background

Claims 11 and 21 of the '176 patent, known as the "Correlation" patent (Appx110(¶1)), are again extremely detailed. They require a system/media to generate "log entries corresponding to … packets ***transmitted*** by" a network device, as well as log entries corresponding to packets "***received*** by" the device. The system/media must then "correlate … the plurality of ***packets transmitted*** by the network device with the plurality of ***packets received*** by the network device" "based on" the two sets of "log entries." Appx309-310(17:6-35, 18:63-19:23).

Centripetal alleged that Cisco's NetFlow records were the claimed "log entries." Appx113(¶13); Appx1977(977:13-25); Appx1983-1984(983:14-984:13). Centripetal argued that a router/switch could generate NetFlow both when receiving packets (ingress NetFlow) and transmitting packets (egress NetFlow). Appx113(¶14); Appx1977-1978(977:13-978:10); Appx1983-1984(983:14-984:4). Centripetal asserted that ingress and egress NetFlow records were sent to Stealthwatch, where they were "correlate[d]." Appx113-114(¶¶15-16); Appx1994-1998(994:21-995:21, 996:17-997:5, 998:8-17).

Based on the products' undisputed operation, Cisco explained that Stealthwatch does not process ingress and egress NetFlow records for a given packet flow, much less use them to "correlate" packets. Rather, the accused

products correlate NetFlow records with ***global threat indicators***, which are ***other information*** received from external sources. Appx3259-3262(2255:5-2258:23); Appx4358(3347:14-20); Appx17563-17566; Appx17855-17859(¶¶48-58). The court agreed with Cisco's expert on this: "Stealthwatch correlates NetFlow … ***with global threat indicators***." Appx120. The court did not explain—because it could not—how Cisco's products practiced the claimed correlation of transmitted packets with received packets, much less how such a correlation would have been based on egress and ingress NetFlow records.

2. The accused product combination does not "correlate" transmitted packets with received packets

Claims 11 and 21 require that the system "correlate … the plurality of packets transmitted by the network device with the plurality of packets received by the network device." The court read out this critical element, finding infringement based on generic references to "correlation" of entirely different things.

a. The accused combination does not "correlate" packets based on ingress and egress NetFlow records

The court's finding that the accused combination correlates a router's or switch's transmitted packets with its received packets based on egress and ingress NetFlow records (Appx114(¶16)) was not supported by any evidence. The court and Centripetal's infringement expert did not rely on any source code explaining how Cisco's products actually function, but rather on documents that merely use

the word "correlate." But the documents do not demonstrate the ***claimed*** correlation; they show only that—as the court found—Cisco's products correlate NetFlow information (not "packets") "with global threat indicators." Appx120. That is not correlation of transmitted/received packets based on egress/ingress NetFlow records, as the claims require. Once again, Centripetal encouraged the district court to ignore the claims' specific limitations and view the '176 patent at too high a level, as though it covered any "correlation" performed when assessing network traffic, regardless of what was being correlated to what. Once again, the court took the bait and clearly erred in doing so.

Centripetal's expert and the court relied on documents that speak only of correlating threats within a Cisco-protected system with information about threats outside the system—***not*** of correlating transmitted and received packets based on egress/ingress NetFlow records. For instance, Centripetal and the court relied on an internal Cisco presentation that mentions "the cloud-based analytics engine that correlates threat behaviors seen in the enterprise ***with those seen globally***." Appx119 (reproducing Appx5222); Appx1995(995:13-18). The court (at Appx120-121) relied on two additional documents (though Centripetal did not) that similarly speak of correlation to global threat behavior. *See* Appx5063 (PTX-202: "Cisco Stealthwatch with Cognitive Analytics … correlates local traffic models with global threat behaviors"); Appx5150 (PTX-569: "Stealthwatch …

correlates threat behaviors seen in the local environment with those seen globally."); *see also* Appx5177 (document cited at Appx268, referring to correlating traffic to "global threat behaviors").

Nothing in these documents suggests that any Cisco product correlates (1) packets "received" by a router/switch with (2) packets "transmitted" by that same router/switch—much less that it performs such a correlation (3) "based on" an ingress NetFlow record and an egress NetFlow record. Appx3259-3261(2255:5-2257:10) ("even though these documents use the word correlate, what they're correlating is not the kind of correlation that's required by the claims").

Centripetal's expert and the court likewise relied on documents that mention correlation of NetFlow and a different "telemetry" type called "WebFlow."[11] Appx114(¶16); Appx1996(996:5-10); *see* Appx5182 (Stealthwatch release notes stating "CTA can now leverage detections from the analysis of WebFlow telemetry to improve the efficacy of analyzing NetFlow telemetry from Stealthwatch. This is accomplished by the system through correlation of both telemetry types."); Appx5210 (CTA release notes, which Centripetal's expert admitted contained the

[11] WebFlow is third-party telemetry reflecting information about web traffic; it is delivered in Syslog format and comes from a non-accused proxy server, not a Cisco router or switch. Appx18403-18404(¶¶9-11); Appx5222.

same language, *see* Appx2111(1110:3-6)); Appx5499 (document cited at Appx268, likewise referring to WebFlow telemetry). These WebFlow-related statements do not discuss correlating received and transmitted packets at all, much less correlating them based on ingress and egress NetFlow records, as Centripetal's infringement theory required. Appx3261-3262(2257:18-2258:10).

Cisco repeatedly explained that the bare use of the word "correlate" in the cited documents did not demonstrate the ***claimed*** "correlation." Appx3259-3262(2255:5-2258:23); Appx4358(3347:14-20); Appx17563-17566; Appx17856(¶51). The court nowhere addressed Cisco's argument. Appx110-126; Appx262-269. The effect was, once again, that the court read out a key disputed limitation.

b. The district court's sua sponte infringement theories are unsupported

The district court, on its own initiative, developed two other theories of infringement. Neither has merit.

Syslog/Webflow: The court mentioned correlation of Syslog information in the form of WebFlow. Appx113-114(¶¶15-16); Appx120. Correlation involving Syslog/WebFlow is irrelevant for three reasons.

First, Centripetal's expert did not rely on correlation of Syslog/WebFlow at trial. Appx1977-1978(977:13-978:10); Appx1986-1987(986:12-987:1); Appx1992-1993(992:23-993:18); Appx2102-2104(1101:4-13, 1102:16-1103:4);

Appx2106-2109(1105:18-1106:8, 1107:23-1108:10). Nor could he have, as Centripetal did not accuse the devices that generate Syslog/WebFlow logs (proxy servers), yet such "generat[ion]" is a claim element. Appx309-310(claims 11 & 21). Cisco was not on notice of any infringement theory based on correlation of Syslog/WebFlow, and the court's post-trial reference to them is unfairly prejudicial. *See Twigg v. Norton Co.*, 894 F.2d 672, 675-676 (4th Cir. 1990) (granting a new trial where "a new theory of liability" was introduced "without warning").

Second, Centripetal presented no evidence—and the court cites none—of correlating transmitted and received ***packets*** based on ***egress and ingress*** Syslog/ WebFlow. Again, the court offers only generic references to "correlating" Syslog/WebFlow, with no attention to the specific claimed correlation. Appx113-114(¶¶15-16); Appx120.

Third, the accused combination's processing of Syslog/WebFlow was not proven to satisfy the other claim limitations, like "generat[ing]" log entries. For those limitations, Centripetal and the court relied only on the system's generation of ***NetFlow*** records (not Syslog/Webflow). Appx113(¶¶13-14); Appx2105(1104:2-15). Thus, they cannot rely on Syslog/WebFlow as "log entries" for the "correlate" limitation.

Multiple device theory: The court alternatively found that the claims could be satisfied by correlation of packets transmitted to and received by ***multiple*** routers/switches. Appx116-118. But the court's theory—which it acknowledges Centripetal's expert did not present (Appx116-118), *Twigg*, 894 F.2d at 675-676—cannot satisfy the "correlate" requirement. After two pages of claim construction, the court conclusorily stated that "the Cisco system correlates ***logs*** between multiple devices within the network on either ingress or egress." Appx118. But nowhere does the court identify how any Cisco product correlates transmitted and received ***packets*** from multiple devices, much less does so based on egress and ingress NetFlow (or other logs); Centripetal certainly did not provide such evidence. Indeed, the court's statement that "the Cisco system correlates logs between multiple devices within the network on ***either*** ingress ***or*** egress" (Appx118) confirms the court's disregard for the claim language, which requires correlation of packets transmitted ***and*** received based on their egress ***and*** ingress log entries. Appx309-310(17:19-25, 19:7-13).

D. '193 "Forward or Drop" Patent

1. Background

The '193 patent is directed to preventing "exfiltration," i.e., causing a device to send confidential data to unauthorized destinations. Appx128(¶6); *see also Centripetal Networks, Inc. v. Cisco Sys., Inc.*, 847 F. App'x 869, 871 (Fed. Cir.

Keysight, EX-1028
Page 58

2021). As the district court recognized, the patent seeks to prevent exfiltration in a particular way: it "identifies a process by which rules can be enabled to filter packets of data ***depending on the type of data transfer*** that is being transmitted." Appx129(¶9). The patent describes a system that allows a user to perform some types of data transfer, such as "surf[ing] … to … web sites," but prevents other types, such as "writing files" or "posting forms … to a web server." Appx319(2:43-54); Appx322(7:10-20). Claims 18 and 19 recite, in relevant part, "rules configured to prevent a particular type of data transfer" from a first network to a second network, by first determining if a packet is "destined for the second network" and then, for any such packets, applying an "operator … configured to drop packets associated with the particular type of data transfer." Appx325-326(14:1-15:3).

The undisputed evidence showed, and the district court correctly found, that the accused combination of Cisco's products—routers or switches combined with ISE—implements a so-called "quarantine rule" that blocks ***all*** traffic between an unpermitted source and an unpermitted destination, while allowing ***all*** traffic between a permitted source and a permitted destination. Appx130-131(¶¶15, 18-20) (finding that Cisco switch/router "drops or transmits packets based upon the destination of the packets"). And the court correctly concluded that the '193 patent's "particular type of data transfer" limitation requires not blocking ***all*** traffic

Keysight, EX-1028
Page 59

between a source and destination, but rather allowing ***some*** communication to flow between source and destination depending on the "type of data transfer that is being transmitted." Appx129(¶9).

These conclusions should have resulted in a finding of noninfringement. But the court inexplicably found infringement, again effectively reading out the key limitation.

2. The accused product combination does not forward or drop packets depending on whether they are "associated with [a] particular type of data transfer"

As the district court recognized, the '193 patent claims are not satisfied simply by blocking all traffic between a particular source and a particular destination. Centripetal could not have patented, and did not patent, such a basic network-permission scheme, which was long known. Rather, the claims are narrowly directed to forwarding or dropping packets depending on whether they are "associated with [a] particular type of data transfer." The court agreed with Cisco's expert Dr. Mark Crovella that this limitation requires considering an added property beyond the packet's source or destination: the "functionality outlined by the asserted claims" requires "a device to 'block some communication between the two networks but allow other communication to flow.'" Appx137 (quoting

Appx3405(2400:8-10)).[12] Indeed, Centripetal relied heavily on this limitation in successfully arguing against institution of Cisco's IPR petition. Appx5681-5682; *see also* Appx4070-4071(3061:22-3062:1) (Centripetal's validity expert stating the '193 patent claims a system "configured to prevent a particular type of data transfer, as opposed to allowing or blocking IP addresses").

Although the court did not explore the technical details, the '193 patent explains what a "particular type of data transfer" means by discussing a communication's data transfer protocol method. For example, surfing the internet is performed using the HTTP GET protocol method, while HTTP POST is used to post or upload data to a website. Appx319(2:46-50). Cybercriminals often use specific protocol methods (e.g., "HTTP PUT [and] POST") "to exfiltrate sensitive data." Appx322(7:18-19). The patent explains that one defense to such exfiltration is "block[ing] all communications to networks that are owned or operated by organizations [a company] does not fully trust." Appx322(7:26-28). The patent criticizes that option, however, because "this would likely result in [the company] blocking access to most of the Internet." Appx322(7:28-32). The '193 patent takes a different approach: communications between a given source and given destination receive different treatment depending on what type of protocol

[12] The court's statement that Dr. Crovella "concede[d]" this point (Appx137) is curious: it was not a concession, but Cisco's affirmative argument.

the communications employ. For example, the patented system may "allow the packet (e.g., if a GET method is specified), or block the packet (e.g., if a PUT or POST method is specified)." Appx319(2:41-43).

Cisco's accused products do not work that way. The court's infringement analysis turned on the fact that Cisco "labels" packets using Security Group Tags (SGTs), and then applies rules called Security Group Access Control Lists (SGACLs) that "block[] or permit[] packets specifically based on SGTs." Appx130-131(¶¶15, 18). But as the court recognized, SGTs "are applied to packets based on their ***source or destination***." Appx130(¶15); *see also* Appx134 (SGTs "are assigned to packets based on where the packet is being transmitted from and/or the destination of the transmitted packet"). They unquestionably are not based on the communication's "particular type of data transfer."

The court itself repeatedly found that Cisco's products forward or drop packets based ***only*** on their source and/or destination. Appx130-131(¶¶15, 18-20) (a Cisco switch or router "drops or transmits packets based upon the ***destination*** of the packets"); Appx131-132(¶24) ("The switch and/or router determines whether the packet should be permitted or blocked based on the SGT assigned ***to that particular source***."); Appx132(¶25) ("if an SGT matches one of the SGACL rules ***because of an unpermitted source or destination***, a deny operator is applied, and subsequently the packet will be blocked"). Centripetal's expert admitted that

Cisco's policies "restrict according to source and destination." Appx1528(528:3-8); *see also* Appx1495(495:9-14); Appx1869(869:8-12). As Dr. Crovella explained without contradiction, Cisco's quarantine SGACL rule "doesn't do any check to see what kind of data transfer is contained in the packet." Appx3390-3391(2386:12-2387:3); *see also* Appx3393-3394(2389:3-2390:1); Appx3394-3395(2390:18-2391:5). The court nowhere found Dr. Crovella's testimony lacking in credibility, nor did it cite any contrary evidence. Rather, it quoted Dr. Crovella's testimony that a quarantine policy like Cisco's "is, in fact, checking the ***destination***." Appx137 (quoting Appx3428-3429(2423:19-2424:15)).

The court nonetheless found infringement by reading out the key limitation. The court believed the claims could be satisfied by a "two-stage process" of "first assigning SGT to packets, based upon the source and/or destination of the packets," and then forwarding or dropping those packets based on the SGT, which reflects the packet's source/destination. Appx136. But the claims describe a different two-stage process: evaluating packets based not just on a packet's source/destination (the first stage), but also on "***the type of data transfer*** that is being transmitted" (the second stage). Appx129(¶9); *see also* Appx322(8:45-52). The court nowhere found that Cisco's products do that. Instead, it apparently concluded that ***any*** two-stage process for filtering data transfers infringes the '193 patent, thereby stretching the patent well beyond its narrow claims.

The court also stated—without citation—that Cisco's products "limit[] a computer located in a first network from accessing sensitive data in a protected network, while simultaneously allowing unsensitive data to be accessed." Appx133. If the court meant, consistent with its findings elsewhere, that Cisco's products block a computer from accessing sensitive data in a protected network, but allow that computer to access unsensitive data in a ***different*** network, then the statement is accurate but does not prove infringement. Infringement would require a finding that Cisco's products block a computer from accessing "sensitive data" from a "protected" destination while allowing that same computer access to other data from the ***same*** destination. The court made no such finding, and no evidence would support one. Rather, as the court repeatedly recognized, Cisco's rules block ***all*** packets, or allow ***all*** packets, between a given source and a given destination. *See supra* pp. 47-48.

Similarly unavailing is the court's assertion that Cisco's products can "den[y users] access to critical data while [those] users can keep working on less critical applications." Appx136 (reproducing Appx5430-5431). Again, this is a description of a basic network-permission scheme, where users can access some network locations but not others; Centripetal's expert explained that this language was "just another way of saying that there may be ***places*** inside or outside to external networks where you're going to allow the user to still work and function

Keysight, EX-1028
Page 64

but there may be ***other parts*** where they're not allowed." Appx1527(527:14-17); *see also* Appx1545(545:16-18); Appx1545-1546(545:22-546:3). In sum, the court simply describes filtering based on source and destination, not based on "a particular type of data transfer" as the claims require.

The district court's failure to enforce the "particular type of data transfer" limitation is particularly egregious because it was critical to the claims' patentability over the prior art. In binding statements opposing institution of IPR, *see Aylus Networks, Inc. v. Apple Inc.*, 856 F.3d 1353, 1361 (Fed. Cir. 2017), Centripetal emphasized that the '193 patent required a "two-stage process … wherein *first* the computing system determines that a first portion of packets … is destined for the second network" and "[*s*]*econd*, and **responsive** to that determination, the computing system applies an operator that is 'configured to drop packets associated with the particular type of data transfer.'" Appx5681 (emphasis Centripetal's); *see also* Appx5682 ('193 patent "introduced the concept of applying an operator that can determine whether the packet is associated with a particular type of data transfer"); Appx5680 (similar). Centripetal's validity expert likewise relied on this limitation at trial. Appx4070-4071(3061:22-3062:1). The court committed legal and clear factual error in allowing Centripetal to assert the "particular type of data transfer" limitation to defend validity while ignoring it for

purposes of infringement. *See Amazon.com, Inc. v. Barnesandnoble.com, Inc.*, 239 F.3d 1343, 1351 (Fed. Cir. 2001).

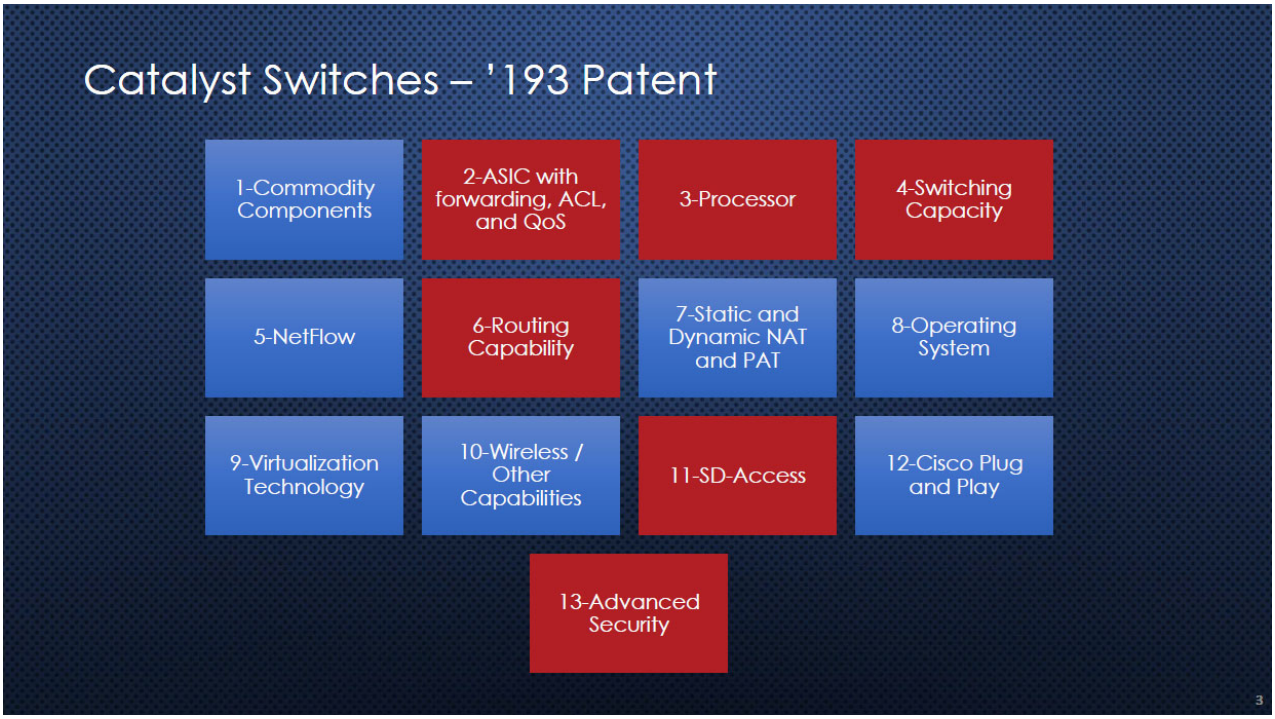
IV. THE DAMAGES AWARD SHOULD BE VACATED

A. The Court Erred By Adopting Centripetal's Flawed Apportionment Analysis

When a patentee seeks royalties on a patent that covers only some features of a multi-feature product, it may "seek only those damages attributable to the infringing features." *VirnetX, Inc. v. Cisco Sys., Inc.*, 767 F.3d 1308, 1326 (Fed. Cir. 2014). That is because a patent "for an improvement, and not for an entirely new machine or contrivance," grants the patentee only the benefit derived from the invention itself. *Garretson v. Clark*, 111 U.S. 120, 121-122 (1884). Moreover, like all damages evidence, evidence of apportionment cannot be "based only on speculation or guesswork." *Lucent*, 580 F.3d at 1310, 1324.

Centripetal failed to offer reliable expert testimony—much less sufficient evidence—that properly apportioned the royalty. *See Commonwealth Sci. & Indus. Research Organisation v. Cisco Sys., Inc.*, 809 F.3d 1295, 1301-1302 (Fed. Cir. 2015). The accused products undisputedly include features that are not part of the accused combinations and generic components (like a processor) that are not part of the "'incremental value that the patented invention adds to the end product.'" *Exmark Mfg. Co. v. Briggs & Stratton Power Prods. Grp., LLC*, 879 F.3d 1332, 1348 (Fed. Cir. 2018); Appx2418-2419; Appx2421. Dr. Aaron Striegel,

Centripetal's apportionment witness, made no effort to separate out those generic components or noninfringing features; in fact, he agreed that he was not even asked to "identify the incremental value that the patented invention adds to the accused end product." Appx2406. Rather, he performed only what he called a "top-level function[]" analysis, using diagrams like the one below (with the red boxes indicating the features included in his damages calculation):



Appx5548; *see also* Appx5546 (slide summarizing top-level function analysis).

Specifically, Dr. Striegel first looked at Cisco marketing documents for each accused product to determine its "top-level functions"—i.e., generic descriptions in the figure above like "advanced security," "processor," "switching capacity," and "routing capability." Appx5546-5579 (listing top-level functions). He then

determined which generic top-level functions he believed "***implicated***" the asserted patents (i.e., were related to the patents in any way and to any degree), rather than considering the specific value added by the patented improvement to the purportedly infringing combinations. Appx2342; *see also* Appx187-189 (district court adopting this analysis).

For example, Dr. Striegel acknowledged that his apportionment analysis included the full value of a ***processor*** in Cisco's accused products, simply because claim 18 of the '193 patent "identified [the] usage of a processor." Appx2418. But Centripetal did not invent the processor; claim 18 admittedly was "not directed at a new and improved processor"; and the accused products' processor "does other things beyond what's identified in the patent." Appx2418-2419. Centripetal did not invent "routing capability" or "switching capacity" either, yet Dr. Striegel included those too. He also believed Centripetal was entitled to the full value of the "Advanced Security" aspect of Cisco's Catalyst switches, even though he admitted that the three specific features listed under that heading (Encrypted Traffic Analytics, AES-256 encryption, and Secure Unique Device Identification) were not accused of practicing any claim element. Appx2421-2422. Dr. Striegel also recognized that his analysis awarded Centripetal damages for entire aspects of technology that were not accused of infringing any patent-in-suit (by treating them as "top-level functions" of accused products). Appx2426 (conceding that "AMP

Keysight, EX-1028
Page 68

for Networks" and sandboxing technology were included in his analysis, even though neither was "accused" of infringing).

When pressed, Dr. Striegel admitted that his apportionment analysis did "not focus on" the extent to which the accused products embodied "the patented improvement" because, in his view, "it would be very difficult to identify" precisely what that improvement was. Appx2416-2417. Dr. Striegel's speculative and result-oriented reasoning led him to conclude that each patent was worth anywhere from 25% to an astonishing 80% of the products' overall value: a flawed analysis that the district court adopted in full. Appx189-190.

The district court's sole explanation for adopting Dr. Striegel's analysis (Appx187) was that his approach was "exactly the type of apportionment analysis" this Court endorsed in *Finjan Inc. v. Blue Coat Sys., Inc.*, 879 F.3d 1299, 1312-1313 (Fed. Cir. 2018). That was incorrect. In the portion of *Blue Coat* the district court cited, the patentee's expert relied on an "architectural diagram" prepared by the defendant itself that showed 24 boxes representing the accused product's features. 879 F.3d at 1312-1313. The expert then identified the number of features that ***actually infringed***, concluding that one feature infringed one asserted patent and three infringed the other. *Id.* at 1313. As a result, the expert concluded that the patents were respectively worth 1/24th (roughly 4%) and 3/24ths (12.5%) of the accused products' value. *Id.*

Nothing in *Blue Coat* justifies Dr. Striegel's approach. Indeed, *Blue Coat* elsewhere rejected a methodology similar to Dr. Striegel's that failed to fully apportion out the accused product's "non-infringing features." 879 F.3d at 1310-1311 ("Because DRTR is itself a multi-component software engine that includes non-infringing features … [f]urther apportionment was required to reflect the value of the patented technology[.]"). And the same district court that decided *Blue Coat* recently excluded Dr. Striegel's "top-level function[]" analysis in another case, holding that it does not satisfy the apportionment requirement. Order at 16-20, *Finjan, Inc. v. SonicWall Inc.*, No. 5:17-cv-04467 (N.D. Cal. May 21, 2021), ECF No. 477.[13]

Dr. Striegel's failure to offer a credible economic analysis made his opinion inadmissible under *Daubert* and led to an arbitrary and excessive damages award. *E.g.*, *MLC Intellectual Prop., LLC v. Micron Tech., Inc.*, __ F.4th __, 2021 WL 3778405, at *11 (Fed. Cir. Aug. 26, 2021) (expert testimony inadmissible where expert failed to "apportion[] for the non-patented aspects of the accused" products).

[13] In its post-judgment order, the district court stated (Appx237) that Centripetal's apportionment analysis was also "expressly approved" in *Ericsson, Inc. v. D-Link Sys., Inc.*, 773 F.3d 1201 (Fed. Cir. 2014). Not so. In *Ericsson*, the Court did not "consider the propriety of [the plaintiff's] apportionment analysis" because the defendant had not "challenge[d]" it. *Id.* at 1228 n.4.

B. The Royalty Rate Was Wrongly Drawn From A Single Non-Comparable License Centripetal Secured As A Settlement

The district court's 10% royalty rate sprang directly from a single settlement agreement between Centripetal and a third party, Keysight. Appx185; Appx5245-5246. The Keysight settlement was "[in]sufficiently comparable to the hypothetical license at issue." *VirnetX*, 767 F.3d at 1330 ("'a loose or vague comparability between different technologies or licenses does not suffice'"). It was a settlement license, which "cannot be taken as a standard to measure the value of the improvements patented." *Rude v. Westcott*, 130 U.S. 152, 164 (1889). *Rude* should have precluded consideration of the Keysight settlement as a matter of law.

At a minimum, the district court should have accounted for the "taint[]" created by the "coercive environment of patent litigation," *LaserDynamics, Inc. v. Quanta Computer*, 694 F.3d 51, 77 (Fed. Cir. 2012), especially given the economic differences between the Keysight settlement and the hypothetical license here. The Keysight settlement involved several "unique circumstances," including the fact that the agreement was a license details reached in the middle of a trial that went badly for Keysight. *See, e.g.*, Appx3874-3875; *see also* Appx2391 (district court expressing "concerns" that settlement occurred only because license details license details it license details). The settlement included the rights to license details U.S. patents—not four—and "license details." Appx3876-3877;

see also, e.g., *MLC*, 2021 WL 3778405, at *13 (finding license non-comparable where litigation involved "only one of th[e] forty-one patents" subject to the license). And Keysight was a [redacted: license details], whereas Cisco neither competes in that market nor produces products that directly compete with Centripetal's technology. Appx3875; Appx3926; *see also* Appx172; Appx2562. At a minimum, Mr. Gunderson's testimony regarding the Keysight settlement should have been excluded for failing to account for the differences between the settlement and the hypothetical negotiation. *Wordtech Sys., Inc. v. Integrated Networks Sols., Inc.*, 609 F.3d 1308, 1320-1321 (Fed. Cir. 2010); *LaserDynamics*, 694 F.3d at 77-78.

C. A New Damages Trial (And Recalculation Of Other Monetary Awards) Is Required If This Court Sets Aside Any Of The Infringement Findings

A new trial on damages is required if this Court holds any patent not infringed. *Omega Patents*, 920 F.3d at 1350; *accord Verizon Servs. Corp. v. Vonage Holdings Corp*., 503 F.3d 1295, 1309-1310 (Fed. Cir. 2007). Moreover, if the damages award is vacated, the ongoing royalty order and prejudgment interest awards should also be vacated and remanded for recalculation. *See, e.g.*, *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1263 (Fed. Cir. 2014) (prejudgment interest); *Whitserve, LLC v. Computer Packages, Inc.*, 694 F.3d 10, 35 (Fed. Cir. 2012) (ongoing royalty).

Notably, the enormous ongoing royalty award—which guarantees Centripetal a minimum of over $754 million over six years—is flawed for an additional reason: It grants Centripetal hundreds of millions of dollars untethered to the number of devices Cisco sells. Appx208-209. Even if Cisco discontinued selling the accused devices today, Centripetal would still be entitled to $754 million in ongoing royalties. Such a result cannot be squared with the Patent Act, which allows ongoing royalties only to "'*prevent the violation* of any right secured by patent.'" *Paice LLC v. Toyota Motor Corp.*, 504 F.3d 1293, 1314 (Fed. Cir. 2007) (quoting 35 U.S.C. § 283).

V. THE DISTRICT COURT CLEARLY ERRED IN FINDING WILLFULNESS AND ABUSED ITS DISCRETION IN ENHANCING DAMAGES

The district court's combined analysis of willfulness and enhancement ignored contrary evidence and failed to explain key conclusions. The enhancement decision was based on "'clearly erroneous factual findings, or a clear error of judgment amounting to an abuse of discretion.'" *Rite-Hite Corp. v. Kelley Co.*, 56 F.3d 1538, 1543 (Fed. Cir. 1995). The district court also committed legal error by collapsing the inquiry into a single review of the *Read* factors, thus wrongly deciding willfulness based on inapposite considerations. *Halo Elecs., Inc. v. Pulse Elecs., Inc.*, 136 S. Ct. 1923, 1933 (2016) (limiting willfulness inquiry to the alleged infringer's subjective state of mind). For example, the district court relied heavily on the closeness of the case, Cisco's size and financial condition, and

Cisco's trial presentation, none of which is relevant to willfulness under *Halo*. *See* Appx200-202; Appx269-270.

A. Cisco Did Not Copy Centripetal

The district court's unsupported belief that Cisco "copied" Centripetal drove its decision, notably its analysis of *Read* factors one, two, four, six, and seven. Appx199-203; Appx269-270. But the court made no finding about *what* Cisco supposedly copied or "appropriated" from Centripetal. Appx202-203. No wonder: the evidence shows only that Centripetal desperately sought Cisco's investment based on ***unclaimed*** aspects of Centripetal's product, such as the ability to process millions of rules. That is reversible error in itself: "[E]vidence of copying … is legally irrelevant unless the [copied feature] is shown to be an embodiment of the claims." *Amazon.com*, 239 F.3d at 1366; *cf. TrafFix Devices, Inc. v. Marketing Displays, Inc.*, 532 U.S. 23, 29 (2001) (unpatented features may be freely copied).

The court could not have found copying of any patented invention, because no evidence supported such a finding.

For example, the district court focused on a Cisco employee's email indicating a lack of interest in Centripetal because the market would not view its rule-processing technology as high-value given that existing systems (like Cisco's) "work[] just fine," but noting that Cisco could "look at [Centripetal's] algorithms" and "study their claims." Appx193; Appx5055. The email shows Cisco

employees expressing skepticism about investing in Centripetal's technology—specifically the ability of Centripetal's RuleGATE product to quickly apply millions of rules, ***a feature Cisco is not accused of copying***. Appx5053-5056. And the uncontradicted testimony was that Cisco never "look[ed]" at any Centripetal algorithms or "stud[ied]" its patent claims. Appx3824-3825(2816:22-2817:25).

The court also relied on a Cisco blog post about RuleGATE. Appx193. Again, the post focused on RuleGATE's ability to quickly apply millions of rules. Appx5135-5138. It said nothing about any functionality accused in this case. Appx2316-2317(1314:7-1315:25).

Similarly, the court relied on a slide deck provided by third party Oppenheimer in a failed effort to attract investment in Centripetal. Appx5813-5818. The Oppenheimer presentation was a high-level sales pitch emphasizing the million-rule-processing feature, not a detailed technical document relating to the claimed features. Appx5813-5818. It included an isolated reference to the '806 patent, but there is no evidence that anyone at Cisco even looked at the deck; Cisco told Oppenheimer it was not interested in Centripetal. Appx2288-2291(1286:17-1289:19); Appx5790-5791.

The court also referred to a meeting on February 4, 2016, after which an email from Centripetal's Jonathan Rogers purported to summarize Cisco's interest

in Centripetal's algorithms and patents. Appx5047. Although the court asserted that Centripetal presented "detailed, highly sensitive, confidential and proprietary information about its patented technology," Appx193, attendees from ***both*** companies expressly contradicted that assertion: most described the information provided as "high-level," which the meeting's slide deck confirms. Appx1393(393:4-17); Appx3818-3820(2810:24-2812:19); Appx5125-5131; Appx5873(36:13-19); Appx5876-5877(76:12-81:22); Appx5897-5898(33:4-34:25).

Finally, the court believed that Cisco's announcement of its rollout of ETA as part of its "network of the future" in June 2017 was when Cisco supposedly copied Centripetal's technology. Appx194; Appx5247-5248. But Cisco provided unrebutted, uncontested testimony that the technology underlying ETA was developed at Cisco by Dr. David McGrew and his team long before Cisco's interactions with Centripetal. Appx2762-2783. Moreover, Centripetal reached out to Cisco yet again in November 2017 for investment and partnership, without suggesting that Cisco's products supposedly included technology stolen from Centripetal or that Cisco needed a license to any patent. Appx3853-3857(2845:19-2849:7); Appx5827-5829; Appx5831.

Contrary to the district court's findings, several Centripetal witnesses admitted that no confidential algorithms or code for implementing the patented

Keysight, EX-1028
Page 76

technology were provided to Cisco. Appx192-193; Appx2281-2283(1279:17-1281:16); Appx5873(36:13-19); Appx5876-5877(76:12-81:22); Appx5897-5898(33:4-34:25). The parties' standard NDA, which is common for initial discussions between companies, is thus a red herring, because the record showed that Cisco did not receive any pertinent confidential information about the claimed technology or copy anything from Centripetal. Indeed, one of Centripetal's experts on copying, Dr. Cole, admitted that he was not aware of Centripetal sharing code with Cisco, Appx2013(1013:3-16); the most he ventured was that the situation looked "suspicious," Appx2031(1031:7-8). Dr. Striegel likewise could not say who at Cisco supposedly copied from Centripetal, and said only that it was "plausible" someone had. Appx4247(3237:16-22). Such bare speculation cannot support a copying finding—let alone over $1 billion in enhanced damages.

B. The Case Was Close

The district court failed to explain why its decisions were "not a close call," Appx202, which is required, particularly where the court "awarded almost the maximum amount of enhanced damages." *Polara Eng'g Inc. v. Campbell Co.*, 894 F.3d 1339, 1355 (Fed. Cir. 2018) (vacating 2.5x enhancement).

Instead of addressing Cisco's defenses, the court impugned Cisco's use of trial animations, claimed the "majority of the Cisco technical documents were introduced by Centripetal," and said that Cisco's invalidity and noninfringement

Keysight, EX-1028
Page 77

arguments were inconsistent. Appx202. These are unfair and irrelevant descriptions about *how* Cisco put on its case, and are incorrect to boot. Both parties used trial demonstratives, which is hardly unusual. Centripetal first offered Cisco documents into evidence because, as the plaintiff, it presented its case first. Cisco relied on many of the same documents in its case and offered substantial additional testimony about how Cisco's products work. The court acknowledged that Cisco called seven technically knowledgeable fact witnesses, though the court largely ignored their testimony without explanation. Appx48-49 (listing Cisco technical witnesses Scheck, McGrew, Llewallyn, Shankar, Jones, Watchinski, and Keanini). And there was no inconsistency between Cisco's noninfringement and invalidity arguments. Cisco's accused products contained the same technology as its prior art products, and therefore a finding that the accused products infringed would demonstrate that the prior art products invalidated—an approach this Court approved in *01 Communique Lab., Inc. v. Citrix Sys., Inc.*, 889 F.3d 735, 742 (Fed. Cir. 2018). As in *Polara*, Cisco's defenses were not weak—they were at the very least reasonable—and if the district court disagreed, it should have explained why. 894 F.3d at 1355.

The closeness of the case must also be viewed in context—Centripetal originally asserted *eleven* patents, and Cisco prevailed on *seven* of them. Appx8006-8010. The PTAB invalidated all claims of six patents and some claims

of the '205 patent, in decisions this Court has affirmed. Appx45-46; *supra* pp. 1-2. The district court found the remaining '205 patent claims not infringed. Appx166; Appx202.

The enhancement should accordingly be reversed or vacated. Alternatively, the willfulness and enhancement findings should be vacated if the Court holds any patent not infringed.

VI. THE JUDGMENT SHOULD BE VACATED BECAUSE THE DISTRICT JUDGE WAS STATUTORILY DISQUALIFIED

In October 2019, well before claim construction or trial, the district judge's wife acquired 100 shares of Cisco stock. Appx30; Appx18320. The judge stated that this purchase was unknown to him until August 2020, when his administrative assistant raised it while preparing his annual financial disclosure. Appx30. By that point, the trial was complete and the judge was writing his merits opinion. The judge explained that he had not known of the purchase because his wife maintained separate accounts and did not recall it, although a trade confirmation was mailed to their home address at the time. Appx18320-18321.

Cisco moved for recusal, because 28 U.S.C. § 455(b) requires a judge to "disqualify himself" when he "knows that … his spouse … has a financial interest in … a party to the proceeding," "however small." 28 U.S.C. § 455(b)(4), (d)(4); *Shell Oil Co. v. United States*, 672 F.3d 1283, 1286-1291 (Fed. Cir. 2012) (spouse owning 97.59 shares required recusal). The district court erred in issuing its merits

Keysight, EX-1028
Page 79

opinion, judgment, and post-judgment order despite knowing of a disqualifying financial interest.

The judge first claimed that Section 455(b)(4) did not apply because his merits opinion was "mostly drafted" when he learned of the stock ownership. Appx39.[14] But Section 455(b) is a bright-line rule, with no exception for a decision that is "virtually" complete. *Id.* There is only one narrow safe harbor: A judge may "divest[] … the interest" instead of recusing if "substantial judicial time has been devoted to the matter." § 455(f). Absent divestment, late discovery is no excuse. *Cf. Shell*, 672 F.3d at 1290 (stock ownership discovered after merits decision, but before reconsideration motion and final judgment). Likewise, ruling against the party whose stock is owned cannot excuse a violation, as the motivation to deflect criticism can also skew the decision-making process.

The judge also believed recusal unnecessary because, in response to Cisco's motion, the stock was placed "into a blind trust." Appx42. That too was error: a blind trust is not divestment, and "[a] judge's use of a blind trust does not obviate the judge's recusal obligations." Judicial Conference of the United States, Committee on Codes of Conduct, Advisory Opinion No. 110; McKeown, *To Judge or Not to Judge: Transparency and Recusal in the Federal System*, 30 Rev. Litig.

[14] The final opinion wound up over 30 pages longer than the 130-page draft the court referenced. Appx18580.

Keysight, EX-1028
Page 80

653, 669 n.57 (2011) ("[A] judge cannot avoid recusal by placing assets in a blind trust…."); *cf.* 5 C.F.R. § 2634.403(a)(2) (similar Executive Branch rule). Indeed, blind trusts violate a judge's separate duty to "make a reasonable effort to inform himself about the personal financial interests of his spouse." 28 U.S.C. § 455(c); *In re Cement Antitrust Litig.*, 688 F.2d 1297, 1314 n.18 (9th Cir. 1982) ("'[Section 455(c)] precludes use of a … blind trust.'" (quoting H.R. Rep. No. 93-1453, 93d Cong., 2d Sess. 1974, *reprinted in* 1974 U.S.C.C.A.N. 6351, 6357)). A judge cannot cure a Section 455(b) violation by violating Section 455(c).

If this Court does not reverse or vacate on other grounds, vacatur here is required because of the harmful impact that the court's error will have on "public confidence in the judiciary." *Chase Manhattan Bank v. Affiliated FM Ins. Co.*, 343 F.3d 120, 128 (2d Cir. 2003). No matter which party prevailed below or when the conflict was discovered, the double statutory violation of Sections 455(b)(4) and 455(c) is "a plain violation" that "risk[s] … injustice to the … parties." *Liljeberg v. Health Servs. Acquisition Corp.*, 486 U.S. 847, 861, 864 (1988). Vacatur in this high-profile case is necessary to encourage judges to "carefully examine possible grounds for disqualification" in a timely manner and to address disqualifying interests when they arise. *Id.* at 868; *see also Shell*, 672 F.3d at 1286 (vacatur required despite mitigating circumstances, including that stock was inherited, not

bought). Absent that remedy, the message will be that Section 455(b)(4) can be safely ignored.

CONCLUSION

The judgment should be reversed or, at the very least, vacated and remanded for further proceedings.

Respectfully submitted,

/s/ William F. Lee

WILLIAM F. LEE
MARK C. FLEMING
ANNALEIGH E. CURTIS
SOFIE C. BROOKS
COURTNEY C. MERRILL
WILMER CUTLER PICKERING
HALE AND DORR LLP
60 State Street
Boston, MA 02109
(617) 526-6000

THOMAS G. SAUNDERS
HEATH A. BROOKS
WILMER CUTLER PICKERING
HALE AND DORR LLP
1875 Pennsylvania Avenue, NW
Washington, DC 20006
(202) 663-6000

THOMAS G. SPRANKLING
WILMER CUTLER PICKERING
HALE AND DORR LLP
2600 El Camino Real, Suite 400
Palo Alto, CA 94306
(650) 858-6000

L. NORWOOD JAMESON
MATTHEW C. GAUDET
DUANE MORRIS, LLP
1075 Peachtree Street, N.E.,
Suite 1700
Atlanta, Georgia 30309-3929
(404) 253-6900

Attorneys for Defendant-Appellant Cisco Systems, Inc.

August 27, 2021

ADDENDUM

TABLE OF CONTENTS

Page(s)

Opinion & Order Memorializing and Explaining the Court's Claim Construction Rulings, Dkt. No. 202 (Feb. 20, 2020)..... Appx1-22

Order on Motions for Summary Judgment Regarding the Issue of Infringement, Dkt. No. 412 (Apr. 27, 2020)..... Appx23-28

Opinion & Order Denying Motion for Miscellaneous Relief, Dkt. No. 619 (Oct. 2, 2020)..... Appx29-43

Opinion & Order re Infringement and Damages, Dkt. No. 621 (Oct. 5, 2020)..... Appx44-221

Opinion & Order Denying Post-Judgment Motions & Declaring the Case Final, Dkt. No. 638 (Mar. 17, 2021)..... Appx222-271

U.S. Patent No. 9,203,806 (JTX-2)..... Appx272-289

U.S. Patent No. 9,560,176 (JTX-3)..... Appx290-310

U.S. Patent No. 9,686,193 (JTX-4)..... Appx311-326

U.S. Patent No. 9,917,856 (JTX-5)..... Appx327-358

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Norfolk Division

CENTRIPETAL NETWORKS, INC.,	)	
	)	
Plaintiff,	)	
	)	
v.	)	**Case No. 2:18-cv-94**
	)	
CISCO SYSTEMS, INC.	)	
	)	
Defendant.	)	

OPINION & ORDER

These matters come to the Court on eight (8) disputed terms found in the asserted claims in this patent case. On February 6, 2020, this Court held a Markman hearing to construe the disputed claim terms. The Court heard arguments of counsel and reviewed the record and ruled from the bench as to six (6) terms and took two (2) terms under advisement. The parties submitted additional briefing on the one (1) term under advisement and resolved their dispute as to the other term under advisement. The Court is prepared to rule on those remaining two (2) terms. The Court hereby issues this Opinion and Order memorialize and explain its claim construction rulings.

I. BACKGROUND

A. FACTUAL BACKGROUND

In 2014, Cisco Systems, Inc. ("Defendant") partnered with ThreatGRID, an entity which included threat intelligence technology which Centripetal Networks, Inc. ("Plaintiff") used in its technology. Doc. 29 ¶ 66. Defendant acquired ThreatGRID later that year. Id. Plaintiff alleges that Defendant gained "increased exposure" to Plaintiff's technology through this acquisition. Id.

Plaintiff alleges that Defendant requested a meeting with Plaintiff through a third-party. Id. ¶ 67. Defendant allegedly asked for a demonstration of Plaintiff's technology at a partner

conference, and Plaintiff did so. Id. Plaintiff argues that Defendant willfully and unlawfully sold products that incorporate Plaintiff's threat detection computer technology. Id. ¶¶ 66-71.

B. PROCEDURAL HISTORY

This case began on February 13, 2018, when Plaintiff filed its original complaint accusing Defendant of direct, indirect, and willful patent infringement. Doc. 1. On March 29, 2018, Plaintiff filed an amended complaint, adding allegations of infringement of an additional patent. Doc. 29. The March 29 amended complaint is the operative complaint in this case.

On April 13, 2018, Defendant moved to dismiss Plaintiff's allegations of indirect and willful infringement. Doc. 37.[1]

On September 19, 2018, Defendant moved to stay the case pending inter partes review ("IPR") by the United States Patent and Trademark Office ("PTO"). The Court granted the stay on February 25, 2019. Doc. 58. On June 10, 2019, Plaintiff moved to life the stay, due to several decision by the PTO in the IPR. Doc. 59. The Court held a hearing on September 11, 2019, and granted the motion to lift the stay IN PART. Doc. 68. The Court lifted the stay as to the patents which were not subject to IPR. Id. Trial on the claims and defenses pertaining to the patents that are not under IPR is scheduled to commence on April 7, 2020. The case remains stayed as to those patents still undergoing IPR. Id.

The parties indicated that a Markman hearing was necessary, Doc. 176 at 1, and the Court convened to hear arguments on the disputed claim terms on February 6, 2020. Doc. 74 ¶ 11.

[1] Before the Court was scheduled to hear arguments on that motion, Defendant withdrew its motion to dismiss.

II. CLAIMS ASSERTED

A. U.S. PATENT NO. 9,137,205 ("THE '205 PATENT")

The '205 Patent generally pertains to "methods and systems for protecting a secured network." '205 Patent at 1. Specifically, it discloses a proactive method of defeating cyber attacks before the attack is successfully launched. Id. at 1:15-24, 10:47-58. Claims 63 and 77 in the '205 Patent are asserted in this case.

B. U.S. PATENT NO. 9,203,806 ("THE '806 PATENT")

The'806 Patent generally pertains to methods for computer systems to change rule sets. '806 Patent at 4:60-65-65. The '806 Patent's methods are intended to facilitate changing between rule sets, as modern rule sets grow in size and complexity. Claims 9 and 17 in the '806 Patent are asserted in this case.

C. U.S. PATENT NO. 9,560,176 ("THE '176 PATENT")

The '176 Patent relates to methods for detecting packets sent between network devices. '176 Patent col. 1 ll. 16-18. The patent discusses the use of log entries corresponding to certain packets, and a packet correlator uses the logs to correlate the packets. '176 Patent col 3 ll. 23-31, col. 8 ll. 46-48. Using the logs, the system can make rules to identify packets. Id. at col. 13 ll. 14-33. Claims 11 and 21 in the '176 Patent are asserted in this case.

D. U.S. PATENT NO. 9,686,193 ("THE '193 PATENT")

The '193 Patent discloses a method for determining whether data packets match given criteria and acting on that determination. '193 Patent at 1, col. 1 ll. 58-59, col. 8 ll. 45-52. This is intended to meet the common problem of cyber security systems' inability to scale to a large volume threat. '193 Patent col. 1 ll. 28-47. Claims 18 and 19 in the '193 Patent are asserted in this case.

E. U.S. PATENT NO. 9,917,856 ("THE '856 PATENT")

The '856 Patent generally relates to a packet-filtering system that receives traffic and applies program rules to detect hidden, encrypted communications. E.g., '856 Patent at col 24 ll. 8-17. Claims 24 and 25 in the '856 Patent are asserted in this case.

III. LEGAL PRINCIPLES OF CLAIM CONSTRUCTION

A. GENERAL PRINCIPLES

The purpose of a Markman hearing is to assist the Court in construing the meaning of the patent(s) at issue. Markman v. Westview Instruments, Inc., 517 U.S. 370, 371 (1996); Markman v. Westview Instruments, Inc., 52 F.3d 967 (Fed. Cir. 1995), aff'd, 517 U.S. 370 (1996). Patents consist of "claims," and the construction of those claims "is a question of law, to be determined by the court." Markman, 517 U.S. at 371; Markman, 52 F.3d at 970–71. A court need only construe, however, claims "that are in controversy, and only to the extent necessary to resolve the controversy." Vivid Techs., Inc. v. Am. Science Eng'g, Inc., 200 F.3d 795, 803 (Fed. Cir. 1999) (citations omitted). To be clear, "[c]laim construction is a matter of resolution of disputed meanings and technical scope, to clarify and when necessary to explain what the patentee covered by the claims, for use in the determination of infringement. It is not an obligatory exercise in redundancy." NTP, Inc. v. Research in Motion, Ltd., 418 F.3d 1282, 1311 (Fed. Cir. 2005) (citing U.S. Surgical Corp. v. Ethicon, Inc., 103 F.3d 1554, 1568 (Fed. Cir. 1997)).

Claim construction begins with the words of the claims. Vitronics Corp. v. Conceptromc, Inc., 90 F.3d 1576, 1582 (Fed. Cir. 1996) ("First, we look to the words of the claims themselves . . . "). Words in a claim are generally given their ordinary meaning as understood by a person of ordinary skill in the art (a "POSITA"). Id. This "person of ordinary skill in the art is deemed to read the claim term not only in the particular claim in which the disputed term appears but also in

the context of the entire patent, including the specification." Phillips v. AWH Corp., 415 F.3d 1303, 1313 (Fed. Cir. 2005) (en banc). "In some cases, . . . the ordinary meaning of claim language as understood by a person of skill in the art may be readily apparent even to lay judges, and claim construction in such cases involves little more than application of the widely accepted meaning of commonly understood words." Id. at 1314. Often, however, "determining the ordinary and customary meaning of the claim requires examination of terms that have a particular meaning in a field of art. Because the meaning of a claim term as understood by persons of skill in the art is often not immediately apparent, and because patentees frequently use terms idiosyncratically, the court looks to those sources available to the public that show what a person of skill in the art would have understood disputed claims language to mean." Id.

Further, the claims themselves can provide substantial guidance as to the meaning of particular claim terms. Id. First, "the context in which a term is used within a claim can be highly instructive." Id. In addition, other claims of the patent in question, both asserted and not asserted, can also be useful because claim terms are "normally used consistently throughout the patent" and therefore "can often illuminate the meaning of the same term in other claims." Id.

The claims should not be read alone, however, but rather should be considered within the context of the specification of which they are a part. Markman, 52 F.3d at 978. As the Federal Circuit stated in Vitronics and restated in Phillips, "the specification is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term." Phillips, 415 F.3d at 1315. The Court, however, must not read in limitations from the specification without clear intent to do so. Thorner v. Sony Comp. Entmt. Am. LLC, 669 F.3d 1362, 1366 (Fed. Cir. 2012). Furthermore, a patentee is free to be his or her own

lexicographer, and thus if the patentee defines a term in the specification differently than its ordinary meaning, the patentee's definition controls. Phillips, 415 F.3d at 1316.

In addition to consulting the specification, a court may also consider the patent's prosecution history, if in evidence, because it provides information regarding how the United States Patent and Trademark Office and the inventor understood the patent. See id. at 1317. It also enables the Court to determine if the inventor limited the invention during the course of prosecution. Id. "[W]here an applicant whose claim is rejected on reference to a prior patent ... voluntarily restricts himself by an amendment of his claim to a specific structure, having thus narrowed his claim in order to obtain a patent, he may not by construction ... give the claim the larger scope which it might have had without the amendments." I.T.S. Rubber Co. v. Essex Rubber Co., 272 U.S. 429, 444 (1926). Thus, consulting prior art reference in the prosecution history is permissible. Vitronics, 90 F.3d at 1583.

These elements of the patent itself—the claims, the specification, and its prosecution history—constitute intrinsic evidence of claim construction. In addition to such intrinsic evidence, a court may consider extrinsic evidence to determine the meaning of disputed claims. Phillips, 415 F.3d at 1317. Such extrinsic evidence "consists of all evidence external to the patent and prosecution history, including expert and inventor testimony, dictionaries, and learned treatises." Phillips, 415 F.3d at 1317 (citing Markman, 52 F.3d at 980). However, the Court should not rely on extrinsic evidence when the intrinsic evidence removes all ambiguity. Vitronics, 90 F.3d at 1583.

Such extrinsic evidence generally is held as less reliable than the intrinsic evidence and "is unlikely to result in a reliable interpretation of patent claim scope unless considered in the context of intrinsic evidence." Id. at 1317–18. With respect to expert evidence, for example,

"[c]onclusory, unsupported assertions by experts as to the definition of a claim term are not useful to a court . . . [and] a court should discount any expert testimony that is clearly at odds with the claim construction mandated by the claims themselves, the written description, and the prosecution history, in other words, with the written record of the patent." Id. at 1318.

With respect to general usage dictionaries, the Federal Circuit noted that "[d]ictionaries or comparable sources are often useful to assist in understanding the commonly understood meaning of words and have been used . . . in claim construction," and further noted that "a dictionary definition has the value of being an unbiased source 'accessible to the public in advance of litigation.'" Id. at 1322 (citing Vitronics, 90 F.3d at 1585). However, the Federal Circuit cautions that (1) "'a general-usage dictionary cannot overcome art-specific evidence of the meaning' of a claim term;" that (2) "the use of the dictionary may extend patent protection beyond what should properly be afforded by the inventor's patent;" and that (3) "[t]here is no guarantee that a term is used in the same way in a treatise as it would be by the patentee." Phillips, 415 F.3d 1322 (quoting Vanderlande Indus. Nederland BV v. Int'l Trade Comm'n, 366 F.3d 1311, 1321 (Fed. Cir. 2004)).[2] Indeed, "different dictionary definitions may contain somewhat different sets of definitions for the same words. A claim should not rise or fall based upon the preferences of a particular dictionary editor . . . uninformed by the specification, to rely on one dictionary rather than another." Id.

[2] In Phillips, the Federal Circuit thus expressly discounted the approach taken in Texas Digital Systems, Inc. v. Telegenix, Inc., 308 F. 3d 1193 (Fed. Cir. 2002), in which the court placed greater emphasis on dictionary definitions of claim terms. Phillips, 415 F.3d at 1319–24 ("Although the concern expressed by the court in Texas Digital was valid, the methodology it adopted placed too much reliance on extrinsic sources such as dictionaries, treatises, and encyclopedias and too little on intrinsic sources, in particular the specification and prosecution history."). The Federal Circuit reaffirmed the approach in Vitronics, Markman, and Innova as the proper approach for district courts to follow in claim construction, but acknowledged that there was "no magic formula" for claim construction, and that a court is not "barred from considering any particular sources . . . as long as those sources are not used to contradict claim meaning that is unambiguous in light of the intrinsic evidence." Phillips, 415 F.3d at 1324.

B. CANONS OF CLAIM CONSTRUCTION

The Federal Circuit has recognized certain guideposts, or "canons of construction," to assist a district court in determining the meaning of disputed claim terms and phrases. These are merely guideposts, however, and are not immutable rules:[3]

1. Doctrine of Claim Differentiation: Ordinarily, each claim in a patent has a different scope. See, e.g., Versa Corp. v. Ag-Bag Int't Ltd., 392 F.3d 1325, 1330 (Fed. Cir. 2004). Ordinarily, a dependent claim has a narrower scope than the claim from which it depends. See, e.g., Phillips, 415 F.3d at 1315. Ordinarily, an independent claim has a broader scope than a claim that depends from it. See, e.g., Free Motion Fitness, Inc. v. Cybex Int'l, Inc., 423 F.3d 1343, 1351 (Fed. Cir. 2005).

2. Ordinarily, claims are not limited to the preferred embodiment disclosed in the specification. See, e.g., Phillips, 415 F.3d at 1323.

3. Ordinarily, different words in a patent have different meanings. See, e.g., Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc., 381 F.3d 1111, 1119–20 (Fed. Cir. 2004).

4. Ordinarily, the same word in a patent has the same meaning. See, e.g., Phillips, 415 F.3d at 1314.

5. Ordinarily, the meaning should align with the purpose of the patented invention. See, e.g., Innovad Inc. v. Microsoft Corp., 260 F.3d 1326, 1332–33 (Fed. Cir. 2001).

6. Ordinarily, general descriptive terms are given their full meaning. See, e.g., Innova/Pure Water, Inc., 381 F.3d at 1118.

7. If possible, claims should be construed so as to preserve their validity. See, e.g., Energizer Holdings, Inc. v. Int'l Trade Comm'n, 435 F.3d 1366, 1370–71 (Fed. Cir. 2006).

8. Ordinarily, absent broadening language, numerical ranges are construed exactly as written. See, e.g., Jeneric/Pentron, Inc. v. Dillon Co., 205 F.3d 1377, 1381 (Fed. Cir. 2000).

9. Ordinarily, absent recitation of order, steps of a method are not construed to have a particular order. See, e.g., Combined Sys., Inc. v. Def. Tech. Corp. of Am., 350 F.3d 1207, 1211–12 (Fed. Cir. 2003).

[3] This list is derived from the one provided in the FEDERAL JUDICIAL CENTER, PATENT LAW AND PRACTICE § 5.I.A.3.d (5th ed. 2006).

10. Absent highly persuasive evidentiary support, a construction should literally read on the preferred embodiment. See, e.g., Cytologix Corp. v. Ventana Med. Sys., Inc., 424 F.3d 1168, 1175 (Fed. Cir. 2005).

IV. AGREED CONSTRUCTIONS

The parties agree to the following constructions:[4]

TERM	AGREED CONSTRUCTION	PATENT
packet security gateway	**a gateway computer configured to receive packets and perform a packet transformation function on the packets**	**'205**
security policy management server	a server configured to communicate a dynamic security policy to a packet gateway	'205
network-threat indicators	**indicators of packets associated with network threats, such as network addresses, ports, domain names, uniform resource locators (URLs), or the like**	**'856**
rule	a condition or set of conditions that when satisfied cause a specific function to occur	'176
log entries	**notations of identifying information for packets**	**'176**

[4] Prior to the Markman hearing, the parties advised the Court that the following, previously-disputed terms require no construction: (1) "preprocess the first rule set and second rule set" for claims 9 and 17 of the '806 Patent; (2) "one or more packet filtering rules" for claims 18 and 19 of the '193 Patent; (3) "determined packets", "filtered packets", and "a determination" for claims 24 and 25 of the '856 Patent. Accordingly, the Court **FINDS** that **NO CONSTRUCTION** is necessary, pursuant to the agreement of the parties.

Additionally, as discussed infra, the parties agreed, after the Markman hearing but before the Court issued a ruling, that the term, "responsive to correlating" should have its plain and ordinary meaning. Accordingly, that term will be given its plain and ordinary meaning as well.

V. DISPUTED CONSTRUCTIONS

A. DISPUTES COMMON TO ALL ASSERTED PATENTS

i. "Packet"

Disputed Term	Plaintiff's Construction	Defendant's Construction	Court's Construction
packet(s)	"a link layer (L2) or network layer (L3) packet"	Plain and ordinary meaning	Plain and ordinary meaning, which will require reference to the context of the specific claim at issue

The dispute with regard to the term, "packet(s)," is whether the term should be given its plain and ordinary meaning in the specific context of each claim, or if the Court should construe the term to only refer to packets operating on "Layer 2" or "Layer 3." At oral arguments, counsel represented that a "packet" in this context is akin to a virtual box of information. Some of the inventions at issue contain seven (7) layers in which information is processed or acted upon. The parties dispute whether "packet(s)" in this context can only refer to "box(es)" of information on Layer 2 or Layer 3.

Plaintiff argues that the Court should construe "packet" to mean "a link layer (L2) or network layer (L3) packet," because a POSITA would understand that to be the meaning of the term. Plaintiff argued that after Layer 3 the "box" is opened and ceases to be a "packet."

Defendant argues that the term "packet" should be given its plain and ordinary meaning, in the context of the particular claim. Defendant argues that in some patents the "L3" or "L2" construction proposed by Plaintiff is too narrow and too broad in other patents. Defendant gives an example that in the '193 patent, "packet" could refer to data units on any of the seven layers. Further, in the '205 patent, claims 62 and 77 only reference packets on the L3 layer. Thus, Defendant argues that the term packet should be read in context of the claim in which it appears.

The Court **FINDS** that the term should be given its **plain and ordinary meaning, which will require reference to the context of the specific claim at issue.** Neither party has proposed a construction of the term, "packet," beyond construing it to include reference to the particular layer at which a packet is used. Accordingly, the Court need not construe the term "packet(s)" beyond whether the term only refers to packets that operate on Layer 2 or Layer 3.

As to construing the term to include reference to the particular layer(s) at which a packet is used, the Court **FINDS** that such a construction requires reference to the particular claims in which the term appears. Although Plaintiff argues that "packets" are only relevant to Layer 2 and 3 in the asserted patents, the patents themselves contemplate "packets" at other layers. E.g., '193 Patent col. 2 ll. 36-44 (referencing an "HTTP packet").[5] Accordingly, whether "packet" refers to any particular layer or layers **should be resolved with reference to the context of the particular claim at issue.**

ii. Whether the Computer-Readable Media Claim Preambles are Limiting

Many of the asserted claims contain preambles. The parties initially disputed whether the preambles of the computer-readable media claims limit the scope of their respective claims. However, at the claim construction hearing, the parties appeared to agree that the claim preambles limit the scope of the claims in the sense that the preambles identify the patented article. For reasons stated on the bench and herein, the Court agrees and **FINDS** that the "computer-readable media" preambles limit the scope of their respective claims.

"Generally, the preamble does not limit the claims." Allen Engineering Corp. v. Bartell Indust., Inc., 299 F.3d 1336, 1346 (Fed. Cir. 2002). However, "when the claim drafter chooses to use both the preamble and the body to define the subject matter of the claimed invention, the

[5] At the Markman hearing, counsel represented that Layer 7 contains "HTTP packets."

invention so defined, and not some other, is the one the patent protects." Bell Communications Research, Inc. v. Vitalink Communications Corp., 55 F.3d 615, 620 (Fed. Cir. 1995) (emphasis in original) (collecting cases). "In those . . . cases where the preamble to the claim or count was expressly or by necessary implication given the effect of a limitation, the introductory phrase was deemed essential to point out the invention defined by the claim or count." Id. at 620-21 (quoting Kropa v. Robie, 187 F.2d 150, 152 (C.C.P.A. 1951)). It is often said that to determine whether a preamble limits a claim, courts should look to whether the preamble is needed to "give life, meaning, and vitality to the claims or counts." E.g., Bell Communications, 55 F.3d at 621 (quoting Kropa, 187 F.2d at 152). In cases involving computer-readable media claims, such as those implicated here, other courts have held that similar preambles are limiting. E.g., United States Auto. Ass'n v. Wells Fargo Bank, N.A., No. 2:18-cv-00245, 2019 U.S. Dist. LEXIS 99285, at *21 (E.D. Tex. June 13, 2019) ("Without reference to the preamble it is not clear whether the claim covers the medium holding the instructions for the processor or performance of the functions irrespective of a processor.").

Claim 77 of the '205 Patent is illustrative; it is quoted below, and the preamble is in bold.

> **One or more non-transitory computer-readable media having instructions stored thereon, that when executed, cause each packet security gateway of one or more packet security gateways associated with a security policy management server to:**
>
> receive, from the security policy management server, a dynamic security policy comprising at least one rule specifying a set of network addresses and a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI);
>
> receive packets associated with a network protected by the packet security gateway;
>
> perform, on the packets, on a packet by packet basis, at least one packet transformation function of multiple packet transformation functions specified by the dynamic security policy;
>
> encapsulate at least one packet of the packets that falls within the set of network addresses and matches the SIP URI with a header containing a network address that is different from

a destination network address specified by the at least one packet and that corresponds to a network device configured to copy information contained in the at least one packet and to forward the at least one packet to the destination network address; and

route, based on the header, the at least one packet to the network address that is different from the destination network address.

'205 Patent cl. 77. Without the preamble, one would not be able to determine what "new and useful process, machine, manufacture, or composition of matter" is claimed by the invention. See 35 U.S.C. § 101; see also 35 U.S.C. § 112(b) ("The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor . . . regards as the invention."). The preamble states what is patented; the balance of the claim states what its patented function is. Thus, the drafter used both the claim preamble and the body of the claim to define to scope of the patented invention.

Accordingly, the Court **CONSTRUES** the computer-readable media preambles to be **LIMITING**, consistent with its analysis and the parties' agreement.

B. CLAIM-SPECIFIC DISPUTES

i. "configured to"

Disputed Term	Plaintiff's Construction	Defendant's Construction	Court's Construction
configured to	**Plain and ordinary meaning - capable of performing a function**	**Plain and ordinary meaning, which requires being actually configured, not merely being capable of being configured**	**Plain and ordinary meaning, which requires being actually configured, not merely being capable of being configured.**

This term appears in asserted claim 63 of the '205 patent. The parties AGREE that "configured to" should be given its plain and ordinary meaning. The parties DISAGREE on whether this requires that the configured device be capable of performing a function (as Plaintiff

argues) or if the device must be actually configured (as Defendant argues). The Court **FINDS** that this term be given its **plain and ordinary meaning, which requires that the device be actually configured to do the function.**

Claim 63 of the '205 Patent reads:

> system, comprising:
> . . .
> one or more packet security gateways associated with the security policy management server, wherein each packet security gateway of the one or more packet security gateways comprises computer hardware and logic **configured to** cause the packet security gateway to:
> . . .
> encapsulate at least one packet of the packets that falls within the set of network addresses and matches the SIP URI with a header containing a network address that is different from a destination network address specified by the at least one packet and that corresponds to a network device **configured to** copy information contained in the at least one packet . . .
> .

'205 Patent, cl. 63.

Plaintiff argues that the plain and ordinary meaning merely requires that the applicable system be capable of performing the given function. Plaintiff argues that the term is only located in system claims, not method claims; therefore, the term should be read as not requiring a step.

Defendant argues that other courts have consistently held that "configured to" does not mean "capable of." Defendant further argues that the claim language does not use a future-tense verb or the phrase "capable of." Accordingly, Defendant argues that the term should require the system to actually be configured.

This Court has previously rejected proposed constructions of "configured" to mean "capable of." E.g., Swimways Corp. v. Zuru, Inc., Case No. 2:13-cv-334, 2014 U.S. Dist. LEXIS 98092, at *17-20 (E.D. Va. July 18, 2014). As this Court recognized, "a construction that an appendage is merely 'capable' of propelling a figure through liquid fails to adequately convey that the appendage is actually 'configured to' propel the figure through the liquid." Id. at *18. Other

district courts have taken similar approaches. E.g., Solocron Media, LLC v. Verizon Communs. Inc., 2:13-CV-01059, 2015 U.S. Dist. LEXIS 26681, *35-36 (E.D. Tex., Mar. 5, 2015) (construing configured to as having its "plain meaning, which the Court understands to require not merely being capable of being configured but rather being actually configured."); Sipco, LLC v. Abb, Inc., No. 6:11-CV-0048, 2012 U.S. Dist. LEXIS 106659, *29-33 (E.D. Tex. July 30, 2012) (same). This construction is consistent with the claim language and patent specification. Accordingly, the Court **CONSTURES** "configured to" as having its plain and ordinary meaning, which requires actual configuration.

ii. Dynamic Security Policy

Disputed Term	Plaintiff's Construction	Defendant's Construction	Court's Construction
dynamic security policy	A non-static set of one or more rules, messages, instructions, files, or data structures associated with one or more packets	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	A changeable set of one or more rules, messages, instructions, files, or data structures, or any combination thereof, associated with one or more packets.

This term appears in claims 63 and 77 of the '205 Patent. Having reviewed the evidence and considered the arguments of counsel, the Court **FINDS** that the appropriate construction of "dynamic security policy" is: "**a changeable set of one or more rules, messages, instructions, files, or data structures, or any combination thereof, associated with one or more packets.**"

Plaintiff devotes much of its argument to emphasize that this term should be construed as being "non-static," i.e., dynamic. Doc. 155 at 10-11. Plaintiff cites the '205 specification where,

at several points, the specification refers to the capability of the security policy to change. Plaintiff also argues that its construction is consistent with the Court's Keysight Markman Order which construed "packet-transformation function specified by the plurality of dynamic security policies" as "function specified by the dynamic security policy where the dynamic security policy is subject to change." Id.

Defendant argues that the patentee acted as its own lexicographer. Doc. 158 at 6. Defendant takes its proposed construction directly from the patent specification, which states "As used herein, a dynamic security policy includes [Defendant's construction]." Doc. 158 at 7.

The Court has already construed a similar term, "packet-transformation functions specified by the plurality of dynamic security policies," as "function specified by the dynamic security policy where the dynamic security policy is subject to change." Centripetal Systems Inc. v. Keysight Technologies, 2:17-cv-383, Doc. 484, at 21 (E.D. Va. Sept. 17, 2018).[6] Accordingly, the Court has already held that a "dynamic security policy" in the context of these patents is "changeable."

The Court notes that a "dynamic security policy," as defined by the '205 Patent, may include more subject matter than is proposed by Defendant's construction. As the specification reads:

> As used herein, a dynamic security policy includes 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. [As Defendant argues.] Optionally, a dynamic security policy may further specify one or more additional parameters as described herein.

'205 Patent col. 4 ll. 43-49 (emphasis added). Upon review of the claims and specification, and considering the arguments of counsel, the Court **FINDS** that Plaintiff's proposed construction is

[6] The "Keysight case" was a patent case involving the same Plaintiff and similar patents and technology. The Keysight case was resolved by settlement of the parties during the jury trial.

the most appropriate. However, the Court makes the following modifications. The Court will use the term, "**changeable,**" instead of "non-static" to facilitate the jury's comprehension of this term. The Court will also add "**or any combination thereof**" after the word, "structure," to reflect that a dynamic security policy may include multiple rules, messages, etc. E.g., '205 Patent col. 5 ll. 61-61 ("dynamic security policy . . . may include one or more rules. . . ."); id. at col. 6 l. 56 ("dynamic security policy . . . may include rules.").

iii. Correlate, Based on the Plurality of Log Entries

Disputed Term	Plaintiff's Construction	Defendant's Construction	Court's Construction
5. correlate, based on the plurality of log entries	packet correlator may compare data in one or more log entries with data in one or more other log entries	correlate by comparing log entries that do not already include information about linked connections	packet correlator may compare data in one or more log entries with data in one or more other log entries

This term appears in claims 11 and 21 of the '176 Patent. The term "correlate" was previously construed by this Court as "packet correlator may compare data in one or more log entries with data in one or more other log entries to identify the host," as Plaintiff argues. Keysight, 2:17-cv-383 at 27-28. Thus, the Court **FINDS** that the appropriate construction is "**packet correlator may compare data in one or more log entries with data in one or more other log entries.**"

Defendant argues that this term should be construed to include log entries that do not use correlation using information that pertains to previously linked connections. Defendant argues that Plaintiff should be precluded from attempting to include previously linked connections, because of statements Plaintiff allegedly made to the PTO during IPR. Specifically, Defendant argues that Plaintiff distinguished prior art by arguing in IPR:

> In fact, because Rajan's trace log already "identifies the end-to-end network traffic activity between a client and server even though the network traffic traverses a plurality of transport layer connections," there would never be any utility in using the trace logs for correlating packets. . . . More specifically, Rajan teaches that a trace manager first identifies linked incoming and outgoing connections and then stores information "on the linked connections in the trace log."

Doc. 158 at 12.

Plaintiff argues that it has not "clearly" disavowed the use of already linked connections in IPR. Plaintiff argues that the PTO found that the prior art referenced here (Rajan) is not actually prior art to Plaintiff's patents.

The Court is not persuaded that prosecution disclaimer[7] is appropriate here. "For prosecution disclaimer to attach, [Federal Circuit] precedent requires that the alleged disavowing actions or statements made during prosecution be both clear and unmistakable." Avid Tech., Inc. v. Hamonic, Inc., 812 F.3d 1040, 1045 (Fed. Cir. 2016) (quoting Omega Eng'g, Inc. v. Raytek Corp., 334 F.3d 1314, 1325-26 (Fed. Cir. 2003)). Indeed, this is a high burden. Id. The Rajan invention correlates information first, then generates log entries. As Plaintiff argued in IPR, if one tried to use Rajan's process in its invention, "the necessary information to create those trace logs would remain unavailable." Doc. 158-6 at 13. The PTO found, "because Rajan's trace log is created on the same 'intermediary device' that receives and transmits the packets being traced, Rajan does not teach using its trace logs to perform any correlation of the received and transmitted packets envisioned by Ivershen." Doc. 158-6 at 9. Additionally, the Court has construed a similar

[7] Although prosecution history estoppel is a doctrine of infringement, prosecution disclaimer, a related doctrine, applies in the claim construction context. Prosecution history estoppel prevents a patentee from re-capturing what it surrendered in prosecution through a doctrine of equivalents infringement theory. Festo Corp. v. Shoketsu Kinzoku Kogyo Kabushiki Co., Ltd., 535 U.S. 722, 733-34 (2002). However, prosecution disclaimer prevents a patentee from re-capturing that which it surrendered in prosecution through claim construction. Omega Eng'g, Inc. v. Raytek Corp., 334 F.3d 1314, 1323 (Fed. Cir. 2003).

term in the prior Keysight litigation. Keysight, 2:17-cv-383 at 27-28. Accordingly, the language which Defendant calls disavowal is neither clear nor unmistakable.

Further, there is no language in the claims or specification to support limiting the scope of the claims as Defendant requests. Without a clear and unmistakable disavowal of territory covered by the plain meaning of the patent's claims, the Court will not limit the scope of the claim as requested by Plaintiff. Accordingly, the Court **FINDS** that the appropriate construction is "**packet correlator may compare data in one or more log entries with data in one or more other log entries.**"

iv. Responsive to Correlating

At the Markman hearing, the Court took this term **UNDER ADVISEMENT**. The Court ordered further briefing to be filed by the close of business on Tuesday, February 11, 2020. The parties advised the Court that they agreed that this term should have its plain and ordinary meaning. Accordingly, the Court will give the term "responsive to correlating" its **PLAIN AND ORDINARY MEANING.**

v. Generate, Based on the Correlating, One or More Rules

Disputed Term	Plaintiff's Construction	Defendant's Construction	Court's Construction
generate, based on the correlating, one or more rules	**Plain and Ordinary Meaning – no construction necessary**	**Generate one or more rules based on the correlating, not based on user defined filters or rules**	**Plain and ordinary meaning.**

At the Markman hearing, the Court took this term **UNDER ADVISEMENT** and ordered additional briefing. The parties filed their supplemental briefing on February 11, 2020. Doc. 192, 193. Having reviewed the opening, rebuttal, and supplemental briefs and considering the evidence

in the record and arguments of counsel, the Court **FINDS** that this term should have its **plain and ordinary meaning.**

The dispute over this term is whether Plaintiff disavowed the use of "user defined filters or rules" during the original prosecution. Defendant argues that in original prosecution, Plaintiff sought to distinguish its invention from prior art, referred to as Pleshek, by arguing that Pleshek "did not generate 'based on the correlating' because the automated rule generation of Pleshek was based on 'user defined filters.'" Doc. 158 at 17.

Plaintiff argues that it did not clearly disavow the use of user-defined rules. Plaintiff argues that it distinguished itself from Pleshek by arguing that Pleshek does not "generate, based on the correlating." Plaintiff argues that it argued against the same "specific implementation" in Pleshek. Doc. 161 at 21-22.

As discussed supra at 18, 18 n.6, "For prosecution disclaimer to attach, [Federal Circuit] precedent requires that the alleged disavowing actions or statements made during prosecution be both clear and unmistakable." Avid Tech., Inc., 812 F.3d at 1045. The specific portion of the record that composes the alleged disavowal is:

> However, the Office Action [rejecting claims due to Pleshek] is incorrect. In paragraph [0065], Pleshek states that "the tool optimizer 102 automatically generates the filter rules 110 based upon these user defined filters 108." Similarly, Pleshek paragraph [0142] states "ASE converts overlapping user-defined filters into filter rules useable with single-forwarding-action per packet switching ICs." Thus, even assuming, arguendo, that the filter rules in Pleshek are similar to the "one or more rules configured to identify packets received from the host located in the first network," Pleshek fails to teach or suggest "generating . . . based on the correlating, one or more rules configured to identify packets received from the host located in the first network," as recited in amended claim 1.

Doc. 159-4 at 13-14. Although Plaintiff refers to "user defined rules," Plaintiff ultimately distinguishes its invention by stating that "Pleshek fails to teach or suggest "generating . . . based on the correlating, one or more rules configured to identify packets received from the host located

in the first network, as recited in amended claim 1." Id. (internal quotations omitted). Thus, it is not clear and unmistakable that Plaintiff sought to distinguish its invention based on the use of user defined rules. Accordingly, importing such a limitation is inappropriate. Therefore, the Court **FINDS** that the **plain and ordinary meaning** is the correct construction.

vi. Proxy System

Disputed Term	Plaintiff's Construction	Defendant's Construction	Court's Construction
proxy system	a proxy system which intervenes to prevent threats in communications between devices	system that intermediates a communication session between network devices to prevent threats in communications between such devices	a proxy system which intervenes to prevent threats in communications between devices

This Court has already construed "proxy system" as "a proxy system which intervenes to prevent threats in communications between devices." Keysight, 2:17-cv-383, Doc. 484, at 33-34. Defendant argues that this construction merely clarifies what a proxy system does, not what it is.

Proxy system is a straightforward term that a POSITA would understand and the Court **FINDS** that no further construction is necessary beyond its Keysight construction. The Court's previous construction clarifies the term insofar as a lay person may be confused. Accordingly, I the Court will apply its previous construction and insofar as Defendant asks the Court to define proxy system, the Court should give the term its plain and ordinary meaning.

VI. CONCLUSION

Accordingly, having considered the arguments of counsel and the record evidence, the Court **CONSTRUES** the disputed terms as follows:

Term	Court's Construction
Packets	Plain and ordinary meaning in the context of the claim in which the term appears.
Preambles	Limiting.
Configured to	Plain and ordinary meaning which requires that the action actually do the function automatically.
Dynamic security policy	a changeable set of one or more rules, messages, instructions, files, or data structures, or any combination thereof, associated with one or more packets.
Correlate, based on a plurality of log entries	Packet correlator may compare data in one or more log entries with data in one or more other log entries.
Responsive to correlating	Plain and ordinary meaning.
Generate, based on the correlating, one or more rules.	Plain and ordinary meaning.
Proxy system	A proxy system which intervenes to prevent threats in communications between devices.

The Clerk is **REQUESTED** to deliver a copy of this Opinion and Order to counsel of record.

It is **SO ORDERED**.

/s/
Henry Coke Morgan, Jr.
Senior United States District Judge

Norfolk, Virginia
February 20, 2020

HENRY COKE MORGAN, JR.
SENIOR UNITED STATES DISTRICT JUDGE

FILED
APR 27 2020
CLERK, U.S. DISTRICT COURT
NORFOLK, VA

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Norfolk Division

CENTRIPETAL NETWORKS, INC.,	)	
	)	
Plaintiff,	)	
v.	)	**Civil Action No. 2:18cv94**
	)	
CISCO SYSTEMS, INC.,	)	
	)	
Defendants.	)	

ORDER

These matters are before the Court on cross motions for summary judgment. Defendant Cisco Systems, Inc, ("Cisco") filed the first Motion for Summary Judgment on March 4, 2020. Doc. 255. Shortly after, Plaintiff Centripetal Networks, Inc. ("Centripetal") filed its Motion for Summary Judgment on March 11, 2020. Doc. 287. For the following reasons herein, the Court **DENIES** both Motions regarding the issue of infringement. Additionally, the Court **RESERVES RULING** on the application of prosecution history estoppel.

I. LEGAL STANDARD

Summary judgment under Rule 56 is appropriate only when the court, viewing the record as a whole and in the light most favorable to the nonmoving party, determines that no genuine issue of material fact exists and that the moving party is entitled to judgment as a matter of law. Fed. R. Civ. P. 56; see, e.g., Celotex Corp. v. Catrett, 477 U.S. 317, 322–24 (1986); Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 248–50 (1986); Terry's Floor Fashions v. Burlington Indus., 763 F.2d 604, 610 (4th Cir. 1985). Once a party has properly filed evidence supporting the motion for summary judgment, the nonmoving party may not rest upon mere allegations in the pleadings but must instead set forth specific facts illustrating genuine issues for trial. Celotex,

477 U.S. at 322–24. Such facts must be presented in the form of exhibits and sworn affidavits. Failure to rebut the motion with such evidence will result in summary judgment when appropriate. "[T]he plain language of Rule 56(c) mandates the entry of summary judgment . . . against a party who fails to make a showing sufficient to establish the existence of an element essential to that party's case, and on which that party will bear the burden of proof at trial." Id. at 322. A mere scintilla of evidence is insufficient to withstand a motion for summary judgment. Rather, the evidence must be such that the fact-finder reasonably could find for the nonmoving party. See Anderson, 477 U.S. at 252.

II. ANALYSIS

A. Infringement

The Federal Circuit has repeatedly stated that the "determination of infringement, whether literal or under the doctrine of equivalents, is a question of fact." Dorel Juvenile Group, Inc. v. Graco Children's Prods., 429 F.3d 1043, 1047 (Fed. Cir. 2005). Therefore, in the case of infringement, the issue is only "properly decided upon summary judgment when no genuine issue of material fact exists." Bai v. L & L Wings, Inc., 160 F.3d 1350, 1353 (Fed. Cir. 1998). Based on the parties' briefing, the Court has determined that there are genuine issues of material fact regarding Cisco's alleged infringement of the '205 and '806 patents. Accordingly, summary judgment is not warranted for either party on the issue of infringement. In so far as the Cisco and Centripetal's motions seek summary judgment on infringement, both motions are **DENIED**.

B. Prosecution History Estoppel

The scope of the legal monopoly of a patent "is not limited to its literal terms but instead embraces all equivalents to the claims described." Festo Corp. v. Shoketsu Kinzoku Kogyo Kabushiki Co., Ltd., 535 U.S. 722, 732 (2002) (citing Winans v. Denmead, 56 U.S. (15 How.)

330, 347 (1854)). The Supreme Court has repeatedly affirmed equivalents as "a firmly entrenched part of the settled rights protected by the patent." Id. at 733. Therefore, the doctrine of equivalents permits protection for the "patentee to claim those insubstantial alterations that were not captured in drafting the original patent claim but which could be created through trivial changes." Id. However, the expanded patent rights granted by the doctrine of equivalents are limited by the proceedings that previously occurred during the Patent and Trademark Office's ("PTO") application process. See id. Accordingly, when "the patentee originally claimed the subject matter alleged to infringe but then narrowed the claim in response to a rejection, he may not argue that the surrendered territory comprised unforeseen subject matter that should be deemed equivalent to the literal claims of the issued patent." Id. at 733-34. Thus, prosecution history estoppel serves to ensure that the patent's claims are interpreted by "reference to those 'that have been cancelled or rejected.'" Id. at 733. Prosecution history estoppel prevents "a patentee from regaining, through litigation, coverage of subject matter relinquished during the prosecution of the application for the patent." Id. at 734 (quoting Wang Laboratories, Inc. v. Mitsubishi Elecs. Am., Inc., 103 F.3d 1571, 1577–78 (Fed. Cir. 1997)).

The application of prosecution history estoppel is to be determined by the Court as a matter of law. See Intervet Inc. v. Merial Ltd., 617 F.3d 1282, 1290-91 (Fed. Cir. 2010) (citing Bai, 160 F.3d at 1354). Generally, a narrowing amendment to a patent carries a presumption that the patentee is professing "abandonment of all that is embraced in that difference." Festo Corp, 535 U.S. at 740 (quoting Ex. Supply Co. v. Ace Patents Corp., 315 U.S. 126, 136 (1942)). The burden of proof is on the patentee to provide evidence that the patent amendment "does not surrender the particular equivalent in question." Id. Therefore, prosecution history estoppel presumptively bars the application of the doctrine of equivalents if claim amendments are "made

to secure the patent and the amendment narrows the patent's scope." Id. at 736-37. Accordingly, based on this guidance, the proper focus of inquiry for the Court is "whether the amendment narrows the overall scope of the claimed subject matter." Honeywell Intern. Inc. v. Hamilton Sundstrand Corp., 370 F.3d 1131, 1141 (Fed. Cir. 2004) (citing Festo Corp. v. Shoketsu Kinzoku Kogyo Kabushiki Co., Ltd., 535 U.S. 722, 736-37 (2002)). The patent's scope may be narrowed when either "(1) a preexisting claim limitation is narrowed by amendment or (2) a new claim limitation is added by amendment." Honeywell Intern. Inc., 370 F.3d at 1140 ("Either amendment will give rise to a presumptive estoppel if made for a reason related to patentability.").

The Supreme Court has made clear that "[t]here some cases, however, where the amendment cannot reasonably be viewed as surrendering a particular equivalent." Festo Corp, 535 U.S. at 736-77. The Court has specifically identified three ways in which a patentee can rebut the estoppel presumption:

> (1) the equivalent may have been unforeseeable at the time of the application;
>
> (2) the rationale underlying the amendment may bear no more than a tangential relation to the equivalent in question; or
>
> (3) there may be some other reason suggesting that the patentee could not reasonably be expected to have described the insubstantial substitute in question.

Festo Corp, 535 U.S. at 740-41. Therefore, even if prosecution history estoppel presumptive applies, it "does not completely bar the benefit of the doctrine of equivalents from all litigation related to the amended claim." Intervet Inc. v. Merial Ltd., 617 F.3d 1282, 1291 (Fed. Cir. 2010). Plainly worded, [t]he scope of the estoppel must fit the nature of the narrowing amendment." Id. The Federal Circuit has highlighted that "[a] district court must look to the specifics of the

amendment and the rejection that provoked the amendment to determine whether estoppel precludes the particular doctrine of equivalents argument being made." Id. Consequently, the Court must compare the narrowing amendment made during the application process and the equivalent in question to determine wether that particular equivalent has been surrendered by the patentee. See Festo Corp, 535 U.S. at 737-38.

In the present case, the Court **FINDS** that there are underlying factual disputes that should be determined before issuing a ruling on the application of prosecution history estoppel. On remand from the Supreme Court in Festo, the Federal Circuit emphasized that while questions surrounding "the application and scope of prosecution history estoppel . . . are questions of law for the court", the rebuttal of the presumption "may be subject to underlying facts" which require the "resolution of factual issues". Festo Corp. v. Shoketsu Kinzoku Kogyo Kabushiki Co., Ltd., 344 F.3d 1359, 1368 n. 3 (Fed. Cir. 2003). Like a ruling on claim construction, the factual issues underlying a legal claim may be properly decided by the court. Id. Therefore, determining the application of prosecution history estoppel, like claim construction, can benefit from the use of extrinsic evidence such as "expert and inventor testimony, dictionaries, and learned treatises . . . to explain scientific principles, the meaning of technical terms, and terms of art that appear in the patent and prosecution history." See Markman v. Westview Instruments, Inc., 52 F.3d 967, 980 (Fed. Cir. 1995), aff'd, 517 U.S. 370 (1996) (in the context of claim construction). Since this case is now proceeding as a bench trial, the parties will have an opportunity to present the disputed facts to the Court at trial. The Court will, then, come to an informed ruling now aided by additional documentary and testimonial evidence. Accordingly, the Court **RESERVES RULING** on summary judgment regarding the application of prosecution history estoppel.

III. CONCLUSION

For the reasons stated, the Court **DENIES** both Motions regarding the issue of infringement. Moreover. the Court **RESERVES RULING** on the issue of prosecution history estoppel. The Clerk is **REQUESTED** to electronically deliver a copy of this Order to all counsel of record.

It is **SO ORDERED**.

/s/
Henry Coke Morgan, Jr.
Senior United States District Judge

HENRY COKE MORGAN, JR.
SENIOR UNITED STATES DISTRICT JUDGE

April 24, 2020
Norfolk, Virginia

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Norfolk Division

FILED
OCT - 2 2020
CLERK, U.S. DISTRICT COURT
NORFOLK, VA

CENTRIPETAL NETWORKS, INC.,

Plaintiff,

v.

CISCO SYSTEMS, INC.,

Defendant.

Civil Action No. 2:18cv94

OPINION AND ORDER

This matter is before the Court on Cisco Systems, Inc.'s, ("Cisco") Motion for Miscellaneous Relief. In its motion, Cisco argues that recusal is mandatory under 28 U.S.C § 455(a) and (b)(4).

I. BACKGROUND

While presiding over this case, the Court has made Cisco and Centripetal's counsel aware of any possible conflict. The first disclosure came on March 2, 2020, where the Court's former law clerk, Neil McBride, entered the case on behalf of Cisco. The Court promptly notified the parties and disclosed that the Court had "visited Neil's home and he has visited mine and we have had family dinners together many times over the years." Counsel for both parties responded that recusal was not necessary as a result of Mr. McBride's representation of Cisco. Next, during the pre-trial conference, the Court disclosed that it had purchased 200 shares of Zoom stock based on a recommendation by a service over the internet. At that time, neither party objected to the ownership of Zoom stock. Thereafter, the Court conducted a bench trial "spanning nearly eight weeks over Zoom, producing a 3,507-page record with twenty-six witnesses and over 300

exhibits." Doc. 564 at 2. As a result of an enormous variation in damages calculations by the opposing damages experts, the Court request additional data relevant to damages and after receipt of this information the Court heard final arguments on June 25, 2020.

On August 11, 2020, the Court's administrative assistant discovered during preparation of the Court's judicial financial disclosure reporting that the Court's spouse owned 100 shares of Cisco stock valued at $4,687.99 and advised the Court. The Court promptly investigated the issue and confirmed that the shares were purchased as a result of her brokers recommendation. The Court's spouse had no independent recollection of approving the transaction. The next day, August 12, 2020, the Court disclosed the existence of the shares to the parties. See Court's Email to Counsel [Attached as Ex. One]. The Court detailed that "full draft of my opinion had been prepared before I received this information yesterday. Virtually every issue was decided prior thereto." Id. Also explaining that the shares "did not and could not have influenced my opinion on any of the issues in this case." Id. Centripetal quickly notified the Court that it had no objection based on the representations by the Court. Cisco responded, nine days later, by filing the instant motion for recusal. The Court ordered a response by Centripetal, if they be so advised. Centripetal responded by objecting to Cisco's motion and Cisco filed a rebuttal brief. The Court conducted a hearing on the motion and heard oral argument on September 9, 2020. At the hearing, the Court informed the parties that he had discussed the issue with his spouse and, as a result, the Court contacted their personal attorney to request the creation of a blind trust to divest the shares. The Court provided the completed trust documents to the parties at the hearing

Moreover, at the hearing on Cisco's current motion, the Court disclosed a previous purchase by the Court and his spouse of 100 shares each of Crowdstrike stock. Similar, to Zoom, Crowdstrike was purchased on the basis of a recommendation of an internet service. The Court

later discovered that Crowdstrike primarily engaged in the business of developing cybersecurity technology and had a previous intelligence sharing agreement with Centripetal. See PTX-1600. After learning of this information, the Court and his spouse divested their shares in Crowdstrike. Due to the indirect nature of Crowdstrike as a potential competitor of both parties, the Court did not disclose this transaction until the hearing date.

II. LEGAL STANDARD AND ANALYSIS

28 U.S.C § 455(a) requires that a judge of the United States "shall disqualify himself in any proceeding in which his impartiality might reasonably be questioned." 28 U.S.C. § 455(a). The next section of the statute, 455(b) lays out specific circumstances where recusal is required. Section 455(b)(4) lays out one of these circumstances at issue here where:

> He knows that he, individually or as a fiduciary, or his spouse or minor child residing in his household, has a financial interest in the subject matter in controversy or in a party to the proceeding, or any other interest that could be substantially affected by the outcome of the proceeding

28 U.S.C § 455(b)(4) (emphasis added). In its rebuttal brief, Cisco argues that the Court should have immediately recused itself and it should not have been required to file its initial motion to recuse.

Under section 455, "[a] judge is as much obliged not to recuse himself when it is not called for as he is obliged to when it is." Muchnick v. Thomson Corp. (In re Literary Works in Elec. Databases Copyright Litig.), 509 F.3d 136, 140 (2d Cir. 2007). Therefore, in deciding a motion for recusal under section 455, judges "must balance our duty to appear impartial against several practical considerations, including the availability of other judges, the cost in judicial resources of recusal and reassignment of the case to different judges, and the interest of the parties and the public in a swift resolution of the dispute." Id. (citation omitted).

In analyzing section 455, the Supreme Court in Liljeberg v. Health Services Acquisition Corp., held that scienter is not a requirement of 455(a), but is a requirement of 455(b)(4). Liljeberg v. Health Services Acq. Corp., 486 U.S. 847, 859 (1988). Therefore, recusal under section 455(b)(4) imposes "actual knowledge" of the disqualifying financial interest. C. Tel. Co. of Virginia v. Sprint Commun. Co. of Virginia, Inc., No. 3:09CV720, 2011 WL 6178652, at *5 (E.D. Va. Dec. 12, 2011) (collecting cases imposing the "actual knowledge" test), aff'd, 715 F.3d 501 (4th Cir. 2013) (on other grounds). However, the test for recusal under section 455(a), is "when a reasonable person, knowing the relevant facts, would expect that a justice, judge, or magistrate knew of circumstances creating an appearance of partiality." Id. at *7 (quoting Liljeberg, 486 U.S. at 850). Therefore, for section 455(a), "recusal is required even when a judge lacks actual knowledge of the facts indicating his interest or bias in the case if a reasonable person, knowing all the circumstances, would expect that the judge would have actual knowledge." Liljeberg, 486 U.S. at 860-61. The Court will first address recusal under 455(a) and then turn to 455(b)(4).

i. Section 455(a)

The Second Circuit, in Chase Manhattan explained that disqualification is required when "(i) a reasonable person, knowing all the facts, would conclude that the judge has a disqualifying interest in a party under Section 455(b)(4), and (ii) such a person would also conclude that the judge knew of that interest yet heard the case." Chase Manhattan Bank, 343 F.3d at 128. Accordingly, recusal under section 455(a) is an objective test looking at "what a reasonable person knowing all the facts would conclude." C. Tel. Co. of Virginia, 2011 WL 6178652, at *7 (quoting Chase Manhattan Bank v. Affiliated FM Ins. Co., 343 F.3d 120, 127 (2d Cir. 2003)).

Cisco, in its motion for recusal, contends that in light of "the Court's decision to order it to trial in unusual circumstances, and its featuring as a topic of marital conversation, a reasonable observer is likely to conclude that, at the very least, the Court 'should have known' of the ownership of Cisco stock when the purchase occurred in October 2019 . . . ." Doc. 557 at 8. Moreover, Cisco avers that the requirement of a judge to take "reasonable efforts inform himself about the personal financial interests of his spouse" under section 455(c) would have allowed the Court to uncover this interest back in October of 2019. See id. at 7. Cisco's contention is that a reasonable inquiry would have revealed the stock interest before trial of the case. It specifically suggests that "any such process—whether it involved preclearing stock purchases before they happen; monitoring purchase confirmation documents as they are issued; or reviewing brokerage statements showing stock holdings—would have revealed the Cisco stock holding shortly after the purchase." Doc. 557 at 7. Cisco argues that a reasonable person would conclude that the Court should have been known because the "purchase confirmation was addressed to the Court's spouse at home" and "the Court has 'frequently' mentioned Cisco and Centripetal to the Court's spouse." Id. at 7. Accordingly, Cisco argues "[a] reasonable observer would believe that—pursuant to a 'reasonable effort' to ascertain investments by the Court's spouse—the Court would have done more than simply complete its annual disclosure." Doc. 569 at 6.

Centripetal, in opposition, responds that the facts presented would not lead a reasonable person to conclude that the Court knew of this interest but proceeded despite that interest. Centripetal notes the "touchstone of the inquiry is reasonableness, not exhaustive and constant vigilance to the point of reviewing mail separately addressed to judges' spouses, as Cisco proposes." Doc. 564 at 8. Centripetal argues that the inquiry is judged on a reasonableness standard and reasonableness is confirmed by the legislative history of the section 455

highlighting that "the judge need not know what they are [his spouse's investments], but must merely make a reasonable effort to inform himself of their investments." Id. (quoting H.R. Rep. No. 93–1453 (1974), 1974 U.S.C.C.A.N. 6351, 6356) (emphasis added).[1] Accordingly, Centripetal concludes "[e]ither way, Cisco's unsupported insinuations do not establish an appearance of bias under Section 455(a)." Id. The Court agrees with Centripetal. The Court **FINDS** that a reasonable person would not conclude that the Court knew of his spouse's ownership and proceeded to hear the case nonetheless, where the Court avers he was notified about the stock during the preparation of his annual financial disclosures and immediately notified counsel.

The factually similar case of Central Telephone Co. of Virginia v. Sprint Commun. Co. of Virginia, Inc., 3:09CV720, 2011 WL 6178652, at *5 (E.D. Va. Dec. 12, 2011) is particularly persuasive. In Central Telephone, "at a time when the preparation of the opinion on Sprint's counterclaim was underway and when the presiding judge was preparing the annual financial disclosure statement required of federal judges, the presiding judge became aware that, at all times during which he had presided over this action, he owned stock in CenturyLink [Plaintiffs]." C. Tel. Co. of Virginia, 2011 WL 6178652, at *1. "As soon as the presiding judge realized that he owned the CenturyLink stock, he informed the parties of the situation during a conference call." Id. at *2. Therefore, the Court promptly notified that parties that "he was unaware" of the share's ownership during the proceedings at issue. Id. at *8. The court determined there that "a reasonable person would understand that it would be unlikely for a

[1] Specifically, Centripetal states:

> what about the importance of this case or the Court's mentioning of Cisco during discussions with his wife should have put the Court on notice of his wife's forgotten financial transaction facilitated by her separate broker? Cisco does not say. Surely Cisco is not arguing that a reasonable observer would believe that the Court's wife does remember her interest and disclosed it to the Court during these conversations and the Court is now lying.

Doc. 564 at 9.

judge, who has all along known about his ownership of disqualifying stock, to suddenly bring that ownership to the parties' attention after devoting many weeks of his time to deciding a complex jurisdictional motion, to resolving summary judgment motions, to presiding over two trial sessions, and to preparing findings of fact and conclusions of law." Id.

These facts are directly analogous to the situation presented here. After learning of his spouse's financial interest while preparing annual financial disclosures, the Court promptly notified counsel that he was unaware that his spouse had purchased shares of Cisco stock. A reasonable person would find it unlikely that a judge would now disclosure his spouse's ownership of disqualifying stock after devoting months of his time engaging in ruling of pre-trial motions, holding a Markman hearing, and conducting an almost six-week bench trial while drafting findings of fact and conclusions of law that total over 150 pages. Like Central Telephone, the circumstances presented here make it difficult to believe that a reasonable person viewing these facts would conclude that the Court "knew of that interest yet heard the case." See Chase Manhattan Bank, 343 F.3d at 128. Cisco, both in their reply brief and on oral argument, noted that Central Telephone is inapplicable because the Fourth Circuit affirmed Central Telephone on the grounds that the stock interest fell under the mutual fund exception outlined in section 455(d)(4)(i). See C. Tel. Co. of Virginia v. Sprint Commun. Co. of Virginia, Inc., 715 F.3d 501, 516 (4th Cir. 2013). The fact that the Fourth Circuit found that the interest fell under a safe harbor provision of the statute, which is not applicable here, does not distract from the persuasiveness of a decision that found recusal, under similar facts, was unwarranted. See C. Tel. Co. of Virginia, 2011 WL 6178652, at *8.

Furthermore, Cisco argues that the factual situation presented here is more akin to that in other cases where recusal was warranted. Specifically, Cisco argues that the reasoning in Central

Telephone "cannot be reconciled with either Chase Manhattan or Shell Oil ; each judge in those cases also 'brought [the] financial interest to the parties' attention, just after [they] discovered the ownership,' and would have been no more likely to 'run the risk of impeachment or perhaps prosecution for knowingly deciding a case from which he knew he should have recused himself.'" However, the factual circumstances in both Chase Manhattan and Shell Oil are quite different than presented in this case.

In Chase Manhattan, the Second Circuit found that the objective observer would have concluded that the presiding judge knew of his ownership in stock where as a result of a merger the stock was not held in the name of the party to the case but was purchased in the name of the previous company. There, "the merger was widely publicized, the judge received letters from officials from the new company (in which he held the stock) on that company's letterhead during litigation, witnesses at trial discussed the merger, and the judge's opinion containing his findings of fact referred to the newly merged company as a party." C. Tel. Co. of Virginia, 2011 WL 6178652, at *9 (discussing Chase Manhattan). None of those circumstances are present here. Therefore, there was no indication the Court at any point in this case knew that his spouse had purchased Cisco before review of his financial reports. Accordingly, this case is factually distinct from Chase Manhattan.

Turning to Shell Oil, the Federal Circuit found that the presiding judge had actual knowledge of his wife's stock ownership in a party for purposes of determining a section 455(b)(4) violation. In that case, the weight of prompt disclosure of an interest under the reasonable observer standard was never discussed because the court was not analyzing the motion under the standard for 455(a) but instead was dealing with 455(b)(4). See Shell Oil Co. v. U.S., 672 F.3d 1283, 1289 (Fed. Cir. 2012) (noting "the subsection at issue here" is 455(b)(4)).

Additionally, in Shell Oil, the record reflects knowledge of his wife's financial interest in Chevron at least as early as May 15, 2009 when he completed his certified Financial Disclosure Report disclosing an interest in "Chevron Texaco Stock.'" Id. at 1291. This "May 15, 2009 disclosure date post-dates the trial judge's February 2, 2008 and March 31, 2009 opinions addressing the oil companies' motions for summary judgment as to liability and damages, it pre-dates his September 28, 2009 decision denying the government's motion for reconsideration with respect to damages, as well as his October 30, 2009 entry of final judgment." Id. The presiding judge in Shell Oil, notified the parties of his knowledge of the interest on November 16, 2009, six-months after completing his disclosure report. Shell Oil involved a six-month period without disclosure and during that period the presiding judge continually made decisions in the interim after actual knowledge of the interest. This is factually distinct that the situation presented here where the Court made immediate disclosure to the parties and had already decided virtually all issues in the bench trial.

Finally, Cisco frequently cites Liljeberg v. Health Services Acq. Corp., 486 U.S. 847 (1988) as support that recusal is warranted. This is another case where the factual circumstances are drastically different. Centripetal highlights these differences in their opposition motion noting the judge there:

> (1) sat on the Board of Trustees of an interested party, yet somehow forgot about its interest in land that was purchased for over $6 million dollars and stood to increase its value by 60% when the litigation arose;
> (2) attended a meeting discussing negotiations relevant to this interest days before the case was filed, which showed he had actual knowledge of the interest even if he later forgot;
> (3) despite ten years of regular Board meeting attendance, missed the one meeting at which his trial was discussed, and the other trustees remarkably chose not to "call to the judge's attention the obvious conflict of interest" of a University trustee presiding over this particular trial; and
> (4) failed to review the minutes mailed to him for that missed meeting, which would have revealed that the trial had been discussed.

Doc. 564 at 10 n. 5 (citing Liljeberg, 486 U.S. at 857, 865-67). The totality of the circumstances present in Liljeberg are fundamentally different than present before the Court. In Liljeberg, the plurality of facts point that the presiding judge had complete awareness of the conflicting interest by sitting on the board of trustees and sitting in on meetings where the interest was discussed. This is drastically different than the Court's spouses independent purchase of stock on the advice of an independent broker without providing any information to the Court.

Moreover, a reasonable observer would consider the Court's candor and history of disclosing possible conflicts in this case. As discussed supra, the Court has continually disclosed potential conflictual issues to counsel including Mr. McBride's representation of Cisco and ownership of Zoom stock. It is unreasonable to assume that this Court would be so forthcoming regarding possible conflicts and at the same time conceal a more direct conflict of stock ownership of a named party. Therefore, a reasonable observer would weigh the Court's repeated candor in favor of a finding that it had no knowledge of its spouse's Cisco stock ownership. Furthermore, the Court evidenced its pattern of dealing with potential stock ownership conflicts by the manner in which it dealt with the Crowdstrike purchase. When the Court discovered that Crowdstrike may be a competitor in the similar cybersecurity technology with Cisco and Centripetal, the Court and the Court's spouse promptly sold their shares. Accordingly, it would an unreasonable presumption that a reasonable person viewing the facts would conclude that the Court would act any differently with knowledge of his spouse's ownership of Cisco.

For all the reasons stated, the Court **FINDS** that a reasonable person would not conclude that the Court knew of that interest and yet heard the case. Therefore, section 455(a) does not warrant recusal.

ii. Section 455(b)(4)

Turning to section 455(b), as stated supra, recusal under this section requires "actual knowledge" of the disqualifying financial interest. C. Tel. Co. of Virginia, 2011 WL 6178652, at *5 (collecting cases imposing the "actual knowledge" test). Here, the case of Central Telephone is again persuasive in the Court's analysis.

In Central Telephone, the presiding judge found section 455(b)(4) to not apply to the facts because there was "no actual knowledge of the conflict." The conflict was discovered by the presiding judge "at a time when the preparation of the opinion on Sprint's counterclaim was underway and when the presiding judge was preparing the annual financial disclosure statement required of federal judges . . ." C. Tel. Co. of Virginia, 2011 WL 6178652, at *1. Similarly, the Court only discovered the ownership during preparation of an annual financial disclosure report. However, here, the Court represented that every issue was "virtually" decided in this case before there was actual knowledge of the Cisco stock. Thus, in Central Telephone, the drafting of the presiding judge's decision was "underway," which is comparable to this Court's mostly drafted opinion. Moreover, this Court rests on the persuasive logic illustrated by the Ninth Circuit in Davis v. Xerox, 811 F.2d 1293, 1296 (9th Cir. 1987). There, the court noted that the right course under section 455(b) is:

> to proceed on a case by case basis, determining the existence of disqualifying knowledge at the time the judge sat, in the way that a state of mind is normally determined, from inspection of all the circumstances. If a reasonable person would conclude from all the circumstances are such that a reasonable person would conclude that the judge had not forgotten but continued to know, his rulings must be vacated.

Davis v. Xerox, 811 F.2d 1293, 1296 (9th Cir. 1987).

iii. Divestment under 455(f)

Based on the findings above, the Court **FINDS** that section 455(a) or 455(b)(4) do not apply to the facts before the Court. The Court still recognizes that any section 455(b)(4) conflict can be cured by the divestment provision of Section 455(f). Section 455(f) states that

> Notwithstanding the preceding provisions of this section, if any justice, judge, magistrate judge, or bankruptcy judge to whom a matter has been assigned would be disqualified, after substantial judicial time has been devoted to the matter, because of the appearance or discovery, after the matter was assigned to him or her, that he or she individually or as a fiduciary, or his or her spouse or minor child residing in his or her household, has a financial interest in a party (other than an interest that could be substantially affected by the outcome), disqualification is not required if the justice, judge, magistrate judge, bankruptcy judge, spouse or minor child, as the case may be, divests himself or herself of the interest that provides the grounds for the disqualification.

28 U.S.C. § 455(f). Therefore, the requirements for divestiture are met when "(i) the district judge devoted 'substantial judicial time' to the matter before 'appearance or discovery' of the conflict; (ii) his financial interest cannot be substantially affected by the outcome of the case; and (iii) he divested himself of the interest once he discovered it." Chase Manhattan Bank, 343 F.3d at 131. The Second Circuit has explained that this section "is meant to help judges strike a balance between the duty to recuse when their impartiality might reasonably be questioned and the need to resolve cases expeditiously and without undue collateral litigation." Muchnick v. Thomson Corp. (In re Literary Works in Elec. Databases Copyright Litig.), 509 F.3d 136, 142 (2d Cir. 2007). It is undisputed in this case that there is substantial judicial time invested. The Court had devoted months of time into this matter engaging in ruling of pre-trial motions, holding a Markman hearing, conducting an almost six-week bench trial and drafting extensive findings of fact and conclusions of law in a 150-plus page opinion.

Cisco argues that section 455(f) is unavailable under these circumstances because the Court has not and cannot promptly divest the stock at issue and the financial interest would be substantially affected by the outcome. See Doc. 557 at 5. The Court disagrees with Cisco on both grounds. Cisco avers divestiture is unavailable because "prompt" disclosure is required by section 455(f). A reading of the statute indicates no mention "as to the timing of the divestiture." Doc. 564 at 12. Centripetal avers Cisco's argument fails because the idea "that divesture is no longer available because the Court's spouse did not divest her shares within Cisco's arbitrary window of undefined 'promptness.'" Upon receipt of the Court's notification, Cisco did not request that the Court's wife immediately divest if she had not done so already. See Doc. 564 at 13 (Centripetal noting that "Cisco's argument that divestiture cannot happen because divestiture has not yet happened is simply wrong."

Additionally, Cisco notes that the interest held by the Court's spouse cannot fall under the divestiture provisions of section 455(f) because the interest would be substantially affected by the account where Centripetal has requested such a high amount of damages. The Court finds the case of Key Pharm., Inc. v. Mylan Laboratories Inc., 24 F. Supp. 2d 480, 483 (W.D. Pa. 1998) as persuasive on this issue. In that case, the judge found divesting 151 shares with a value of $10,185.18 "was an effective cure for the discovery of the interest, particularly where the investment had been in a 'large, publicly held corporation with diverse interests and revenues in the billions.'" Doc. 564 at 14 (quoting Key Pharm., Inc. v. Mylan Laboratories Inc., 24 F. Supp. 2d 480, 483 (W.D. Pa. 1998)). Here, the Court's spouse owned 100 shares of Cisco stock valued at $4,687.99. Cisco, similar to the company in Key Pharm is a large, publicly held corporation with billions in revenue. Therefore, the Court finds that divesture is appropriate under the circumstances. Cisco points to the previously discussed case of Chase Manhattan as an example

that divestiture is unavailable in this case. As noted supra, that case has substantially different facts. In Chase Manhattan, the "disqualifying circumstances here appeared in 1997, [as such] they cannot be cured by a divestiture in 2000, long after the district judge's conduct of the bench trial, findings of fact, and issuance of judgment." Chase Manhattan Bank, 343 F.3d at 132. A three-year gap between identification of conflicting ownership and divestiture is drastically different than the less than a month gap presented in this case.

In light of this guidance, the Court's spouse has proceeded to divest the Cisco shares into a blind trust. Divestment to a blind trust is the proper remedy as the Court finds that an outright sale of the stock would undermine the purpose of section 455. Generally, section 455 "is designed to promote public confidence in the impartiality of the judicial process . . . ." Muchnick v. Thomson Corp. (In re Literary Works in Elec. Databases Copyright Litig.), 509 F.3d 136, 140 (2d Cir. 2007) (citing H.R. Rep. No. 93-1453, reprinted in 1974 U.S.C.C.A.N. 6351, 6355). Section 455(f) was incorporated for exactly the type of situations where the Court discovers an interest after substantial time and resources have been devoted to the case. See Kidder, Peabody & Co. v. Maxus Energy Corp., 925 F.2d 556, 561 (2d Cir. 1991) ("We think that section 455(f) directly applies to this situation. Nearly three years of the litigants' time and resources and substantial judicial efforts have been devoted to the litigation.")

If the Court were to decide in Centripetal's favor then that decision may be seen to benefit the Court if his spouse's stock is sold. In arguments on liability and damages, the Court noted the enormous discrepancy in the damages amounts of the parties' respective damages experts and asked for further financial data. A reasonable attorney might conclude that the Court intended to award damages and apparently both sides did so.

Centripetal promptly waived any objection while Cisco filed a motion to recuse nine days later. Under the circumstances, the Court **FINDS** nine days to be a reasonable time within which Cisco may act.

The situation is somewhat of a reverse bias allegation as it is Cisco, in which the stock is owned, seeking recusal. Cisco's theory is that the Court would change its opinion to one less favorable to it in order to shore up its appearance of propriety. Such an allegation makes it difficult for the Court to consider the outright sale of this stock. During the interim period between notification of counsel regarding the stock and the issuance of this opinion, the Court has performed no further work on its draft opinion on the merits. An outright sale of the stock would be inappropriate as the Court may appear to benefit itself in order to comply with the provisions of 455(f). Accordingly, the Court's spouse has divested her shares of Cisco stock by placing them in a blind trust to remove control from the Court and his spouse. This solution intends to abide by the statutory purposes of impartiality required by section 455 as well as the timely divestiture required by 455(f).

III. CONCLUSION

In conclusion, the Court **DENIES** Cisco's Motion for Miscellaneous Relief. The Clerk is **REQUESTED** to distribute a copy of this Opinion and Order to counsel of record.

It is **SO ORDERED**.

/s/
Henry Coke Morgan, Jr.
Senior United States District Judge

Norfolk, Virginia
October 2, 2020

HENRY COKE MORGAN, JR.
SENIOR UNTIED STATES DISTRICT JUDGE

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Norfolk Division

CENTRIPETAL NETWORKS, INC.,	)	
	)	
Plaintiff,	)	
	)	
v.	)	**Civil Action No. 2:18cv94**
	)	
CISCO SYSTEMS, INC.,	)	
	)	
Defendant.	)	

OPINION AND ORDER

After hearing the evidence presented by the parties during the trial on this matter, and considering the entire trial record before this Court, the Court enters the following findings of fact and conclusions of law pursuant to Federal Rule of Civil Procedure 52(a). Any item marked as a finding of fact which may also be interpreted as a conclusion of law is hereby adopted as such. Any item marked as a conclusion of law which may also be interpreted as a finding of fact is hereby adopted as such.

I. PROCEDURAL POSTURE[1]

1. This patent trial concerns five United States patents involving complex issues in cybersecurity technology heard by the Court without a jury.

2. The case began when Centripetal Networks, Inc. ("Centripetal") filed a Complaint against Cisco Systems, Inc. ("Cisco") for infringement of a number of Centripetal's U.S. Patents on February 13, 2018. Doc. 1.

[1] All matters discussed in this Procedural Posture are procedural background and findings of fact.

3. On March 29, 2018, Centripetal filed an Amended Complaint, asserting infringement of U.S. Patent Nos. 9,566,077 ("the '077 Patent"), 9,413,722 ("the '722 Patent"), 9,160,713 ("the '713 Patent"), 9,124,552 ("the '552 Patent"), 9,565,213 ("the '213 Patent"), 9,674,148 ("the '148 Patent"), 9,686,193 ("the '193 Patent"), 9,203,806 ("the '806 Patent"), 9,137,205 ("the '205 Patent"), 9,917,856 ("the '856 Patent"), and 9,500,176 ("the '176 Patent"). Doc. 29.

4. Cisco has filed numerous petitions for inter partes review ("IPR"), between July 12, 2018 and September 18, 2018, before the Patent Trial and Appeals Board ("PTAB") against nine (9) of the eleven (11) Centripetal patents originally asserted against Cisco and filed a Motion to Stay Pending Resolution of IPR Proceedings. The Court granted the stay request on February 25, 2019. Doc. 58.

5. Upon the motion of Centripetal, on September 18, 2019, the Court issued an order, lifting the stay in part with respect to patents and claims not currently subject to IPR proceedings and set the case for trial in April 2020. Doc. 68. The parties later waived a jury trial following the jury trial limitations resulting from the COVID-19 pandemic.

6. At trial, Centripetal asserted that Cisco infringes Claims 63 and 77 of the '205 Patent, Claims 9 and 17 of the '806 Patent, Claims 11 and 21 of the '176 Patent, Claims 18 and 19 of the '193 Patent and Claims 24 and 25 of the '856 Patent (the 'Asserted Claims'). Doc. 411 ("Amended Final Pre-Trial Order").

7. Of the claims not at issue for trial, the PTAB granted institution of IPR of all of the claims of the '552 Patent, the '713 Patent, the '213 Patent, the '148 Patent, the '077 Patent, and the '722 Patent and granted institution of IPR of claims of the '205 Patent that are not the subject of this bench trial. Doc. 411.

8. The PTAB has, thus far, invalidated all of the claims of the '552 Patent, the '713 Patent, the '213 Patent, the '148 Patent, and the '077 Patent and invalidated the unasserted claims of the '205 Patent. Centripetal has appealed or may be appealing the PTAB decisions regarding the '552 Patent, the '713 Patent, the '213 Patent, the '148 Patent, the '077 Patent, and unasserted claims of the '205 Patent. Doc. 411.

II. WITNESSES AT TRIAL

9. During the twenty-two-day bench trial, and at a later hearing on damages evidence, both parties were given the opportunity to present their evidence live through a video platform approved by the Eastern District of Virginia after Court's staff was instructed in its operation. Cisco objected to proceeding through a video platform, and also objected to using the platform utilized in favor of its own platform. In its order of April 23, 2020, the Court overruled Cisco's objections for the reasons stated therein. In light of the use of the video platform, the parties implemented specific trial protocols that are detailed in Appendix B. See Appendix B; Doc. 411 (Amended Pre-Trial Order). At the conclusion of the 22nd day of trial, the parties joined in congratulating the Court's staff for their handling of the trial evidence by means of the video platform.

10. Due to the complex nature of the technology at issue in the case, the Court requested that each party present a technology tutorial on the first day of trial. The Court has compiled a list of the abbreviations used in the testimony and documents throughout the trial and attached it as Appendix A. For Centripetal, Dr. Nenad Medvidovic presented the technology tutorial and Dr. Kevin Almeroth presented the technology tutorial for Cisco.

11. Centripetal, in its case in chief, called a variety of live fact and expert witnesses including:

- Mr. Steven Rogers – Founder and CEO of Centripetal. Tr. 228:8;
- Dr. Sean Moore – Chief Technology Officer and Senior Vice President of Research at Centripetal. Tr. 301:24-25. Dr. Moore is an inventor on all of the asserted patents in this case. Tr. 314:25, 315:1-2;
- Dr. Michael Mitzenmacher – an independent expert witness in cybersecurity who presented opinion testimony that the accused products infringe the '193 Patent, the '806 Patent and the '205 Patent. Tr. 431:16-23;
- Dr. Eric Cole – an independent expert witness in cybersecurity who presented opinion testimony that the accused products infringe the '856 Patent and the '176 Patent. Tr. 886:9-11, 975:19-21;
- Dr. Nenad Medvidovic – an independent expert witness in cybersecurity who opined about the importance of the patent technology in relation to the accused products. Tr. 1144:22-25, 1145:1-2;
- Mr. Jonathan Rogers – Chief Operating Officer at Centripetal. Tr. 1194:11;
- Mr. Christopher Gibbs - Senior Vice President of Sales at Centripetal. Tr. 1297:1-2;
- Dr. Aaron Striegel – an independent expert witness in computer networking who opined regarding apportionment and the top-level infringing functions of the accused products. Tr. 1337:19-23;
- Mr. Lance Gunderson – an independent expert witness in patent damages who opined regarding damages and a reasonable royalty. Tr. 1441:2-14;
- Mr. James Malackowski – an independent expert witness in business, intellectual property valuation and patent licensing who opined regarding

the impact of the asserted infringement on Centripetal and damages going forward. Tr. 1573:14-19.

12. Centripetal, additionally, presented testimony from Cisco employees by video deposition including:

- Mr. Saravanan Radhakrishnan;
- Mr. Rajagopal Venkatraman;
- Dr. David McGrew;
- Mr. Sunil Amin;
- Mr. Sandeep Agrawal.

13. Cisco, in its case in chief, called a variety of live fact and expert witnesses including:

- Mr. Michael Scheck – Senior Director of Incident Command at Cisco. Tr. 165:23-24;
- Dr. David McGrew – Cisco Fellow who was responsible for leading a research and development project at Cisco that became the Encrypted Traffic Analytics solution. Tr. 1759:10-12;
- Dr. Douglas Schmidt – an independent expert witness in networking and network security who opined regarding non-infringement, invalidity, and damages of the ‘856 Patent. Tr. 1813:4;
- Mr. Daniel Llewallyn – Software Engineer for Cisco who previously worked at Lancope. Tr. 2141:19;

- Dr. Kevin Almeroth – an independent expert witness in computer networks and network security who opined regarding non-infringement, invalidity and damages of the '176 Patent. Tr. 2212:12-18;
- Dr. Mark Crovella – an independent expert witness in networking and network security who opined regarding non-infringement, invalidity and damages of the '193 Patent. Tr. 2349:18-24;
- Mr. Hari Shankar – Principal Engineer and Software Architect at Cisco who is responsible for the design of certain features of the accused products. Tr. 2500:3-5;
- Mr. Peter Jones – Distinguished Engineer in the Enterprise Network Hardware Group at Cisco. Tr. 2543:12-17;
- Dr. Narasimha Reddy – an independent expert witness in computer networking and computer security who opined regarding non-infringement, invalidity and damages of the '806 Patent. Tr. 2580:6-10;
- Mr. Matt Watchinski – a Cisco employee responsible for Cisco's Talos organization, which is Cisco's threat intelligence organization. Mr. Watchinski previously worked for Sourcefire. Tr. 2682:11-13;
- Dr. Kevin Jeffay – an independent expert witness in computer networks and network security who opined regarding non-infringement and damages of the '205 Patent. Tr. 2727:11-19;
- Mr. Timothy Keanini – Distinguished Engineer at Cisco involved with the Stealthwatch product line. Tr. 2810:4-6;

- Mr. Karthik Subramanian – Partner at a venture capital firm called Evolution Equity Partners. Mr. Subramanian previously led Cisco's Corporate Development Team for Cybersecurity for about four to four and a half years. Tr. 2827:23, 2828:17-18;
- Dr. Stephen Becker – an independent expert witness in economic damages analysis who opined regarding damages if the Court finds the Asserted Patents are infringed and valid. Tr. 2863:3-18.

14. Cisco, additionally, presented testimony from current and former Centripetal employees by video deposition including:

- Mr. Douglas DiSabello;
- Mr. Haig Colter;
- Dr. Sean Moore;
- Mr. Jess Parnell;
- Mr. Justin Rogers;
- Mr. Christopher Gibbs;
- Mr. Gregory Akers.

15. Centripetal, in its rebuttal validity case, called live expert witnesses:

- Dr. Alexander Orso – an independent expert witness in computer networking and security who opined regarding the validity of the '193 Patent and the '806 Patent. Tr. 2989:22-25;
- Dr. Trent Jaeger – an independent expert witness in computer and network security who opined regarding the validity of the '856 Patent and the '176 Patent. Tr. 3102:18-23;

- Dr. Aaron Striegel – an independent expert witness in computer networking who opined regarding secondary considerations of non-obviousness for the Asserted Patents. Tr. 3196:16-18.

16. Having had the opportunity to observe the demeanor and hear the live testimony of witnesses by video / audio and by deposition at trial, the Court has made certain credibility determinations, as well as determinations relating to the appropriate weight to accord the testimony. Such determinations are set forth herein where relevant.

III. TECHNOLOGY TUTORIAL

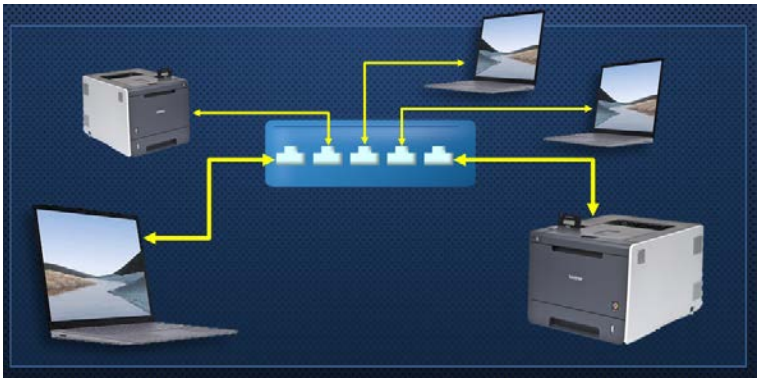
A. NETWORKING AND CYBERSECURITY TUTORIAL

The asserted patents in this case deal with systems that engage in complex computer networking security functions. Accordingly, the Court heard detailed technological testimony regarding the structure and function of computer networks in general, as well as the specific processes employed to secure these networks. The Court begins its factual findings by reciting a review of the presented technology tutorial.

i. Overview of Networking

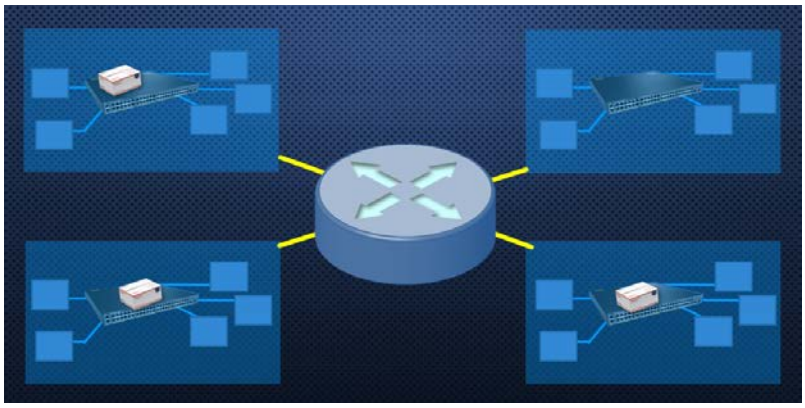
The three principal devices that comprise computer networks are switches, routers and firewalls. Tr. 20:5-10. Beginning with switches, Centripetal's expert Dr. Medvidovic used analogies to explain these complex network devices. He compared the operation of a switch to that of a telephone switchboard operator. Tr. 20:13-22. Therefore, similar to an operator connecting people, switches in a network operate to automatically connect different devices together such as a computer with another computer or a computer to a printer. Tr. 20:24-21:2; see Fig. 1.

FIG. 1



Comparatively, routers function similarly to a 911 dispatcher who sends and controls the distribution of emergency vehicles to the intended location. Tr. 22:9-19. Routers decide the most optimal way to automatically send computing data to a desired location. Tr. 22:24-23:2. They are constantly evaluating current computer traffic and sending data along the most efficient path to its intended destination. Tr. 23:8-14. The combination of routers and switches are the fundamental building blocks of computer networks. Tr. 23:17-23. Together, switches connect local devices into small networks and routers operate to transmit data between these smaller networks – thus forming larger networks. Tr. 26:1-4; see Fig. 2.

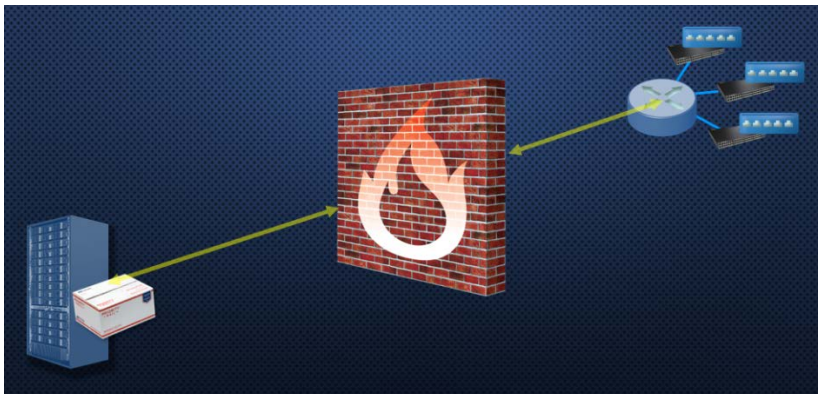
FIG. 2



The next and final relevant device in computer networks is the firewall. Firewalls, in the context of computer networking, are similar to that of a firewall in an office building or hotel. Tr.

24:13-19. They operate to automatically put a "wall" between valuable assets and any potential danger. Tr. 24:13-19. Therefore, data entering a network is often transmitted in through a firewall and the firewall can perform a variety of functions, such as disallowing the data to enter the network by blocking it. Tr. 25:1-4; see Fig. 3.

FIG. 3



Dr. Medvidovic used video access to ESPN.com from a web server as an example of the operation of a firewall. He explained that:

> any data you try to see or retrieve from the ESPN servers would be on that web server. And that data would travel to you, but before it gets to your computer, it would first go through this firewall, and the firewall may decide to permit that data to go through because it does not violate any policies or rules that you may have for the firewall. . . . So for example, it [the firewall] could be in a company where the company policy is you can't watch sports during work hours. So in that case, that data from ESPN would be dropped at the firewall and never arrive to you.

Tr. 25:8-20. Accordingly, firewalls often sit at the edge of individual networks to control the entry of data from the internet. Tr. 26:1-12. As technology develops, firewall type functionality is often now included inside of other devices such as routers and switches. These devices may be located at different locations within a network – not just at the outside barrier. Tr. 82:8-18. This inclusion of firewall functionality in other devices is in contrast with older network technology where firewalls were responsible for the security of the network, by blocking malicious packets from

entering it, while the routers and switches focused on speed and performance in the transmitting data. Tr. 26:16-22.

The combination of thousands of these networking devices into larger and larger networks is responsible for the creation of nationwide networks and the global internet. Tr. 23:24-25, 24:1-3. Therefore, the global internet as we know it is a network of networks. Tr. 74:1-12. Internet providers, such as Earthlink, Verizon, AT&T, and Cox are in the business of creating large scale networks to connect users to other business networks in order to access data. Tr. 74:1-12, 76:10-19. Companies like Netflix, Facebook, Zoom, Google and Amazon operate their own independent networks that connect to the larger internet to send data across the internet to end-users. Tr. 75:23-76:9; see Fig. 4.

FIG. 4



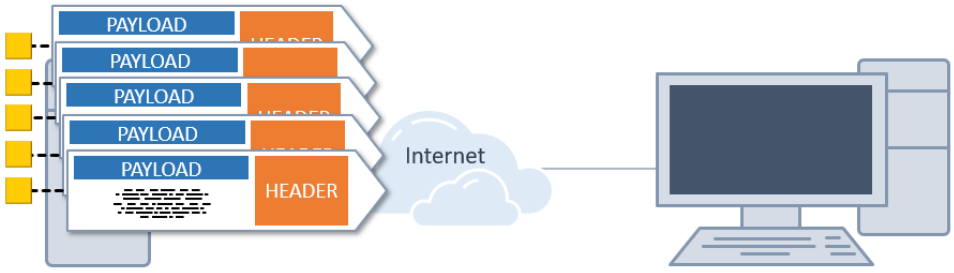
The international nature of the internet requires that the sending of data between all of these providers be based on uniformly developed standards that are globally applicable. Tr. 77:5-17. One such organization, the Internet Engineering Task Force ("IETF") is responsible for developing universal internet related standards. Tr. 77:5-17. There are many different standards that are developed to facilitate the transmission of data over the internet. Tr. 77:5-17. These standards are often in the form of protocols. Protocols are the rules of engagement for two computers that specify

how the two computers can work together to communicate back and forth. Tr. 954:5-17. For example, the Hypertext Transfer Protocol ("HTTP") is used in web pages to transfer data over the internet from computer to computer, the Internet Protocol ("IP") is a building block in allowing data to use interconnected networks, and the Transmission Control Protocol ("TCP") is used to deliver information across the internet. Tr. 77:23-78:2, 89:18-21. These protocols are the methods by which data transfer is possible over nationwide and global networks. Tr. 88:19-21. This is a general "high level" overview of these networking concepts. Internet professionals and "experts" use the term "high level" to categorize these basic concepts involved in the transmission of data electronically, as well as the imposition of security upon such transmissions.

Moving into the specifics, the transmission of computing data through these devices is done in the form of a network packet or packets. Tr. 26:23-25. The packet is similar to that of a package sent through the United States Postal Service. Tr. 26:24-27:3, 89:2-3. For example, when a user on their computer attempts to watch a video from ESPN.com, that video is a very large amount of information and cannot efficiently be sent in one package. It is, therefore, broken up into a number of smaller units known as packets. Tr. 27:3-14. The packet will flow from the internet and through multiple devices on the network and transmit the requested information to the end user. Tr. 88:1-14. At any time, there are trillions of packets being exchanged through global networks. Tr. 88:16-19.

Packets consist of two different parts: the header and the payload; see Fig. 5.

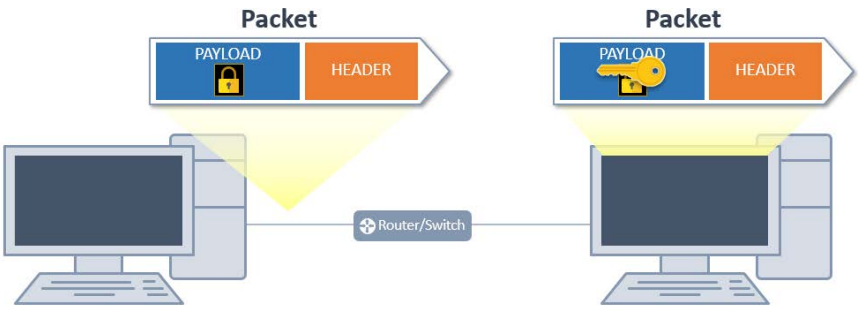
FIG. 5



The header contains information such as the source address, source port, destination address, destination port number, and the protocol being used to transmit the packets. Tr. 107:16-23. These five pieces of information are known as the "5-tuple." Tr. 108:4. The information contained in the header is inspected by the router or switch to determine where and how to send that individual packet. Tr. 108:7-16. This information can be thought of as a mailing label on a package which contains an individual's name and mailing address as well as a return address. Tr. 27:24-25. The payload is the portion of the packet that contains the actual content of the data. This information is similar to the content within a postal package, such as a new football or baseball glove. In the ESPN video hypothetical, this would be the actual portion of the video sent by each individual packet. Tr. 28:4-10. This data in the payload part of the packet can be encrypted, meaning the information in the payload can be transmitted in code. Tr. 28:18-25. For example, the hypothetical video from ESPN.com would not usually be encrypted, but often data sent in a packet's payload containing sensitive information, such as banking or credit card data, will be encrypted. Encryption becomes vital so that this sensitive data is not stolen by bad actors hacking the network. Tr. 28:18-25. Encryption works to lock up the data in the payload section of the packet so it cannot be seen

without decryption. Tr. 29:1-5. Consequently, just as with a sealed package, snoopers of network traffic would be unable to see what is in the packet unless it could be unlocked and opened, which is generally known as decrypting the data. But, even when a packet is encrypted, the header information, such as the source and destination, is not encrypted and is visible. Tr. 29:10-16; see Fig. 6.

FIG. 6



As previously noted, the hypothetical ESPN video is set in a collection of packets that comprise the video. The collection of all the packets together that make up the transmitted video is known as a packet flow. Tr. 106:15-16. Thus, the header of each packet in this particular flow would contain identifying information that distinguishes this collection of packets from other flows. Tr. 107:16-13. This allows for routers to keep the packets in order and properly distribute the packets to the correct destination.

ii. Overview of Networking Security

As explained supra, the internet is a very large and complex organization of networks that utilize protocols to relay data from one network device to another resulting in the transmission of data to an end user. Tr. 112:1-6. As a result of the internet's complexity, there are many methods employed by cyber criminals to transmit malware and gain access to encrypted, secure and confidential information. Tr. 112:7-14. Cyber criminals can use malware or other methods to infect

a network and steal data using a process known as exfiltration. Tr. 343:19-15. Exfiltration is the process by which cyber criminals "exfiltrate" data out of a network by stealing valuable confidential data. Tr. 343:19-15.[2] Therefore, to prevent malware and data exfiltration, cyber defense systems often use a concept known as defense-in-depth, the deployment of a variety of network security devices at different layers of the network, to protect sensitive network data. Cisco's expert, Dr. Almeroth, compared network defense-in-depth to that of the security used by a federal courthouse, which contains a series of secured entry points to the building, a courtroom or a judge's chambers. Tr. 112:18-22. Consequently, just like any type of modern security system, there must be different layers of security in a network to be effective in preventing evolving methods of cyberattacks. Tr. 113:3-10, 51:17-21. Therefore, to maximize effectiveness, security measures are often placed at different devices/locations in a network, such as within a firewall, a security gateway, in routers and switches, and also within the end user's computer. Tr. 113:11-18. Dr. Almeroth outlined that there are multiple approaches used by cybersecurity professionals to effectively develop defense-in-depth security systems. Tr. 117:22-24. Two of the relevant approaches, for purposes of this trial, are known as detect and block through "inline" analysis and "out-of-band" also known as allow and detect. Tr. 118:2-7. These approaches can be used unilaterally or combined to create different styles of network security based on the needs of network administrators.

Older security technology focused on a firewall at the border of the network to detect and block malicious packets from entering a network. Tr. 118:8-119:25. The process begins when a packet is sent from the internet to another smaller network. A firewall device, usually located at the entry of the network, operates by inspecting information in the packet to determine if that

[2] Typically, this sensitive data often consists of usernames and passwords to your bank accounts, Social Security Numbers, credit card numbers, or confidential financial data of a business. Tr. 444:4-8.

packet is malicious. Tr. 119:18-25. This process is completed by matching information from the header or payload of the packet to rules that are pre-enabled in the firewall type device. Tr. 119:18-25. These rules are comprised of previously known information about sources of malicious or otherwise unauthorized traffic. Tr. 122:11. Thus, if information from a packet header is matched to a rule, then the packet is unauthorized to enter the network and is blocked / dropped.[3] Tr. 120:6-12. A blocked packet is virtually thrown away or could be re-routed to another location for additional inspection. Tr. 120:15-18. If there is no rule that matches the packet, the packet is allowed to proceed into the network and to its final destination. Tr. 120:2-5.

Rules are the mechanism that determines which packets are allowed in and out of the network. The collection of rules that are being applied by network devices can also be referred to as Access Control Lists ("ACLs"). Tr. 537:18-21, 2550 1-4. Threats are continually evolving, and as a result, rules can be automatically updated or swapped in switches, routers and firewalls by other management devices in the network that intake "threat intelligence" information. Tr. 126:5-11. Threat intelligence information is an everchanging collection of information from known viruses and malware that is compiled by third-party providers. Tr. 126:5-11. Devices that manage switches, routers and firewalls often operate by digesting threat intelligence, converting that intelligence into rules, and sending those rules out to intra-network devices such as firewalls, routers and switches that match rules to packets. Tr. 126:5-11. The ability to apply measures in real-time to new or different rules after the packet has cleared the gatekeeping firewall is called proactive security, which is a newer and more effective technology.

This process of proactively blocking packets as they travel through the network comes with distinct challenges. The efficacy of this method rests on the ability of network devices to

[3] Dropping and blocking can be used interchangeably as they have the same definition in the context of cybersecurity. Tr. 466:23-467:4

continually apply new or different rules to packets. Therefore, as the volume of packets and rules increase, so must the number of devices or the processing speed of current devices to remain effective. Tr. 124:6-19. Without increased speed or adding hardware, there will be extensive delay/latency because the system will be overwhelmed trying to match new or different rules to an overwhelming number of packets. Consequently, this delay can affect user performance on the network (i.e., increase web page loading times). Tr. 126:20-24. Another issue is that a network might have different entry points or destination points for data. Tr. 127:5-8. Therefore, firewall capable devices must be placed at all possible entry and destination points or risk that data could reach an improper destination without the application of updated rules. Tr. 127:5-8.

The older allow and detect model operates retroactively by monitoring the entry of packets into the network based upon prior threats to the network. Tr. 129:2-11. The flows are monitored by sensors in network devices and sent to another management device for review. Tr. 132:13-19. When malicious traffic is found, the devices can operate retrospectively, and update rules based upon information found in the forensic investigation. Tr. 133:2. Instead of blocking traffic at the gate, this method allows traffic to go through to its destination and then performs post facto analysis on the flow of the information in the packet headers to determine if there was malicious activity afoot. Tr. 133:24-134:2. The challenges of this model include the lack of the ability to be proactive. It is different than an inline intrusion prevention system because malicious packets are still allowed into the network and then passed on to the destination without blocking. Tr. 141:11-14.

Both approaches may be combined in different ways to create a defense-in-depth strategy. Tr. 144:5-11. Network administrators can use different combinations of these devices and methods to achieve optimal security personalized for their network. Tr. 144:5-11.

B. OVERVIEW OF THE ACCUSED PRODUCTS

In this case, Centripetal accuses various Cisco network devices of using its new solutions and infringing the Asserted Patents. The Court will provide a brief summary of these products.

i. Cisco's Switches

The switches at issue in the case are the Catalyst 9000 series ("Catalyst Switches") including the Catalyst 9300, 9400 and 9500. Tr. 53:20-23. This newer line of switches contains functionality utilized by Cisco to integrate proactive security capabilities within the network. Tr. 54:1-3.

ii. Cisco's Routers

There are three different types of routers at issue. These routers are the 1000 series Aggregation Services Router ("ASR") and the 1000 / 4000 series Integrated Services Router ("ISR"). Tr. 54:22-25, 55:1-2. Their purpose in the network is to provide performance, reliability, and integrate proactive security functionality within networks. Tr. 55:7-10. Like the switches, the routers contain functionality utilized by Cisco to integrate proactive security capabilities within the network.

iii. Cisco's Digital Network Architecture

Cisco's Digital Network Architecture ("DNA") operates as a network management device. Tr. 55:17-21. It operates to configure and troubleshoot problems in the network. Tr. 55:17-21. Therefore, the primary function is to interact and operate routers and switches. Tr. 55:17-21, 147:19-21. DNA may continually provision the routers and switches so they are capable of being used effectively in the operation of the network. Tr. 56:1-7. The DNA device uses advanced artificial intelligence and machine learning to observe past traffic on the network and has the

capability to change configuration in the network in real time. Tr. 57:20-25. Accordingly, DNA takes that intelligence, operationalizes it, and turns it into rules and policies that Cisco's switches and routers use for security purposes. Tr. 451:3-24.

iv. Cisco's Stealthwatch

The new and improved Stealthwatch device currently provides the ability to collect various security analytics and use it to predict network threats. Tr. 59:1-7. Stealthwatch is, now, enabled to work with other Cisco technologies, such as Cognitive Threat Analytics ("CTA") and Encrypted Traffic Analytics ("ETA"). Tr. 59:10-15.

v. Cognitive Threat Analytics

Cognitive Threat Analytics ("CTA") has various features for monitoring the network. For example, CTA monitors for security breaches within the network by using machine learning. Tr. 60:17-23. CTA is embedded in the Stealthwatch device. Tr. 60:21-23

vi. Identity Services Engine

The Identity Services Engine ("ISE") is a device that ensures user control over the network from any location. Tr. 61:10-16. It provides network-based security regardless of location of the user. Tr. 61:10-16. It is also responsible for tracking the identity of users and user computers on a network and for setting the limits of user and user computer access to other devices in the network. Tr. 149:20-23.

vii. Encrypted Traffic Analytics

Encrypted Traffic Analytics ("ETA") is an element of the new Stealthwatch technology and also is embedded in Cisco's switches and routers. Tr. 61:17-24. ETA deals with the ability to track and analyze encrypted traffic in the network without decrypting said traffic. Tr. 61:19-21.

ETA completes this objective by looking at non-encrypted information in the packet (i.e., header information, 5-tuple) in order to track and analyze particular packet flows. Tr. 62:1-5.

viii. Cisco's Firewalls

There are five different firewall products at issue. Tr. 63:10-17. First, there is the Adaptive Security Appliance ("ASA") with Firepower. Tr. 63:10-17. Then, there are the four series of firewalls: the 1000; 2100; 4100; and the 9300. Tr. 63:10-17. These devices are newly equipped to operate proactively with packet filtering functionality. Tr. 151:23-25.

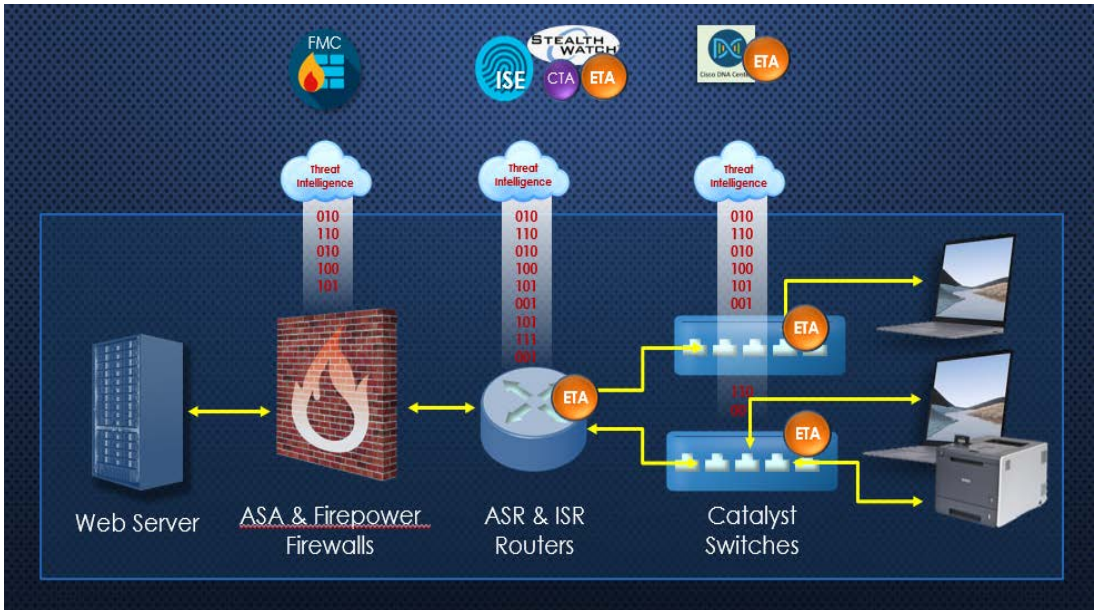
ix. Firepower Management Center

The Firepower Management Center ("FMC") operates the firewalls and does typical firewall functions like managing the network at that particular point in the network, protecting against malware, and checking and proactively blocking attempts at malicious intrusions into the network. Tr. 64:7-10. The FMC, in particular, can configure and operate all the firewall devices in the network. Tr. 153:6-8.

x. Complete Picture of a Cisco Network

To put all the devices and components together, Figure 7 depicts a Cisco network that utilizes all of the Accused Products:

FIG. 7 (FROM CENTRIPETAL'S TECHNOLOGY TUTORIAL SLIDES)



C. THE PARTIES

Centripetal is a corporation duly organized in 2009 and existing under the laws of the State of Delaware, with its principal place of business in Herndon, Virginia. Doc. 411 at 1; Tr. 233:22. Centripetal formed as a start-up cybersecurity company focused on using threat intelligence software and firewall hardware to protect cyber networks. Tr. 235:23-25. Centripetal operated to solve the conventional cybersecurity problems in an ever changing and developing industry using both inline and out-of-band methods. Tr. 239:6-15; see PTX-1591; DTX 1270.

Cisco is a California corporation with its principal place of business in San Jose, California. Doc. 411. Cisco was founded in 1984 as a hardware networking company. Cisco has dealt in network devices throughout its operation, selling hardware including routers, switches, firewalls and other technologies. Cisco represents itself as the largest provider of network infrastructure and services in the world. PTX-570 at 991. More recently, Cisco has started conducting market

research and has acquired technology start-up companies specialized in software advancements to incorporate security functionality into its hardware.

IV. OVERVIEW OF THE EVIDENCE

As the technology at issue involves important cybersecurity technology, the Court endeavored to accommodate Centripetal's motion for an early trial date. The many requests for inter partes review, by necessity, delayed the trial. The Court, therefore, scheduled a trial on those asserted patent claims for which such review had not been requested, as well as those which had survived this review process. Both parties' technologies are not only at the forefront in protecting intellectual property and confidential personal information, but also operate in the national defense context. With the rapidly developing technology in the field, the Court found it would not be in the public interest to delay the trial until the unknown time when courtrooms would open for traditional civil trials. Accordingly, the Court first scheduled the trial in April of 2020, then due to the restrictions imposed by the COVID-19 pandemic, finally scheduled it for May 8, 2020, to be heard on a court approved video platform. See Doc. 74; 328.

Following the tutorial, the initial phase of the trial dealt with Centripetal's allegations of infringement of ten patent claims, two of which were contained in each of five different patents. However, the two claims at issue in each patent were identical, save for their being designed for different forms of hardware or media utilization. Therefore, the Court dealt with the issues of infringement, validity and damages as to five sets of claim elements.

In the presentation of its infringement case, Centripetal called its top-level employees in person, Cisco employees by video deposition, and two expert witnesses. Centripetal presented numerous Cisco technical documents and other Cisco publications which postdated the alleged initial infringement date of June 20, 2017. Cisco's own documents from this time frame, and the

evidence in general, strongly supported Centripetal's infringement case as to four of the five asserted patents. Therefore, the Court **FINDS** that the '856 Patent, the '176 Patent, the '193 Patent, and the '806 Patent are valid and directly infringed. Cisco abandoned its claim that the '205 Patent was invalid, but argues that it was not infringed and the Court agrees and so **FINDS**.

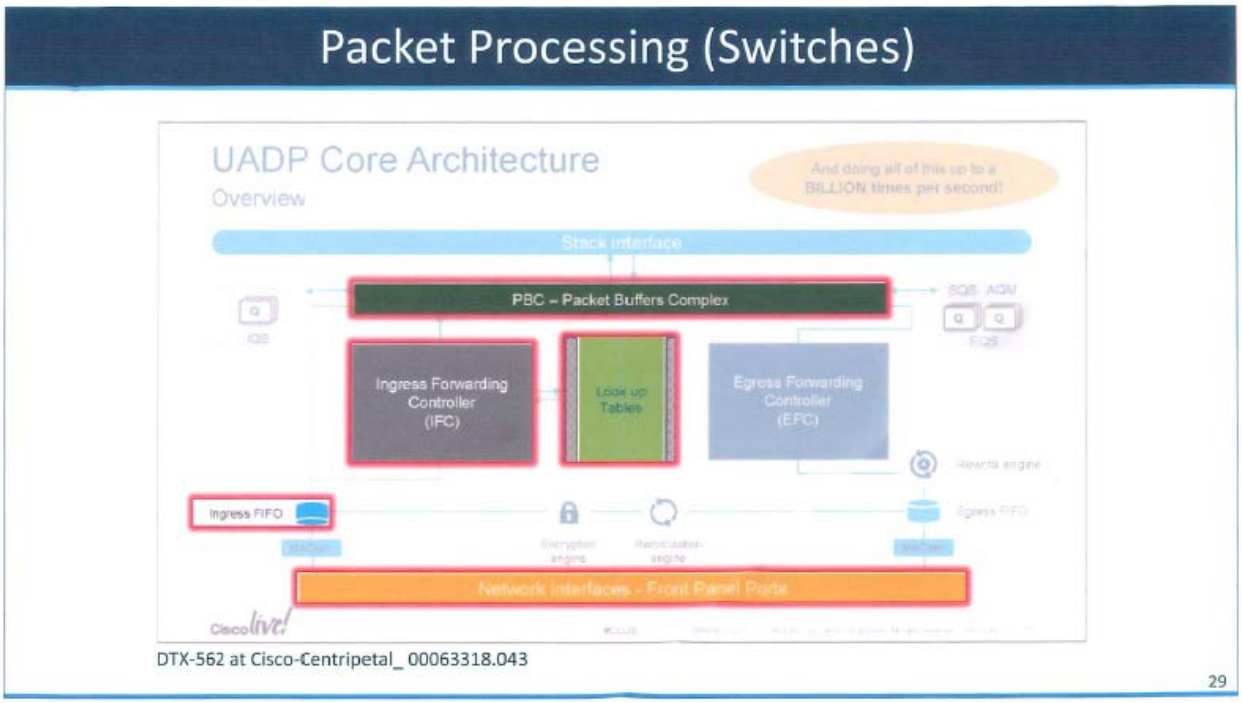
With regard to the infringement and validity claims, Cisco presented different independent experts witness as to each of the four. All four testified that based upon the infringement theories of Centripetal's experts, there was no infringement, but if the Court found infringement, that the asserted patents were invalid. Each of them also testified that the prosecution history of the patents precluded the application of the doctrine of equivalents. They also testified that if the patents were found infringing and valid, each of the four had minimal value. The alleged date of the first infringement was June 20, 2017, but virtually all of Cisco's exhibits, technical documents and demonstratives presented in its infringement and invalidity defense focused on its old technology, not on the current accused products. Their demonstratives of the functionality of Cisco's accused products were not based upon their own current technical documents, but rather upon inaccurate animations produced post facto for use in the litigation which served to confuse the issues, rather than inform the Court. By contrast, Centripetal utilized Cisco's own technical documents as exhibits and demonstratives to illustrate the functionality of Cisco's post June 20, 2017 technology and how it infringed the asserted claims.

Moreover, Cisco's experts also testified that Cisco's products did not infringe any of the claims of any of the patents at issue, while focusing on distinct elements of the claims. The testimony of these experts on infringement and validity all focused on old Cisco technology, as did most of the testimony of Cisco's employee witnesses. Cisco's lockstep strategy of denying any infringement of any of the elements of the four claims where infringement is found, and

backstopping this position by contending that if the Court found infringement the patents were ipso facto invalid, led to a number of factual conflicts in its presentation of its evidence.

Cisco's retained expert witnesses often contradicted Cisco's own documents as well as Cisco's own engineers. This common thread weaved a very tangled web, as is illustrated by Dr. Reddy, Cisco's expert on the '806 Patent. Dr. Reddy, in referring to slide 29 of his presentation, opined:

SLIDE 29 OF DR. REDDY'S PRESENTATION



> Q. And, Dr. Reddy, I would like to turn to an exhibit that the Court just saw with Mr. Jones. And I think Mr. Jones provided a pretty good explanation of this exhibit, but if you could just focus on what we've highlighted in red and explain to the Court why that will be relevant to your opinions.
>
> A. Okay. So the highlighted box at the bottom that says, "network interfaces," that's the box to which packets come into the switch, router, or the firewall. And in this example we're only talking about the switch here. And the packet, as it comes through the network interface, goes through the ingress FIFO, FIFO center, first-in-first-out, and from there the packet is moved into the packet buffers complex, on the top, and the header of the packet is given to the ingress forwarding controller, and the ingress forwarding controller consults the lookup tables, compares the packet header information, and makes decision about this

packet; whether to allow this packet to go forward or to drop the packet or to take any other action at the level of the lookup table.

Q. And just to be clear, what is the lookup table?

A. This is the product that has the information related to the ACLs, Access Control Lists.

Q. Now, Dr. Reddy, have you prepared an animation that shows how the Cisco systems that are being accused process packets that is basically using the diagram we just discussed?

A. Yes, I have.

Q. Okay. So let's turn to that, and if you could explain to the Court what this diagram is showing.

A. Okay.

THE COURT: Can you explain it on the prior slide?

THE WITNESS: Yes, Your Honor.

MR. JAMESON: This one here, Your Honor?

THE COURT: Yes. This is the one that Mr. Jones explained it on, so why not use the same one.

MR. JAMESON: He is using the same one. This is an animation, Your Honor, that he has created to try to provide an easier explanation as to what's happening in the accused products, using the component parts that are shown here.

THE COURT: All right. Go on.

BY MR. JAMESON:

Q. Explain what you're showing here, Dr. Reddy.

THE COURT: Well, that's a whole different setup. That doesn't help me any.

MR. JAMESON: Okay.

BY MR. JAMESON:
Q. Dr. Reddy, if you can walk through the steps of the ordinary course of processing packets, even when a rule swap is not being implemented in the accused products, using diagram 29.

A. Okay, will do. So what is -- the box that is highlighted here, the packet enters the switch through the network interface – that's the yellow/orange box at the bottom -- and the packet is moved from there to ingress FIFO, first-in-first-out, and the packet from there is copied into the packet buffers complex, which is at the top, which is in green. The header of the packet is copied to the ingress forwarding controller to make decision on what to do with this packet. Now, the ingress forwarding controller looks up the ACL rules, the Access Control List rules in the lookup table, and makes decision about this packet, whether packet should be allowed, denied, or whatever other action we need to take. And what I'm going to show, in order to simplify this process, in the next slide as I show the animation, I'm going to start with ingress FIFO and show the packet buffers complex, show the ingress forwarding controller and the lookup table, so those four boxes as we move forward, of the packets.

Q. Dr. Reddy, using slide 29, does every packet that comes into the Cisco accused products go through this process?

A. The process that I just described is exactly the same for every packet that comes through the switch.

Q. So with respect to the packet buffer, does every packet go into the packet buffer as part of processing?

A. That's correct. Every packet is copied there, and the header is inspected by the ingress forwarding controller to make a decision about that packet.

Q. And does the packet go into that packet buffer whether a rule swap is taking place or not?

A. That's correct. So every packet -- for every step of the way, every packet that comes in through the switch, no matter what's going on, is moved into the packet buffer.

Q. Okay. Now, using slide 29, what happens when a new rule set has been downloaded and Cisco wants to swap rule sets?

A. While the new rule set is being configured, the switch continues processing with the old rule set. So while the new rule set is being configured, the process -- the Cisco switches will continue using the old rule set and continue processing, contrary to what '806 teaches, and this is exactly what's in the background of the '806 patent. It's a continuous processing of the old rule set.

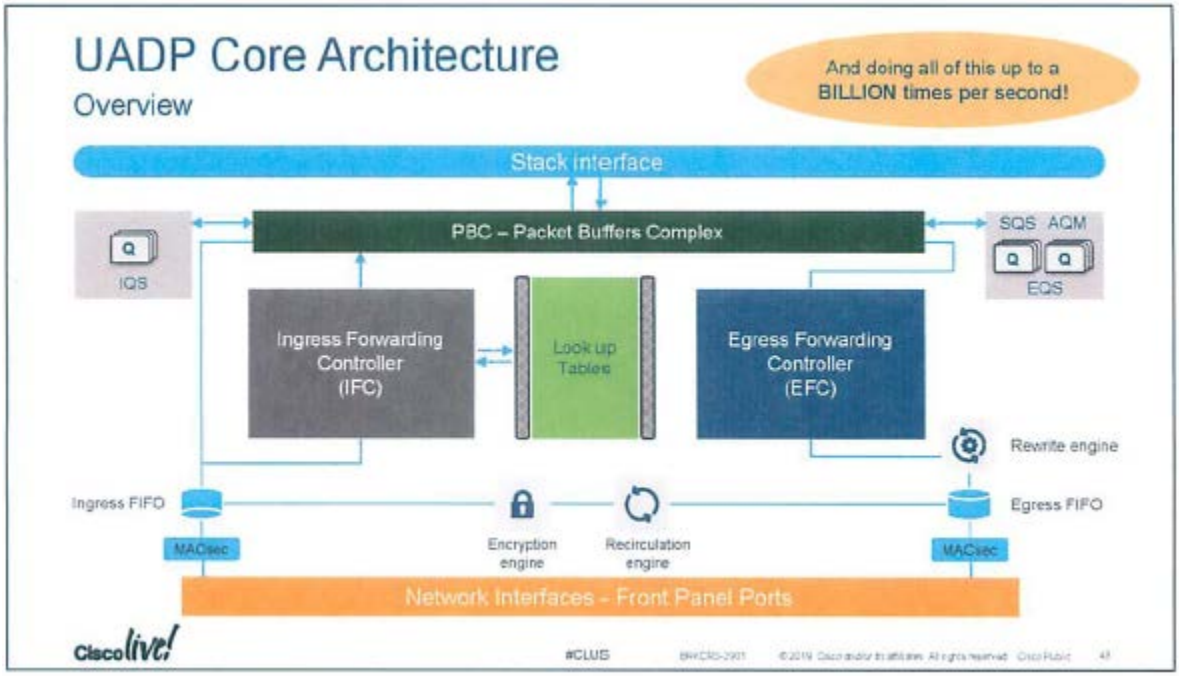
Q. And while the accused system is continuing to process packets with the old rule set, are packets moved into a cache?

A. No, there is no notion of a cache here. Every packet is taking the same sort of steps. Whether the rule set is being swapped or during the normal course of action, the packets

> come though the network interface, into the ingress FIFO. From there, the packets are moved to the packet buffers complex, and there's no notion of a cache here.
>
> Q. Okay. And what happens when the new rule set, rule set 2, has been configured and it's ready for use?
>
> A. At that point, we continue processing the packets as in the normal course of action, and the only difference is that when the packet is now being processed against the rule set, the pointer that was pointing to the old rule set now points to the new rule set, and the packet will be processed for the ingress forwarding controller during the normal course, and now, instead of using the old rule set, it starts using the new rule set.

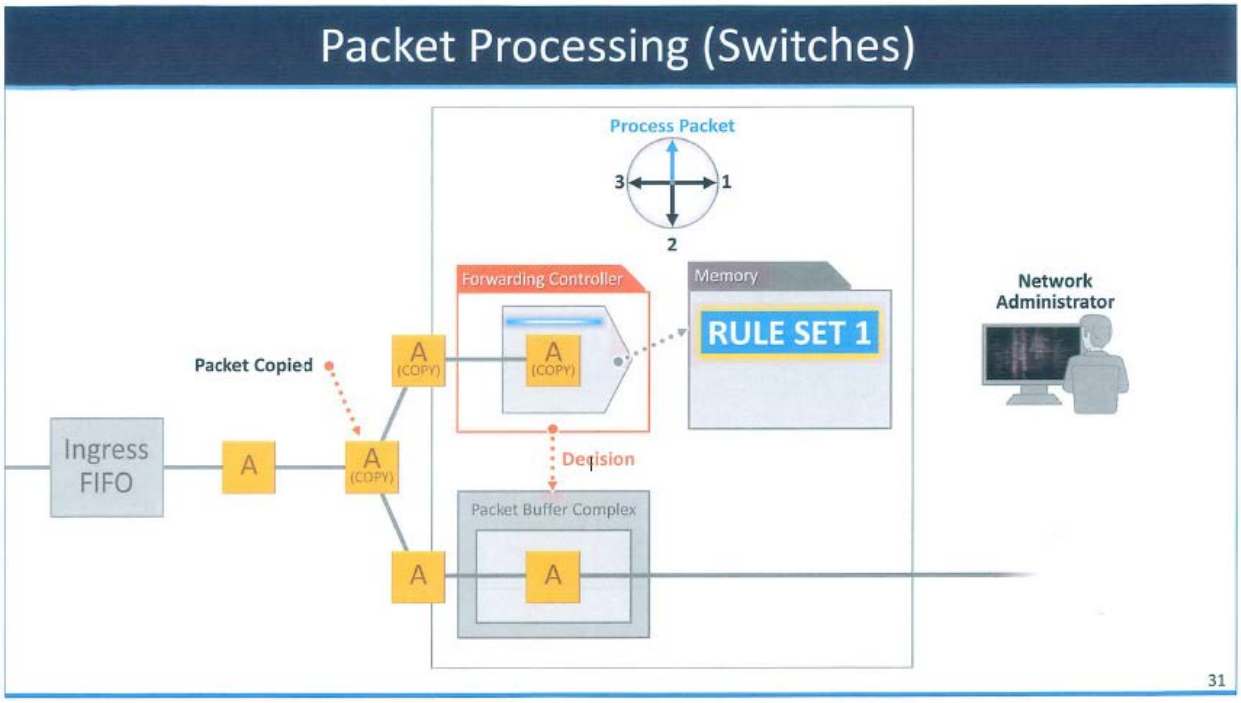
Tr. 2615:2-2619:13. Slide 29 is a representation of a Cisco technical document described by Dr. Jones, DTX-562. The animated slide 29 includes ex post facto red highlighting that limits the operation of transmitting packets to only the ingress and completely ignores egress. Cisco's noninfringement argument was based upon the packets being subjected to rules only one time and at only one step in the process. Therefore, Dr. Reddy opined on only the application of rules on the ingress half of packet processing performed by the switches and routers. In contrast, Mr. Jones specifically noted that rules are applied on both ingress and egress in describing the processing of packets by using strictly the Cisco technical document in an unaltered form. A more detailed explanation of all these issues in contained in the findings of fact and conclusions of law with respect to the '806 Patent. Here is Cisco's technical diagram used by Mr. Jones in his testimony:

DTX-562



In this diagram, there is a full picture of a packet's process through a switch or router without any highlighting limitation only on ingress. Therefore, Mr. Jones provided a complete picture of how rules are applied within the accused products on both ingress and egress. To support his opinions, Mr. Jones used Cisco's own technical documents where Dr. Reddy used an animation prepared for litigation in addition to his own modified version of the technical documents. Tr. 2614-2616. In addition to using a highlighted version of the technical document, Dr. Reddy, in his testimony, ignored Mr. Jones's egress explanation of the technical document itself, and attempted to explain the product's functionality by using his own created animation on slide 31:

SLIDE 31 OF DR. REDDY'S PRESENTATION



In this animation produced solely for litigation, Dr. Reddy continues to omit the egress processing of packets out of Cisco's switches and routers. The Court made distinct note of Dr. Reddy's use of an animation during his direct examination. Tr. 2616:10-20. Dr. Reddy's testimony is just one example of how Cisco's experts used their own modified exhibits and ex post facto animations while Centripetal's experts and Cisco's own employees relied on Cisco's technical documents in an unaltered form.

Cisco's experts attempted to challenge every element of all of the claims at issue in its non-infringement case. However, the Court **FINDS** that Centripetal has proven the direct infringement of each element of the asserted claims in the '856 Patent, the '176 Patent, the '493 Patent, and the '806 Patent by a preponderance of the evidence. Most of Cisco's challenges amounted to no more than conclusory statements by its experts without evidentiary support. Accordingly, in its findings of fact and conclusion of law, the Court has focused on only those elements cited by Cisco's

infringement experts in their patent by patent outlines of noninfringement theories. The Court will analyze each patent individually, and outline all relevant findings of fact and conclusions of law regarding infringement, validity, and damages. The Court will address the patents in the following order: the '856 Patent; the '176 Patent; the '193 Patent; the '806 Patent; and the '205 Patent.

V. FINDINGS OF FACT AND CONCLUSIONS OF LAW REGARDING INFRINGEMENT AND VALIDITY

A. THE '856 PATENT

i. Findings of Fact Regarding Infringement

1. The '856 Patent has been informally known as the Encrypted Traffic Patent. Tr. 884:25.

2. The '856 Patent was issued on March 13, 2018. JTX-5. The application for the '856 Patent was filed on December 23, 2015. JTX-5.

3. The asserted claims of the '856 Patent are Claim 24 and Claim 25. Doc. 411. Claim 24 and Claim 25 are, respectively, a system and computer readable media claims.

4. Claim 24 is laid out below:

> A packet-filtering system comprising:
>
> at least one hardware processor; and memory storing instructions that when executed by the at least one hardware processor cause the packet-filtering system to:
>
> > receive data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprise a domain name identified as a network threat;
> >
> > identify packets comprising unencrypted data;
> >
> > identify packets comprising encrypted data;
> >
> > determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-

> threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;
>
> filter, based on at least one of a uniform resource identifier (URI) specified by a plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules:
>
> packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators; and
>
> the determined packets comprising the encrypted data that corresponds to the one or more network threat indicators; and
>
> route, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.

JTX-5.

5. Claim 24 is identical to Claim 25 in every respect except that Claim 25 is a computer readable media[4] claim. Tr. 885:14-24. Claim 25 modifies the introductory language of Claim 24, replacing "[a] packet-filtering system comprising: at least one hardware processor; and memory storing instructions that when executed by the at least one hardware processor cause the packet-filtering system to:" with "[o]ne or more non-transitory computer-readable media comprising instructions that when executed by at least one hardware processor of a packet-filtering system cause the packet-filtering system to:." JTX-5. For purposes of infringement, the parties treated Claims 24 and 25 the same.

[4] Computer readable media is software comprising of source code that is loaded into computer hardware through a device such as a CD-ROM, memory card or flash drive. This media comprises of readable instructions for the intended computer to operate. Tr. 473:4-23.

6. Dr. Sean Moore, an inventor of the '856 Patent, describes the '856 Patent as a system for stopping cyber-attacks even when the malicious data is embedded within encrypted packets. Tr. 347:8-9. Therefore, the '856 Patent deals specifically with Centripetal's threat filtering technology as applied to encrypted packets. Tr. 347:8-9.

7. The process at the core of this technology involves using unencrypted information located in a packet to determine if there is a threat embedded in the encrypted portion. Centripetal developed this technology as a response to the ever-growing trend of cyber criminals encrypting packets as a way to bypass traditional security procedures. See Tr. 310:20-24, 889:6-12. Thus, Dr. Moore identifies the '856 Patent as one of Centripetal's solutions to operationalize threat intelligence to determine if encrypted packets contain network threats. Tr. 348:1-16.

8. This system is considered an advancement over previous security systems that would fail to detect hidden attacks because the payload was encrypted by cyber criminals. Tr. 887:4-17.

9. Centripetal accuses Cisco's Catalyst 9000 series switches, the Aggregation Services Router 1000 series routers and Integration Services Router 1000 and 4000 series routers in combination with Cisco's Stealthwatch and Identity Services Engine of infringing Claims 24 and 25 of the '856 Patent. Tr. 886:9-11. Source code for Stealthwatch is compiled in Atlanta. PTX-1932.

10. All of the accused devices for the '856 Patent are embedded with Cisco's new 2017 technology known as Encrypted Traffic Analytics ("ETA"). Tr. 887:25-888:6, 890:19-22; PTX-561 at 630. Cisco utilized ETA as a response to the growing number of attackers that were using encrypted traffic to bypass standard security protocols. Tr. 889:2-12; PTX-561 at 629 (Cisco

noting that "attackers are also using encryption to conceal malware and evade detection by traditional security products.").

11. ETA became a critical component of Cisco's security infrastructure because it provided a new method for identifying hidden threats within encrypted traffic without having to perform the time consuming process of decryption. PTX-561 at 630 (Cisco, in 2019, highlighting ETA as an "innovative and revolutionary technology" that "illuminate[s] the dark corners in encrypted traffic without any decryption by using new types of data elements or telemetry . . .").

12. In order to detect threats in encrypted traffic without decryption, ETA uses data from the unencrypted portion of the packet and performs advanced security analytics. Tr. 892:7-10; PTX-561 at 630. Cisco's documents describe the four main elements of information that is extracted from packets by the ETA technology:

1. **Sequence of Packet Lengths and Times** ("SPLT") – SPLT conveys the length (number of bytes) of each packet's application payload for the first several packets of a flow, along with the interarrival times of those packets.
2. **Initial Data Packet** ("IDP") **–** IDP is used to obtain packet data from the first packet of a flow. It allows extraction of interesting data such as an HTTP URL, DNS hostname and address, and other data elements.
3. **Byte Distribution** – The byte distribution represents the probability that a specific byte value appears in the payload of a packet within a flow.
4. **TLS Specific Features –** The TLS handshake is composed of several messages that contain interesting, unencrypted metadata used to extract data elements, such as cipher suite, TLS version, and the client's public key length.

PTX-561 at 630 (A 2019 Cisco Technical Document). Cisco's ETA amended NetFlow technology to enable the capture of new information from packets including the IDP and SPLT. Tr. 3127:6-13; see PTX-996 at 005 (showing that a 2019 version of ETA was updated to include these new categories).

13. Centripetal's infringement expert, Dr. Eric Cole, outlined and showed Cisco's technical documents that illustrated the analytical process of how these elements are used by Stealthwatch to detect threats in encrypted traffic. Tr. 910:10-913:4.

14. First, the accused routers and switches will make a determination if the packets are encrypted or unencrypted. Tr. 910:15-17, 943:9-14, 1064:8-14; PTX-989 at 004, 033 (the text accompanying Cisco's ETA PowerPoint presentation from 2019 that denotes that Cisco "enhanced the network as a sensor to detect malicious patterns in not only non-encrypted traffic but also in encrypted traffic); PTX-1849 at 244 (source code confirming that there is a determination made whether the packet flow is encrypted or unencrypted).

15. After this determination, representations of information from the unencrypted portion of encrypted packets are sent up to Stealthwatch, which is running both ETA and Cognitive Threat Analytics ("CTA"). Tr. 910:15-911:9; PTX-989 at 033; PTX-578 at 061 (noting ETA "[m]akes the most out of the unencrypted fields" in the packet).

16. This information from the unencrypted packets is sent up to Stealthwatch using Cisco's proprietary logging framework known as NetFlow. Tr. 1078:10-18, 1082:20-24.

17. Using ETA and CTA, Stealthwatch analyzes the NetFlow from the packets and identifies malware threats in encrypted traffic without running any form of standard decryption. Tr. 910:15-911:9, 936:4-20, 941:4-8; PTX-989 at 033; PTX-1010 at 001 (stating Stealthwatch "can detect malware in encrypted traffic without any decryption using **Encrypted Traffic**

Analytics.") (emphasis in original); PTX-1009 at 012 (Cognitive Threat Analytics technical release notes illustrating that ETA "[e]nhances existing Stealthwatch / CTA integration with malware detection capability for encrypted traffic without decryption.").

18. In order to perform the required analysis, Stealthwatch receives real-time threat intelligence indicators contributed by a third-party intelligence provider or directly from Cisco's Threat Intelligence Group known as Talos. Tr. 912:16-19, 921:13-16; PTX-20 at 001 (showing Stealthwatch has the ability to take threat indicators and "correlate[] suspicious activity in the local network environment with data on thousands of known command-and-control servers . . ." and indicating that Stealthwatch uses ETA to "pinpoint malicious patterns in encrypted traffic to identify threats . . ."); PTX-1081 at 013 (illustrating Stealthwatch's integration of CTA by using the Global Risk Map to identify known malicious domain data).

19. This threat intelligence sent into Stealthwatch contains many known malicious IP addresses, domain names, protocol versions and other indicators of malicious traffic. Tr. 927:4-10; PTX-1926 (Mr. Amin, a principal engineer at Cisco, confirming that the new Stealthwatch receives IP addresses and domain names in its threat intelligence information).

20. Using these indicators, Stealthwatch filters the representation of packets in the form of NetFlow. Then, Stealthwatch determines if any encrypted traffic in the network matches any known malicious signatures based on unencrypted information provided in NetFlow such as the IDP, Server Name Indicator ("SNI") or Transport Layer Security ("TLS"). Tr. 920:22-921:10, 956:3-958:8, 1054:15-20; see PTX-1009 at 012; PTX-996 at 005.

21. Using a platform known as xGRID, Stealthwatch then sends the results of its analysis to the Identity Services Engine ("ISE"). Tr. 910:15-911:9, 912:1-12; PTX-989 at 033.

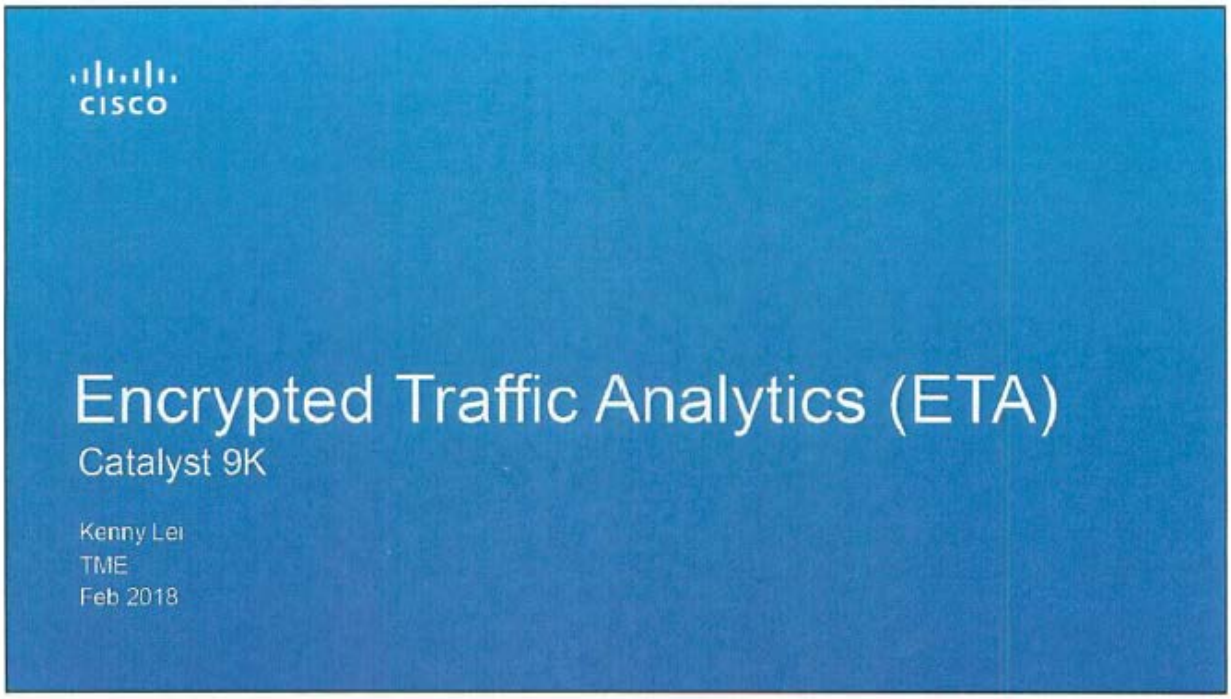
22. After this communication, ISE will provision rules or change of authorizations ("CoAs") to the switches and routers. The switches and routers operate inline and are able to drop incoming packets from the malicious source and outgoing packets containing sensitive data attempting to be exfiltrated by embedded malware. Tr. 1965:16-18.

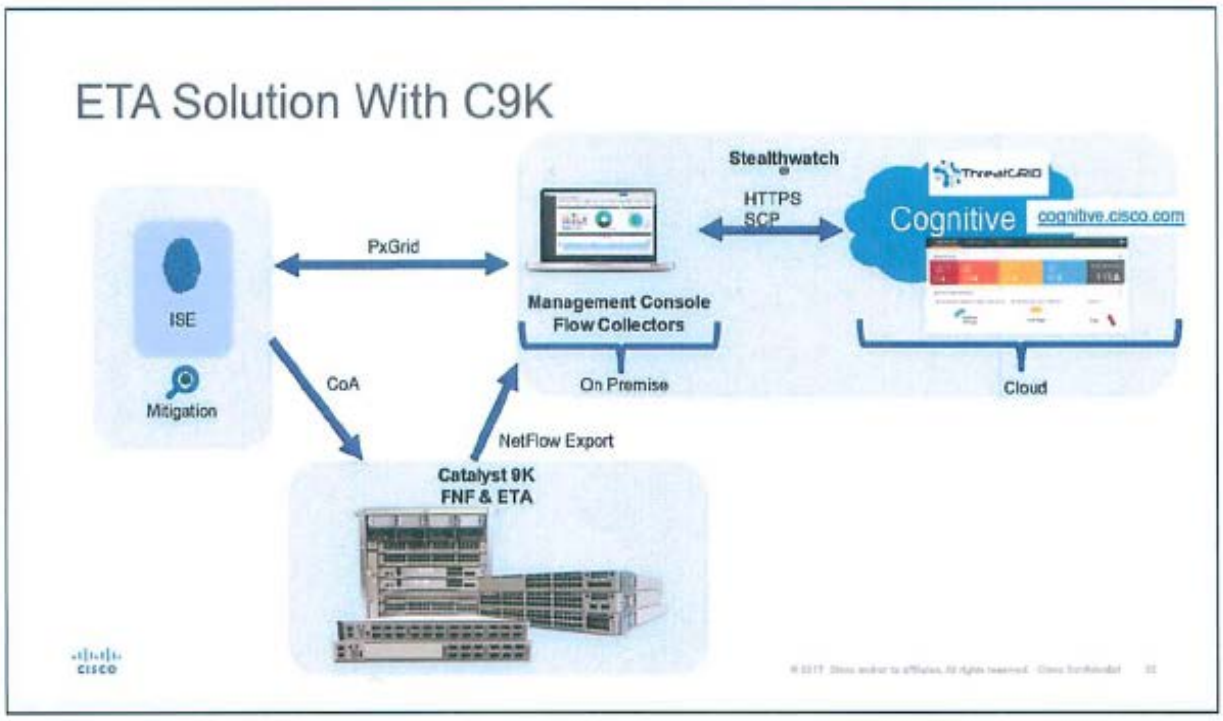
23. Blocked packets are routed to a proxy system, known as a null interface, that is used to drop packet traffic. Tr. 963:24-966:19; PTX-256 at 082,083; see Tr. 2199:21-2203:25.

24. This process is shown by a Cisco technical demonstration of ETA provided in February of 2018. PTX-989. The title page and relevant page are shown below:

PTX-989

Cisco Encrypted Traffic Analytics Technical Presentation from February of 2018





25. Cisco's expert has failed to cite any Cisco technical document produced post June 20, 2017.

26. Cisco has not called any witness who authored any of the Cisco technical documents relied upon by Centripetal in their infringement case.

27. Cisco's expert witness relies on animations, produced ex post facto, which were designed for litigation and do not accurately portray the current functionality of the accused products.

ii. Conclusions of Law Regarding Infringement

The Federal Circuit has concisely stated that "[i]nfringement analysis is a two-step process: '[f]irst, the court determines the scope and meaning of the patent claims asserted ... [and secondly,] the properly construed claims are compared to the allegedly infringing device.'" N. Am. Container,

Inc. v. Plastipak Packaging, Inc., 415 F.3d 1335, 1344 (Fed. Cir. 2005) (quoting Cybor Corp. v. FAS Techs., Inc., 138 F.3d 1448, 1454 (Fed. Cir. 1998)).

First, the Court hereby incorporates its Markman Claim Construction Order for purposes of construing the terms in the Asserted Claims. Doc. 202. The Court has made a modification to one of the terms previously construed via Markman due to a developed understanding of the technology in the case. See Pressure Prods. Med. Supplies v. Greatbatch Ltd., 599 F.3d 1308, 1316 (Fed. Cir. 2010) ("district courts may engage in a rolling claim construction, in which the court revisits and alters its interpretation of the claim terms as its understanding of the technology evolves"). The Court, in analyzing the applicable law, includes a table of the previously construed terms:

Term	Construction
Configured to	Plain and ordinary meaning which requires that the device be capable of configuring to do the function. **(amended definition)**
Correlate, based on a plurality of log entries	Packet correlator may compare data in one or more log entries with data in one or more other log entries.
Dynamic security policy	A changeable set of one or more rules, messages, instructions, files, or data structures, or any combination thereof, associated with one or more packets.
Generate, based on the correlating, one or more rules.	Plain and ordinary meaning.
log entries	Notations of identifying information for packets.

network-threat indicators	Indicators of packets associated with network threats, such as network addresses, ports, domain names, uniform resource locators (URLs), or the like.
packet security gateway	A gateway computer configured to receive packets and perform a packet transformation function on the packets.
Packets	Plain and ordinary meaning in the context of the claim in which the term appears.
Preambles	Preambles are limiting.
Proxy system	A proxy system which intervenes to prevent threats in communications between devices.
Responsive to correlating	Plain and ordinary meaning.
Rule	A condition or set of conditions that when satisfied cause a specific function to occur.
Security policy management server	A server configured to communicate a dynamic security policy to a packet gateway.

The Court has made one notable change from the previous claim construction order. The Court revises the construction of the term "configured to" from "Plain and ordinary meaning which requires that the action actually do the function automatically" to "Plain and ordinary meaning which requires that the device be capable of configuring to do the function." See Tr. 1646:11-1647:1. This change is made in light of the Court's developing knowledge of the patented technology.

To prove infringement, the plaintiff must show the presence of every claim element or its equivalent in the accused device by a preponderance of the evidence. Uniloc USA, Inc. v. Microsoft Corp., 632 F.3d 1292, 1301 (Fed. Cir. 2011); see Cross Med. Prods., Inc. v. Medtronic Sofamor Danek, Inc., 424 F.3d 1293, 1310 (Fed. Cir. 2005) (showing preponderance of the evidence as the proper standard for infringement analysis). This standard does not require a patent owner to present "definite" proof of infringement, but instead requires the patent owner to establish that "infringement was more likely than not to have occurred." See Warner–Lambert Co. v. Teva Pharms. USA, Inc., 418 F.3d 1326, 1341 n.15 (Fed. Cir. 2005) (citing Advanced Cardiovascular Sys., Inc. v. Scimed Life Sys., Inc., 261 F.3d 1329, 1336 (Fed. Cir. 2001)). This comparison of the claims to an accused product is a fact specific inquiry and may be based on "direct or circumstantial evidence." W.L. Gore & Assoc, Inc. v. Medtronic, Inc., 874 F. Supp. 2d 526, 541 (E.D. Va. 2012) (citing Martek Biosciences Corp. v. Nutrinova, Inc., 579 F.3d 1363, 1372 (Fed. Cir. 2009)).

Literal infringement requires an accused product to embody each and every limitation of the patented claim. V-Formation, Inc. v. Benetton Group SpA, 401 F.3d 1307, 1312 (Fed. Cir. 2005). In contrast, "under the doctrine of equivalents, 'a product or process that does not literally infringe upon the express terms of a patent claim may nonetheless be found to infringe if there is 'equivalence' between the elements of the accused product or process and the claimed elements of the patented invention.'" W.L. Gore & Associates, Inc., 874 F. Supp. 2d at 541 (quoting Warner–Jenkinson Co. v. Hilton Davis Chem. Co., 520 U.S. 17, 21 (1997)). A finding that the doctrine of equivalents applies requires either that "the difference between the claimed invention and the accused product or method was insubstantial or that the accused product or method performs substantially the same function in substantially the same way with substantially the same result as

each claim limitation of the patented product or method." Id. (quoting AquaTex Indus., Inc. v. Techniche Sols., 479 F.3d 1320, 1326 (Fed. Cir. 2007)).

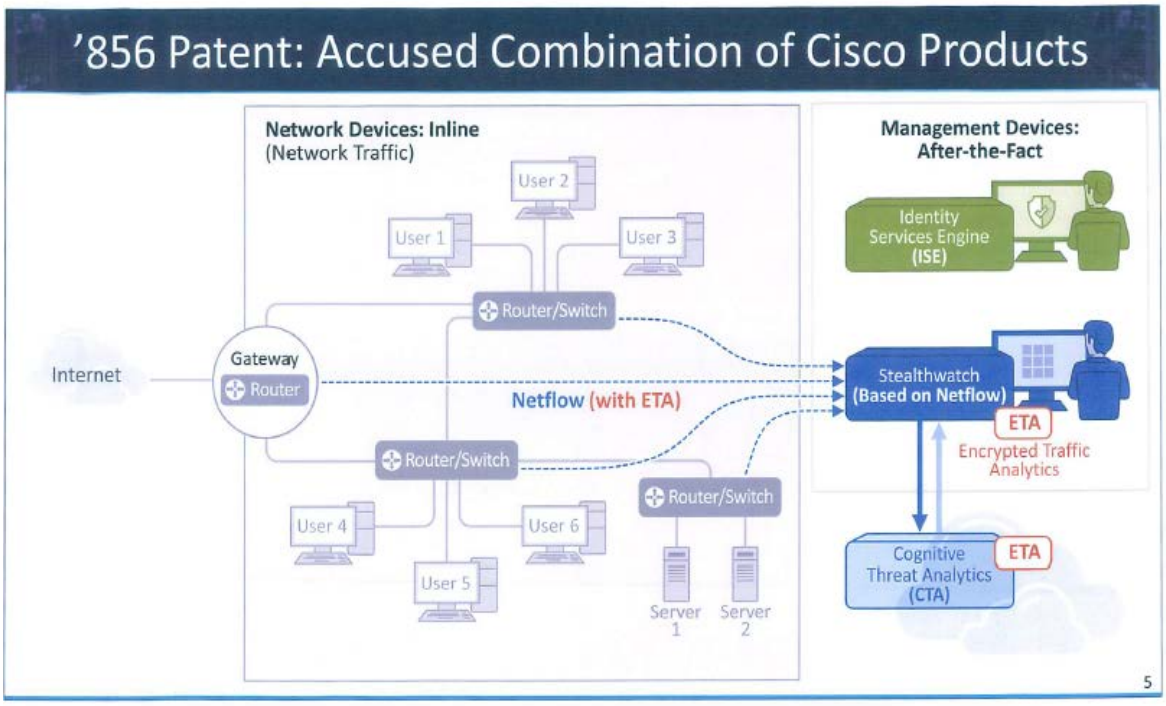
Based on the Court's factual findings, Centripetal has proven by a preponderance of the evidence that Cisco's Catalyst 9000 series switches, the Aggregation Services Router 1000 series routers and Integration Services Router 1000 and 4000 series routers in combination with Cisco's Stealthwatch and Identity Services Engine literally **INFRINGE** Claims 24 and 25 of the '856 Patent. Cisco's expert on the '856 Patent, Dr. Douglas Schmidt testified:

> I was asked to look first at whether or not the accused Cisco product suite infringed the '856 patent. I was also asked to opine on whether the '856 patent was valid relative to the prior art. And I was also asked to assume if, in fact, the patent was valid and the accused products infringed, what damages should be assessed, looking at this from a technical point of view of any benefit that the patent provided over what was already known in the prior art.

Tr. 1817:13-23. Dr. Schmidt opined that the '856 Patent is not-infringed on three different theories, First, Dr. Schmidt concludes that the current Cisco system is exclusively after the fact analysis and does not work on determined packets as required by the claims. Second, he states that the null interface used in the Cisco system is not a proxy system as required by the claims. Third and finally, he argues that packets are not filtered by the Cisco system. The Court disagrees with all of Dr. Schmidt's theories of non-infringement.

Turning to the first theory, Dr. Schmidt began his infringement analysis with a description of slide five of his demonstrative presentation. This slide was used in various forms throughout his presentation, as well as by other Cisco experts, and is reproduced here:

SLIDE FIVE OF DR. SCHMIDT PRESENTATION



Dr. Schmidt used the animated slide five, produced ex-post facto for use in the litigation, to support the following opinion:

> Q. And by the time that telemetry information gets sent along that blue dotted line to the right-hand side -- by the time that happens, where is the packet itself?
>
> A. The packets will have long since been received. The packets will typically arrive in a millisecond time frame, which is extremely fast, and the information that's processed on the right-hand side by the so-called after-the-fact management devices could take minutes, hours, perhaps even days to be processed.

Tr. 1815:10-18. Dr. Schmidt indicates throughout his testimony that the new Cisco system is all after the fact analysis and the system "doesn't work on determined packets." In his testimony and on slide five, Dr. Schmidt opined that after the fact management devices include Identity Service Engine ("ISE"), Stealthwatch (based on NetFlow), and Encrypted Traffic Analytics ("ETA"). He opined:

> Q. The accused systems don't block.

A. Again, don't block, don't block what? What are we talking about?

Q. Don't block malware before it infects the host.

A. I think my testimony this whole time has been that the accused products here, particularly the ones that are the after-the-fact ones, allow the information to go to the destination and then conduct so-called after-the-fact analysis in order to determine what issues have occurred and what remediations to take place.

Tr. 1923:14-23.

Dr. Schmidt presented excruciatingly detailed evidence, including animations and text of the old Stealthwatch product, which it acquired from Lancope. Before 2017, Stealthwatch functionality appeared to focus on after the fact forensics, however this was not the case beginning in 2017, as its own software engineer, Mr. Llewallyn, testified while referring to PTX-965:

Q. Do you see this is a Cisco Stealthwatch document? It looks like it's "At a Glance." Do you see that?

A. Yes.

Q. And there's a copyright date on the bottom there of 2017. It might be hard to see, but I'll pull it up. This is a 2017 document?

A. Uh-huh.

Q. Now, you talked about how Stealthwatch works to monitor internal in the network, correct?

A. That's correct.

Q. You also mentioned how it is integrated with Cisco's Identity Services Engine, right?

A. That's correct.

. . .

Q. It says, "Helps organizations get 360-degree view of their extended network." Now, what I want to focus on is at the bottom, where it says, "Simplify segmentation throughout your network with centralized control and policy enforcement and address threats faster, both proactively with threat detection and retroactively via advanced forensics." Now, Stealthwatch, working with other

products in Cisco's Security Suite, in this case the Identity Services Engine, can proactively protect against threats, correct?

A. Well, it's based on a manual operation, though.

Q. But it's in the code. The computers can do it, right?

A. Yes. It provides a way to quarantine the host, by clicking a button.

Q. And you can address threats faster, you can proactively -- both proactively with threat detection and retroactively via advanced forensics, correct?

A. That's correct.

Tr. 2198:5-2198:20, 2199:3-2199:20. Significantly, Cisco and Dr. Schmidt failed to cite any technical documents or diagrams illustrating the new post 2017 Stealthwatch or other products accused of infringing the '856 Patent. An examination of Cisco's own technical documents and diagrams from post 2017, illustrating the functionality of the accused products, explain why it adopted this new functionality. The diagrams and the accompanying text from Cisco's technical explanation of ETA, PTX-584 and PTX-570, illustrate why slide five, and the testimony grounded upon it and its variations, are inaccurate:

PTX-584

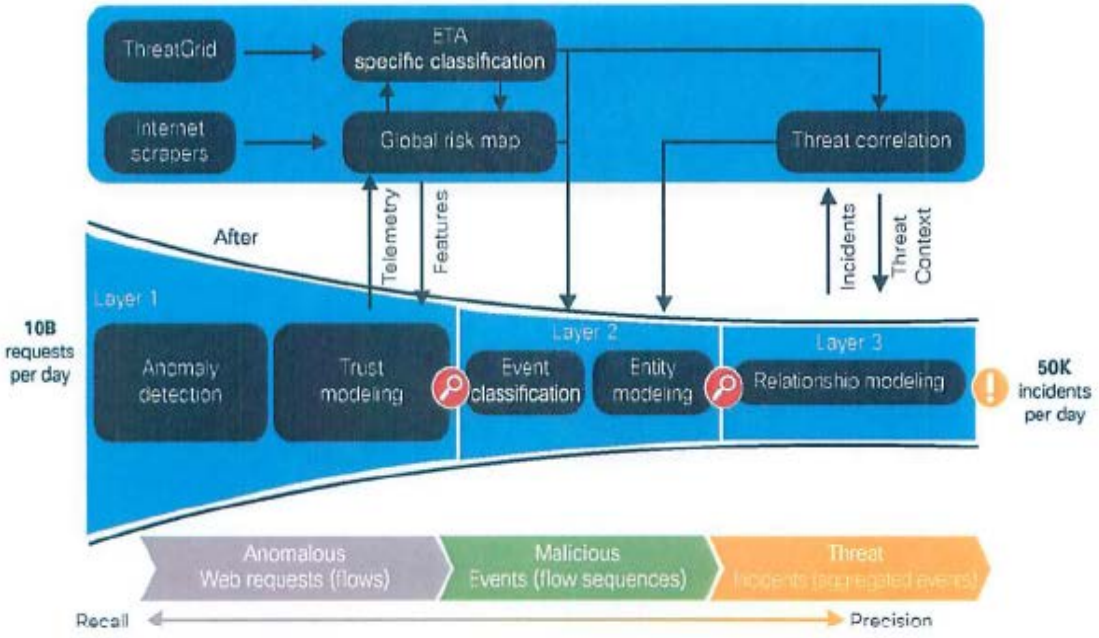
Cisco Encrypted Traffic Analytics Technical White Paper from 2019

Cisco Stealthwatch

Cisco Stealthwatch uses NetFlow, proxy servers, endpoint telemetry, policy and access engines, and traffic segmentation as well as behavioral modeling and machine learning to establish baseline "normal" behavior for hosts and users across the enterprise. Stealthwatch can correlate traffic with global threat behaviors to automatically identify infected hosts, command-and-control communication, and suspicious traffic.

Stealthwatch maintains a global risk map—a very broad behavioral profile about servers on the Internet, identifying servers that are related to attacks, may be exploited, or may be used as a part of an attack in the future (Figure 3). This is not a blacklist, but a holistic picture from a security perspective. Stealthwatch analyzes the new encrypted traffic data elements in enhanced NetFlow by applying machine learning and statistical modeling. The global risk map and Encrypted Traffic Analytics data elements reinforce using advance security analytics. Rather than decrypting the traffic, Stealthwatch uses machine learning algorithms to pinpoint malicious patterns in encrypted traffic to help identify threats and improve incident response.

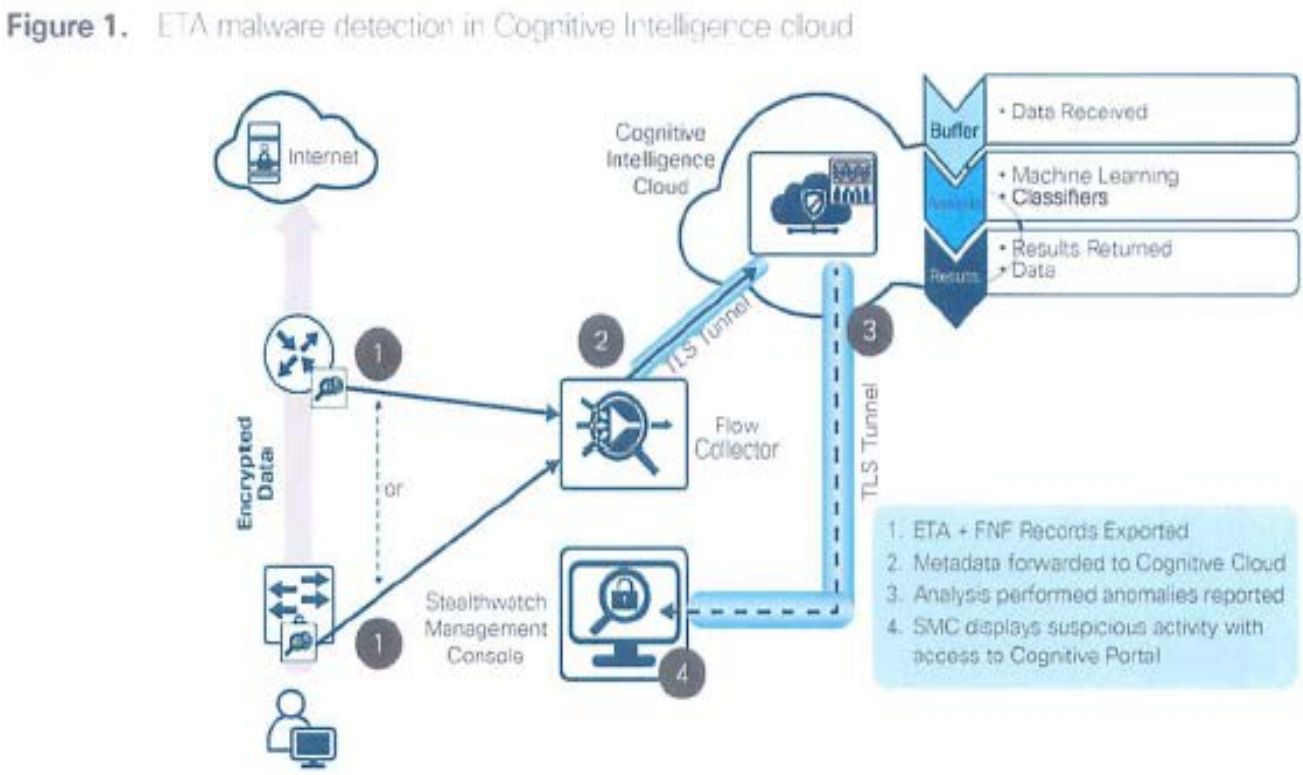
Figure 3. Stealthwatch multi-layer machine learning



PTX-584 at 402.

PTX-570

Cisco Encrypted Traffic Analytics Technical Deployment Guide from July 2019



PTX-570 at 593. This is further supported by the Cisco Stealthwatch Technical Data Sheet, PTX-482:

> Analyzing this data can help detect threats that may have found a way to bypass your existing controls, **before** they are able to have a major impact.
>
> The solution is Cisco Stealthwatch, which enlists the network to provide end-to-end visibility of traffic. This visibility includes knowing every host-seeing who is accessing which information at any given point. From there, it's important to know what is normal behavior for a particular user or "host" and establish a baseline from which you can be alerted to any change in the user's behavior the instant it happens.

PTZ-482 at 664 (emphasis added). Moreover, Dr. Schmidt's testimony attempting to contradict PTX-1287, a 2018 Cisco document, is revealing:

Q. So we go to 1287. This is a document describing the Catalyst 9000 switch. "Foundation for a New Era of Intent-based Networking." Do you see that, Dr. Schmidt?

A. I do.

Q. Okay. You know Dr. Cole relied on this document in his direct testimony of infringement, correct?

A. I believe so.

Q. Okay. Now if we turn to Page 28 of that document ending in Bates Number 028, there's a graphic at the top here and it talks about the Catalyst 9000 Advanced Security Capabilities. Do you see that?

A. I do.

Q. And you recall Dr. Cole relying on this document, correct?

A. Not particularly, no.

Q. Okay. Well, if you look at the very bottom it says, "Detect and stop threats, exclamation point." Do you see that?

A. I do.

Q. And Dr. Cole used it to show that the Catalyst switches and the routers that have the same operating systems can detect and stop threats prospectively right? Or proactively, correct?

A. I don't believe that that's what it says, no.

Q. So you don't think this says it's going to detect and stop threats proactively?

A. I don't know what this slide says in this context. I know that Dr. Cole had an analysis that read the claims in a way that was essentially a non-sequitur, a series of non-sequiturs, and accused things as being part of -- the read on the claims, the patent claims that had nothing to do with the way in which the products operate.

Q. I'm asking about your opinion now. When it says, "Detect and stop threats," does that mean it's detecting and stopping the threat before they get to the host?

A. It's not clear what it means in this context. I see the words "detect and stop threat." I don't see how it applies to the patent that we're talking about here.

Q. So you don't know what "detect and stop threat" means is what you're telling the Court?

A. No. I'm just saying I don't know whether it means what you're saying it means.

THE COURT: Well, what do you think it means over on the right where it says "Before, During and After"?

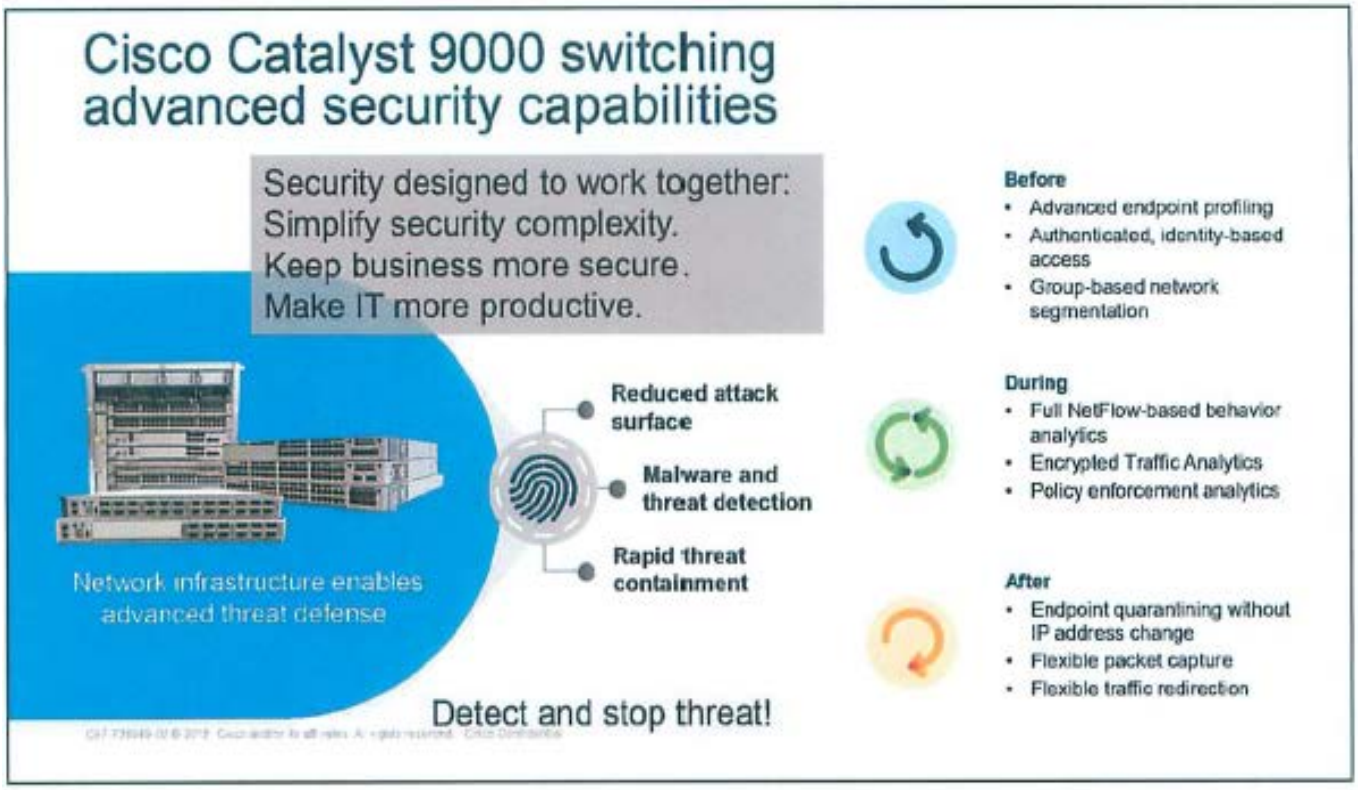
THE WITNESS: It looks like it's saying that -- so it looks like it's talking about the fact it's possible to quarantine something, but I don't know how that refers to the -- I don't know how that refers to the way in which it reads on the claims and whether what Dr. Cole was alleging has anything to do with what the claims are asserting.

BY MR. ANDRE:
Q. So when it says "During", during the packets coming in, Full NetFlow-based behavior analytics, Encrypted Traffic Analytics, Policy Enforcement Analytics. You don't have an understanding of what that's referring to?

A. Again, this particular slide is coming out of thin air here, so I would have to spend a little bit of time looking at it to understand the way it's being used in this particular context.

Tr. 1925:16-1927:21; see PTX-1287 at 028 (depicted below).

PTX-1287
Cisco Catalyst 9000 Switching Technical Presentation from 2018



It's difficult to comprehend why Dr. Schmidt would state, in his rebuttal of Dr. Cole, that he cannot understand a Cisco post 2017 document because it is "coming out of thin air." In his preparation for his expert testimony, the Court is unaware how or why he overlooked this crucial Cisco document. Dr. Schmidt, when questioned again about this point, stated:

> Q. When we talk about Stealthwatch, if we go to the next page, you keep talking about this after-the-fact stuff. On that table on the left there it says, "Real-time detection of attacks by immediately detecting malicious connections from the local environment to the Internet." Do you see that?
>
> A. I do.
>
> Q. So does that make you rethink your opinion that the real-time doesn't mean immediately?
>
> A. No, it does not.

> Q. So the word "immediately" doesn't mean immediately in that sentence?
>
> A. Again, immediately is always relative to something. We already know that the packets are always delivered to the destination by the time the work goes up, by the time the NetFlow goes up to Stealthwatch and Cognitive Threat Analytics. And so it will detect it as quickly as it can, but it doesn't say, it doesn't say before the packets are delivered to the destination, does it? It says real-time detection of attacks by immediately detecting malicious connections. But there's nothing there about it blocking the traffic, it just says it's detecting it.

Tr. 2113:17-2114:12. Dr. Schmidt's testimony is directly refuted by Cisco's own technical documents. For example, Cisco's Catalyst 9000 at-a-glance guide highlights that this line of switches can "detect **and stop** threats, even with encrypted traffic." PTX-199 at 224. (emphasis added). Cisco portrays the benefits of Stealthwatch as "[r]eal time detection of attacks by immediately detecting malicious connections from the local environment to the Internet." PTX-383 at 356. The Stealthwatch Data Sheet confirms that Stealthwatch uses "advanced security analytics to detect **and respond** to threats in **real time**." PTX-482 at 664 (emphasis added). These documents confirm that the accused products are not solely used for detecting, but also for stopping those threats. Furthermore, the Stealthwatch Data Sheet notes that "Stealthwatch can recognize these early signs [of attacks] to **prevent** high impact . . . [o]nce a threat is identified, you can **also** conduct forensic investigations to pinpoint the source of the threat . . ." PTX-482 at 665 (emphasis added). The Court asked Dr. Schmidt about the word "also" in PTX-482:

> THE COURT: Why do you think it says "also" there?
>
> THE WITNESS: I think what it's talking about there, Your Honor, if you take a look, it says "You can determine where else it may have propagated." If you look at the --
>
> THE COURT: Do you think maybe it means you can do the things in the first two sentences and also do the thing in the third sentence? Do you think that's what "also" means?
>
> THE WITNESS: I think it's trying to say, sir, that if you look -- the forensic investigations they are specifically calling out here are pinpointing where the

> problem was, so identifying who the bad guy is, and then determining what else might be infected. So that's the problem with network threats; they often spread rapidly like viruses. That's why they're called viruses. So this is saying you can do additional analysis to not just say one person has a problem, but all the other things in the network that that person's connected to somehow, that computer has been connecting to, may also be a problem too. I think that's what "also" means here.
>
> THE COURT: I think "also" means "also" . . .

Tr. 1974:13-1975:6. Notably when Mr. Schmidt previously read the same sentence from PTX-482, he omitted the word "also" "Once a threat is identified, you can ____ conduct forensic investigations." Tr. 1936:16-17. From his own testimony, it is clear to the Court that Dr. Schmidt is solely limiting his testimony to the forensic after the fact analysis feature in the old pre-2017 Stealthwatch. The Court accepts that Stealthwatch has the features to conduct forensic investigations after the fact. However, Dr. Schmidt, throughout his testimony ignores the presence of the word "also" and "detect and stop" in the technical documents, which denotes that the after the fact investigation is a feature that operates in addition to the ability to stop threats in real time. See Tr. 1974:3-1975:8.

Turning to the second theory, this Court, in its Claim Construction Order, has construed a proxy system as a "A proxy system which intervenes to prevent threats in communications between devices." Mr. Llewallyn, a Cisco software engineer, confirms that Stealthwatch and ISE, working in conjunction, can reconfigure the switches and routers to re-route malicious packets intended for a particular host to a null interface. Tr. 2199:21-2203:25. Cisco contends this use of a null interface falls outside of the Court's Markman construction. It clearly does not. Cisco's technical documents describe the null interface as a "virtual interface [that] never forward[s] or receive[s] traffic but packet[s] route[ed] to null interface are dropped." PTX-256 at 082, 083 In this manner, the null interface causes "packets destined for a particular network to be dropped." PTX-256 at 082, 083. The technical evidence shows that the null interface is a method,

incorporated into Cisco's quarantine procedure, for re-routing packets from the intended host serving as an intervening process in the communication to drop packets.

Dr. Schmidt opined that the proxy system required by the '856 Patent specification must perform some form of decryption. Dr. Schmidt testified as follows:

> Q. And you actually cited to the specification to show that a proxy system, the analysis had to actually decrypt, correct? You said that this claim requires decryption. Do you recall that?
>
> A. I do.
>
> Q. All right. So let's go back to the patent. Column 10, line 15. 15 to 20. Now, this is the point that's part of the specification you pointed to. Proxy device may receive the packet and decrypt the data in accordance with the parameters as in session 306. Do you see that?
>
> A. I do.
>
> Q. And you took that to mean that it must decrypt the data in accordance with the parameters, correct? Not that it may, that it must.
>
> A. Well, so to be consistent, there's quite a number of places in columns, basically 8 through 12, where they talk about the role of proxy device, 112, which is the part here. And when they talk about proxy device 112, they're talking about it in the context, going back to figure 3B, where there is a SSL/TLS session set up that involves sending encrypted packets. And whenever they talk about it in all those different places in columns 8, 9, 10, 11, and 12, they always make it clear that proxy device 12 [sic] receives packets that are encrypted packets and then decrypts them, and then sends the unencrypted data to what they call the man in the middle RuleGate, which is RuleGate 124. And RuleGate 124 then, as it talks about just a little bit further down in the specification, it talks about actually doing the filtering. And it talks about filtering based on the URI, they talk about filtering based on the request, on the method, on the command and so on. And then right after that it talks about how RuleGate 124 sends that information, which at that point is still decrypted – because of course we couldn't be analyzing it unless it was decrypted -- it then sends it to proxy device 114. And as you read in the spec, it makes it very clear that proxy device 114 then re-encrypts the data and sends it on to the destination. So in all the cases where proxy system is disclosed – and like I said, there are three or four of them in the specification – it's always talked about in the context of receiving encrypted data and then proxy device 112 will decrypt it and then pass it on in some way. So those are the ways that proxy system are -- proxy system is used in the spec. So that's where I come up with the reasoning that, A, proxy system is involving decryption and encryption, because it says so very clearly

in the specification, and then reading claims F, F1 and F2, it's very clear that the analysis that's done to the filtering, for the most part can't be done unless the packets are decrypted.

MR. ANDRE: Your Honor, I don't want to interrupt the witness, but I move to strike most of that. It's not even responsive to my question. He's going on these long tirades and -- I just asked a very simple question. Anyway. I'll just ask this question:

BY MR. ANDRE:
Q. Okay. So I looked at this entire patent. I did a word search. The word "decrypt" shows up one time in this entire patent. One single time. And it's right there.

A. That's true. And the word unencrypted –

Q. Doctor, you just said that –

A. -- appears in multiple places.

Q. You said that decryption shows up every time they talked about the proxy server. You just testified to that just two seconds ago.

A. No, what I said was that if you read the other parts of the patent spec they don't use the word decrypt, they talk about unencrypting the data. So it says it will send over unencrypted data. So the word decrypt and unencrypted or sending unencrypted data necessarily implies that the data is unencrypted or decrypted. Unencrypted and decrypted are essentially synonyms. So it makes it very clear throughout the specification that, especially to the parts in columns 9, 10, 11 and 12, that that's what proxy device 112 is doing on the outgoing path. And also they talk about it in terms of proxy device 114 on the incoming path.

Q. So you're saying that unencrypted data -- data that has never been encrypted ever -- and decrypted are synonyms?

A. No, thats that's not what I'm saying.

Q. You just said that.

A. Well, that's not what I'm saying. What I'm saying here is very clear: The patent spec talks repeatedly, especially in reference to figure 3B, where information is being received from, I believe it's on session 306, I think it's from host 108, if I'm not mistaken, and that information is coming in over an encrypted session. And it makes it very clear in the patent spec that this is an encrypted session. And then it says proxy device 112 receives the encrypted data and then either decrypts it or they sometimes say then send on unencrypted data.

. . .

Q. Is there ever a disclosure of the proxy system in the specification that doesn't do any analysis at all; that just drops without first doing analysis?

A. No.

Q. And a null interface, does it do any analysis at all before it drops a packet?

A. No, it does not.

Tr. 1941:2-1944:15, 1976:14-20. The specification specifically confirms that another option is to drop the packets. Column 8 starting at line 5 provides:

and one or more of log or drop the packets. Responsive to receiving the packets from proxy device **112,** host **106** may generate packets comprising data configured to establish the connection between proxy device **112** and host **106** (e.g., a TCP:ACK handshake message) and, at step **#14,** may communicate the packets to proxy device **112.** Rules **212** may be configured to cause rule gate **120** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of steps **#6, #7, #12,** or **#13),** and one or more of log or drop the packets.

Responsive to receiving the packets from proxy device **114,** host **142** may generate packets comprising data con-Figured to establish the connection between proxy device **114** and host **142** (e.g., a TCP:SYN-ACK handshake message) and, at step **#15,** may communicate the packets to proxy device **114.** Rules **212** may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on

> data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6, 7, or 12-14),** and one or more of log or drop the packets.
>
> Responsive to receiving the packets from host **142,** proxy device **114** may generate packets comprising data configured to establish the connection between proxy device **114** and host **142** (e.g., a TCP:ACK handshake message) and, at step **#16,** may communicate the packets to host **142.** Rules **212** may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6, 7, or 12-15),** and one or more of log or drop the packets.
>
> Referring to FIG. **3B,** proxy device **112** may receive the packets comprising data configured to establish the connection between proxy device **112** and host **106** communicated by host **106** in step **#14,** and connection **302** (e.g., a TCP connection) between proxy device **112** and host **106** may be established. Similarly, host **142** may receive the packets comprising data configured to establish the connection between proxy device **114** and host **142** communicated by proxy device **114** in step **#16,** and connection **304** (e.g., a TCP connection) between proxy device **114** and host **142** may be established.

JTX-5 at 724. Columns 9-12 of the specification all contain the same alternate phrase "or drop the packets." In fact, there is at least one mention of "or drop the packets" in each of columns 8-23 of the specification. These multiple references directly contradict Dr. Schmidt. Therefore, it is abundantly evident that Cisco's null interface serves as a proxy system because it prevents threats in communications between devices, and this type of dropping of packets is shown by the specification to be an alternative to the further analysis of the packets. Therefore, the Patent does not require decryption as "or drop the packets" is already identified as an alternative.

Lastly, Cisco contends that Stealthwatch does not "filter" packets as required by the asserted claims. The Court disagrees. As outlined, Stealthwatch receives NetFlow, which contains representations of the unencrypted portions of encrypted packets. See PTX-578 at 061 (noting ETA "[m]akes the most out of the unencrypted fields" in the packet). These representations contain relevant header information from the packet and flow information utilized by Stealthwatch's system to determine if the packets were being used in a malicious communication within the network. In this manner, sending these representations containing all header and flow information is no different than sending the packet directly to Stealthwatch because the representation is essentially a copy of the unencrypted portion of the packet. Using this unencrypted data, Stealthwatch discovers a user device infected with malware and "a malicious encrypted flow can be blocked or quarantined by Stealthwatch." PTX-584 at 403.

The Stealthwatch user interface known as the Stealthwatch Management Console ("SMC") "provides a view of affected users identified by risk type." Tr. 1920:20-22 (Dr. Schmidt confirming that Stealthwatch may provide alarms and alerts based on views within Stealthwatch), 2205:25-2206:4 (Mr. Llewallyn, a Cisco engineer, confirming Stealthwatch triggers alerts). The SMC allows for the representation of packets currently being processed within the network to be filtered and ordered by information within the unencrypted part of the packet such as protocol version, server name or domain name. Tr. 951:16-20; PTX-570 at 640. Dr. Cole highlights that this process meets the filter element because the Cisco system can identify and filter flows of packets that use certain versions of protocols that may be more vulnerable to malware incorporation. Tr. 953:22-954:2. For example, an outdated version 1.0 of a specific protocol such as TCP may be more vulnerable to be infected with malware than an updated and more secure version 2.0. See Tr. 953:22-955:24; see PTX-570 at 640. The Cisco system is able to filter the

flows of packets to visualize outdated versions and filter flows based on outdated and vulnerable protocol versions. See Tr. 953:22-955:24. Seeing those packet flows, the system responds by implementing rules based solely on blocking an older protocol that may leave the network open to attack. Tr. 953:22-954:2, 2202:5-25 (Mr. Llewallyn highlighting that Stealthwatch and ISE can send rules to routers and switches based on identified packet information such as protocol). Additionally, besides protocol version, Stealthwatch can perform this filtering based on server name, a component embedded within a Uniform Resource Identifier ("URI"). Tr. 957:12-21; see PTX-996 at 005 (noting that server name is part of the Initial Data Packet sent up in a Flow Record to Stealthwatch). URI, like protocol version, can be used to design rules that prevent the exfiltration of packets to that identified destination server. Accordingly, Cisco's technical documents, as well as its own engineers, confirm that the Cisco system filters packets as required by the asserted claims of the '856 Patent.

For all the aforementioned reasons, the Court **FINDS** the accused Cisco products literally infringe Claims 24 and 25 of the '856 Patent.

iii. Findings of Fact Regarding Validity

28. The priority date of the '856 Patent is December 23, 2015. JTX-5.

29. As prior art, Cisco asserts multiple different versions of the old Stealthwatch system (i.e., versions 6.3, 6.5.4, and 6.5.5), and Identity Services Engine version 1.3 including NetFlow functionality embedded in other switches and routers. DTX-311, DTX-312, DTX-343, DTX-364, DTX-380, DTX-409 (All of which are pre-2017 documents).

30. The old Stealthwatch system received information from NetFlow provided by Cisco's switches and routers. DTX-311 at 010; Tr. 3112:5-11.

31. The old Stealthwatch system operated as an after the fact analysis tool to gather information, after packets reached their final destination, and displayed that information to network administrators. Tr. 3123:18-21. Old Stealthwatch lacked the functionality to use unencrypted portions of data to determine if encrypted portions of traffic had threats hidden within. Tr. 3124:12-3125:6; see DTX-409. Old Stealthwatch did not possess the functionality to differentiate between unencrypted and encrypted traffic. Tr. 3112:4-11, 3122:13-3126:7, 3127:24-3133:10.

32. The technical documents for the old Stealthwatch system contain no mention of the ability of determining network threat indicators with respect to encrypted packets or analyzing data with respect to the unencrypted portion of encrypted packets, as it did not possess the functionality to determine what portion of the packets are unencrypted or encrypted. Tr. 3111:2-25.

33. Cisco incorporated the functionality from Centripetal's technology to differentiate the unencrypted portion of packets from the encrypted portion of packets with its Encrypted Traffic Analytics ("ETA") technology. ETA was added to Cisco's network devices after it was released around November 2017. PTX-1009 at 012; PTX-1135 at 046-047; PTX-464 at 066, 069-070; PTX-970 at 969; Tr. 3219:13-3223:6; 3238:21-3239:2, 3239:18-24.

34. The prior art asserted by Cisco contained no mention of the identification of encrypted information and/or packets. Tr. 3124:1-3125:1; see DTX-312, DTX-409.

35. Before the addition of ETA, Cisco's system required using expensive and time-consuming decryption measures to detect threats in encrypted traffic. Tr. 2100:24-2101:18; PTX-1417 at 107.

36. Cisco's ETA also amended Cisco's preexisting NetFlow technology in 2017 to enhance the capture of new and different information from the unencrypted portion of encrypted packets including the Initial Data Packet ("IDP") and Sequence of Packet Lengths and Times ("SPLT"). Tr. 3127:6-13, 2103:5-6; see PTX-996 at 005.

iv. Conclusions of Law Regarding Validity

Patents and their claims are presumed to be valid. 35 U.S.C. § 282(a). This presumption may be rebutted by clear and convincing evidence that the patent at issue is invalid. Sciele Pharma Inc. v. Lupin Ltd., 684 F.3d 1253, 1260 (Fed. Cir. 2012); Tech. Licensing Corp. v. Videotek, Inc., 545 F.3d 1316, 1327 (Fed. Cir. 2008). This high burden of proof lends the necessary deference to the Patent and Trademark Office's decision to grant the patent. See Sciele Pharma Inc., 684 F.3d at 1260 ("This notion stems from our suggestion that the party challenging a patent in court bears the added burden of overcoming the deference that is due to a qualified government agency presumed to have done its job."). The clear and convincing standard "is an intermediate standard which lies somewhere between 'beyond a reasonable doubt' and a 'preponderance of the evidence.'" Buildex Inc. v. Kason Indus., Inc., 849 F.2d 1461, 1463 (Fed. Cir. 1988) (quoting Addington v. Texas, 441 U.S. 418, 425 (1979)). This standard is met when the evidence "produces in the mind of the trier of fact an abiding conviction that the truth of [the] factual contentions are highly probable." Id. Throughout the trial, Cisco's experts opined that the patents were invalid based on anticipation, obviousness, and in some claims, lack of adequate written description.

Starting first with anticipation, in order to anticipate a claim, "a single prior art reference must expressly or inherently disclose each claim limitation." Finisar Corp. v. DirecTV Group, Inc., 523 F.3d 1323, 1334 (Fed. Cir. 2008). This disclosure must go beyond a mere mention of each

claim limitation, as anticipation "requires the presence in a single prior art disclosure of all elements of a claimed invention arranged as in the claim." Id. (emphasis in original).

To invalidate a patent on the basis of obviousness, a party "must demonstrate by clear and convincing evidence that a skilled artisan would have been motivated to combine the teachings of the prior art references to achieve the claimed invention, and that the skilled artisan would have had a reasonable expectation of success in doing so." Cumberland Pharms. Inc. v. Mylan Institutional LLC, 846 F.3d 1213, 1221 (Fed. Cir. 2017) (quoting Kinetic Concepts, Inc. v. Smith & Nephew, Inc., 688 F.3d 1342, 1360 (Fed. Cir. 2012)).

Dr. Schmidt, in his invalidity testimony, assumed the infringement analysis by Dr. Cole and opined that all of the same functionality that Dr. Cole relies on for infringement was in the accused products prior to the priority date of the '856 Patent. Tr. 1984:23-1985:4. Cisco's technical documents refute this characterization and confirm that Encrypted Traffic Analytics ("ETA") was truly a new advancement in the identification of threats within encrypted traffic without decryption and not simply an improvement over the previous system. The Catalyst 9000 Switch Guide shows how the accused products, with the addition of ETA, solved difficulties of detecting threats in encrypted traffic:

> Before the introduction of the Catalyst 9000 series, detecting attacks that hide inside encrypted sessions required unwieldy and expensive measures. In short, it meant installing decryption hardware in the middle of encrypted flows . . .

PTX-1417 at 107. Dr. Schmidt's testimony on the Catalyst 9000 switches confirmed this technical statement that the prior art system employed by Cisco, before ETA, required some form of decryption to detect threats in encrypted traffic. He testified:

> Q. Okay. Well, why don't we turn to Page Bates No. 107 of this document. I want to turn your attention to the second -- this is talking about the Encrypted Traffic Analytics on the Catalyst switches. I want to turn your attention to the second paragraph. It states "Before the introduction of the Catalyst 9000 series, detecting

> attacks that hide inside encrypted sessions required unwieldy and expensive measures. In short, it meant installing decryption hardware in the middle of encryption flows." Do you see that?
>
> A. I do.
>
> Q. And you agree with that statement that's in the Catalyst manual?
>
> A. I think that's referring -- I think that's contrasting the so-called inline systems which I believe the '856 patent to be focusing on with the after-the-fact analysis that they're talking about here. Because if you look, **"In short, it means installing decryption hardware in the middle of encrypted flows." I believe that's what a firewall does and that's what the prior art Cisco Systems did, and that's also of course what the '856 patent covers.**

Tr. 2100:24-2101:18 (emphasis added). Dr. Schmidt stated that he accepted Dr. Cole's construction of the claims to find that the prior art system performs all of the infringing functionality. Based on this testimony, Dr. Schmidt opined that the '856 Patent covers a system that uses "decryption hardware" to detect threats in encrypted traffic. The Court agrees that the functionality of Cisco's prior art primarily employed decryption to deal with threats in encrypted traffic. See PTX-1417 at 107. However, accepting Dr. Cole's infringement construction of the asserted claims, the Court, in order to find invalidity, would be required to find that Cisco's prior art disclosed the functionality to identify threats in encrypted traffic **without** the use of decryption. It is evident to the Court that Cisco lacked this functionality before 2017, yet this infringing functionality is exactly what was embedded in the accused products with the addition of ETA in 2017.

The technical documents confirm that Cisco represented it had solved the problems of expensive decryption by delivering "Encrypted Traffic Analytics (ETA) on Catalyst 9000 switches. ETA identifies malware communications in encrypted traffic via passive monitoring: no extra equipment is required and unnatural traffic redirection need not be performed." PTX-1417 at 107. Cisco completed malware identification in encrypted traffic by "ETA introducing new flow

metadata to help it identify malicious activity hiding within an encrypted flow." PTX-1417 at 107. Cisco, through ETA, added both the "Initial Data Packer (IDP) and the Sequence of Packet Length and Times (SPLT)" to its use of NetFlow. PTX-1417 at 107. ETA was incorporated into all of the accused products in order to implement the functionality of detecting threats in encrypted traffic by using unencrypted portions of those packets. When asked about the functionality employed in the old Stealthwatch technology, Dr. Schmidt asserted that the 2013 version of Stealthwatch was able to detect and stop threats in encrypted traffic without decryption:

> Q. All right. Let's talk a little bit about Stealthwatch. You're saying that Stealthwatch from 2013 is the same as the Stealthwatch from today essentially? Functionally equivalent?
>
> A. I don't think that's quite what I said, but my point was with respect to what Dr. Cole is alleging in his infringement analysis as far as what does the filtering and the determining the filtering and the routing, that the capabilities existed in the prior art version of the accused products to do the same capabilities, **to be able to detect threats in encrypted traffic without decrypting the traffic** as we saw with the botnets, for example; the ability to do other kinds of analysis. I believe his use of the word filtering is inconsistent with the specification, but if that's the way he wants to use it, there were ways to filter information as we saw in the bot net example as well in my testimony yesterday.

Tr. 2110:17-2111-7 (emphasis added). This opinion is directly refuted by Dr. Schmidt's own prior testimony, Tr. 2100:24-2101:18, as well as the technical documents that describe the functionality of Stealthwatch. PTX-383, a Stealthwatch technical guide from 2018, incorporated language that the 2017 ETA solution enabled Stealthwatch as the "first and only solution in the industry that can detect malware in encrypted traffic without any decryption using Encrypted Traffic Analytics." PTX-383 at 355. Dr. Schmidt continually attempts to characterize the ETA solution as enhancing previously existing technology to identify threats in encrypted traffic but cites to no Cisco documents pre-2017 showing that the older Stealthwatch system had the capability to do the same functionality as the ETA solution. The only technical documents that confirm this functionality

are from later than the priority date of the '856 Patent. In this manner, the technical documents affirm that the infringing functionality was added after the priority date of the '856 Patent.

Cisco's press releases from the 2017 timeframe reinforce Centripetal's contentions based on the technical documents. These releases show Cisco considered Encrypted Traffic Analytics as solving a "network security challenge previously thought to be unsolvable." PTX-452 at 648. David Goeckeler, Cisco's senior vice president and general manager of networking and security, highlighted the main advancement as: "ETA uses Cisco's Talos cyber intelligence to detect known attack signatures even in encrypted traffic, helping ensure security while minting privacy." PTX-452 at 648; see PTX-1135. These statements are shown in PTX-1135, a Cisco Press Release from June 20, 2017, reproduced below:

The Network (/home)

Home (/home)

News Release (/Pressreleases)

Cisco unveils network of the future that can learn, adapt and evolve

June 20, 2017



Plaintiff's Trial Exhibit
PTX-1135
Case No. 18-cv-00094-HCM

Designed to be intuitive, Cisco's new network can recognize intent, mitigate threats through encryption, and learn over time, unlocking opportunities

SAN FRANCISCO — June 20, 2017 — Today Cisco unveiled intent-based networking solutions that represent one of the most significant breakthroughs in enterprise networking. The introduction is the culmination of Cisco's vision to create an intuitive system that anticipates actions, stops security threats in their tracks, and continues to evolve and learn. It will help businesses to unlock new opportunities and solve previously unsolvable challenges **in an era of increasing connectivity and distributed technology.**

This new network is the result of years of research and development by Cisco to reinvent networking for an age where network engineers managing hundreds of devices today will be expected to manage 1 million by 2020.

"The network has never been more critical to business success, but it's also never been under more pressure," said Chuck Robbins, chief executive officer for Cisco. "By building a more intuitive network, we are creating an intelligent platform with unmatched security for today and for the future that propels businesses forward and creates new opportunities for people and organizations everywhere."

Today companies are managing their networks through traditional IT processes that are not sustainable in this new age. Cisco's approach creates an intuitive system that constantly learns, adapts, automates and protects, to optimize network operations and defend against today's evolving threat landscape.

"Cisco's Encrypted Traffic Analytics solves a network security challenge previously thought to be unsolvable," said David Goeckeler, senior vice president and general manager of networking and security. "ETA uses Cisco's Talos cyber intelligence to detect known attack signatures even in encrypted traffic, helping to ensure security while maintaining privacy."

With the vast majority of the world's internet traffic running on Cisco networks, the company has used its unique position to capture and analyze this immensely valuable data by providing IT with insights to spot anomalies and anticipate issues in real time, without compromising privacy. By automating the edge of the network and embedding machine learning and analytics at a foundational level, Cisco is making the unmanageable manageable and allowing IT to focus on strategic business needs.

Already, 75 leading global enterprises and organizations are conducting early field trials with these next-generation networking solutions, including DB Systel GmbH, Jade University of Applied Sciences, NASA, Royal Caribbean Cruises Ltd., Scentsy, UZ Leuven and Wipro.

Informed by context and powered by intent

With this new approach, Cisco is changing the fundamental blueprint for networking with reimagined hardware and the most advanced software. This shift from hardware-centric to software-driven networking will enable customers to experience a quantum leap in agility, **productivity** and performance. The intuitive network is an intelligent, highly secure platform — powered by intent and informed by context:

- **Intent:** Intent-based networking allows IT to move from tedious traditional processes to automating intent, making it possible to manage millions of devices in minutes — a crucial development to help organizations navigate today's ever expanding technology landscape.
- **Context:** Interpreting data in context is what enables the network to provide new insights. It's not just the data that's important, it's the context that surrounds it — the who, what, when, where and how. The intuitive network interprets all of this, resulting in better security, more customized experiences and faster operations.
- **Intuition:** The new network provides machine-learning at scale. Cisco is using the vast data that flows through its networks around the world, with machine learning built in, and unleashing that data to provide actionable, predictive insights.

The technologies that power the intuitive network

Cisco Digital Network Architecture (DNA) (http://www.cisco.com/c/en/us/solutions/enterprise-networks/index.html) provides customers with a portfolio of innovative hardware and software to bring the new era of networking to life. Today Cisco is introducing a suite of Cisco DNA technologies and services designed to work together as a single system and empower customers to move at digital speed:

CENTRIPETAL-CSCO 472946

Dr. Schmidt testified to his characterization of these press releases:

> Q. But is it your testimony that Cognitive Threat Analytics was on Stealthwatch in 2013?
>
> A. It was my testimony that Stealthwatch was capable of doing behavioral analytics, enabling it to be able to detect encrypted threat -- encrypted threats -- or threats in encrypted traffic without requiring decryption. That was my testimony when I talked yesterday.
>
> Q. So all these testimony we, all this, the press releases, the documents about Encrypted Traffic Analytics, that's just all marketing puff; it was really not true, they could do it way before then, right?
>
> A. I didn't say it was marketing puff, I said that the capabilities that were added with ETA, Encrypted Traffic Analytics, were very valuable, and the value came from the additional machine learning insights and classification capabilities that were added at that time frame. It was, in fact, possible for them to do it before that, but they were able to do it better now because they've added these additional capabilities.
>
> Q. So when they said they solved the unsolvable problem, they had it solved years before, right?
>
> A. Well, we don't know what the unsolvable problem is from that quote. It could very well have been solving it more precisely or solving it more efficiently or solving it more thoroughly. So the insurmountable or unsolvable problem, I never saw an actual definition of that term, so I'm simply assuming that what they meant was they could do a much better job now that they added these enhancements, but that in no way, shape or form means they couldn't do a good job before.

Tr. 2105:1-2106:4. This characterization by Dr. Schmidt of Cisco's language of "solving the unsolvable problem" as simply an improvement of a previous functionality is insupportable when compared with the technical documents. For all these reasons, Cisco has failed to present clear and convincing evidence that the '856 Patent is invalid for anticipation or obviousness. The prior art does not disclose the functionality to identify encrypted packets and then make determinations based on unencrypted information within those packet headers and flows.

The Court now turns to Cisco's written description argument. To meet the written description requirement, the patentee "must 'convey with reasonable clarity to those skilled in the art that, as of the filing date sought, he or she was in possession of the invention,' and demonstrate that by disclosure in the specification of the patent." Idenix Pharms. LLC v. Gilead Scis. Inc., 941 F.3d 1149, 1163 (Fed. Cir. 2019) (quoting Carnegie Mellon Univ. v. Hoffmann-La Roche Inc., 541 F.3d 1115, 1122 (Fed. Cir. 2008)); see Hynix Semiconductor Inc. v. Rambus Inc., 645 F.3d 1336, 1351 (Fed. Cir. 2011); Ariad Pharms., Inc. v. Eli Lilly & Co., 598 F.3d 1336, 1351 (Fed. Cir. 2010). The hallmark of the written description test is disclosure. Ariad, 598 F.3d at 1351. Therefore, the "test requires an objective inquiry into the four corners of the specification from the perspective of a person of ordinary skill in the art." Id.; see Idenix, 941 F.3d at 1163.

Dr. Schmidt contends that the '856 Patent specification does not disclose any type NetFlow invention and, therefore, the claims fail for lack of written description. He opined that if the claims are infringed for filtering representation of packets, then the Patent is invalid for lack of written description because there is no disclosure of this type of scenario within the specification. Tr. 2067:6-25. The Court disagrees with Dr. Schmidt's conclusion. The specification specifically contains language that a "Packet-filtering system may be configured to correlate packets identified by the packet-filtering system with packets previously identified by packet-filtering system based on data stored in logs." JTX-5 col. 5 ln. 25-30. The specification continues to mention that:

> For example, for one or more packets logged by packet-Filtering system **200** (e.g., the packets comprising the DNS query or the packets comprising the reply to the DNS query), logs **214** may comprise one or more entries indicating one or more of network-layer information (e.g., information derived from one or more network-layer header fields of the packets, such as a protocol type, a destination network address, a source network address, a signature or authentication information (e.g., information from an Internet protocol security (IPsec) encapsulating security payload (ESP)),

> or the like), transport-layer information (e.g., a destination port, a source port, a checksum or similar data (e.g., error detection or correction values, such as those utilized by the transmission control protocol (TCP) or the user datagram protocol (UDP)), or the like), application-layer information (e.g., information derived from one or more application-Layer header fields of the packets, such as a domain name, a uniform resource locator (URL), a uniform resource identifier (URI), an extension, a method, state information, media-type information, a signature, a key, a timestamp, an application identifier, a session identifier, a flow identifier, sequence information, authentication information, or the like), other data in the packets (e.g., payload data), or one or more environmental variables (e.g., information associated with but not solely derived from the packets themselves, such as one or more arrival (or receipt) or departure (or transmission) times of the packets . . .

JTX-5 col. 5 ln. 31-56; see Tr. 3144:3-21. This section of the specification clearly illustrates the '856 Patent invention discloses the logging of certain information from the packets by the packet filtering system. Dr. Jaegar confirmed that viewing this section of the specification as a person skilled in the art would disclose the information required to be used by the packet filtering system. Tr. 3144:3-21. This is the exact type of network information that is contained in NetFlow records. Therefore, looking at the four corners of the '856 Patent's specification, it is evident to a person skilled in the art that the '856 Patent made the required disclosure of the logging of information from packets to be used by the packet filtering system.

Accordingly, the Court **FINDS** that Cisco has not proven by clear and convincing evidence that the '856 Patent was anticipated, obvious or lacked adequate written description.

B. THE '176 PATENT

i. Findings of Fact Regarding Infringement

1. The '176 Patent has been informally known as the "Correlation" Patent.

2. The '176 Patent was issued on January 31, 2017. JTX-3. The '176 Patent was filed on May 15, 2015 as a continuation of application No.14/618,967, giving the '176 Patent a priority date of February 10, 2015. JTX-3.

3. The asserted claims of the '176 Patent are Claim 11 and Claim 21. Doc. 411. Claim 11 and Claim 21 are, respectively, a system and computer readable media claim.

4. Claim 11 is laid out below:

> A system comprising:
>
> at least one processor; and a memory storing instructions that when executed by the at least one processor cause the system to:
>
> identify a plurality of packets received by a network device from a host located in a first network;
>
> generate a plurality of log entries corresponding to the plurality of packets received by the network device;
>
> identify a plurality of packets transmitted by the network device to a host located in a second network;
>
> generate a plurality of log entries corresponding to the plurality of packets transmitted by the network device;
>
> correlate, based on the plurality of log entries corresponding to the plurality of packets received by the network device and the plurality of log entries corresponding to the plurality of packets transmitted by the network device, the plurality of packets transmitted by the network device with the plurality of packets received by the network device; and
>
> responsive to correlating the plurality of packets transmitted by the network device with the plurality of packets received by the network device:
>
> generate, based on the correlating, one or more rules configured to identify packets received from the host located in the first network; and

provision a device located in the first network with the one or more rules configured to identify packets received from the host located in the first network.

5. Claim 11 is identical to Claim 21 in every respect except that Claim 21 is a computer readable media claim. Tr. 885:14-24. Claim 21 modifies the introductory preamble language of Claim 11 replacing "[a] system comprising: at least one processor; and a memory storing instructions that when executed by the at least one processor cause the system to:" with "[o]ne or more non-transitory computer-readable media comprising instructions that when executed by a computing system cause the computing system to:". JTX-3. For purposes of infringement, the parties have treated the two claims as identical.

6. Dr. Moore, an inventor of the '176 Patent, describes the technology of the '176 Patent as the development of a system for identifying malware-infected computers through use of correlation. Tr. 341:3-15.

7. A single communication between two computers on different networks is often broken down into many different segments of packets. Tr. 340:20-341:2. These segments are compared to ascertain if they are a part of the same communications and then the system can make a determination that a computer within the network has been communicating with a computer of a cybercriminal. Tr. 341:3-15. Therefore, the correlation technology in the '176 Patent serves as a method to identify computers in a network that have been infected with malware. Tr. 341:18-19.

8. Centripetal accuses Cisco's Catalyst 9000 series switches, the Aggregation Services Router 1000 series routers and Integration Services Router 1000 and 4000 series routers in combination with Cisco's Stealthwatch of infringing Claims 11 and 21 of the '176 Patent. Tr. 975:19-21.

9. The accused Cisco's switches and routers share the same operating system known as IOS XE. Tr. 448:11-24; 449:19-450:4; PTX-242 at 816, 817.

10. The accused switches and routers contain processors and memory that stores software instructions. Tr. 477:12-478:14, 484:13-485:3; PTX-1303 at 056.

11. The accused Cisco switches and routers contain processors that function to transmit packets across different external and internal networks. Tr. 977:18-21.

12. Cisco has utilized its own proprietary packet logging technology known as NetFlow. Tr. 983:18-25; PTX-1060 at 008.

13. As packets are transmitted, the accused switches and routers generate NetFlow logs, which are summaries of information from the transmitted packets. Tr. 977:18-25; 984:7-13; PTX-1060 at 008. NetFlow includes information such as the source and destination IP address, the source and destination port, and the protocol being used. Tr. 984:7-13; PTX-1060 at 008.

14. The accused switches and routers are capable of generating NetFlow records for packets at both the ingress of the packet into the device and on egress out of the device. Tr. 986:18-987:1; PTX-1060 at 023 (showing that the Catalyst 9400 switch is capable of supporting 384,000 NetFlow entries – 192,000 on ingress and 192,000 on egress); PTX-572 at 762; see Tr. 988:12-22 (Dr. Cole explaining PTX-572 showing "When you configure a flow record, you are telling the device to show all of the flow data traffic that enters" -- which is ingress – "or leaves" -- egress – "the device.").

15. These NetFlow records are sent up to Stealthwatch, which by 2018 was embedded with Cognitive Threat Analytics (CTA) that digests the information from the ingress and egress NetFlow records. PTX-1009 at 009; Tr. 1009:3-14. The new Stealthwatch with CTA also has the functionality to be sent data from proxy sources using another type of logging called Syslog. PTX-

1065 at 005; Tr. 1115:4-116:13 (noting the Stealthwatch "solution uses the Proxy ingestion feature to consume Syslog information . . .") Customers may use either NetFlow or Syslog data or both within Stealthwatch. PTX-1065 at 005.

16. Stealthwatch correlates NetFlow and/or Syslog information sent by devices on the network and correlates the information to provide a detailed overview of all traffic that is occurring on the network. PTX-1065 at 005. CTA, working within Stealthwatch, can leverage the correlations of NetFlow telemetry to detect malicious threats to the security of the network. PTX-1009 at 009; PTX-591 at 522 (using identical language to PTX-1009 in the Stealthwatch Release Notes); see Tr. 997 at 7-12 ("'telemetry' is just another word for the NetFlow log information. So the NetFlow telemetry, the NetFlow logs, these are all synonymous terms, so this is another way of referring to logs").

17. In response to these correlations, Stealthwatch creates a baseline of normal traffic behavior within the network. Based on these normal patterns and known threat indicators, Stealthwatch employs a funnel of analytical techniques to detect advanced threats. PTX-569 at 272; PTX-584 at 402.

18. Stealthwatch, in response to suspicious activity or threats, allows the Identity Services Engine or Stealthwatch Management Console to provision rules to proactively stop that threat. Tr. 1002:13-1003:21; PTX-1089 (showing the use of the Adaptive Network Control ("ANC") to implement rules). The ANC operates by applying new policies and changing individual user's authorization on the network according to rules and policies configured by the Identity Services Engine in response to correlated threats on the network. PTX-595 at 179; Tr. 1005:10-19. Both the Identity Services Engine and the Stealthwatch Management Console operate in this fashion. Tr. 1006:19-1007:5. PTX-989.

ii. Conclusions of Law Regarding Infringement

Based on the Court's factual findings, Centripetal has proven by a preponderance of the evidence that Cisco's Catalyst 9000 series switches, the Aggregation Services Router 1000 series routers and Integration Services Router 1000 and 4000 series routers in combination with Cisco's Stealthwatch literally **INFRINGE** Claims 11 and 21 of the '176 Patent. Cisco's expert on the '176 Patent, Dr. Kevin Almeroth:

> was asked to offer opinions, after performing an analysis, on noninfringement as it related specifically to the '176 patent; similarly, to offer opinions about whether or not the '176 patent was valid; and then several additional opinions relating to the benefits of the patent, technical issues related to damages, and then also copying, to the extent it still exists in this trial.

Tr. 2212:12-18. Dr. Almeroth advanced two non-infringement theories. Tr. 2239:17-2240:14. First, that the accused system does not correlate a plurality of transmitted packets with a plurality of received packets as required by the asserted claims of the '176 Patent. Tr. 2247:18-2248:4. Second, that the accused system does not generate and provision rules in response to those claimed correlations. Tr. 2247:18-2248:4.

Turning to the first theory, Dr. Almeroth opined that Dr. Cole's infringement opinion relied on the systems' use of logs provided by Cisco's proprietary logging technology, NetFlow, as the logs outlined by the claim language. Dr. Almeroth construed the claims to require identification and generation of logs out of the same network device on ingress and egress. Therefore, Dr. Almeroth avers that the Cisco system cannot infringe, because in his opinion, the accused switches and routers do not generate NetFlow on both ingress into a device and egress out of one network device. Tr. 2249:4-18. Cisco's technical documents refute Dr. Almeroth's conclusion.

Dr. Cole pointed directly to PTX-1060, a Cisco technical document dated December of 2017, showing that the Catalyst switches have the ability to export NetFlow on ingress and egress.

Tr. 986:18-987:1; PTX-1060 at 023 (showing that the Catalyst 9400 switch is capable of supporting 384,000 NetFlow entries – 192,000 on ingress and 192,000 on egress). Dr. Almeroth, on cross-examination, even admitted that the accused switches and routers can be configured to export ingress and egress NetFlow.

> Q. Isn't it correct, Dr. Almeroth, that this Cisco document says right here that MPLS Egress and NetFlow Accounting feature can be used -- being use to capture ingress and egress flow statistics for router B, one device. Is that correct?
>
> A. That's what it says. But my last answer was qualified for Stealthwatch. This document, at least what you're pointing me to here, does not mention Stealthwatch. And that was really my whole point: That you can certainly configure NetFlow ingress and egress, but when you get to troubleshooting Stealthwatch, it's considered an error within Stealthwatch.

Tr. 2286:10-19. In this exchange, Dr. Almeroth confirms that NetFlow can be configured on ingress and egress but shifts the crux of his non-infringement opinion to the fact that Stealthwatch produces an error based on producing both types of NetFlow. To support that claim, Dr. Almeroth relied solely on the presentation of source code from the 6.5.4 version of Stealthwatch that operated without enhanced NetFlow or the integration of Cognitive Threat Analytics (CTA). Tr. 2287:1-19; see DTX-1616 (showing source code from a previous 6.5.4 version of Stealthwatch that is not accused by Centripetal). He cites to no technical document that confirms that the accused/current version of Stealthwatch produces an error when exporting both ingress and egress NetFlow. In fact, the technical release notes for CTA, which was incorporated into Stealthwatch in 2018, support that CTA produced the ability for the correlation of NetFlow telemetry. PTX-1009 at 009.

Dr. Cole, in his infringement opinion on the "identify and generate" elements, relied on a similar claim scope as Dr. Almeroth to show that the claims required that one network device generate logs on a packets' ingress and egress out of the device. Moreover, Dr. Cole does not explicitly limit his construction of the asserted claims to the limitation of only ingress and egress

out of one device. The Court **FINDS**, based on the testimony and technical documents, that the accused switches and routers do identify and generate logs on ingress and egress. However, a look at the specification of the '176 Patent informs the Court that this is not the only construction that would infringe the asserted claims. These claim elements would also be met if there was identification, generation and correlation of logs from two different network devices on either ingress or egress. Column 8 line 46 of the specification highlights that:

> At step **16,** packet correlator **128** may utilize log(s) **142** to correlate the packets transmitted by network device(s) **122** with the packets received by network device(s) **122.** For example, packet correlator **128** may compare data in entry **306** with data in entry **312** (e.g., network-layer information, transport-layer information, application-layer information, or environmental variable(s)) to correlate **Pl'** with **Pl** (e.g., by determining that a portion of the data in entry **306** corresponds with data in entry **312).** Similarly, packet correlator **128** may compare data in entry **308** with data in entry **314** to correlate **P2'** with **P2,** packet correlator **128** may compare data in entry **310** with data in entry **316** to correlate **P3'** with **P3,** packet correlator **128** may compare data in entry **318** with data in entry **324** to correlate **P4'** with **P4,** packet correlator **128** may compare data in entry **320** with data in entry **326** to correlate **PS'** with **PS,** and packet correlator **128** may compare data in entry **322** with data in entry **328** to correlate **P6'** with **P6.**

JTX-3 col. 8 ln. 46-63. This section of the specification indicates that the network device that generates the correlated logs may be plural as well as singular. Additionally, this section is showing the correlation may occur between data entries that were processed through two different network devices. Compare JTX-3 col. 8 ln. 46-63 with JTX-3 Fig. 3. Dr. Almeroth, on cross examination, confirms that the use of "a network device" in the claim language may mean more than one network device:

> Q. And then you said this had to be a single network device, correct?

A. Not quite. It says a network device here, and then later it's the network device. So it's the same network device across the limitations.

Q. But you do understand that in a patent, when it says A, it can mean one or more; is that correct?

A. That's my understanding.

Q. So this could be more than one network device, correct?

A. It could be.

Tr. 2278:11-20. Therefore, even if the Court were to accept Dr. Almeroth's conclusion that the accused devices do not process ingress and egress out of the same device, it would still find infringement on the basis that the Cisco system correlates logs between multiple devices within the network on either ingress or egress.

Moreover, Dr. Almeroth states that the accused system does not generate and provision rules in response to correlation performed as a result of Stealthwatch and CTA. Dr. Almeroth admits that Stealthwatch with CTA performs correlations, just not those required by the claim language. In explaining the diagram of PTX-1065, Dr. Almeroth opined:

Q. Can you explain what's going on here, Dr. Almeroth?

A. Yes. What's being shown here, if you start in the bottom, it shows two different sources of information that ultimately get correlated. There's proxy data and there's NetFlow data. And when Dr. Cole testified, he represented that that NetFlow data included ingress and egress records from the same device, which was actually not the case, as the evidence and the correct operation of the devices show. And then from there, his analysis principally turned on the fact that these documents describe correlation. They absolutely use the word correlation, but it's not the correlation of the type required by the claims. And the example that's shown in this particular figure and what's described in the text below is that you're correlating NetFlow data, which is not the NetFlow data required by the claim for the reasons I've given, with other data. In this case, proxy data. And so even though these documents use the word correlate, what they're correlating is not the kind of correlation that's required by the claims.

Q. Okay. And if we look, Mr. Simons, at the text below?

BY MR. JAMESON:

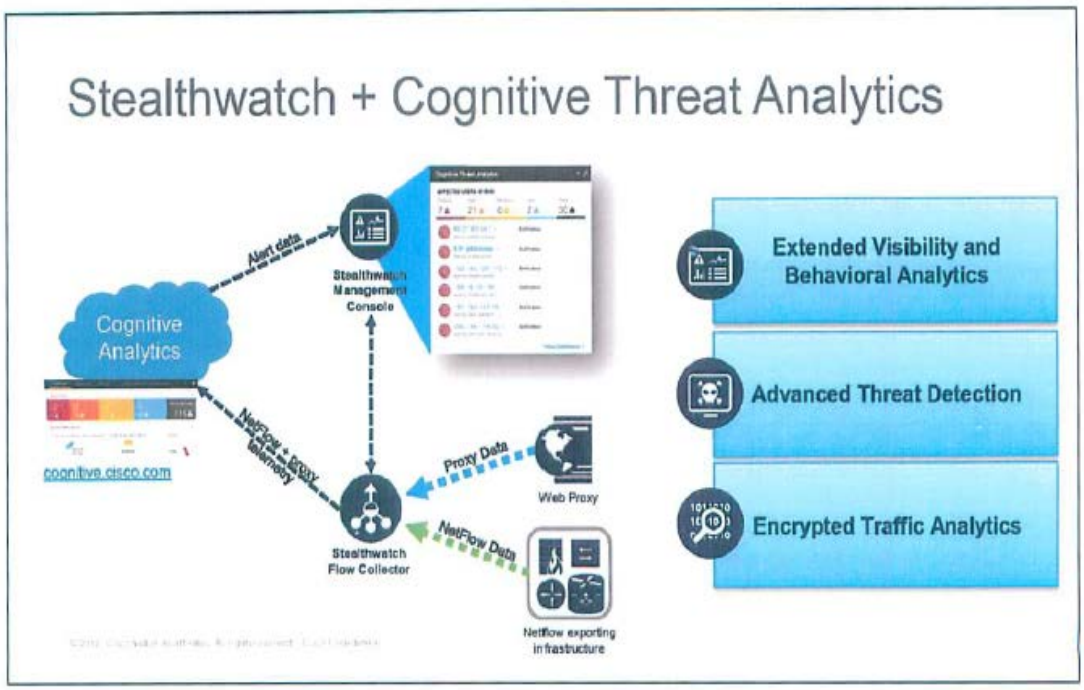
Q. And I don't want to go through all of this, but is the same point made in the text below with respect to the comments you made, about the diagram?

A. Yes. It's absolutely the case that Stealthwatch correlates I think what we've referred to as threat intelligence with NetFlow records. But what it is not comparing, what it is not correlating is it's not correlating the NetFlow records to themselves as required by the elements of the claims, because it tries to block or double count those NetFlow records. And so all of this evidence that Dr. Cole relied on that uses the word correlate, over and over again it describes correlation of threat intelligence with NetFlow data, which is not what the claim requires and also is not what the '176 patent is about.

Tr. 2256:3-2257:10.

PTX-1065

Cisco Technical Presentation Involving Operation of Stealthwatch in Combination with CTA in November 2017



Stealthwatch integrates with Cognitive Analytics ("CA" - aka Cognitive Threat Analytics). This involves the addition of a new information panel on the SMC's WebUI, and enhances Stealthwatch further by leveraging CA's cloud based analytics engine, that correlates threat behaviors seen in the enterprise with those seen globally. It uses machine learning and statistical modeling to learn from what it sees and adapt to changing network behavior over time.

The Court agrees with Dr. Almeroth's assessment that Stealthwatch correlates NetFlow and Syslog information with global threat indicators. PTX-202 states that Stealthwatch "correlates local traffic models with global threat behaviors to give you rich threat context around network traffic . . . and applies encrypted traffic analytics to enhance NetFlow analysis." PTX-202 at 242. Therefore, it is clear that Stealthwatch uses the NetFlow information within the network to correlate those records to global threat indicators. However, this is not the only use of correlation that Stealthwatch uses in its operation. In order to make use of behavioral analytics, Stealthwatch correlates NetFlow that passes through network devices to create a baseline of normal types of traffic that would pass through the network. This correlation occurs between both NetFlow and other logs provided to Stealthwatch in the form of WebFlow telemetry through the use of Syslog. Therefore, along with matching threats to global threat indicators, Stealthwatch can also detect threats based on abnormal activity that occurs within the network. For example, a large amount of data being transported throughout the network at a time where an office is closed or not conducting business would send up an alert that something malicious may be afoot.

Cisco's technical guide for configuring Netflow and Stealthwatch, PTX-569, illustrates how Stealthwatch "[c]reates a baseline of normal behavior" and "correlates threat behaviors seen in the local environment with those seen globally."

PTX-569

Cisco Technical Guide for Configuring and Troubleshooting NetFlow for Cisco Stealthwatch from 2018*

Doc type
Cisco public

Stealthwatch Enterprise also integrates with a cloud based multi-stage machine learning analytics engine, that correlates threat behaviors seen in the local environment with those seen globally. It employs a funnel of analytical techniques to detect advanced threats.

Figure 3: Detect anomalies and threats



For more information about the Stealthwatch components and architecture, please refer to the Stealthwatch Enterprise Data Sheet.

*The heading in the blue box above states 'Collect and analyze telemetry'.

PTX-569 at 272. This process would require Stealthwatch to correlate NetFlow within the network between multiple devices in order to recognize normal traffic patterns within the network.

Accordingly, it is axiomatic that Stealthwatch could then provision rules to stop threats that are detected based on internal network NetFlow correlation with or without global threat indicators. PTX-595 at 179. Therefore, the Court **FINDS** by a preponderance of the evidence that

Stealthwatch performs the exact type of correlation and provisioning of rules in response to correlations required by the '176 Patent.

iii. Findings of Fact Regarding Validity

19. The priority date of the '176 Patent is February 10, 2015. JTX-4.

20. Sometime in 2012 or 2013, Cisco released and marketed a system known as the Cyber Threat Defense Solution. This system was a collection of Cisco switches and routers, the Identity Services Engine and Lancope's Stealthwatch. Compare Tr. 2430:1-3; DTX-311 with Tr. 2485:5-10; DTX-664 at 004.

21. Cisco asserts its Cyber Threat Defense Solution, using an older version of Stealthwatch, as the prior art that renders the '176 Patent invalid. DTX-311; DTX-312; DTX-343; DTX-463 (All documents from pre-2017).

22. The asserted prior art system leverages Cisco networking technology, including NetFlow, Identity Services Engine, and Stealthwatch. The Stealthwatch version asserted as prior art is version 6.5.4. Tr. 2344:22. This version of Stealthwatch incorporated Stealthwatch Labs Intelligence Center ("SLIC") threat intelligence information, which contained human collected threat indicators. Tr. 3153:14-19; DTX-312 at 001.

23. Old Stealthwatch was able to automatically respond to alarms generated by worms, viruses and internal policy violations. DTX-463 at 014 (noting Stealthwatch responds to alarms). There is no indication in the pre-2017 documents that Stealthwatch issued rules in response to correlations of NetFlow.

24. Cisco Stealthwatch incorporated Cognitive Threat Analytics in Stealthwatch in 2017. Tr. 2342:6-7. In version 7.0.0 of Stealthwatch released in 2019, CTA was improved with

the ability to leverage threat detection from the analysis of WebFlow, produced by Syslogs, and NetFlow telemetry by correlating the data. PTX-1893 at 011.

25. In response to these correlations, new Stealthwatch creates a baseline of normal traffic behavior within the network. Based on these normal patterns and known threat indicators, Stealthwatch, using CTA, employs a funnel of analytical techniques to detect advanced threats. PTX-569 at 272; PTX-584 at 402 (post-2017 documents).

26. Stealthwatch, in response to suspicious activity or threats, allows the Identity Services Engine or Stealthwatch Management Console to provision rules to proactively stop that threat. Tr. 1002:13-1003:21; PTX-1089 (showing the use of the Adaptive Network Control ("ANC") to implement rules). The new ANC, which replaced the old quarantine functionality, operates by applying new policies and changing individual user's authorization on the network according to rules and policies configured by the Identity Services Engine in response to correlated threats on the network. PTX-595 at 179; Tr. 1005:10-19. Both Identity Services Engine and the Stealthwatch Management Console operate in this fashion. Tr. 1006:19-1007:5.

iv. Conclusions of Law Regarding Validity

Dr. Almeroth opined that the '176 Patent is invalid for anticipation, obviousness, and based on written description. Turning first to obviousness, Dr. Almeroth averred, by using Dr. Cole's testimony, that all of the infringing functionality of the Cisco products is present in the prior art, particularly the Cisco Cyber Threat Defense System. Tr. 2304:9-20. Specifically, Dr. Almeroth contended that prior to the priority date of the '176 Patent, Stealthwatch was able to "raise alarms, and then be able to generate and provision rules [based on] the routers and switches exporting NetFlow in combination with Stealthwatch." Tr. 2305:2-5. The Court disagrees with Dr. Almeroth's characterization.

Dr. Jaegar, Centripetal's validity expert in his rebuttal testimony, highlights that the prior art confirms that the old Stealthwatch system is designed as a visibility system allowing administrators to view traffic in the network:

> Q. How do they characterize the old Stealthwatch Management Console?
>
> A. Well, I would characterize the old Stealthwatch systems, Stealthwatch Management Console, or SMC as its shown here, as the core visibility component of the old Stealthwatch system. This is the component that does the showing of information about flows in your network. And as you can see in the bottom paragraph, it talks about administrators, and so this SMC or Stealthwatch Management Console is designed for administrators to be able to look at what's going on in their networks.

Tr. 3152:13-22. The technical documents, from 2014, confirm Dr. Jaegar's opinion highlighting that [t]he Stealthwatch system by Lancope is a leading solution for network visibility and security intelligence . . . ." PTX-343 at 001. Stealthwatch operates by providing "in-depth visibility and security context needed to thwart evolving threats . . . [and] quickly zooms in on any unusual behavior, immediately sending an alarm to the SMC . . . ." PTX-343.

Additionally, the old Stealthwatch operated in response to these alarms. Dr. Jaegar opined:

> Q. Could you give us your memory of Dr. Almeroth's testimony and why you disagree with it?
>
> A. My recollection is that he was saying that this shows that this adaptable mitigation that's responsive to alarms, this would satisfy the responsive to correlation limitation.
>
> Q. And why do you disagree with his interpretation of this?
>
> A. Well, it specifically says in the first sentence that "Lancope customers can direct the Stealthwatch appliance to automatically respond to alarms generated by worms, viruses and internal policy violations." And so this indicates that the, any -- any addition or automation or -- well, activation, I guess is the word I'm looking for -- of these mitigation actions in the old Stealthwatch system is done in response to alarms being triggered and not in response to correlation of logs as is required by the claims. And my understanding is that previous inter partes reviews found that technology that only discloses being responsive to alarms rather than responsive to

> correlation of log entries as required by the claim elements, that doesn't satisfy the responsive to correlation claim element.

Tr. 3154:6-25; see DTX-463 at 014. The post-2017 documents illustrate that the generation of rules responsive to correlations was an added functionality with the addition of CTA into Stealthwatch. The release notes for Version 7.0.0 of Stealthwatch, PTX-1893, contain a section titled "What's New" which shows the additions made to Stealthwatch in this version. PTX-1893 at 011. In this section, the technical document indicates that "CTA can now leverage detections from the analysis of WebFlow telemetry to improve the efficacy of analyzing NetFlow telemetry from Stealthwatch. This is accomplished by the system through correlation of both telemetry types." PTX-1893 at 011 (a technical document from 2019 showing this type of correlation is an enhancement to the Cognitive engine). Cisco identifies that this technology increases the number of both confirmed and detected threats in the network. Id. Cisco's presentation on the incorporation of CTA into Stealthwatch shows that the technology "uses the Proxy ingestion feature to consume Syslog information sent from proxy sources . . . [and] then correlate the received syslog and relates it to the flows collected from network devices before and after the proxy . . . ." PTX-1065 at 005 (November 2017 document). This same document highlights that "[b]ringing CTA and Stealthwatch detection together gives us unique ability to combine our local and global detection capabilities." Id. In response to the local correlations of WebFlow and NetFlow, new Stealthwatch can provision Adaptative Network Control policies based on the identification of behavioral anomalies. See PTX-569 at 272; PTX-595 at 179 (a technical document from 2019 showing how "ANC policies have replaced the previous quarantine and unquarantine feature"). Accordingly, Cisco has failed to present clear and convincing evidence that the "correlate" and "responsive to" functionality was in the Cisco prior art system. Therefore, the prior art does not render the asserted claims anticipated or obvious.

Switching to Cisco's argument regarding written description. Dr. Almeroth opined that the specification does not disclose to a person skilled in the art that the inventors were in possession of the invention that is covered by the scope of the claims that is alleged in Centripetal's infringement allegations. Tr. 2333:2-8. He avers that the '176 Patent is invalid because the specification of the '176 Patent contains no description of Cognitive Threat Analytics, machine learning, artificial intelligence, integrating threat feeds, or NetFlow. Tr. 2333:22-2334:12. The Court **FINDS** that both the challenged "correlate" and "responsive to" claim elements are adequately disclosed in the specification to meet the written description requirement.

Dr. Jaegar opined that a person skilled in the art would be able to look at column 8, lines 46 through 63 of the '176 Patent specification and determine that the invention "utilize[s] logs to correlate packets transmitted by one or more network devices with packets received by one or more network devices." Tr. 3155:16-18; see JTX-3 at col. 8 ln. 46-63. Additionally, for the "responsive to" element, Dr. Jaegar points to column 12, line 55 through column 13, line 13. This section of the specification clearly shows that the invention identifies hosts associated with malicious entities and communicates messages identifying that host. JTX-3 at col. 12 ln. 55 – col. 13 ln. 13. Further, the specification notes that this process occurs in response to the correlation of data, as described in column 8, lines 46 through 63 of the specification. Tr. 3156:9-3157:14. Based on these sections of the specification, the Court finds that a person skilled in the art would have been in possession of the invention at issue.

Accordingly, the Court **FINDS** that Cisco has not proven by clear and convincing evidence that the '176 Patent was anticipated, obvious or lacked sufficient written description.

C. THE '193 PATENT

i. Findings of Fact Regarding Infringement

1. The '193 Patent was informally known throughout the trial as the "Forward or Drop / Exfiltration Patent." Tr. 2356: 2-6.

2. The '193 Patent was issued on June 20, 2017. JTX-4. The '193 Patent was filed on February 18, 2015 as a continuation of application No.13/795,882, giving the '193 Patent a priority date of March 12, 2013. JTX-4.

3. The asserted claims of the '193 Patent are Claims 18 and 19. Doc. 411. Claims 18 and 19 are, respectively, a packet filtering system and computer readable media claim.

4. Claim 18 is laid out below:

> A system comprising:
>
> at least one processor; and
>
> a memory storing instructions that when executed by the at least one processor cause the system to:
>
> > receive, from a computing device located in a first network, a plurality of packets wherein the plurality of packets comprises a first portion of packets and a second portion of packets;
> >
> > responsive to a determination that the first portion of packets comprises data corresponding to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network, wherein the data indicates that the first portion of packets is destined for the second network:
> >
> > apply, to each packet in the first portion of packets, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and drop each packet in the first portion of packets; and
> >
> > responsive to a determination that the second portion of packets comprises data that does not correspond to the criteria, wherein the data indicates that the second portion of packets is destined for a third network:

> apply, to each packet in the second portion of packets, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, a second operator configured to forward packets not associated with the particular type of data transfer toward the third network; and
>
> forward each packet in the second portion of packets toward the third network.

JTX-4.

5. Claim 19 is identical to Claim 18 in every respect except it is a computer readable media claim. Claim 19 substitutes the introductory language of Claim 18, "A system comprising: at least one processor; and a memory storing instructions that when executed by the at least one processor cause the system to . . .", with "[o]ne or more non-transitory computer-readable media comprising instructions that when executed by one or more computing devices cause the one or more computing devices to: . . . ." JTX-4; see Tr. 472:21. For purposes of infringement, the parties treated Claims 18 and 19 the same.

6. Dr. Sean Moore, one of the inventors of the '193 Patent, testified that the technology claimed in the patent centered around preventing the exfiltration of confidential data by cyber criminals. Tr. 343:14-16.

7. Centripetal's expert, Dr. Mitzenmacher, defined the asserted claims of the '193 Patent as being related to the process of forwarding and dropping packets related to preventing exfiltrations. Tr. 465:18-21. Additionally, Dr. Mitzenmacher opined that the '193 Patent applies to the prevention of many different types of data exfiltration. Tr. 467:14-468:17.

8. As previously noted, exfiltration can occur in the context of cyber criminals hacking into the network and stealing data, but it also can occur within networks internally. For example, within one large corporate network there are many different departments or subnetworks, such as finance and human resources. See Tr. 490:17-25. It is common within these multi-departmental

companies that certain departments have access to confidential materials, while for others that access is restricted.

9. Accordingly, the network must restrict the ability of packets with this sensitive information to travel to unauthorized internal departments and external networks, while also allowing packets with no sensitive information to be freely transmitted to other employees within the network. Tr. 467:14-468:17. Therefore, the '193 Patent specifically identifies a process by which rules can be enabled to filter packets of data depending on the type of data transfer that is being transmitted throughout the network. Tr. 468:21-469:9.

10. Centripetal accuses Cisco's Catalyst 9000 series switches, the Aggregation Services Router 1000 series routers and Integration Services Router 1000 and 4000 series routers of infringing Claims 18 and 19 of the '193 Patent. Tr. 433:20-434:1.

11. The accused Cisco's switches and routers share the same operating system known as IOS XE. Tr. 448:11-24; 449:19-450:4; PTX-242 at 816, 817.

12. Cisco compiles the source code that operates the accused switches and routers in the United States. Tr. 462:5-463:18, 464:4-14; PTX-1409 at 5-6.

13. The accused switches and routers contain processors and memory that stores software instructions. Tr. 477:12-478:14, 484:13-485:3; PTX-1303 at 056. One of the processers within the accused Cisco devices are programmable Applied Specific Interred Circuits ("ASIC"), known as Unified Access Data Planes ("UADP"). Tr. 477:24-478:5; PTX-1262 at 994. This type of processer is commonly referred to as a UADP ASIC. Tr. 477:24-478:5; PTX-1262 at 994; PTX-1390 at 029.

14. In their operation, the processors work within the accused Cisco switches and routers to receive and transmit packets across a network. PTX-1276 at 216 (2011 Cisco

document); Tr. 488:1-489:3. During the transmission of packets, the operating system ("IOS XE"), working in conjunction with UADP ASICs, apply a variety of different rules to packets to determine if the packet should be permitted or dropped. PTX-1276 at 215-16.[5]

15. Access Control Lists ("ACL") are often applied to packets on ingress into the device and egress out of the device. PTX-1276 at 215-16. To simplify the process of applying rules, Cisco's IOS XE utilizes a specific method where labels are applied to packets based on their source or destination. These labels are known as Secure Group Tag / Scalable Group Tag ("SGT").[6] Tr. 494:12-24; see PTX-1276 at 211.

16. SGTs are attached to categorize packets into different numerical groupings based on information such as the packet's source IP, destination IP and/or both. PTX-1280 at 021. SGT can also be based on other information that is included in the 5-tuple, such as source port, destination port and protocol. Tr. 2400:24-25 (Dr. Crovella, Cisco's expert witness, highlighting that a quarantine rule has the ability to look at all information in the 5-tuple), 2404:4 ("[t]he quarantine rule only looks at the 5-tuple…").

17. As packets enter the switch and router, they perform an initial check to see if there is a specific source SGT attached to each packet that is entering through the switch or router. Tr. 2421:2-8.

18. After the initial check, the switch and/or router applies an initial collection of rules known as a Group Access Control List ("GACL"). A Security Group ACL ("SGACL") is an

[5] The technical document for the switch and router operating system shows that the switches and routers support the application of multiple different ACL rule sets including: Port ACL ("PACL"); Vlan ACL ("VACL"); Router ACL ("RACL"); Client Group ACL ("CGACL"); Security Group ACL or Role Based ACL ("SGACL or RBACL"). PTX-1276 at 215.

[6] Cisco's non-infringement expert, Dr. Crovella, confirmed that Secure Group Tag and Scalable Group Tag are in fact the same. Different names are being used at different times because of a marketing change. Tr. 2420:17.

example of a GACL that blocks or permits packets specifically based on SGTs. Tr. 2389:1-3. PTX-1276 at 215-16; see Tr. 2423:9-15.

19. On a packet's ingress into the device, the switch and/or router applies an input SGACL based upon the SGT associated with the source of where the packet was transmitted from. Tr. 2389:1-8; see PTX-1288 at 012 (showing input GACL applied based on ingress client); see also PTX-1276 at 216; PTX-1390 at 86 (2019 document).

20. On a packet's egress out of a device, the switch and/or router applies an output SGACL based upon the SGT associated with the source, and drops or transmits packets based upon the destination of the packets. Tr. 2389:15-19; see PTX-1288 at 012 (showing output GACL applied based on egress client); see also PTX-1276 at 216; PTX-1390 at 86 (2019 document).

21. Cisco's expert, Dr. Crovella, confirms that SGACLs are applied on a packet ingress into the switch and/or router and applied on a packet's egress out of the router and/or switch. Tr. 2389:15-19, 2399:22; PTX-1288 at 012.

22. This SGACL rule-based packet blocking by comparing SGTs is more commonly referred to by Cisco as the quarantine rule. Tr. 2383:12-19, 2423:9-15 (Dr. Crovella noting that other ACLs besides the SGACL are not accused).

23. The quarantine rule operates to block or allow packets that are being transmitted throughout the network. Tr. 494:3-495:14, 496:17-497:13, 536: 24-25, 2419:3-15; see PTX-1262 at 999.

24. The switch and/or router determines whether the packet should be permitted or blocked based on the SGT assigned to that particular source. Tr. 535:10-17; PTX-1280 at 21; see PTX-1262 at 999. This process is completed by the switch and/or router by applying operators,

such as permit or deny, to incoming and exiting packets based upon their assigned SGT. Tr. 531:18-21; PTX-1280 at 021. 22.

25. If a packet's SGT is not correlated to a SGACL rule on either ingress or egress, then a permit operator is applied to the packet, and it is permitted to be transmitted through the router or switch on to its destination. Tr. 542:17-24; PTX-1288 at 012. But if an SGT matches one of the SGACL rules because of an unpermitted source or destination, a deny operator is applied, and subsequently the packet will be blocked. Tr. 545:8-546:12, 548:11-19; PTX-1288 at 012.

26. In their presentation of evidence, Cisco has failed to cite any technical document produced post June 20, 2017. Cisco relies on ex post facto animations which were designed for litigation, and do not accurately portray the current functionality of the accused products.

27. Cisco has not called any witness who authored any of the Cisco technical documents relied upon by Centripetal in their infringement case.

ii. Conclusions of Law Regarding Infringement

Based on the Court's factual findings, Centripetal has proven by a preponderance of the evidence that the Cisco's Catalyst 9000 series switches, the Aggregation Services Router 1000 series routers and Integration Services Router 1000 and 4000 series routers literally **INFRINGE** Claims 18 and 19 of the '193 Patent. Cisco's expert on the '193 Patent, Dr. Mark Crovella testified:

> I was asked to consider whether the '193 patent was infringed by the accused Cisco technology, I was asked whether it should be considered valid in light of the prior art, and I was also asked about potential damages if we were to assume that it were valid and infringed, whether there were significant benefits over the prior art.

Tr. 2349:18-24. Dr. Crovella advanced two theories in his non-infringement opinion. First, that the function which is referred to as a "quarantine" blocks all traffic from a source computer and does not block a "particular data transfer," as required by the language in the claim. Second, he

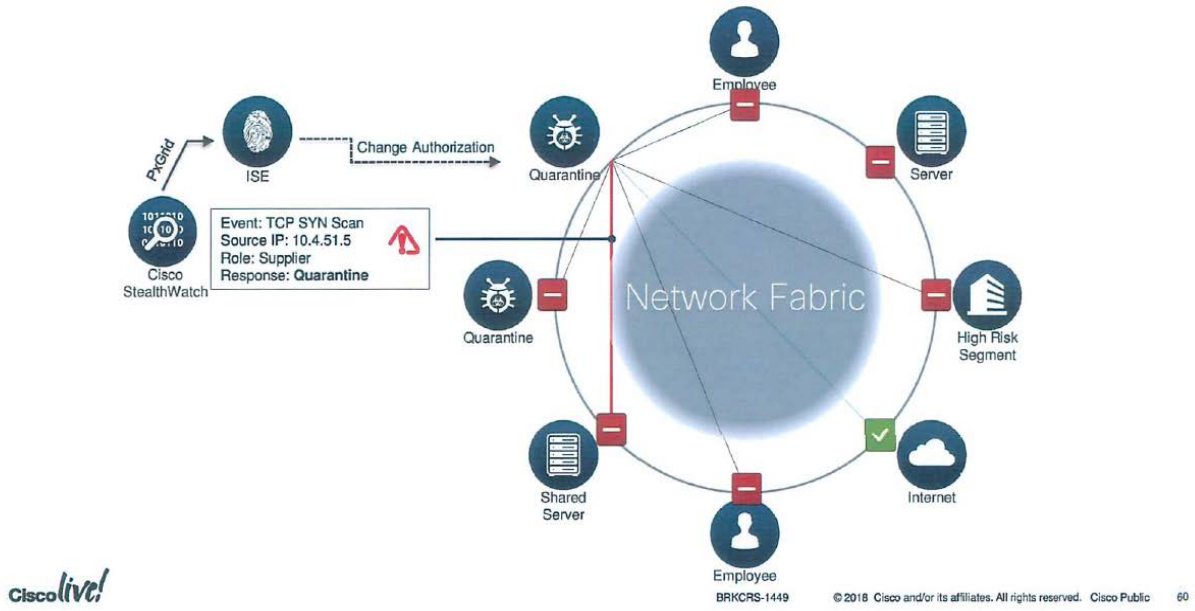
averred that Stealthwatch, using NetFlow, cannot identify exfiltrations until it is too late to drop the packet.

As to the first theory, Dr. Crovella admits on cross examination to the "two stage" process. This testimony, coupled with Cisco's technical information from PTX-1284 and PTX-1326, prove that the accused switches and routers have been aided with Cisco's Identity Services Engine to measure the vulnerability level of individual network risk and assign roles to certain devices based on this analysis. Walking through the operation of the accused products illustrates that the Cisco system operates in a two-stage process that meets the functionality required by the asserted claims.

The Cisco packet-filtering system operates by using the Identity Services Engine to assign certain endpoint devices "roles" that determine what type of packets may be sent and/or received by that specific endpoint computer. PTX-1326. Therefore, the Identity Services Engine has the ability to monitor levels of vulnerabilities based on the packets that are being transmitted by switches and routers in the network, and to adjust the permissions based on real-time network operations. As a general example, the Cisco system operates by limiting a computer located in a first network from accessing sensitive data in a protected network, while simultaneously allowing unsensitive data to be accessed. In this manner, packets from the computer in the first network may be allowed to access unprotected resources on the larger internet, but would be restricted from transmitting packets containing secure information. This is shown by Cisco's technical demonstration, PTX-563:

PTX-563

Cisco Technical Presentation on Rapid Threat Containment from 2018



The accused switches and routers are the specific network devices used to institute this packet filtering system. In their operation, the accused products receive different portions of packets from a first computing network. PTX-1276 at 216. Upon entry into an accused device, each packet is assigned a Scalable/Security Group Tag ("SGT"). The SGT that is attached to each packet is based on the role and/or privileges that is assigned to that specific endpoint computer. Therefore, SGTs, at their most basic level, are assigned to packets based on where the packet is being transmitted from and/or the destination of the transmitted packet. In this manner, the 5-tuple information in the header of the packet, such as the source of the packet's origin and/or the destination to which it is being transmitted, is the operative data being used to determine the packet's SGT. This assignment of SGT to packets as they enter the switch or router is the first step in the operation of the quarantine process.

After SGT attachment, the switches and routers execute the second stage. The accused devices utilize specialized rules, known as SGACLs, that deal specifically with forwarding and dropping packets based on what type of SGT is attached to the packet. SGACLs are applied to packets on both ingress in and egress out of switch and/or router. See PTX-1390 at 86. On ingress, the device looks at the SGT that is associated with the source of the packets. This application of SGACLs by the device determines whether packets are allowed to be transmitted by this specific SGT. If packets are allowed to be transmitted by the specific SGT, the packets are permitted into the device where the packets would be subject to another set of SGACLs on egress. On egress, different SGACLs are applied based on the packet's destination. Egress SGACLs determine if packets associated with this SGT can be sent to the specific destination.

Centripetal's expert, Dr. Mitzenmacher, used PTX-1326 to confirm that Cisco's quarantine rule operates with this rule-based blocking functionality. Moreover, technical documents, such as Cisco's Rapid Threat Containment Guide, confirm that switches and routers are programmed to "manually or automatically change your user's access privileges when there's suspicious activity, a threat or vulnerabilities discovered." Tr. 527:4-17; PTX-1326 at 011. Accordingly, the accused Cisco system attaches SGT to packets, and then uses the SGACL quarantine functionality within the switches and/or routers to contain malware infected computers by blocking "access to critical data while their users can keep working on less critical applications." PTX-1326 at 011. Thus, the Cisco system operates by blocking packets affiliated with a particular type of data transfer to a protected resource, while allowing packets unaffiliated with a protected type of data transfer to be transmitted to their final destination. In this manner, the technical documents confirm that the accused products utilize "packet filtering-rules" that operate to prevent "a particular type of data

transfer" from a first to second network. This functionality is shown by text and diagram included in Cisco's technical document that outlines the operation of the quarantine feature:

PTX-1326

Cisco Identity Services Engine Technical Ordering Guide from August 2019

With integrated network access control technology, you can manually or automatically change your users' access privileges when there's suspicious activity, a threat, or vulnerabilities discovered. Devices that are suspected of being infected can be denied access to critical data while their users can keep working on less critical applications.

1.6.2 How does Rapid Threat Containment work



See PTX-1326 (showing infected endpoints can be denied access to certain types of data while being allowed access to other types of data).

This functionality confirms the accused devices operate in the "two-stage" process outlined by both the claims and the specification of the '193 Patent. The accused products perform a two-stage process by first assigning SGT to packets, based upon the source and/or destination of the packets, and then applies different "operators" or functions, such as permit/deny, to those packets based on the associated packet SGT. Cisco's infringement expert, Dr. Crovella, on cross

examination confirmed that the accused products perform all the functionality required to infringe the claims:

> Q. . . .So we have multiple steps. First, the SGT tag is checked to see if it's present, right?
>
> A. That's right.
>
> Q. Then, if the SGT tag is present and it says, "quarantine," then a quarantine policy is applied, correct?
>
> A. That's right.
>
> Q. If the quarantine policy is applied, you check the destination, and if the destination is a protected resource in which it says, do not allow this packet to go there, it will prevent the data transfer from going to that destination, correct?
>
> A. That is, in fact, the quarantine policy. In other words, there's not two steps there. A quarantine policy is, in fact, checking the destination.
>
> Q. Okay. And if it says, block the packet, it will be prevented from the data transfer going there, right?
>
> A. That's right.
>
> Q. If it's not in there, and if there is a – it's able to go through to a permitted network or permitted resource, then the packet would be allowed to go through by the switch or the router. Isn't that right?
>
> A. That's right.

Tr. 2423:19-2424:15; see PTX-563; PTX-1326. Dr. Crovella even concedes that the '193 Patent requires a device to "block some communication between the two networks but allow other communication to flow." Tr. 2400:8-10. This is the exact functionality outlined by the asserted claims.

This described system, without the use of Stealthwatch, can identify exfiltrations and drop packets as a result. Therefore, the Court **FINDS** that Cisco's second theory of non-infringement is irrelevant to the Court's determination because the accused system operates to block packets based

on the particular type of data transfer as required by the claims. Cisco's technical documents, such as PTX-1294 and PTX-1326, demonstrate that Stealthwatch is not involved in the two stages of the infringing functionality. Accordingly, any evidence regarding Stealthwatch has no bearing on infringement for the '193 Patent. Based on its analysis, the Court **FINDS** that the packet filtering system instituted by the accused products infringes Claim 18 and 19 of the '193 Patent.

iii. Findings of Fact Regarding Validity

28. The priority date of the '193 Patent is March 12, 2013. JTX-4.

29. Sometime in 2012 or 2013, Cisco released and marketed a system known as the Cyber Threat Defense Solution. This system was a collection of Cisco switches and routers, the Identity Services Engine and Lancope's Stealthwatch. Compare Tr. 2430:1-3; DTX-311 with Tr. 2485:5-10; DTX-664 at 004.

30. Cisco asserts the Cyber Threat Defense Solution as the prior art that renders the '193 Patent invalid. DTX-311.

31. Switches and routers within Cisco's Cyber Threat Defense Solution both received packets and created records of packet flows using Cisco's proprietary logging system known as NetFlow. DTX-311 at 004.

32. The Cyber Threat Defense Solution operates by analyzing NetFlow data and inspecting that data for exfiltrations in the network. DTX-588 at 002.

33. The Cyber Threat Defense Solution contained a quarantine function. At that time, the quarantine function operated by completely isolating a source computer by blocking all packets sent from the computer into the network. Tr. 3011:1-9; DTX-711 at 002. Within this quarantine functionality, there is no mention of allowing access to certain resources while denying access to others. Tr. 3012:1-2.

34. The prior art does not contain any mention of Secure Group Tags or Identity Service Engine's role-based quarantine functionality. See DTX-588; PTX-1193.

35. The prior art does not contain any mention of the application of operators to filter packets based on the attachment of Secure Group Tags. Tr. 3015:11-18, 3016:10-21, 3017:4-10; see DTX-588.

36. The prior art does not contain any information showing the application of SGACL to filter packets in the same manner shown by Cisco's technical documents produced after March 12, 2013. Compare PTX-1276 at 211, 216 (showing the application of Secure Group Tags and SGACLs by the IOS-XE operating system) with PTX-1193 at 007 (showing the same diagram, but failing to make mention of any rules attached and filters based on the application of Secure Group Tags).

iv. Conclusions of Law Regarding Validity

For the '193 Patent, Cisco contends it is invalid based on anticipation by the prior art under 35 U.S.C. § 102, and based on obviousness in view of the prior art under 35 U.S.C § 103. First, Cisco has presented no compelling evidence that the alleged prior art system, the Cisco Cyber Threat Defense Solution, operates in a two-stage filtering process, as illustrated by the claims of the '193 Patent. See DTX-311. The most complete version of prior art, the Cisco Cyber Threat Defense Solution 1.0 Design and Implementation Guide, makes no mention of the attachment of Secure Group Tags or the application of operators to filter portions of packets based on that packet information. Throughout Dr. Crovella's testimony, there is clear reliance on multiple prior art references to prove the invalidity case. For those reasons, it is apparent that a single prior art fails to contain all elements of the claimed invention, and Cisco has failed to show anticipation by clear and convincing evidence.

Turning to obviousness, the prior art references advanced by Cisco do not show that a skilled artisan would have been able to combine the teachings in these technical documents and produce the patented invention. Cisco argues that the '193 Patent must be invalid because the previous system, that includes older versions of similar switches, routers, ISE and Stealthwatch, has had some method of quarantining and blocking functionality. However, the Court rejects Cisco's contention that these products have operated in the same manner and functionality just because the system had preexisting baseline functionality and consistent nomenclature. The prior art makes no mention of the infringing packet filtering process. Dr. Crovella relies on PTX-588, DTX-711, DTX-311, and PTX-1193 to contend that a person skilled in the art would have combined these references in order to teach the functionality outlined in the claims of the '193 Patent. A review of the asserted prior art shows no mention of the Identity Services Engine packet filtering system that utilizes switches and routers to attach Secure Group Tags, apply operators and then allow certain packets to be transmitted while other packets are subsequently blocked.[7] It is that system which contains the functionality taught by the claims of the '193 Patent. Cisco's own technical documents that were used to show infringing functionality are all from post-2013. See PTX-1288 at 012; PTX-1276 at 216; PTX-1280 at 21; PTX-1294; PTX-1326. Not one selection of asserted prior art shows the infringing switch and router functionality was embedded in any of the Cisco products before the '193 Patent's priority date. These conclusions allow the Court to infer that the infringing functionality was added as a result of newly designed versions of the accused products that occurred after March of 2013.

[7] The Patent and Trademark Office denied Inter Partes Review on the '193 Patent citing similar concerns regarding the operator limitation. Tr. 3013:20-3014:9; DTX-370.

Accordingly, the Court **FINDS** that Cisco has failed to present clear and convincing evidence that the prior art would allow a person skilled in the art to combine the prior art to produce a packet filtering system with the functionality taught by Claims 18 and 19 of the '193 Patent.

D. THE '806 PATENT

i. Findings of Fact Regarding Infringement

1. The '806 Patent was informally known throughout the trial as the "Rule Swap Patent."

2. The '806 Patent was issued on December 1, 2015. JTX-2. The application for the '806 Patent was filed on January 11, 2013.

3. The asserted claims of the '806 Patent are Claim 9 and Claim 17. Doc. 411. Claim 9 and Claim 17 are, respectively, a system and computer readable media claim.

4. Claim 9 is laid out below:

> A system comprising:
>
> a plurality of processors; and
>
> a memory comprising instructions that when executed by
>
> > at least one processor of the plurality of processors cause the system to: receive a first rule set and a second rule set; preprocess the first rule set and the second rule set to optimize performance of the system for processing packets in accordance with at least one of the first rule set or the second rule set;
> >
> > configure at least two processors of the plurality of processors to process packets in accordance with the first rule set; after preprocessing the first rule set and the second rule set and configuring the at least two processors to process packets in accordance with the first rule set, receive a plurality of packets;
> >
> > process, in accordance with the first rule set, a portion of the plurality of packets; signal, each processor of the at least two processors, to process packets in accordance with the second rule set; and

> configure, each processor of the at least two processors to, responsive to being signaled to process packets in accordance with the second rule set: cease processing of one or more packets; cache the one or more packets; reconfigure to process packets in accordance with the second rule set;
>
> signal completion of reconfiguration to process packets in accordance with the second rule set; and
>
> responsive to receiving signaling that each other processor of the at least two processors has completed reconfiguration to process packets in accordance with the second rule set, process, in accordance with the second rule set, the one or more packets.

JTX-2.

5. Claim 9 is identical to Claim 17 in every respect except that Claim 17 is a computer readable media claim. JTX-2. Claim 17 substitutes the introductory language of Claim 9, replacing "[a] system comprising: a plurality of processors; and a memory comprising instructions that when executed by at least one processor of the plurality of processors cause the system to:" with "[o]ne or more non-transitory computer-readable media comprising instructions that when executed by a computing system cause the computing system to:" JTX-2. For purposes of infringement, the parties treated Claims 9 and 17 the same.

6. Dr. Moore, one of the inventors of the '806 Patent, defined the technology in the '806 Patent as a process by which a network device could perform a live swap of rules without sacrificing any security concerns or dropping packets. Tr. 338:22-339-2.

7. Cyber threat intelligence is often changing, so the rules that are embedded in switches and routers need to be continually updated. Tr. 339:5-10. Therefore, the rules that are being applied need to be continually swapped out from old rules to new rules. Tr. 339:13-25. The most efficient way to do this is by swapping rules while live traffic is going through the device and without any packets being dropped. Tr. 339:13-25.

8. Centripetal accuses Cisco's Catalyst 9000 series switches, the Aggregation Services Router 1000 series routers and Integration Services Router 1000 and 4000 series routers in combination with Cisco's Digital Network Architecture of infringing Claims 9 and 17 of the '806 Patent. See PTX-1263 at 180 (highlighting Cisco networks are intent-based networks which provide "[p]erimeter-based, reactive security that has been supplanted by network-embedded, content-based security that reaches from the cloud to the enterprise edge") (2019 document).

9. Additionally, Centripetal accuses Cisco's Adaptive Security Appliance 5500 series with Firepower services and Cisco's Firepower Appliance 1000, 2100, 4100, and 9330 series that run Firepower Threat Defense ("Cisco's Firewalls") with Firepower Management Center infringe Claims 9 and 17 of the '806 Patent. See PTX-1291 at 668 (noting the rule swapping procedures of the Cisco firewall products) (September 2017 document).

10. Cisco compiles source code for the accused switches, routers, and firewalls in the United States. Tr. 462:5-463:18, 464:4-14; PTX-1409 at 5-6. The accused products have a plurality of processors and computer memory which stores software instructions. Tr. 573:8-575:6, 642:4-647:11.

11. Cisco's Digital Network Architecture ("DNA Center") is the management structure that allows the system to take in or utilize threat intelligence, operationalize it, and turn it into rules and policies that Cisco's switches and routers use for security purposes. Tr. 451:3-24.

12. The DNA Center receives rule sets from various sources and preprocesses the rule sets to create optimized policies which are distributed to Cisco's switches and routers. Tr. 575:15-577:8, 579:18-580:24, 584:14-585:4, 586:15-587:18, 588:12-589:18, 2571:12-2573:8; PTX-992 at 2; PTX-1294 at 3 (2019 document).

13. Similar to the DNA Center, Firepower Management Center's Threat Intelligence Director receives rule sets from various sources and preprocesses the rule sets to create optimized policies which are distributed to firewalls. Tr. 655:10-656:20, 673:21-675:5, 680:11-681:10; see Tr. 2537:3-7, 2539:11-17.

14. When new rules are available and sent to Cisco's switches and routers by the DNA Center, the switches and routers will perform a rule swap without dropping any packets. Tr. 597:10-601:8, 606:15-608:14, 633:24-634:14; see also Tr. 2571:12-2573:8; PTX-1915; PTX-1195 at 001, 003-04.

15. Similarly, when new rules are available and sent to Cisco's firewalls from the Firepower Management Center, Cisco's firewalls will perform a rule swap without dropping any packets. PTX-1196 at 001, 007; Tr. 694:22-696:12, 698:8-22, 705:15-707:1.

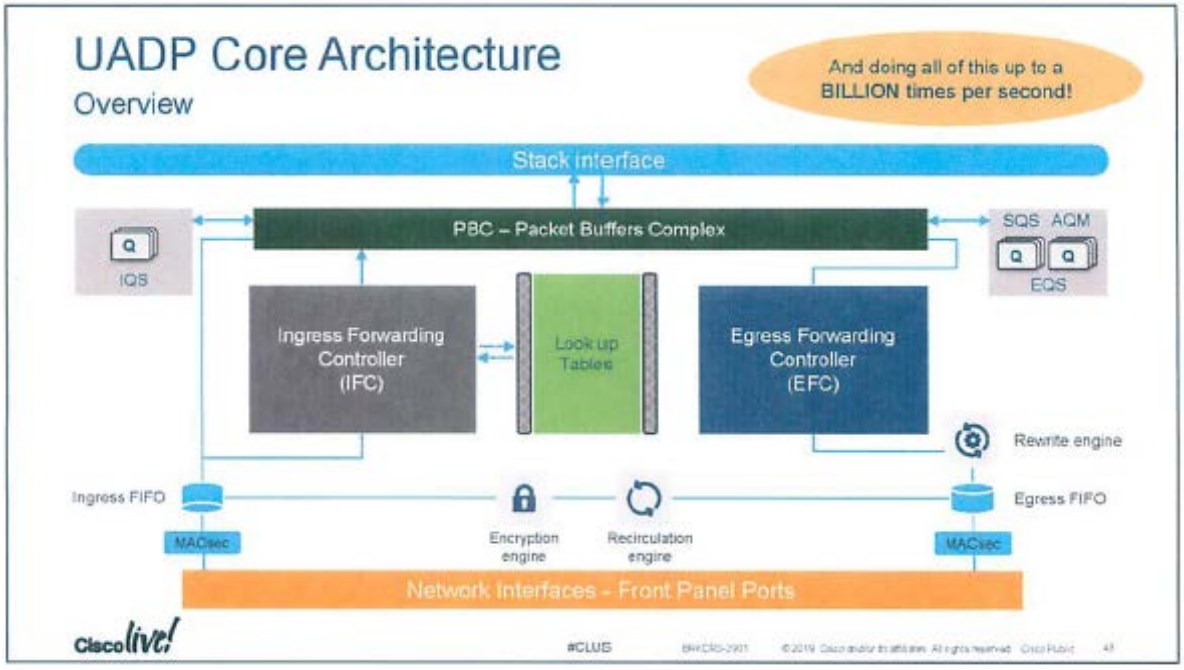
16. Mr. Peter Jones[8], a distinguished Cisco engineer responsible for building the switching, routing and enterprise network, explained in detail how the accused products process packets and swap rules. Tr. 2543:9-11, 2561:25-2562:1.

17. Mr. Jones explained that the architecture that enables packet processing functionality within the switch and/or router is the Uniform Access Data Plane ("UADP") processor. Tr. 2562:10-18; DTX-562 at 043. The figure below shows the core architecture in detail:

[8] Mr. Jones was one of the architects for the design of the UADP processer used by Cisco's accused switches and routers. Tr. 2549:10. He also provided multiple technical presentations regarding the operation of the UADP at many Cisco events. See DTX-562 at 006.

DTX-562

Cisco Technical Presentation on UADP Core Architecture in 2019



18. Mr. Jones noted that as packets arrive into a router and/or switch, they enter through the front panel ports and head into the Media Access Control Security ("MACSec"). Tr. 2567:18-25. The MACSec serves as an encryption block. Tr. 2567:23.

19. The packet then moves into the Ingress FIFO. The FIFO, or First In First Out, is a small buffer that serves to order packets as they enter the device. Tr.2567:23-2568:3.

20. After the FIFO, the payload of the packet is then sent to the Packet Buffer Complex ("PBC") for storage. Tr. 2568:4. Simultaneously, the header and address of the packet is sent to the Ingress Forwarding Controller.

21. The Ingress Forwarding Controller processes the packet by matching the header information to a variety of Access Control Lists ("ACL") that are stored in the look-up tables. Tr. 2568:10-16. Based on those ACLs, the Ingress Forwarding Controller then decides to either drop the packet or transmit it forward. Tr. 2568:10-16.

22. Mr. Jones explicitly noted that if the packet is to be forwarded, it is sent to the Egress Forwarding Controller. Tr. 2568:21-24. He highlighted that the Egress Forwarding Controller operates identically to the Ingress Forwarding Controller. Tr. 2568:21-24. Therefore, for a second time on exit, the payload of the packet is sent to an egress Packet Buffer Complex while the header is sent to the Egress Forwarding Controller. Tr. 2568:21-24; PTX-1390 at 86.

23. It is in the Egress Forwarding Controller that the packet headers are again compared to ACLs that are located in the look-up tables. Tr. 2568:21-24. On egress, the packet can be dropped or further transmitted. Tr. 2568:21-24; PTX-1390 at 86.

24. If the packet is transmitted, it goes through an Egress FIFO, an Egress MACSec, and then out a port on the device. Tr. 2569:1-4.

25. Mr. Jones noted that the UADP operates on its own fixed time pipeline, meaning there will be a packet processed every two or four internal clock periods. The internal clock periods are not set to a normal time scale, but operate in milliseconds. Tr. 2554:22-24.

26. The accused products contain a new FED 2.0 Hitless ACL update. Tr. 3550:18-25. Mr. Jones testified that before the 2.0 Atomic Hitless feature was added to the accused products, performing rule swaps often resulted in a discard of a number of packets. Tr. 2552:20-23. Therefore, the new 2.0 Hitless version updated the products so that new ACLs can be placed into the device and be activated without displacing packet processing. Tr. 2551:2-5; PTX-1303 at 073. Compare the older ACL Process:

PTX-1195 at 003

Cisco FED 2.0 Hitless ACL Update Software Functional Specification[9] from July 2017

2.1 Current ACL Change Flow

Currently whenever there is a change to the ACE in an ACL, the data will drop packets during the change to hardware programming.

This is the sequence of events today:

1. ACE added, removed, modified or re-sequenced
2. An ACL Class Group (CG) change event is sent to FED
3. FED CFM is updated with new Policy CG information
4. All features using this Policy CG are updated
   a. Create new Policy to use temporarily
   b. Generate a new VMR list
   c. Merge and Optimize new VMR list
   d. Write the Drop Policy label to every LE attached to the old Policy
   e. Remove existing TCAM entries
   f. Overwrite old Policy with new Policy in SDK
   g. Delete new Policy
   h. Write new TCAM entries
   i. Validate which will write the Policy label back into all LE attached to Policy
   j. Return SUCCESS

On ERROR returned from writing entries into TCAM:

- If TCAM is full then leave with Drop Policy label programmed (UNLOADED)
- Display UNLOADED or ERROR message to console to indicate hardware was not programmed with new Policy
- Drop all packets for this protocol type, in this direction on the interface
- Return ERROR

PTX-1195 at 003.

[9] The 2.1 in front of Current ACL Change Flow within Exhibit PTX-1195 does not refer to a version number, but this is a numerical heading within the document.

With the new 2.0 Hitless ACL Update:

PTX-1195 at 003

Cisco FED 2.0 Hitless ACL Update Software Functional Specification from July 2017[10]

2.2 Hitless (Atomic) ACL Change Flow

For this new feature Hitless (Atomic) ACL Change, no packets should drop while programming the new TCAM entries. To allow this to happen a new policy will be created and attached to the interface before deleting the existing policy.

This will always be enabled for all features that set the flag acknowledging support for hitless acl change; and is only available to features that go through ACL common code.

This is the new sequence of events:

1. ACE added, removed, modified or re-sequenced
2. An ACL Class Group (CG) change event is sent to FED
3. FED CFM is updated with new Policy CG information
4. All features using this Policy CG are updated
5. Generate a new VMR list
6. Merge and Optimize new VMR list
7. Verify if feature supports hitless ACL change
   - If supported, continue to Step 8
   - If not, use old method starting at Section 2.1 step 4d
8. Add new VCUs into hardware
9. Add new TCAM entries
10. Delete old entries from TCAM
11. Return SUCCESS

On ERROR returned from either of the new steps 7 or 8 will cause it to go back to use the old method of programming described in Section 2.1 starting with step 4d. So then, it will no longer be hitless.

[10] The 2.2 in front of Hitless (Atomic) ACL Change Flow within Exhibit PTX-1195 does not refer to a version number, but this is a numerical heading within the document.

In the same Cisco software technical specification, the requirements of the software dictate that "there will be a short period where both sets of VMR ("Virtual Media Recorder") rule entries will be installed before the old entries are deleted." See PTX-1195 at 003. Here is a copy of those Software Requirements:

PTX-1195 at 003

Cisco FED 2.0 Hitless ACL Update Software Functional Specification from July 2017

3 Software Requirements

The label will not be changed on the Policy. Just as the current Hitless QoS feature does, the new entries will be added with the existing label and there will be a short period where both sets of VMR entries will be installed before the old entries are deleted.

This will only be supported for these ACL features:
PACL, RACL, VACL, CGACL, and SGACL

27. ACLs are sent to switches and/or routers from a variety of sources - including Cisco's Digital Network Architecture. Tr. 2571:12-17. In order to use the rules, the switches and routers must compile them. Tr. 2571:18-21. Accordingly, the DNA Center begins the process by signaling the switches and routers to perform a swap from old to new ACLs. Tr. 2572:14-17.

28. While the ACLs are being compiled within the device, the device uses the old rule set to process packets. Tr. 2571:22-2572:1. The device, after compilation is finished, then signals the processor to begin processing packets with the new updated ACL rule set. Tr. 2572:2-6.

29. This swap of ACL rules within the device occurs in the middle of the two to four clock cycles, when the device is operating in idle and there is no processing of packets. Tr. 2572:10-13. Accordingly, there is a short period where the VMR contains both sets of new and old rules will be installed before the old rules are cleared. See PTX-1195 at 003-04.

30. After the swap is complete, the device performs a memory write and shows a return success function to the end user. Tr. 2573:5-8.

31. After the return is complete, packets are then processed with the newly updated second rule set. Tr. 2572:14-17.

32. Cisco's expert has failed to cite any technical document produced post June 20, 2017. Cisco's expert witness relies on animations, produced ex post facto, which were designed for litigation and do not accurately portray the current functionality of the accused products. Exhibit DTX-562, which was altered from its original form as cited by Cisco's employee Mr. Jones, had emphasis added to it to exclude egress from the presentation of Cisco's expert Dr. Reddy. See supra sec. IV. Overview of the Evidence (discussing Dr. Reddy's animations).

33. Cisco has not called any witness who authored any of the Cisco technical documents relied upon by Centripetal in their infringement case.

ii. Conclusions of Law Regarding Infringement

Based on the Court's factual findings, Centripetal has proven by a preponderance of the evidence that the Cisco's Catalyst 9000 series switches, the Aggregation Services Router 1000 series routers and Integration Services Router 1000 and 4000 series routers in combination with Cisco's Digital Network Architecture literally **INFRINGE** Claims 9 and 17 of the '806 Patent. Additionally, the Court **FINDS** Cisco's Adaptive Security Appliance 5500 series with Firepower services and Cisco's Firepower Appliance 1000, 2100, 4100, and 9330 series that run Firepower Threat Defense ("Cisco's Firewalls") with Firepower Management Center literally **INFRINGE** Claims 9 and 17 of the '806 Patent.

For Cisco, Dr. Narasimha Reddy testified regarding the '806 Patent as to infringement, validity and damages. Dr. Reddy opined that:

> The accused product combinations do not infringe the '806 [P]atent. Secondly, if the Court were to find that the accused product combinations infringe, the asserted claims are invalid on existing prior art of Cisco before the patents were filed. And for damages, assuming that the products are found to be infringing and that the claims are valid, the contribution of the patent claims are minimal.

Tr. 2580:15-23. Dr. Reddy advances three theories of non-infringement for the '806 Patent. He avers that the accused products: (1) do not cease processing of packets responsive to a signal; (2) do not cache the packets responsive to a signal; and (3) do not reprocess packets according to a second rule set. To prove that the products do not perform this functionality as required by the claims, Dr. Reddy relied on an animation produced for litigation that directly contradicts Cisco's own employee testimony and Cisco's own technical documents. Using this animation, Dr. Reddy opined that the Cisco products never cache or cease processing packets during a rule swap. Tr. 2610-2-8.

Turning to the first theory, Cisco employee, Peter Jones, testified that in the operation of packet processing, Cisco's switches and routers will store packets in a part of the UADP ASIC processor known as the Packet Buffer Complex ("PBC"). The PBC operates as a holding spot for the data in the payload of the packet while the header information is forwarded to another part of the processor for the application of rules. This operation in the Cisco switches and routers is designed to maximize the speed and efficiency of packet processing through software. Tr. 622:16-18. Dr. Mitzenmacher highlights that computer scientists use the term buffer and cache interchangeably as a word denoting the use of memory to hold packets for a short period of time. Tr. 628:7-25. Dr. Mitzenmacher referenced that a buffer is a "memory that holds something . . . [o]ften for future use." In reference to the Court's question about defining a cache, Dr. Mitzenmacher gave a similar definition of cache in the following exchange:

> Q. What's a cache?

> A. A cache is also often used, is used in the same way as a memory for holding things. They're very similar. And with a cache you don't typically or necessarily have an ordering associated with it. I mean, it can have an ordering, but it doesn't have to. But a cache is typically used as a memory that holds information that you expect to be using in the near future.

Tr. 836:17-23. Martin Hughes, a Cisco Engineer, confirmed Dr. Mitzenmacher's opinion that a packet buffer is a cache. Mr. Hughes was asked:

> Q. When the router products receive a packet, do router products store the packet in the cache?
>
> A. All products have packet buffers where packets are stored before processing.

DTX-1650; see Tr. 628:3-25, 866:8-22. Based on this testimony, it is apparent that the Packet Buffer Complex within the accused switches and routers clearly acts as a memory storage to hold packet information for further use, and therefore performs the same function of a cache, however, Cisco uses a different nomenclature, calling it a packet buffer. Tr. 836:17-23. Accordingly, in the course of packet processing, the accused devices store packets in a cache as required by the claims.

As their second theory of non-infringement, Cisco advances that the accused products do not cease processing of packets in response to a rule swap. Mr. Jones, a Cisco Engineer, testified contrary to this assertion. He explained that the newly compiled rules are swapped for the old rules in-between the two to four clock periods that occur within the switches and routers. This swap occurs directly during an idle period where the accused switches and routers are not processing any packets. Tr. 2572:10-20. Therefore, it is apparent that the switches and routers do cease packet processing, at least momentarily, to implement the newly compiled rule set.

With regard to both of these theories, Cisco argues that because this process is the normal processing functionality of the accused products, Cisco cannot in theory infringe the claims of the '806 Patent. The Court disagrees with Cisco's argument. It is true that the Cisco products do cache and cease processing packets during their normal packet processing operation. However, Cisco

has implemented the rule swap functionality outlined in the '806 Patent to greatly improve the security functionality of its products without dropping packets. The devices, in response to an initial signal, operate to stop processing packets during an idle period, and during the idle period, unprocessed packets are cached within the Packet Buffer Complex. This process is the exact functionality as described by the cease and cache elements of the '806 Patent.

Lastly, Cisco argues that packets are not reprocessed by a second rule set as required by the claims. First, Cisco is incorrect when it states the claims require a reprocess of packets. The claims clearly state that all that is required is a process through a second rule set. JTX-2. In other words, packets must just be processed by the second rule set – not processed a first time then reprocessed as Cisco suggests. Second, Cisco's non-infringement expert, Dr. Reddy, does not opine upon or even discuss the egress portion of a packet's transmission through a switch, router or firewall. Mr. Jones and Cisco's technical documents confirm that the accused devices apply rules on both ingress into the device and on egress out of the device. Therefore, in their operation, the devices are configured to apply one set of rules on ingress while the very same packet would be subject to a second set of rules on egress within the same device. This process would meet the claim language of the '806 Patent to process packets with a first rule set and then in accordance with a second rule set.

Accordingly, the accused products practice every claim limitation in Claims 9 and 17 of the '806 Patent. Therefore, the Court **FINDS** the rule swap system instituted by the accused Cisco products literally infringe Claims 9 and 17 of the '806 Patent.

iii. Findings of Fact Regarding Validity

34. The priority date of the '806 Patent is January 11, 2013.

35. Cisco asserts the functionality from a previous Cisco switch, the Catalyst 6500, and the Cisco Prime Network Control System as prior art for the '806 Patent. Tr. 3023:23-25.

36. The prior art functionality asserted within the Catalyst 6500 contains the older version of the Atomic ACL Hitless Update.

37. The Atomic ACL Hitless Update, within the Catalyst 6500 switch, operates by adding a new Access Control List ("ACL") in the Ternary Content-Addressable Memory ("TCAM") alongside the old ACL, and merging the two lists together. DTX-686 at 001. This process often overwhelms the TCAM and causes packets to be unintentionally dropped. See DTX-686 at 037-038.

38. The Atomic ACL Hitless Update was updated to the FED 2.0 version in 2017. PTX-1195 at 001; Tr. 3036:12-3037:4. The FED 2.0 Hitless Atomic ACL Update Software Functional Specification shows the differences between the older version of Hitless and the new 2.0 version. PTX-1195 at 002-03; Tr. 3040:2-3042:20. The newer version is accused of infringement by Dr. Mitzenmacher within the Catalyst 9000 switches and accused routers. Tr. 3035:15-25.

39. The older version of Hitless operated by completely stopping the system, eliminating ACLs, merging and replacing those ACLs, then reactivating the processing system. Tr. 3034:23-3035:2. This system resulted in overlap between the old rules and the new rules within the TCAM. This caused packets to be dropped because old ACLs were being applied alongside the new ACLs, causing conflict and disruption. Tr. 3035:3-15, 3040:2-12; see PTX-1195 at 003.

40. The 2.0 Atomic ACL Hitless Update modified the process by eliminating the overlap and implementing rapid swap and replacement of the old ACLs with updated ACLs. Tr. 3041:7-18; see PTX-1195 (technical document from July 2017).

41. Cisco Prime Network Control System's Release Notes show that Prime operated by monitoring and troubleshooting support for a maximum of packets through the 5000 series Cisco Catalyst switches, allowing viability into critical performance metrics for interfaces, ports endpoints, users and basic switch inventory. DTX-525 at 002. The Release Notes for Prime and Dr. Reddy's testimony contains no mention of the preprocessing of rules or allowing switches to receive rules sent by Prime. Tr. 3043:10-24; see DTX-525 at 002. There is no evidence that the predecessor 6500 series switch, aided with Cisco Prime, could swap new rules for the old, as opposed to merging old and new rules together.

iv. Conclusions of Law Regarding Validity

Cisco asserts that the asserted claims of the '806 Patent are anticipated and/or are obvious based on the Atomic ACL Hitless Update in the Cisco Catalyst 6500 Supervisor Engine 2T and the Cisco Prime Network Control System. Tr. 2656:5-2657:22. Cisco's invalidity expert, Dr. Reddy, presented various documents opining that the functionality of Claims 9 and 17 of the '806 Patent was included within the prior art. This Court disagrees with the conclusions of Dr. Reddy and **FINDS** the '806 Patent valid.

First, the Atomic ACL Hitless Update embedded within the Catalyst 6500 was an older and different functioning process than that which was embedded within the accused switches and routers. The accused devices contain a FED 2.0 version of the Atomic ACL Hitless Update. As evidenced by Centripetal's expert, Dr. Orso, and PTX-1195, this 2.0 version provided a meaningful update to the system by which old ACLs were swapped for new ACLs. See PTX-1195,

Tr. 3040:2-3042:20. The older version of the Hitless Update, embedded in the 6500, involved merger and application of old and new ACLs that resulted in disruption of packet processing and the unintentional dropping of packets. This rule swapping technique outlined by the '806 Patent solved the problem that the old Hitless Update was having. See JTX-2 col. 1 (noting that the '806 Patent was addressing the problems faced by network devices "processing packets in accordance with an outdated rule set"). Therefore, it is axiomatic that the claimed invention would have not been obvious in the prior art because the '806 invention of rule swapping was the solution to the exact problem outlined by the original Hitless Update.

Second, the Cisco Prime technical documents do not contain any functionality of the asserted claims for the '806 Patent. The only document presented by Dr. Reddy identifies that Prime provided monitoring and troubleshooting support for Cisco's switches. There is no clear and convincing evidence from Dr. Reddy's testimony, or this one document offered by Cisco, that Prime served a similar function as Cisco's Digital Network Architecture. Accordingly, there is not clear and convincing evidence for the Court to find that Prime caused the Cisco devices to receive first and second rule sets as required by the claims. Therefore, both asserted prior art references fail to teach the invention as described by Claims 9 and 17 of the '806 Patent. Accordingly, the Court **FINDS** that Cisco has not proven by clear and convincing evidence that the '806 Patent was anticipated or obvious.

E. THE '205 PATENT

i. Findings of Fact Regarding Infringement

1. The '205 Patent has been commonly known as the "dynamic security policy" Patent. Tr. 432:17-20.

2. The ‘205 Patent was issued on September 15, 2015. JTX-1. The application for the ‘205 Patent was filed on October 22, 2012. JTX-1.

3. The asserted claims of the ‘205 Patent are Claims 63 and 77 of the ‘205 Patent. Claims 63 and Claim 77 are, respectively, a system and computer readable media claim.

4. Claim 63 is laid out below:

> A system, comprising:
>
> a security policy management server; and one or more packet security gateways associated with the
>
> > security policy management server, wherein each packet security gateway of the one or more packet security gateways comprises computer hardware and logic configure to cause the packet security gateway to:
> >
> > receive, from the security policy management server, a dynamic security policy comprising at least one rule specifying a set of network addresses and a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI);
> >
> > receive packets associated with a network protected by the packet security gateway;
> >
> > perform, on the packets, on a packet by packet basis, at least one packet transformation function of multiple packet transformation functions specified by the dynamic security policy;
> >
> > encapsulate at least one packet of the packets that falls within the set of network addresses and matches the SIP URI with a header containing a network address that is different from a destination network address specified by the at least one packet and that corresponds to a network device configured to copy information contained in the at least one packet and to forward the at least one packet to the destination network address; and
> >
> > route, based on the header, the at least one packet to the network address that is different from the destination network address.

JTX-1.

5. Claim 63 is identical to Claim 77 in every respect, except that Claim 77 is a computer readable media claim. Claim 77 substitutes the introductory language of Claim 63, replacing "[a] system, comprising: a security policy management server; and one or more packet security gateways associated with the security policy management server, wherein each packet security gateway of the one or more packet security gateways comprises computer hardware and logic configured to cause the packet security gateway to" with "[o]ne or more non-transitory computer-readable media having instructions stored thereon, that when executed, cause each packet security gateway of one or more packet security gateways associated with a security policy management server to:." JTX-1. For purposes of infringement, the parties have treated the two claims as identical.

6. Dr. Moore, the inventor of the '205 Patent, characterizes the technology in the '205 Patent as Centripetal's network protection system that enforces threat intelligence policies on network traffic.

7. Dr. Moore identified that there is a thriving ecosystem of companies that observe behavior on the internet and collect information on who are the cyber criminals, what computers are being controlled, and what types of attacks are being implemented. This information is collected and turned into threat intelligence.

8. Dr. Moore specifically credits the technology in the '205 Patent as a system for operationalizing threat intelligence into policies of rules that are uploaded into network devices to block dynamic threats. Tr. 321:5-9, 320:16-25.

9. Cisco's expert on the '205 Patent, Dr. Kevin Jeffay, challenges Dr. Moore's characterization by noting that the specific claims at issue have no relation to the blocking of malicious traffic. Instead, Dr. Jeffay characterizes the claims at issue as dealing with the

encapsulation, copying and forwarding of voice traffic over the internet. Tr. 2727:11-19, 2732:2-19. More generally, Dr. Jeffay describes the claims at issue as enabling law enforcement to potentially wiretap internet calls. Tr. 2732:13-16.

10. Centripetal accuses Cisco's Catalyst 9000 series switches, the Aggregation Services Router 1000 series routers and Integration Services Router 1000 and 4000 series routers, in combination with Cisco's Digital Network Architecture, of infringing Claims 63 and 77 of the '205 Patent. Additionally, Centripetal accuses Cisco's Adaptive Security Appliance 5500 series with Firepower services and Cisco's Firepower Appliance 1000, 2100, 4100, and 9330 series that run Firepower Threat Defense ("Cisco's Firewalls") with Firepower Management Center of infringing Claims 63 and 77 of the '205 Patent. Tr. 7235:16-20.

11. The accused switches, routers and firewalls have the ability to act as packet security gateways. Tr. 732:24-734:22, 735:15-20, 737:24-738:5.

12. Cisco's Digital Network Architecture Center serves as the "foundational controller . . . at the heart of Cisco's intent-based network . . . [and] provides a single dashboard for every fundamental management task." PTX-1294. Accordingly, both the DNA Center and Cisco's Firepower Management Center manage and update security policies that are employed by the accused devices. Tr. 728:21-730:9; 736:3-13; PTX-1294 at 15.

13. The accused devices process a certain type of network traffic sent by Session Initiation Protocol ("SIP"). Tr. 739:13-18, 2782:12-17; PTX-1408 at 19. SIP is one of the many protocols that is used to transmit information over the internet. Tr. 739:5-9. SIP is primarily used for the sending of voice data, but can be used for video and instant messaging. Tr. 739:5-9, 741:15-24, 2729:13-19.

14. Each device, when making a call using SIP, has a unique identifier know as a SIP Uniform Resource Identifier ("SIP URI") that functions similarly to a telephone number. Tr. 2729:16-23. SIP URI is embedded within SIP traffic to identify the party to the call. Tr. 2729:16-23.

15. Cisco's expert, Dr. Kevin Jeffay, opined that a SIP URI consists of SIP and then a unique identifier of the individual device that is being called. Tr. 2739:1-7. He provided an example of a SIP URI as sip:jeffay@unc.edu. Tr. 2739:8-10.

16. Dr. Jeffay's opinion is confirmed by the Internet Engineering Task Force's Request for Comment ("RFC") 3261 that outlines the procedures for the SIP protocol. RFC 3261 confirms that a SIP URI contains the word SIP, and the document provides a specific example as "sip:user:password@host:port;uri-parameters?headers." DTX-1296 at 148. RFC 3261 contains many examples of SIP URIs that all contain the word sip. DTX-1296 (listing examples of SIP URIs such as "sip:alice@atlanta.com.").

17. Centripetal's expert, Dr. Michael Mitzenmacher, presented that the Firepower Management Center enables the network firewalls to monitor traffic sent by SIP for network exploits. Tr. 748:6-13; PTX-1289 at 912. The technical documents confirm that if any SIP traffic is found to be a threat to the network, rules may be created to prevent any dangers to the network. Tr. 748:19-24; PTX-1289 at 912.

18. The accused products have the capability to handle SIP traffic and can block that traffic that is determined to be malicious. Tr. 750:11-17.

19. However, Dr. Mitzenmacher presented no technical documents that confirm that the accused firewalls have specific rules that contain both a network address and a SIP URI. Tr.

2756:18-2757:2. Furthermore, no Cisco technical document confirms that the accused switches and routers have any rules that contain both a network address and a SIP URI. Tr. 2756:18-2757:2.

20. Dr. Mitzenmacher and Cisco's technical documents do confirm that the accused switches, routers and firewalls can forward and block packets. Tr. 754:11-756:7; PTX-1276 at 216; PTX-1493 at 009.

21. The accused devices can encapsulate and route packets. Tr. 756:8-758:21, 760:5-764:16; PTX-1262 at 994; PTX-524 at 309; PTX-1229 at 69; PTX-1293 at 062. However, Dr. Mitzenmacher presented no evidence that the accused devices perform a "copying" of information contained in the packets. Tr. 2749:24-2750:4 (Dr. Jeffay confirming no testimony or evidence on copying).

ii. Conclusions of Law Regarding Infringement

Cisco expert, Dr. Jeffay, opined that the '205 Patent was not infringed for two distinct reasons. First, he opined that Centripetal's infringement theory relies on the "blocking" of packets, but the asserted claims of the '205 Patent require encapsulation and forwarding. Second, he averred that Centripetal has not asserted any proof that the accused products have "at least one rule specifying a set of network addresses and a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI)," as required by the claims. The Court agrees with Dr. Jeffay on both of his non-infringement theories. The Court affirms Dr. Jeffay's characterization that the '205 Patent teaches a method of tapping internet-based phone communications and potentially video via the internet. It may be characterized as a method of spying upon or "hacking" internet communications, which is the converse of the four previous patents that are found as valid and infringed, the function of which is to provide network security.

On his first theory, Dr. Jeffay outlined the main focus of the invention in the '205 Patent is on Voice over IP traffic and the encapsulation and forwarding of data. He opined:

> Q. And turning to slide 5, how many disputes -- on the infringement issue, how many major disputes do you intend to focus on today?
>
> A. Well, in my report I documented several disputes, but in the interest of time, we're going to focus on two here, and these are the two that I think are the easiest to see. And the first one is really sort of a black/white issue; that Centripetal's theory of infringement focuses on the blocking of packets. And blocking has really been the key to most of this case; that the accused products block packets. But the '205 [P]atent is not about blocking packets, it's about precisely the opposite. It's about doing things that we'll come to see are called encapsulation and forwarding, but the point here is that we want the packets to go through to their destination. We're going to see that the patent is really about enabling law enforcement to potentially wiretap phone calls, so we want the package to go through. And so the '205 claims are really about the opposite of what we've heard in this case; they're about letting packets make it to their destination.

Tr. 2731:24-2732:19. Dr. Jeffay explained in detail Figure 6 of the '205 Patent, walking through the major outline of the invention, as described by the claims:

FIG. 6 from the '205 Patent

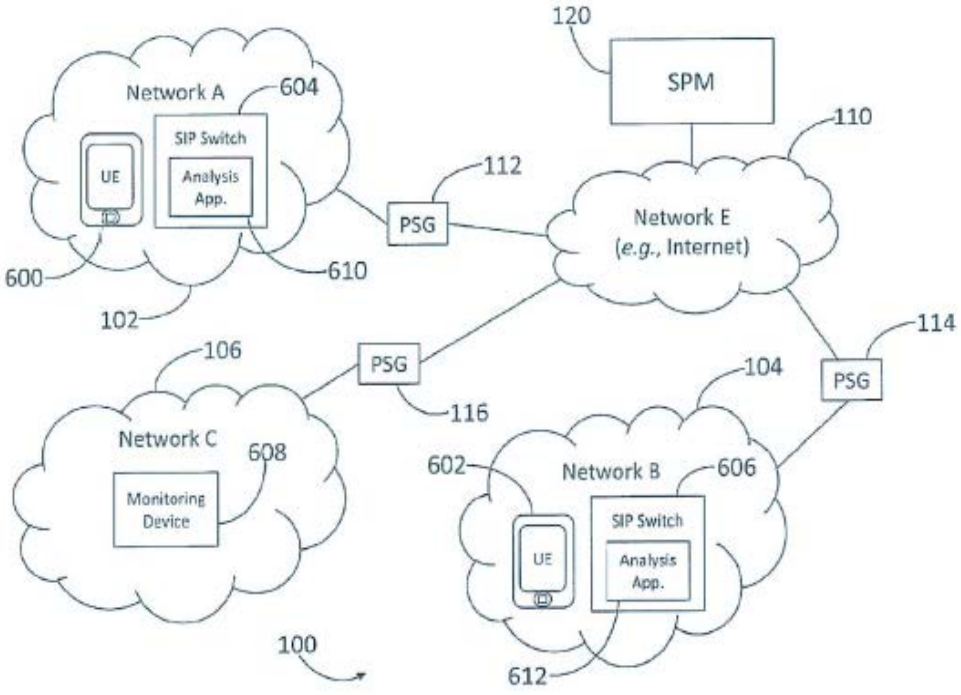


FIG. 6

Q. We've got figure 6 up now. Dr. Jeffay, could you, using figure 6, walk the Court through the major components of the claimed invention.

A. Sure. So this is the world -- this a version of the world in which the claimed invention would operate. So let's focus first on network A, which is in the upper left-hand corner. And in network A there is a device, UE 600. Now, UE in the patent stands for User Equipment, but what I'd like the Court to think of it -- think of it as a phone. And you can kind of see it's drawn kind of like an iPhone. So it's a phone. And what's going to happen here is that this user in network A is going to make a phone call, a Voice over IP phone call, to a user in network B. So let's highlight network B, which is on the lower right. And we can see that also there's a UE 602, User Equipment, just basically another phone, that's in network B. So a user in network A makes a call to a user in network B, and what the patent is about is using an SPM 120 -- SPM is going to stand for Security Policy Management server; this is the entity that creates security policies. The SPM is going to send a policy that contains a rule to a packet security gateway 112. So the packet security gateway is the thing that actually looks at the packets. Now the rule -- the policy contains a rule, and the rule that's going to be sent to the packet security gateway is going to contain information to allow the packet security gateway to identify the packets corresponding to this Voice over IP phone call. And when it identifies the right kind of packets, what it's going to do is a little unusual. It's going to let the packets go through. It's not going to block the packets, but it's not going to send the packets

> to their intended destination, which is network B. It's going to send them to network C, which is shown on the lower left. And in network C you can see that there's a monitoring device, and what's going to happen is the packets are going to be routed from the packet security gateway, to network C, to this monitoring device. The monitoring device is then going to copy some information from the packets. It's going to keep that copied information, because, in theory, that's what law enforcement wants to see, but then we need the call to go through, so it's -- the network device 608 is going to unencapsulate the packet, get the original packet, and send it on its way back to network B.

Tr. 2735:5-2736:24. In this explanation of the claims, Dr. Jeffay noted explicitly that the claims do not require the blocking of packets because "[i]f the call is blocked, then the packets would be dropped at the packet security gateway 112, and there would be nothing to monitor." Tr. 2742:19-21. Based on an independent reading of the claims, the Court agrees with Dr. Jeffay that the scope of the asserted claims of the '205 Patent deal specifically with the functionality to encapsulate, copy and then forward on packets to a different network.

To prove infringement, Centripetal's expert Dr. Mitzenmacher specifically identified the '205 Patent as:

> Q. If we can go to your demonstrative, can you briefly explain what this is showing, in terms of the '205 [P]atent, with the dynamic security policy?
>
> A. As we've seen for all of these systems, they will be given threat intelligence, or gather or absorb threat intelligence, and they can use that to update the rules. In particular, just generally, they have dynamic security policies. They're constantly getting new information, and over time, they will often update the rule sets in order to deal with new threats accordingly.

Tr. 726:21-727:5. Dr. Mitzenmacher, in his infringement opinion, specifically focused on the use of threat intelligence being used to block malicious traffic in the network. In his testimony, Dr. Mitzenmacher confirms that the accused products can perform the encapsulation of packets. Tr. 756:8-758:21, 760:5-764:16. This is confirmed by the Cisco technical documents. PTX-1262 at 994; PTX-524 at 309; PTX-1229 at 69; PTX-1293 at 062. But the encapsulation of packets

described by Dr. Mitzenmacher and the technical documents is not all that is required by the asserted claims. This element of the claim reads:

> encapsulate at least one packet of the packets that falls within the set of network addresses and matches the SIP URI with a header containing a network address that is different from a destination network address specified by the at least one packet and that corresponds to a network device **configured to copy information** contained in the at least one packet and to forward the at least one packet to the destination network address . . .

JTX-1 (emphasis added). Dr. Mitzenmacher presented no testimony or technical documents that confirmed that the accused products are "configured to" or have the ability to copy information, as outlined by the asserted claims. Tr. 2749:24-2750:4; see PTX-1262 at 994; PTX-524 at 309; PTX-1229 at 69; PTX-1293 at 062. Additionally, there is no evidence in the documents presented by Dr. Mitzenmacher that the encapsulated packets are those that "fall within the set of network addresses and matches the SIP URI with a header containing a network address . . . ." See PTX-1262 at 994; PTX-524 at 309; PTX-1229 at 69; PTX-1293 at 062. For these reasons, Centripetal has failed to prove by a preponderance of the evidence that the accused products embody each and every limitation of the patented claim. See V-Formation, Inc. v. Benetton Group SpA, 401 F.3d 1307, 1312 (Fed. Cir. 2005).

Turning to the second theory, Dr. Mitzenmacher presented no document that specifies that the accused products contain" at least one rule specifying a set of network addresses and a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI)," as required by the claims. For the accused routers and switches, Dr. Mitzenmacher points to a presentation, PTX-1408, that shows that SIP traffic passes through Cisco's products. This document's mere mention of SIP traffic is not compelling evidence that Cisco's routers and switches have rules that contain SIP URI and network addresses. See Tr. 2756:18-2757:2. PTX-1408. Similarly, for the accused firewalls, Dr. Mitzenmacher turns to PTX-1289 to show that the Cisco firewalls have four SIP keywords that

allow the user to monitor SIP traffic for exploits. PTX-1289 at 808. This document contains no mention of having specific rules that contain SIP URIs in combination with network addresses. Viewing all of the documents and testimony presented by Dr. Mitzenmacher, there is sufficient evidence to conclude that the accused products process SIP traffic. However, there is no compelling evidence to show that the accused products have rules that possess both a SIP URI and a network address, as required by the claims. See Tr. 2756:18-2757:2.

Additionally, the Court **FINDS** that there is no infringement of the '205 Patent under the doctrine of equivalents. Dr. Mitzenmacher, in his equivalents testimony, stated:

> Q. So, go ahead. Can you, please, explain for the Court how the switches, routers, and firewalls perform substantially the same function.
>
> A. Certainly. So it provides substantially the same function, which is to block potentially malicious network traffic that's been determined or related to a Session Initiation Protocol URI. It does this in the same way; by specifying a rule that would block this corresponding traffic. It may do so -- it does so by establishing a rule containing relevant SIP information, such as a domain or an IP address, and it achieves substantially the same result, which is to block that potentially – or create rules which would either block or monitor, or whatever action you want to take, on the corresponding Session Initiation Protocol traffic.

Tr. 774:23-775:12. The Court has already determined that the asserted claims cover the encapsulation, copying and forwarding of packets. Blocking packets, as identified by Dr. Mitzenmacher, would not perform substantially the same function in substantially the same way as encapsulation, copying and forwarding. Accordingly, there is no infringement under the doctrine of equivalents.

For both of these reasons, the Court **FINDS** that Centripetal has not met its burden to prove by a preponderance of the evidence that the accused products infringe Claims 63 and 77 of the '205 Patent literally or under the doctrine of equivalents.

iii. Validity

During trial, Cisco withdrew its claim that the '205 Patent was invalid. Tr. 2795:16-24. Therefore, this Court will not address the validity of the '205 Patent as it is not required to rule upon the validity of a patent which has not been found infringed.

VI. FINDINGS OF FACT AND CONCLUSIONS OF LAW REGARDING DAMAGES

A. PAST DAMAGES

i. Findings of Fact and Conclusions of Law Regarding Reasonable Royalty Base and Rate

"Upon finding for the claimant the court shall award the claimant damages adequate to compensate for the infringement, but in no event less than a reasonable royalty for the use made of the invention by the infringer, together with interest and costs as fixed by the court." Lucent Techs., Inc. v. Gateway, Inc., 580 F.3d 1301, 1324 (Fed. Cir. 2009) (quoting 35 U.S.C. § 284). In awarding damages under the governing statute, 35 U.S.C. §284, "a reasonable royalty is the minimum permissible measure of damages." Deere & Co. v. Int'l Harvester Co., 710 F.2d 1551, 1558 n.9 (Fed. Cir. 1983). The Supreme Court has framed reasonable royalty damages achieved through litigation as a court's duty to assess "the difference between [the patentee's] pecuniary condition after the infringement, and what his condition would have been if the infringement had not occurred." Yale Lock Mfg. Co. v. Sargent, 117 U.S. 536, 552 (1886). The burden of proving damages as a result of infringement falls on the patentee. Lucent Techs., Inc., 580 F.3d at 1324. The Federal Circuit has determined two acceptable "alternative categories of infringement compensation." Id. The first category is based on a patentee's lost profits. Id. To recover lost profits, "a patent owner must prove a causal relation between the infringement and its loss of profits." Shockley v. Arcan, Inc., 248 F.3d 1349, 1362 (Fed. Cir. 2001). The patentee is required to "show a reasonable probability that 'but for' the infringing activity, the patentee would have

made the infringer's sales." Id. The four-factor test for utilizing the lost profit model is laid out in Panduit Corp. v. Stahlin Bros. Fibre Works, Inc., 575 F.2d 1152, 1156 (6th Cir. 1978).[11] The lost profits method is not at issue in this case since Centripetal has not presented any evidence of a causal relationship between suspected lost profits and Cisco's sales of the infringing technology. The second category, which the Court adopts in this case, is based on the "the reasonable royalty . . . [the patentee] would have received through arms-length bargaining." Lucent Techs., Inc., 580 F.3d at 1324.

In determining this reasonable royalty, patentees have primarily used two distinct methods of calculation. "The first, the analytical method, focuses on the infringer's projections of profit for the infringing product." See id. (citing TWM Mfg. Co. v. Dura Corp., 789 F.2d 895, 899 (Fed. Cir. 1986) (describing the analytical method as "subtract[ing] the infringer's usual or acceptable net profit from its anticipated net profit realized from sales of infringing devices")). Here, there was insufficient evidence submitted to the Court based on the infringer's profit projections and thus this method is inappropriate for calculating damages. "The second, more common approach, called the hypothetical negotiation or the 'willing licensor-willing licensee' approach, attempts to ascertain the royalty upon which the parties would have agreed had they successfully negotiated an agreement just before infringement began." Id. The date used for the occurrence of the hypothetical negotiation is the date that infringement began. Wang Labs., Inc. v. Toshiba Corp., 993 F.2d 858, 870 (Fed. Cir. 1993). The evidence at trial supports a first infringement date of June 20, 2017. The Court **FINDS** the reasonable royalty method to be appropriate based on the evidence presented by both Centripetal and Cisco.

[11] "To obtain as damages the profits on sales he would have made absent the infringement, i.e., the sales made by the infringer, a patent owner must prove: (1) demand for the patented product, (2) absence of acceptable non-infringing substitutes, (3) his manufacturing and marketing capability to exploit the demand, and (4) the amount of the profit he would have made." Panduit Corp. v. Stahlin Bros. Fibre Works, Inc., 575 F.2d 1152, 1156 (6th Cir. 1978).

To determine a reasonable royalty, the Court bases its economic analysis on the factors laid out in Georgia-Pacific Corp. v. U.S. Plywood Corp., 318 F. Supp. 1116, 1120 (S.D.N.Y. 1970). Determining a reasonable royalty involves the Court's analysis into each of the relevant Georgia-Pacific factors:

(1) Any royalties received by the licensor for the licensing of the patent-in-suit, proving or tending to prove an established royalty.

(2) The rates paid by licensee to license other patents comparable to the infringed patents.

(3) The nature and scope of the license, as exclusive or non-exclusive, or as restricted or non-restricted in terms of its territory or with respect to whom the manufactured product may be sold.

(4) The licensor's established policy and marketing program to maintain its right to exclude others from using the patented invention by not licensing others to use the invention, or by granting licenses under special conditions designed to preserve that exclusivity.

(5) The commercial relationship between the licensor and the licensee, such as whether or not they are competitors in the same territory in the same line of business.

(6) The effect of selling the patented product in promoting other sales of the licensee; the existing value of the invention to the licensor as a generator of sales of its non-patented items; and the extent of such collateral sales.

(7) The duration of the infringed patents and the term of the license.

(8) The established profitability of the product made under the infringed patents; its commercial success; and its popularity.

(9) The utility and advantages of the patented invention over the old modes or devices, if any, that had been used for achieving similar results.

(10) The nature of the patented invention; the character of the commercial embodiment of it as owned and produced by or for the licensor; and the benefits to those who have used the invention.

(11) The extent to which the infringer has made use of the invention; and any evidence that shows the value of that use.

(12) The portion of the profit or of the selling price that may be customary in the particular business or in comparable businesses to allow for the use of the invention or analogous inventions.

(13) The portion of the profit that arises from the patented invention itself as opposed to profit arising from unpatented features, such as the manufacturing process, business risks, or significant features or improvements added by the accused infringer.

(14) The opinion testimony of qualified experts.

(15) The amount that a licensor (such as Centripetal) and a licensee (such as Cisco) would have agreed upon (at the time the infringement began) if both sides had been reasonably and voluntarily trying to reach an agreement; that is, the amount which a prudent licensee -- who desired, as a business proposition, to obtain a license to manufacture and sell a particular article embodying the patented invention -- would have been willing to pay as a royalty and yet be able to make a reasonable profit and which amount would have been acceptable by a patentee who was willing to grant a license.

See Georgia-Pacific Corp. v. U.S. Plywood Corp., 318 F. Supp. 1116, 1120 (S.D.N.Y. 1970), modified sub nom. Georgia-Pacific Corp. v. U.S. Plywood-Champion Papers, Inc., 446

F.2d 295 (2d Cir. 1971). The Court will examine each of the relevant Georgia-Pacific factors that guide its determination of a proper reasonable royalty rate.[12]

Beginning with Georgia-Pacific factors one and two, the only comparable license of the patents-in-suit is the Confidential Binding Term Sheet agreed to in a previous case tried by this Court – Centripetal Networks, Inc., v. Keysight Technologies, Inc. and Ixia, Case No. 2:17-cv-383 (E.D Va.). The Court is limited to this license granted by Centripetal as the only comparable license, as neither party presented any comparable licenses for similar patented inventions or similar infringing products. Tr. 1498:2-10. Although Cisco licensed Stealthwatch for a period of years from Lancope before Cisco acquired the company in 2013, neither Centripetal nor Cisco presented evidence of this or any other license in which Cisco was involved, and the Keysight agreement is the only licensing agreement in which Centripetal has been involved. The Keysight agreement was entered into by Centripetal and Keysight/Ixia during trial to settle the patent claims at issue in that litigation. The patents asserted in the Keysight case are comparable to those in this litigation. Both the '205 Patent and the '856 Patent were asserted in the Keysight case. The '176 Patent, the '193 Patent and the '806 Patent are in the same patent family and covered similar fields of technology as the patents that were asserted in Keysight. Therefore, the Keysight agreement covers sufficiently similar technology to serve as a comparable technology license in this case.

The Keysight agreement granted Keysight/Ixia a three year "worldwide, non-transferable, irrevocable, non-terminable, non-exclusive license" to Centripetal's worldwide patent portfolio in exchange for a $25 million-dollar lump-sum payment and a 10% royalty of directly competing products and a 5% royalty on non-competing products. See PTX-1125; Tr. 1487:5-1491:2. The

[12] Certain factors may be relevant regarding other factors and, therefore, the Court will often address two factors at a time. Additionally, the Court may incorporate relevant information from one factor into its analysis of another factor. For example, the Court often uses factor fourteen (i.e., the opinion testimony of qualified experts) to support its analysis of other factors.

Court agrees with Centripetal's damages expert, Lance Gunderson, that the 10% running royalty instituted in the Keysight agreement is sufficiently comparable to provide a starting point for determining a reasonable royalty based on a hypothetical negotiation. See Tr. 1486:1-24. This 10% royalty in Keysight was instituted for products that directly compete with Centripetal's RuleGate gateway product. Cisco's damages expert, Dr. Becker, contends that the Keysight license is not directly comparable because Keysight was a direct competitor in the threat intelligence gateway market, and Cisco is not. Although Centripetal does not market and sell switches and routers, Cisco has embedded the patented software functionality from the Centripetal patents into the infringing switches and routers that provides the same functionality as the RuleGate product. Centripetal does market and sell firewalls. Accordingly, the Court **FINDS** that Centripetal and Cisco are direct competitors with respect to the infringing software, as well as firewalls. This incorporation of infringing functionality persuades the Court that the infringing Cisco products are more comparable to the 10% royalty on competing products than the 5% royalty for non-competing products in Keysight. Accordingly, the 10% royalty on directly competing products in the Keysight case provides a comparable baseline license from which the Court can determine a reasonable royalty in this case.

The Court recognizes that the Keysight license was obtained in the coercive environment of litigation and not the result of open negotiation. See LaserDynamics, Inc. v. Quanta Computer, Inc., 694 F.3d 51, 77 (Fed. Cir. 2012) (highlighting that "[t]he notion that license fees that are tainted by the coercive environment of patent litigation are unsuitable to prove a reasonable royalty is a logical extension of Georgia–Pacific . . ."). Generally, these types of settlement agreements "should not be considered evidence of an established royalty." Id. (citing Hanson v. Alpine Valley Ski Area, Inc., 718 F.2d 1075, 1078-79 (Fed. Cir.1983). However, the Federal Circuit has recently

permitted reliance on such agreements "under certain limited circumstances." Id. In the case of ResQNet.com, Inc. v. Lansa, Inc., the Federal Circuit "permitted consideration of the settlement license on remand" because the "settlement license to the patents-in-suit in a running royalty form was 'the most reliable license in [the] record.'" Id. (discussing and quoting language from ResQNet); see ResQNet.com, Inc. v. Lansa, Inc., 594 F.3d 860, 872 (Fed. Cir. 2010).

Similarly, here, the Court, has only one comparable license in the form of a settlement agreement from the Keysight case. The Court, in its use of this license to determine a reasonable royalty, heeds the guidance of the Federal Circuit to "consider the license in its proper context within the hypothetical negotiation framework to ensure that the reasonable royalty rate reflects "the economic demand for the claimed technology." Id. Therefore, the Court will analyze the Keysight rate in the context of the other Georgia-Pacific factors to account for the similarities and differences in the Keysight license and the facts present in this case. See AstraZeneca AB v. Apotex Corp., 782 F.3d 1324, 1335 (Fed. Cir. 2015) (finding no error when the district court accounted for similarities and differences between past negotiations and the hypothetical negotiations); see also Elbit Sys. Land & C4I Ltd. v. Hughes Network Sys., LLC, 927 F.3d 1292, 1300 (Fed. Cir. 2019) (collecting cases that show it is appropriate to rely on prior licenses, even in a settlement context, when they are sufficiently compared to the facts and circumstances of the case at issue).

Turning to Georgia-Pacific factor three, the scope and nature of the Keysight license weighs in favor of reducing the baseline royalty percentage, because the license presented to Cisco would be limited to the infringing patents instead of a full patent portfolio that was granted in Keysight. Consequently, the Court agrees with Dr. Becker that this factor promotes in favor of a royalty rate reduction. Tr. 2869:2-12.

Georgia-Pacific factor four has some influence on the royalty figure. The Court can infer that Centripetal was at least willing to license its patent portfolio to Keysight, for the terms outlined in the agreement, in order to settle ongoing litigation. This comparable license shows that Centripetal may have been willing to license the asserted patents to Cisco. It is a consideration that would sway the Court to adjust the royalty somewhat in a downward direction. The license is a major consideration in Centripetal's request for injunctive relief.

Georgia-Pacific factor five has minimal impact on the royalty figure. This factor asks the Court to inquire into the commercial relationship of the parties at the hypothetical negotiation. The Court notes that Centripetal has presented evidence that Cisco's incorporation of the patented functionality into its products would result in substantial lost profits from the competing RuleGate product. Generally, this fact would weigh in favor of increasing the royalty as Centripetal, in the hypothetical negotiation, would consider the substantial loss that may be attributed to licensing the patented technology.[13] From Cisco's perspective, it would gain substantially from licensing the asserted patents as it could incorporate advanced security functionality into its products, thus improving the profitability of its networking products. See Carnegie Mellon Univ. v. Marvell Tech. Group, Ltd., 807 F.3d 1283, 1304 (Fed. Cir. 2015) (noting "a basic premise of the hypothetical negotiation is the opportunity for making substantial profits if the two sides [are] willing to join forces by arriving at a license of the technology").

[13] "It is a step further, and we think a necessary one, to say that, when the patentee's business scheme involves a reasonable expectation of making future profits by the continuing sale to the purchaser of the patented machine, of supplies to be furnished by the patentee, which future business he will lose by licensing a competitor to make the machine, this expectant loss is an element to be considered in retroactively determining a reasonable royalty." Panduit Corp. v. Stahlin Bros. Fibre Works, Inc., 575 F.2d 1152, 1163 (6th Cir. 1978) (quoting Egry Register Co. v. Standard Register Co., 23 F.2d 438, 443 (C.C.A. 6th Cir. 1928)).

However, the Court must consider that Cisco has incorporated the infringing technology into hardware products, such as switches and routers, that Centripetal does not produce or sell. Additionally, even if Centripetal sold versions of the infringing products, it would be difficult to meet the customer demand of these products that Cisco, as the largest provider of network infrastructure and services in the world, would be able to accomplish. See Tr. 1449:17-1451:2. Therefore, Centripetal's bargaining position in the hypothetical negotiation would be limited by the incentive of Centripetal to license the patented software technology to Cisco in order to take advantage of Cisco's substantial market share. See Tr. 1449:17-1451:2. The Court **FINDS** that all these considerations generally neutralize each other and warrant no variance to the royalty number.

Georgia-Pacific factor six does call for some upward influence. Cisco has incorporated the patented software functionality into a variety of its routers, switches and firewalls in its network security system. Therefore, the effect of the sales and the profits therefrom are promoted by Centripetal's software. The upward influence is somewhat offset by the apportionment analysis of Centripetal's experts. There was no evidence presented that the infringing products contributed to increased sales of any of Cisco's other non-infringing products.

Georgia-Pacific factor seven inquires as to the duration of the patent and terms of the license. The Court's inquiry into the length of the license is more appropriately construed in terms of an ongoing royalty, and will be addressed in that portion of the Court's findings.

Georgia-Pacific factor eight deals with the profitability of products made under the patent and the commercial success of those products. One of Centripetal's damages experts, Mr. Gunderson, presented detailed evidence of Cisco's profitability of the infringing products. The Federal Circuit has expressly noted that "anticipated incremental profits under the hypothesized conditions are conceptually central to constraining the royalty negotiation . . . [and] . . . [e]vidence

of the infringer's actual profits generally is admissible as probative of his anticipated profits." Aqua Shield v. Inter Pool Cover Team, 774 F.3d 766, 772 (Fed. Cir. 2014); see Sinclair Refining Co. v. Jenkins Petroleum Process Co., 289 U.S. 689, 698 (1933) (noting "[e]xperience is then available to correct uncertain prophecy"). In the context of the hypothetical negotiation, "the core economic question is what the infringer, in a hypothetical pre-infringement negotiation under hypothetical conditions, would have anticipated the profit-making potential of use of the patented technology to be, compared to using non-infringing alternatives." Aqua Shield, 774 F.3d at 770-71 (emphasis in original) (noting that "[i]f a potential user of the patented technology would expect to earn X profits in the future without using the patented technology, and X + Y profits by using the patented technology, it would seem, as a prima facie matter, economically irrational to pay more than Y as a royalty—paying more would produce a loss compared to forgoing use of the patented technology").

As probative evidence of anticipated profits, Mr. Gunderson provided percentages of Cisco's actual gross profit in the infringed products from June 20, 2017 to December 31, 2019:

Product	Gross Profit %
Catalyst Switches	67.8%
Aggregation Services Router	79.2%
Integration Services Router	82.0%
Adaptive Security Appliance	56.6%
Firepower Appliance	71.1%
Firepower Management Center	76.5%

Stealthwatch	81.4%
Identity Service Engine	91.5%
Digital Network Architecture	-1.9%

An examination of this data establishes that Cisco was reaping considerable profit margins on products that incorporate the infringing functionality. See Tr. 1495:16-1496:19. Moreover, a Cisco article, published on November 7, 2019, expresses the very high profitability of the new Catalyst 9000 series switches as compared to older models:

PTX-515

Cisco Article Published on Website from November 7, 2019


Cisco Blogs / Networking / Cisco Catalyst 9000 – The best keeps getting better.

November 7, 2019 5 Comments

Networking

Cisco Catalyst 9000 – The best keeps getting better.

While we recognize that we cannot predict the future, we understand that we can plan for the unknown by building flexibility into both our hardware and software. This was the design philosophy behind the Cisco Catalyst 9000 family and likely why it has been so successful. With the modular Cisco IOS XE and the programable UADP ASIC as its foundation, combined with the automation and assurance of Cisco DNA Center and SD-Access, Catalyst 9000 switches open the door for IT to shift focus from reactive analysis to predictive analytics, from using hands-on CLI-based, box-by-box interaction to network-wide automation and assurance.



Cisco More Than Doubles Its Catalyst 9000 Customer Base
Cisco winner in campus switching market

Venerable Cisco Catalyst 6000 switches ousted by new Catalyst 9600

Cisco's Catalyst 9K Switch
Propels the Company's Finances

Cisco CEO trumpets Catalyst 9K advances,
Robbins has said the Catalyst 9000 is the company's fastest-selling product ever.

Cisco drove Q1 campus switching market growth: report
Cisco's Catalyst 9000 switches helped fuel campus switching market growth in the first quarter of this year, according to a report by Dell'Oro Group.

There have been many highlights and headlines about the Catalyst 9000 product family and its meteoric rise since it was launched in June 2017:

- fastest ramping product in Cisco's history
- fastest to exceed $1B quarterly run rate
- over a million units shipped to tens of thousands of customers in every geography, vertical, and market segment.
- recognized by CRN as Product of the Year for 2017 and 2018 (when does 2019 awards come out?)

This is not by accident. And the positive headlines are not likely to stop. Key innovations like multigigabit technology, 90W UPOE+, Encrypted Traffic Analytics, and onboard app hosting help our

PTX-515. Additionally, Cisco presented no evidence to contest these profit margins or the cost of any non-infringing alternative that would achieve the same functionality as incorporated in the patented technology. See Tr. 1602:8-16 (Mr. Malackowski noting that "Cisco did not suggest or offer any alternatives or even what it would cost to come up with alternatives"). Therefore, at a hypothetical negotiation, Centripetal would hold a considerable advantage due to the lack of non-infringing alternatives and the ability for Cisco to make large profits from the use of the technology. This evidence of high profits and lack of alternatives supports a higher reasonable royalty rate. See Lucent Techs., Inc., 580 F.3d at 1335 (noting that approximately 70–80% profit margin of the products at issue supports a higher versus a lower reasonable royalty).

Additionally, Mr. Malackowski, Centripetal's expert on patent evaluation, testified to his understanding that the Keysight license was structured in the manner it was due partly to the fact that Keysight had no available alternative to infringing the patent technology. See Tr. 1602:8-23. Accordingly, the 10% rate on competing products in the Keysight license had incorporated Keysight's necessity of using the infringing technology. Here, similar circumstances would be prevalent at the hypothetical negotiation, such as Cisco's "anticipated" profit margins in using the patented functionality and also the fact that there are no suitable alternatives available. Consequently, this factor supports the Court's imposition of a higher royalty rate.

Georgia-Pacific factor nine asks the Court to look at the utility and advantages of the patented property over the old modes or device. When developing its cybersecurity software system, Cisco repeatedly spent considerable monies to acquire smaller companies that produced software security technology. From 2013 to 2015, Cisco acquired Sourcefire for $2.7 billion, Lancope for $435 million and ThreatGRID for an undisclosed amount. See Tr. 1605:6-15.

Combinations of technology acquired from these companies form the basic elements of the older Cisco technology which preceded the infringing systems. See Tr. 1605:6-23. Cisco took the acquired technology and came up with what it described as the first cybersecurity solution of its type in the industry by adding Centripetal's patented functionality. Accordingly, these dollar amounts that Cisco paid to acquire two of the three companies is compelling evidence that the underlying older components of the infringing system needed enhancement by adding the infringing functionality from Centripetal to become the industry leader in this new technology as it claims to be.

During trial, each of Cisco's experts on infringement, validity, and damages testified that the patented inventions add minimal value to the products. Their testimony is in direct conflict with Cisco's technical and marketing documents which contribute the addition of the infringing functionality as a "breakthrough" in building "an intelligent platform with unmatched security." PTX-1135 (Cisco Press Release from June 20, 2017, reproduced below); PTX-963.

The Network (/home)

Home (/home)

News Release (/Pressreleases)

Cisco unveils network of the future that can learn, adapt and evolve

June 20, 2017



Plaintiff's Trial Exhibit
PTX-1135
Case No. 18-cv-00094-HCM

Designed to be intuitive, Cisco's new network can recognize intent, mitigate threats through encryption, and learn over time, unlocking opportunities

SAN FRANCISCO — June 20, 2017 — Today Cisco unveiled intent-based networking solutions that represent one of the most significant breakthroughs in enterprise networking. The introduction is the culmination of Cisco's vision to create an intuitive system that anticipates actions, stops security threats in their tracks, and continues to evolve and learn. It will help businesses to unlock new opportunities and solve previously unsolvable challenges in an era of increasing connectivity and distributed technology.

This new network is the result of years of research and development by Cisco to reinvent networking for an age where network engineers managing hundreds of devices today will be expected to manage 1 million by 2020.

"The network has never been more critical to business success, but it's also never been under more pressure," said Chuck Robbins, chief executive officer for Cisco. "By building a more intuitive network, we are creating an intelligent platform with unmatched security for today and for the future that propels businesses forward and creates new opportunities for people and organizations everywhere."

Today companies are managing their networks through traditional IT processes that are not sustainable in this new age. Cisco's approach creates an intuitive system that constantly learns, adapts, automates and protects, to optimize network operations and defend against today's evolving threat landscape.

"Cisco's Encrypted Traffic Analytics solves a network security challenge previously thought to be unsolvable," said David Goeckeler, senior vice president and general manager of networking and security. "ETA uses Cisco's Talos cyber intelligence to detect known attack signatures even in encrypted traffic, helping to ensure security while maintaining privacy."

With the vast majority of the world's internet traffic running on Cisco networks, the company has used its unique position to capture and analyze this immensely valuable data by providing IT with insights to spot anomalies and anticipate issues in real time, without compromising privacy. By automating the edge of the network and embedding machine learning and analytics at a foundational level, Cisco is making the unmanageable manageable and allowing IT to focus on strategic business needs.

Already, 75 leading global enterprises and organizations are conducting early field trials with these next-generation networking solutions, including DB Systel GmbH, Jade University of Applied Sciences, NASA, Royal Caribbean Cruises Ltd., Scentsy, UZ Leuven and Wipro.

Informed by context and powered by intent

With this new approach, Cisco is changing the fundamental blueprint for networking with reimagined hardware and the most advanced software. This shift from hardware-centric to software-driven networking will enable customers to experience a quantum leap in agility, productivity and performance. The intuitive network is an intelligent, highly secure platform — powered by intent and informed by context:

- **Intent:** Intent-based networking allows IT to move from tedious traditional processes to automating intent, making it possible to manage millions of devices in minutes — a crucial development to help organizations navigate today's ever expanding technology landscape.
- **Context:** Interpreting data in context is what enables the network to provide new insights. It's not just the data that's important, it's the context that surrounds it — the who, what, when, where and how. The intuitive network interprets all of this, resulting in better security, more customized experiences and faster operations.
- **Intuition:** The new network provides machine-learning at scale. Cisco is using the vast data that flows through its networks around the world, with machine learning built in, and unleashing that data to provide actionable, predictive insights.

The technologies that power the Intuitive network

Cisco Digital Network Architecture (DNA) (http://www.cisco.com/c/en/us/solutions/enterprise-networks/index.html) provides customers with a portfolio of innovative hardware and software to bring the new era of networking to life. Today Cisco is introducing a suite of Cisco DNA technologies and services designed to work together as a single system and empower customers to move at digital speed:

CENTRIPETAL-CSCO 472946

Cisco repeatedly described the addition of Encrypted Traffic Analytics ("ETA") as solving the "network security challenge previously thought to be unsolvable." PTX-1135 (David Goeckeler, Cisco's Senior Vice President of Sales, representing Cisco's new technology). Additionally, these representations made by as dominant a company as Cisco would have a devastating impact upon Centripetal as the original inventor of the technology. Therefore, under factor nine, Cisco's technical and marketing documents, as well as previous business acquisitions, support a higher royalty rate, as the addition of the infringing technology greatly improved Cisco's sales and the profitability of its new infringing versions of the products over older models. See Deere & Co. v. Int'l. Harvester Co., 710 F.2d 1551, 1558 (Fed. Cir. 1983) (supporting a higher royalty rate in light of descriptions that the infringing product had a "bright future").

Cisco's representations are confirmed by the increase in revenues from previous non-infringing versions of the products vs. the new infringing models. Moreover, the increase in revenues can be analyzed under Georgia-Pacific factor eleven to show the great extent which Cisco has made use of the patented invention. The Court, at the end of the trial, requested both parties to supplement their damages reports with revenue data from the predecessor products compared to the infringing products. See Tr. 2967:17-2973:5. This table summarizes Centripetal's estimates regarding Cisco's revenue increase for the infringing products, after the date of first infringement, as compared to the predecessor products sales for the fiscal year before June 20, 2017:

Product	Increase in Revenues %	Increase in Revenues $ (in millions)
Switches	40.9%	$3,973.4
Routers	13.2%	501.5
Adaptative Security / Firepower	29.5%	550.4
Stealthwatch	36.0%	70.2
Firepower Management Center	3.5%	1.7
Identity Services Engine	52.0%	225.3
Digital Network Architecture[14]	100%	252.9
Total Increase		5,575.4

Tr. 3464:8-14 (Mr. Malackowski describing the increases in revenues for the infringing products). This data supports a finding that the addition of the infringing software functionality to older models of the infringing products support the economic reality of the enormous increase in revenues. There is no evidence that these increases in sales revenue were attributed to improvements in the hardware itself. The infringing software significantly improved existing hardware by not only adding security functionality, but speed and scalability as well. See Tr.

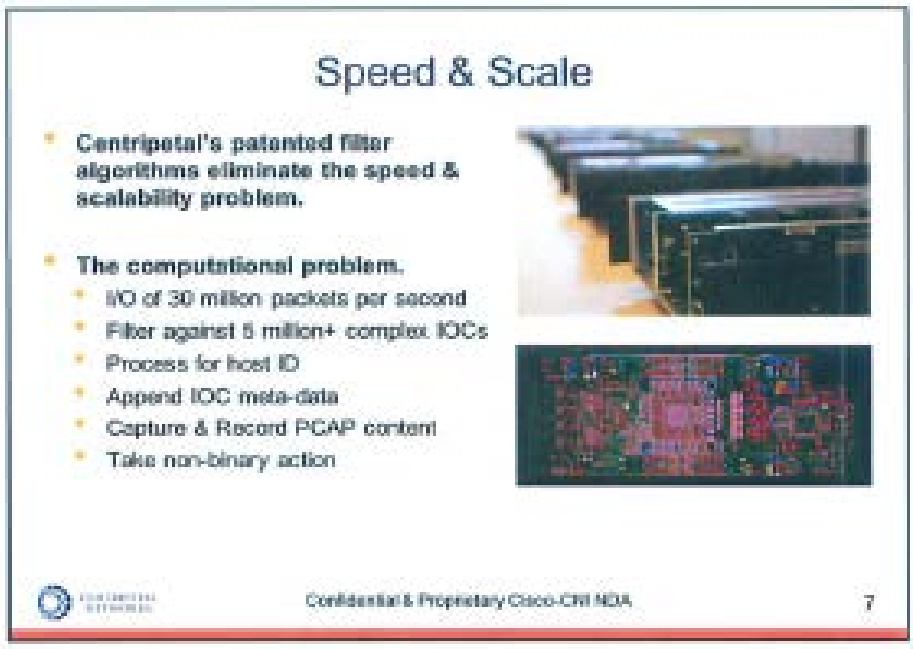
[14] There is 100% revenue increase for the Digital Network Architecture, as this product was released in mid-2017, and had no defined predecessor.

2621:5-10, 2634:14-18 (showing how ASICs process packets at high speeds and how Centripetal's rule swap technology aids that process and is disclosed in the '806 Patent); see PTX-547.

PTX-547

Centripetal Demonstrative Presentation Presented to Cisco About Patented Technology





Viewing both Cisco's technical documents, marketing representations and the sales data, the Court **FINDS** that the patented functionality added very significant value to the older technology. Therefore, this factor supports a substantially increased royalty figure.

Accordingly, based upon its analysis of the Georgia-Pacific factors, the Court determines that the weight of the factors as a whole strongly favors Centripetal. As a result, the Court **FINDS** that the Keysight royalty rate of **10%** of the apportioned value of its infringed technology is a reasonable royalty rate to compensate Centripetal for Cisco's past infringement. This figure is supported both by the comparable factors in the Keysight license and the weight of the Georgia-Pacific factors. Now that the Court has determined a reasonable royalty rate, it must determine the proper royalty base to which to apply the rate in order to reach the final lump sum pretrial damages.

Georgia-Pacific factor thirteen looks at the portion of the profit that arises from the patented invention itself as opposed to profit arising from unpatented features, such as the manufacturing process, business risks, or significant features or improvements added by the accused infringer. Therefore, instead of having a primary effect on the royalty rate, this factor is often used to determine the royalty base to which the rate is applied.

With regard to the proper royalty base, the Federal Circuit has noted that patent damages awarded for infringement "must reflect the value attributable to the infringing features of the product, and no more." Commonwealth Sci. & Indus. Research Org. v. Cisco Sys., Inc., 809 F.3d 1295, 1301 (Fed. Cir. 2015) (quoting Ericsson, Inc. v. D–Link Sys., Inc., 773 F.3d 1201, 1226 (Fed. Cir. 2014)). When an infringing product is comprised of multiple components, the infringing portions must be apportioned to represent the value contributed by solely the infringing functionality. See id. "The patentee must 'give evidence tending to separate or apportion the

[infringer]'s profits and the patentee's damages between the patented feature and the unpatented features, and such evidence must be reliable and tangible, and not conjectural or speculative.'" Finjan, Inc. v. Blue Coat Sys., Inc., 879 F.3d 1299, 1310 (Fed. Cir. 2018). The Federal Circuit has recognized "there may be more than one reliable method" in order to prove proper damages in an apportionment case. Id. at 1302. Therefore, the apportionment can be done by various ways including "by careful selection of the royalty base to reflect the value added by the patented feature, where that differentiation is possible; by adjustment of the royalty rate so as to discount the value of a product's non-patented features; or by a combination thereof." Ericsson, Inc. v. D-Link Sys., Inc., 773 F.3d 1201, 1226 (Fed. Cir. 2014).

This flexibility in methodology is centered on "the difficulty that patentees may face in assigning value to a feature that may not have ever been individually sold." Virnetx, Inc. v. Cisco Sys., Inc., 767 F.3d 1308, 1328 (Fed. Cir. 2014). Therefore, the integral inquiry is "whether the data utilized in the methodology is sufficiently tied to the facts of the case." Finjan, Inc., 879 F.3d at 1301-02 ("[C]ourts must be proactive to ensure that the testimony presented—using whatever methodology—is sufficiently reliable to support a damages award."). Sufficient reliability has "never required absolute precision in this task; on the contrary, it is well-understood that this process may involve some degree of approximation and uncertainty." Virnetx, Inc., 767 F.3d at 1328.

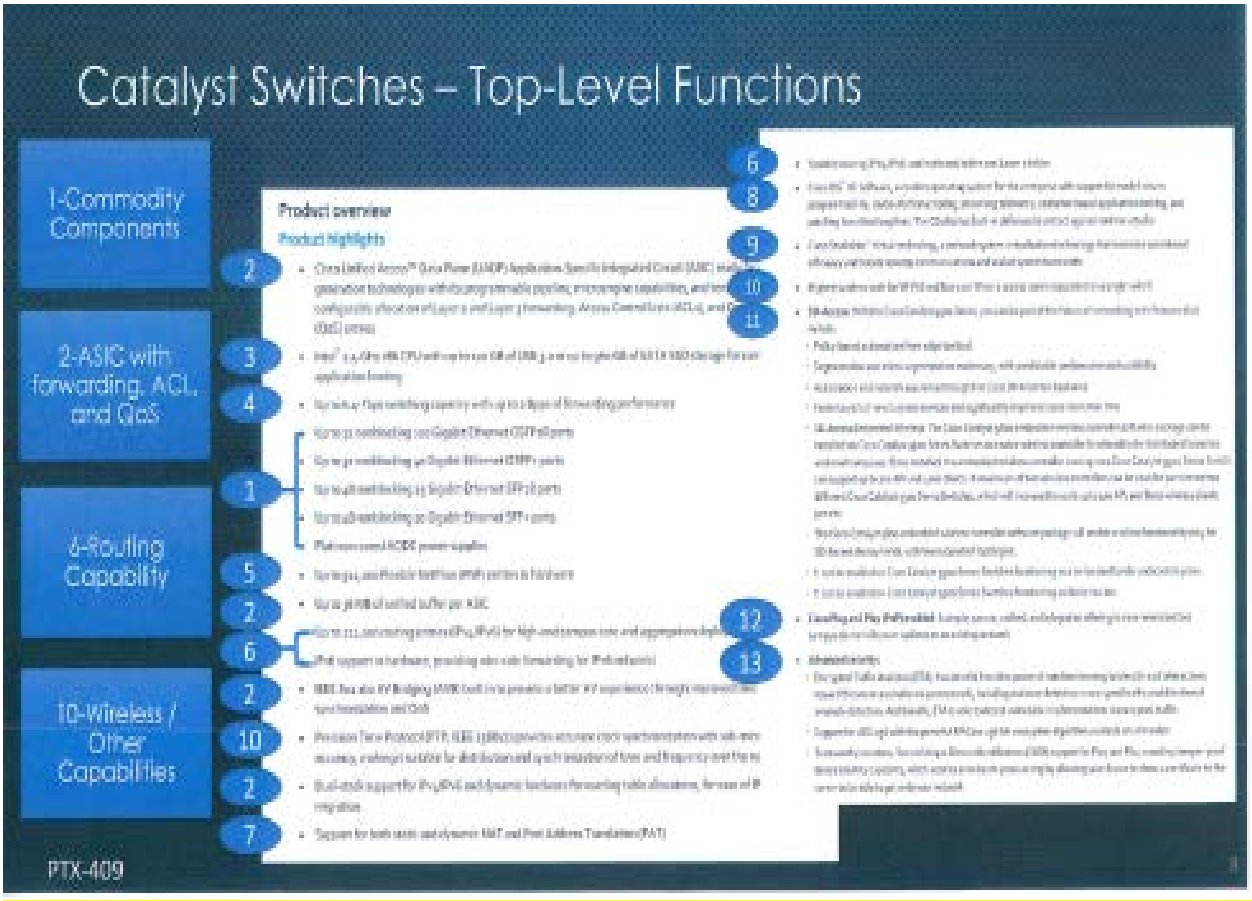
Here, Centripetal presented extensive apportionment evidence of the infringing products using the analysis of their apportionment expert, Dr. Striegel. Tr. 1337:19-1342:14. Before Dr. Streigel's testimony, Cisco objected to Dr. Streigel's apportionment opinion on the basis that his opinions do not satisfy the essential requirement for reliability under Daubert. Additionally, Cisco's expert, Dr. Becker, contends that "Dr. Striegel didn't do an incremental value analysis,"

and simply checked off functions as infringing that did not provide "any improvement to that aspect of the products." The Court disagrees on both grounds.

This is exactly the type of apportionment analysis that was performed in Finjan, Inc. v. Blue Coat Sys., Inc., for which the Federal Circuit found the jury was entitled to rely upon as substantial evidence to support damages. Finjan, Inc., 879 F.3d at 1313-14. In Finjan, Finjan's expert, Dr. Layne–Farrar, used the defendant's technical documents to separate the functionality of the accused product. Id. She assumed each box in a diagram of the product "represented one top level function and that each function was equally valuable." Id. Dr. Layne-Farrar relied on deposition testimony from defendant's employees and discussions with Finjan's technical expert, who "identified certain components within the diagram that did and did not infringe." Id. at 1313.

Here, Dr. Striegel performed an almost identical type of apportionment analysis to that of Dr. Layne-Farrar in Finjan. Using Cisco's technical specification of each of the products, Dr. Striegel identified the top-level functions of each of the products. Tr. 1337:21-23; see PTX-409. Dr. Striegel's process of identifying the top-level functions by using Cisco's technical documents is shown by slide eight from his demonstratives (using Catalyst Switches Product Overview, PTX-409, as an example for the analysis done with each product):

SLIDE 8 FROM DR. STRIEGEL PRESENTATION



See PTX-409 (for clear image of technical features). He then identified which of those top-level functions for each product are implicated by the asserted patents and their asserted claims. See PTX-1931. In order to analyze and present this technical apportionment, Dr. Striegel highlighted all of the materials he relied upon in this analysis:

> I looked at both public documentation as well as confidential documents including various articles, various videos, various tutorials. I also browsed through numerous depositions. I did have the opportunity to go and browse through the source code on-site. And then I also had discussions with our two other infringing technical experts, Dr. Cole and Dr. Mitzenmacher.

Tr. 1338:9-15. This is exactly the type of materials relied upon by Dr. Layne-Farrar in the Finjan case, where the Federal Circuit determined that the jury was entitled to rely upon such information as substantial evidence to support a damages award. Accordingly, the Court **FINDS** that Dr.

Striegel's analysis is admissible as "reliable and tangible" evidence of apportionment of the infringing products. See Ericsson, Inc., 773 F.3d at 1226 (highlighting that a court or jury must "apportion the defendant's profits and the patentee's damages between the patented feature and the unpatented features" using 'reliable and tangible' evidence"). Accordingly, the Court **FINDS** Dr. Striegel's apportionment evidence and analysis to be a reliable method to determine a royalty base.

As shown supra, Dr. Striegel opined on each of the infringing products, and determined how many of the top-level functions were implicated by infringement of the asserted patents. Dr. Striegel then determined an apportionment percentage for each of the infringing products based off this analysis. PTX-1931 is a summary of those findings made by Dr. Striegel (recreation of PTX-1931):

Product	Total # of Top-Level Functions	# Infringing Top-Level Functions	Apportionment %
Catalyst Switches	13	6 ['856 and '193 Patent] 5 ['176 Patent] 4 ['806 Patent]	31%[15]
Integrated Services Routers	9	4 [All Patents]	44%
Aggregated Services Routers	8	2 [All Patents]	25%

[15] Even though Dr. Striegel found that six of the thirteen functions were infringed by the '856 Patent and '193 Patent, he relied on the lower apportionment percentage of 31%. Therefore, the Court adopts that number for its determination of the royalty base in lieu of the 46% alternative based on the '856 Patent and the '193 Patent.

Firepower / ASA (including Firepower Management Center)	13	7 [‘806 Patent] [16]	54%
Digital Network Architecture	10	3 [‘806 Patent]	30%
Stealthwatch	5	4 [‘806 Patent]	80%
Identity Services Engine	13	5 [‘856 Patent]	38%

After Dr. Striegel’s technical apportionment, Centripetal’s expert on patent evaluation, Mr. Gunderson, applied these apportionment percentages to total sales revenues from the infringing products since the date of first infringement, June 20, 2017, through December 31, 2019. At the final damages hearing, these figures were updated through Cisco’s sales data ending on June 20, 2020 and totaled $21,467,079,878.00 billion. See Doc. 488, Ex. 7 (updated version produced at damages hearing). The Court adopts Centripetal’s exhibits outlining the sales revenues of Cisco. Cisco presented a patent by patent damages breakdown instead of a full picture of the sales of infringing products. The Court rejected the proposed patent by patent calculation of damages by Cisco’s expert Dr. Becker, in favor of the appointment method utilized by Centripetal’s experts approved by the Federal Circuit in Finjan, Inc. v. Blue Coat Sys., Inc., 879 F.3d 1299, 1310 (Fed. Cir. 2018).

[16] Since the ‘205 Patent was found to not infringe the higher number of infringing functionalities found for the ‘806 Patent is used for the Firepower / ASA because this would be the most accurate apportionment ratio. The Court has removed the ‘205 Patent from Dr. Striegel’s chart and applied a 54% apportionment for products where the apportionment was based on the ‘205 Patent. See Doc. 488, Ex. 7.

Here is a reproduction of the apportionment percentages applied to Cisco's gross revenues from June 20, 2017 through June 20, 2020, by using Centripetal's update to PTX-1629, Doc. 488, Ex. 7:

Product	Invoice Gross Revenue June 20, 2017 – June 20, 2020[17]	Apportionment Factor Percentage	Apportioned Revenue June 20,2017 – June 20, 2020
Catalyst Switches	$11,839,742,927	31%	$3,670,320,307
Integrated Services Routers	$2,375,633,299	44%	$1,045,278,652
Aggregated Services Routers	$3,456,557,172	25%	$864,139,293
Firepower Appliance (plus subscription)	$2,283,221,005	54%	$1,232,939,343
Adaptative Security Appliance (plus subscription)	$428,380,587	54%	$231,325,517
Firepower Management Center	$67,635,757	54%	$36,523,309
Digital Network Architecture	$252,855,962	30%	$75,856,789
Stealthwatch	$266,052,460	80%	$212,841,968
Identity Services Engine	$497,000,709	38%	$188,860,269
TOTAL	$21,467,079,878 (billion)		$7,558,085,447 (billion)

[17] As stated, supra, Centripetal's exhibit outlining the sales revenues of Cisco goes from June 20,2017 to June 20, 2020. See Doc. 488, Ex. 7 (updated version produced at damages hearing).

Accordingly, based on Mr. Gunderson and the Court's analysis, the Court **FINDS** that the correct apportioned royalty base is $7,558,085,447[18] for all of the infringing products based upon gross revenue through June 20, 2020. Doc. 488, Ex. 7. Moreover, as determined supra based on the Georgia-Pacific factors and the analysis of a hypothetical negotiation, the Court **FINDS** a **10%** royalty is appropriate in this case. Accordingly, before the Court adjusts for enhanced damages, the total past damages award is $755,808,545 million (10% royalty rate applied to $7,558,085,447 million royalty base).

ii. Findings of Fact Regarding Willful Infringement and Enhanced Damages

1. Centripetal's RuleGate product practices the patents found to be infringing in this case. Centripetal marks its RuleGate product with the patents that it practices. Tr. 1203:12-1204:3; PTX-528; Tr. 1383:18-1385:15; PTX-1215.

2. In 2015, Centripetal CEO Stephen Rogers had a meeting with Pavan Reddy, a Cisco employee, where Mr. Rogers disclosed Centripetal product offerings and the effectiveness of their solutions. Mr. Reddy and Mr. Rogers had a follow-up meeting in 2015, where Centripetal provided a demonstration of their system and explained why it was an effective method of cyber defense. Tr. 256:8-257:12.

3. As a result of these meetings, on January 26, 2016, Centripetal and Cisco entered into a nondisclosure agreement ("NDA"), requiring Cisco to keep Centripetal's confidential, proprietary or non-public information "strictly confidential" and "not use any Information in any manner . . . other than solely in connection with its consideration of" a possible partnership. Tr. 1213:16-20; PTX-99.

[18] The royalty base begins with the gross sales of the infringing products, whereas the chart outlining the increase in sales of the infringing products as compared to pre-June 20, 2017 sales of Cisco's predecessor products is estimated as $5,575.4 billion.

4. After Cisco executed the NDA, Centripetal, on February 4, 2016, presented in a WebEx meeting detailed, highly sensitive, confidential and proprietary information about its patented technology and products to Cisco, including details of its patented technology for the Asserted Patents. For example, Centripetal detailed how its "patented filter algorithms eliminate the speed and scalability problem," how its "patented system, live update, and correlation technologies 'automate workflow' and how its "patented" "instant host correlation" conveys "real time analytics." PTX-547 at 389-91; Tr. 258:21-25, 260:2-18; 1220:1-1222:25.

5. After the WebEx meeting, Cisco's Engineer, TK Keanini, who attended the WebEx meeting, wrote an internal email, stating the team should "look at these algorithms" that Centripetal had and "study their [patent] claims." Tr. 1128: 8-1129:5; PTX-134 at 3.

6. The next day, on February 5, 2016, Centripetal's Jonathan Rogers sent an e-mail to Cisco summarizing the WebEx meeting, noting that Cisco "seemed to hone in on our filter technology and algorithms. The algorithms are a significant networking technology with broad application that we've productized for security. There were also a few questions on our patents..." Tr. 1226:10-1227:18; PTX-102; PTX-1046

7. There were a number of follow up meetings with Cisco, including a request from Cisco's security architect, Joseph Muniz, who was very interested in Centripetal's patented technology. He requested and received a demonstration of Centripetal's patented RuleGate product, which he described in an online blog that educates Cisco employees entitled "Cool Tool: Centripetal Networks RuleGate – Threat Intelligence Tool," and where he stated, "I found this tool to be a pretty cool new approach to leveraging threat data." Tr. 1299:16-1300:7; 1308:5-15; PTX-548, PTX-550 at 647-49, 51.

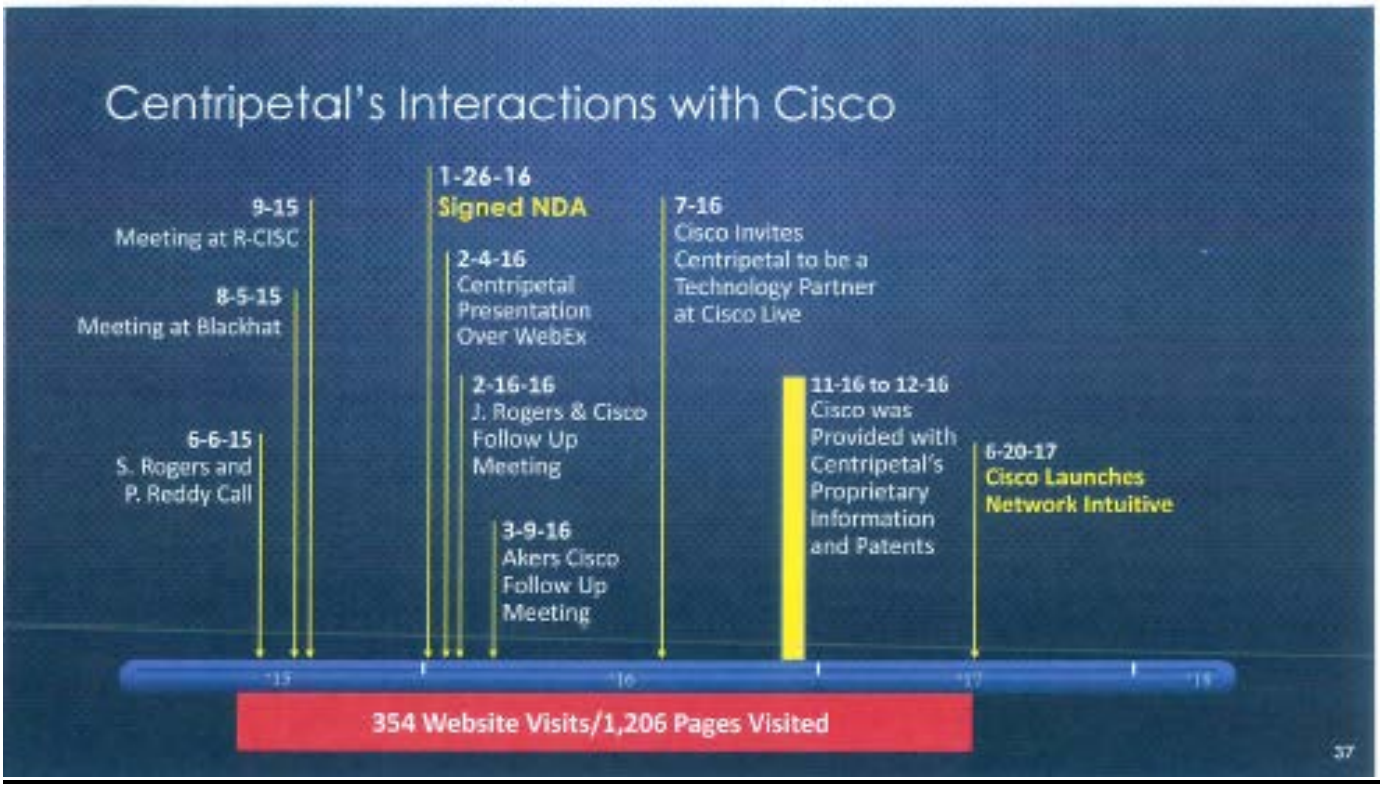
8. In November and December 2016, Cisco had several meetings with Oppenheimer

& Co., Inc. about Centripetal, pursuant to Centripetal's engagement with Oppenheimer to evaluate companies who were interested in making a strategic investment in Centripetal. In December 2016, Oppenheimer presented to Cisco additional information about Centripetal, including a list of Centripetal's patents issued at the time, product offerings that practice the patents, and a highly sensitive, detailed technical disclosure which detailed the core RuleGate functionalities covered by the Asserted Patents. Tr. 1235:11-20, 1237:25-1238:9, 1242:17-1243:11; DTX-1270 at 1, 25-28, 30.

9. After all of these detailed meetings with Centripetal, Cisco released its "network of the future" products on June 20, 2017, which incorporated Centripetal's patented technology. See PTX-1135. Below is Centripetal's demonstrative, Slide 37, presented during opening statements which accurate reflects the evidence presented at trial surrounding the events of Centripetal and Cisco's relationship[19].

[19] This slide does not attempt to reflect the numerous "hits" on Centripetal's website by Cisco's employees.

SLIDE 37 FROM CENTRIPETAL's OPENING STATEMENT



iii. Conclusions of Law Regarding Willful Infringement and Enhanced Damages

Under the patent damages provisions of 35 U.S.C. § 284, a court "may increase the damages up to three times the amount found or assessed." Halo Elecs., Inc. v. Pulse Elecs., Inc., 136 S. Ct. 1923, 1931 (2016) (quoting 35 U.S.C. § 284). The use of "may" in the statute indicates that enhancement under § 284 is within the discretion of the district court. Id. The Supreme Court in Halo Elecs., Inc. v. Pulse Elecs., Inc., explicitly noted that a court exercising discretion to award enhanced damages merits an analysis of "the particular circumstances of each case" unencumbered by the "inelastic constraints" of a rigid framework. Id. at 1932. Although the statute does not include a "precise rule or formula" for an enhanced damages award, the "court's discretion should be exercised in light of the considerations underlying the grant of that discretion." Id. Halo,

additionally, mandated that the award of enhanced damages is governed by a preponderance of the evidence standard. Id. at 1934.

Historically, enhanced damages have been reserved for infringement behavior that was found to be "egregious." Id. (explaining "through nearly two centuries of discretionary awards and review by appellate tribunals, "the channel of discretion ha[s] narrowed . . . so that such damages are generally reserved for egregious cases of culpable behavior"). The Halo decision highlights that enhanced damages are warranted as a "punitive" or "vindictive" sanction for egregious conduct described as "willful, wanton, malicious, bad-faith, deliberate, consciously wrongful, flagrant or – indeed – characteristic of a pirate." Id. at 1932.

Additionally, the Supreme Court noted that even if these types of conduct traditionally underlie enhanced damages, there is no requirement that the court find egregious conduct to award enhanced damages. Id. at 1933. Accordingly, in deciding to award enhanced damages, a court, in its discretion, "should take into account the particular circumstances of each case," while remembering the historical underpinnings that enhanced damages should generally "be reserved for egregious cases typified by willful misconduct." Id. at 1933-34.

The factors laid out in Read Corp. v. Portec, Inc., 970 F.2d 816, 826-827 (Fed. Cir. 1992), overruled on other grounds by Markman v. Westview Inst. Inc., 52 F.3d 967 (Fed. Cir. 1995), have been used post-Halo to aid a district court's determination of whether a case's circumstances warrant enhanced damages. See Mich. Motor Techs. LLC v. Volkswagen Aktiengesellschaft, No. 19-10485, 2020 U.S. Dist. LEXIS 122276, at *11 (E.D. Mich. July 13, 2020) (noting that the Read factors are a useful guide, but stating that Halo has eliminated "any rigid formula or set of factors"). These factors are not an exhaustive list, but provide a meaningful guide to determine if the infringer's conduct was "willful, wanton, malicious, bad-faith, deliberate,

consciously wrongful, or flagrant." See id.; Finjan, Inc. v. Blue Coat Sys., Inc., 13-CV-03999-BLF, 2016 WL 3880774, at *16 (N.D. Cal. July 18, 2016) (applying the Read factors to determine if the infringing conduct warrants enhanced damages). The Read factors are:

> (1) deliberate copying;
>
> (2) defendant's investigation and good faith-belief of invalidity or non-infringement;
>
> (3) litigation behavior;
>
> (4) defendant's size and financial condition;
>
> (5) closeness of the case;
>
> (6) duration of the misconduct;
>
> (7) remedial action by the defendant;
>
> (8) defendant's motivation for harm; and
>
> (9) attempted concealment of the misconduct.

Green Mt. Glass LLC v. Saint-Gobain Containers, Inc., 300 F. Supp. 3d 610, 628 (D. Del. 2018) (citing Read Corp., 970 F.2d at 816, 826–27). The Federal Circuit in WBIP, LLC v. Kohler Co., distinctly declined to interpret Halo as changing the requirement that willfulness should be decided by the finder of fact before the court determines whether enhanced damages are warranted as a matter of law. See WBIP, LLC v. Kohler Co., 829 F.3d 1317, 1341 (Fed. Cir. 2016). Therefore, the Court, as fact-finder, will address the issue of willful infringement and enhanced damages in tandem, as the Read factors adequately address both issues.

Moreover, the Federal Circuit has outlined that "[k]nowledge of the patent alleged to be willfully infringed continues to be a prerequisite" to the court finding that enhanced damages are warranted. Id. Therefore, prior knowledge of the patents at issue appears to be "a necessary but

not sufficient condition for an award of enhanced damages." Mich. Motor Techs. LLC, 2020 U.S. Dist. LEXIS 122276, at *11-13 (collecting cases noting pre-suit knowledge of the patent is not alone sufficient to uphold a finding of willfulness and requires more factual allegations to meet Halo's egregious conduct standard). Accordingly, in light of this guidance, the Court will first determine if Cisco has pre-suit knowledge of the patents at issue. Second, the Court will use the Read factors to aid its analysis of whether infringement of the patents was willful, and to what degree enhanced damages should be assessed under the circumstances. The Court **FINDS** that Cisco willfully infringed the '856 Patent, the '176 Patent, the '193 Patent, and the '806 Patent, therefore enhanced damages are warranted under the evidence.

The facts illustrate that Cisco had pre-suit knowledge of Centripetal's asserted patents. First, after signing an NDA, Centripetal presented a detailed PowerPoint presentation to Cisco employees that laid out their patented technology. PTX-547 at 389-91; Tr. 258:21-25, 260:2-18; 1220:1-1222:25. This meeting was presented by Jonathan Rogers, who testified that, at this meeting, he:

> highlighted the technologies that were patented. We had a number of questions there, and I was offering to have additional discussion on that, as well, if it would be helpful.

Tr. 1227:15-18. Contemporaneous emails sent by Jonathan Rogers to the Cisco team state that he was willing to share more information on the patented technology, as the group asked, "a few questions on our patents." PTX-102. This knowledge of the patents is confirmed by internal emails of Cisco's engineer, TK Keanini, which detailed the type of functionality covered by Centripetal's intellectual property and expressing interest in "study[ing] their claims." PTX-134 at 3; see Tr. 1128:8-1129:5. Moreover, a third-party firm, Oppenheimer, met with Cisco to discuss Centripetal's product offerings that practice the patents, and presented a highly sensitive, detailed

technical disclosure, which detailed the core RuleGate functionalities covered by the Asserted Patents. Tr. 1235:11-20, 1237:25-1238:9; 1242:17-1243:11; DTX-1270 at 1, 25-28, 30.

Second, Centripetal has marked its RuleGate product with a notice indicating the patents practiced by the device. PTX-528 (showing a photograph of the RuleGate device clearly marked with the asserted patents). The evidence presented at trial indicates that the RuleGate device was presented and demonstrated to Cisco employees, indicating that they had direct contact with the label showing the practiced patents. See WBIP, LLC, 829 F.3d at 1342 (noting the marking of a device with the asserted patents is supporting evidence that the infringer knew of the patents). Accordingly, the pre-infringement events indicate that Cisco had direct knowledge of the asserted patents and the functionality of the claims. The Court broadly considers all the circumstances of the case, but several of the Read factors are particularly instructive in the Court's analysis of enhanced damages.

Turning to the Read factors, factor one inquires whether there was deliberate copying of the "ideas and design" of the elements of the claim or the commercial embodiment of the patent. See Read, 970 F.2d at 827 n.7; Arctic Cat Inc. v. Bombardier Recreational Prods., Inc., 198 F. Supp. 3d 1343, 1350 (S.D. Fla. 2016), aff'd, 876 F.3d 1350 (Fed. Cir. 2017). The case of Arctic Cat Inc. v. Bombardier Recreational Products, Inc has similar factual relation to the case here. There, defendant BRP had multiple meetings with Arctic Cat, including testing and demonstrations of its patented embodiment. Id. After meetings and testing, BRP stated that they were not interested in the technology and stopped negotiations with Arctic Cat. Id. Then, four years later, BRP began infringing Arctic Cat's patents after abandoning its own process. Id. The district court found that BRP's development of "a very similar system under these circumstances [was] strong evidence of copying and favor[ed] enhancing damages." Id. Similarly, here, Cisco had multiple meetings with

Centripetal employees and provided detailed presentations of the patents and their functionality. See Georgetown Rail Equip. Co. v. Holland L.P., 6:13-CV-366, 2016 WL 3346084, at *17 (E.D. Tex. June 16, 2016), aff'd, 867 F.3d 1229 (Fed. Cir. 2017) (showing disclosure of patented systems under a non-disclosure as evidence of copying).

As detailed in the Court's factual findings, Cisco was provided with demonstrations of the product and confidential information regarding Centripetal's proprietary algorithms. Within a year of these meetings, Cisco released the "network of the future," involving the release of older products embedded with new software functionality that was outlined and detailed to them by disclosure of the patents and multiple technical discussions and demonstrations. The fact that Cisco released products with Centripetal's functionality within a year of these meetings goes beyond mere coincidence. Therefore, the fact that Cisco's system mirrors the functionality of the Centripetal patents is compelling evidence that damages should be enhanced for copying. See Crane Sec. Techs., Inc. v. Rolling Optics AB, 337 F. Supp. 3d 48, 57 (D. Mass. 2018) ("The Court observes that the similarities of RO's technology to Crane's patented invention, coupled with RO's extensive knowledge of Crane's intellectual property rights and products, support the inference of copying that favors enhancement.")

The second Read factor is "whether the infringer, when he knew of the other's patent protection, investigated the scope of the patent and formed a good-faith belief that it was invalid or that it was not infringed." Read, 970 F.2d at 827. Cisco presented no evidence of any such investigation and its own technical and marketing documents suggest it would have been difficult to form such a belief.

With respect to Read factor three, Cisco's trial attorneys' hands were tied by Centripetal's use of Cisco's own technical documents, coupled with the adverse testimony of Cisco engineers.

Cisco had to shield the engineers who authored its current technical documents and the executives who praised its new security functionality for "solving problems previously thought unsolvable" from answering to their own writings and statements.

On the other hand, while Cisco objected to trying the case on a video/audio platform, and specifically the platform upon which the Court's staff was trained, its counsel teamed with Centripetal's counsel to formulate protocols which expanded and improved upon the Court's standard protocols to promote a more reliable and efficient trial by remote means. Counsel for both parties faithfully followed all of the protocols, were both very well prepared, were mostly courteous to one another and joined in congratulating the Court's staff on its efficient handling of the trial. Accordingly, while this factor favors enhanced damages, it is mitigated by the professional performance of its trial counsel.

The fourth Read factor looks at the infringer's size and financial condition. Cisco represents itself as the largest provider of network infrastructure and services in the world. PTX-570 at 991. As discussed supra, Cisco saw an increase of approximately $5.575 billion dollars over three years by adding the infringing functionality to the predecessor non-infringing product lines. Additionally, Cisco had substantial profit margins during the infringing period from 52% to 92% on the infringing products.[20] See Creative Internet Advert. Corp. v. Yahoo! Inc., 689 F. Supp. 2d 858, 866 (E.D. Tex. 2010) (showing high profit margins as evidence that favors enhanced damages). Accordingly, for a company as large as Cisco with these levels of revenues and profits, an enhanced damages award would not "unduly prejudice [Cisco's] non infringing business." Georgetown Rail Equip. Co., 2016 WL 3346084, at *19 (quoting Creative Internet Advert. Corp.,

[20] The Court leaves out the Digital Network Architecture from this range, as it represents a statistical outlier and it was stated that DNA was a new product with no defined predecessor.

689 F. Supp. 2d at 866). Therefore, based on Cisco's immense size and commercial success with the infringing products, this factor weighs strongly in favor of enhanced damages.

Read factor five deals with the closeness of the case. The Court **FINDS** that the rulings on the four patents that were found infringed and valid were clear and not a close call. In the presentation of its defense, Cisco repeatedly relied upon animations prepared ex post facto for trial, while ignoring their own technical documents. The great majority of the Cisco technical documents were introduced by Centripetal. Not only did the animations conflict with Cisco's own technical documents, but in several instances contradicted Cisco's employee witnesses. Cisco avoided calling the authors of its technical documents as well. There was no testimony that Centripetal attempted to broaden the reach of the four infringed patents, thus opening the door to additional prior art. See 01 Communique Lab., Inc. v. Citrix Sys., 889 F.3d 735, 742 (Fed. Cir. 2018). Nonetheless, Cisco, in its invalidity case, cited its old technology as prior art, while claiming its new technology did not infringe. This led to many inconsistencies in its evidence, on both issues. Of course, Cisco could not rely upon its own documents, as they proved Centripetal's case.[21] Therefore, this factor weighs heavily in favor of enhanced damages.

Read factor six addresses the duration of the misconduct and Read factor seven weighs the remedial action taken by the infringer. While Read factor nine looks at whether the infringer attempted to conceal any misconduct.[22] The infringing conduct has been continuous and unabated without any form of remedial action from June 20, 2017 to the present time. See Acantha LLC v. Depuy Synthes Sales, Inc., 406 F. Supp. 3d 742, 761 (E.D. Wis. 2019) (citing Broadcom Corp. v. Qualcomm Inc., No. SACV 05-467-JVS, 2007 U.S. Dist. LEXIS 62764, 2007 WL 2326838, at *3

[21] The ruling on the '205 Patent was equally clear in favor of Cisco, yet this was the sole patent found not to clearly infringe.
[22] Read factor eight addresses the infringer's motivation for harm. There was no evidence presented on this factor.

(C.D. Cal. Aug. 10, 2007) ("The length of [defendant's] infringement (approximately two years), coupled with the fact that infringement continued after [plaintiff] filed suit, supports an increase in damages.")); see also Crane Sec. Techs., Inc. v. Rolling Optics AB, 337 F. Supp. 3d 48, 59 (D. Mass. 2018) (no remedial action supporting treble damages). Moreover, Cisco, through its course of conduct, continually gathered information from Centripetal as if it intended to buy the technology from Centripetal. Cisco, then, appropriated the information gained in these meetings to learn about Centripetal's patented functionality and embedded it into its own products. See Liqwd, Inc. v. L'Oréal USA, Inc., No. 17-14-JFB-SRF, 2019 U.S. Dist. LEXIS 215668, at *21 (D. Del. Dec. 16, 2019) (noting how the defendants "concealed their misconduct in gathering information from the plaintiffs so as to create the infringing products" and weighing this factor in favor of enhanced damages). Therefore, all three of these factors weigh in favor of enhanced damages.

The Court **FINDS** that Cisco did not advance any objectively reasonable defenses at trial as to the four infringed and valid patents including the '856 Patent, the '176 Patent, the '193 Patent, and the '806 Patent. Its non-infringement case was grounded upon their old technology. The infringing functionality was added to their accused products post June 20, 2017, and resulted in a dramatic increase in sales which Cisco touted in both technical and marketing documents.

Cisco's invalidity evidence often contradicted its non-infringement evidence and failed to recognize the new functionality which it copied from Centripetal during and after the Nondisclosure Agreement. PTX-99. It embedded the copied software functionality from the patents in its post June 20, 2017 switches, routers and firewalls and then ignored the accused products while claiming its pre-June 20, 2017 technology as prior art. Moreover, its damages evidence was deeply flawed in attempting to base its calculations on each patent separately instead

of considering its own sales of the infringing products. Again, the increase in its sales of the accused products illustrates how completely unrealistic its damages evidence was compared to the reality of the marketplace. Accordingly, in the exercise of its discretion, the Court considers the sound legal principles underlying the history of enhanced damages and **FINDS** this is an egregious case of willful misconduct beyond typical infringement. Halo Elecs., Inc., 136 S. Ct. at 1935.

However, there are other considerations. Cisco did prevail as to one of the patents. In considering the cases awarding enhanced damages, and comparing these cases to this case, the Court **FINDS** that enhancing the damages by a factor of 2.5 is appropriate. Accordingly, the Court's past damages award of $755,808,545 is properly enhanced by a multiple of 2.5 times to award lump sum past damages of $1,889,521,362.50.

iv. Pre-judgment Interest

35 U.S.C. § 284 grants the Court discretionary authority to award interest and costs. 35 U.S.C. § 284; see General Motors Corp. v. Devex Corp., 461 U.S. 648, 653 (1983). The Supreme Court has interpreted the interest provision of section 284 and has instructed courts that pre-judgment interest should ordinarily be awarded, "absent some justification for withholding such an award." Id. at 657. The Supreme Court determined that the "fixed by the court" language in section 284 leaves the court's some discretion in awarding pre-judgment interest. Id. at 656-57. In determining the rate of pre-judgment interest, "the district court has the discretion to determine whether to use the prime rate, the prime rate plus a percentage, the U.S. Treasury rate, state statutory rate, corporate bond rate, or whatever rate the court deems appropriate under the circumstances." Century Wrecker Corp. v. E.R. Buske Mfg. Co., 913 F. Supp. 1256, 1280 (N.D. Iowa 1996) (citing Allen Archery, Inc. v. Browning Manuf. Co., 898 F.2d 787, 789 (Fed. Cir. 1990)).

Here, the Court will use the statutory post-judgment rate from the date of first infringement June 20, 2017, of 1.21%. See 28 U.S.C. § 1961. The Court calculates simple interest at the 1.21% rate over the infringement period of three years from June 20, 2017 to June 20, 2020 using the award of damages (excluding enhanced damages) of $755,808,545. This calculation makes an interest determination of $27,243,850.[23] The Court divides this number by two to account for the fact that infringement occurred over this three-year period. Accordingly, the total interest number awarded by the Court is $13,717,925. This interest is added to the final damages award, including the damages enhancement, to reach a final past damages award of $1,903,239,287.50.

B. FUTURE DAMAGES

"There are several types of relief for ongoing infringement that a court can consider: (1) it can grant an injunction; (2) it can order the parties to attempt to negotiate terms for future use of the invention; (3) it can grant an ongoing royalty; or (4) it can exercise its discretion to conclude that no forward-looking relief is appropriate in the circumstances." Whitserve, LLC v. Comput Packages, Inc., 694 F.3d 10, 35 (Fed. Cir. 2012). As described herein, the Court has considered the evidence presented at trial and the arguments and proposed findings of fact and conclusions of law advanced by all parties, and **FINDS** that a permanent injunction is not appropriate relief for the infringement of the '856 Patent, the '176 Patent, the '193 Patent, or the '806 Patent, and that an ongoing, future royalty should be imposed for all four Patents.

i. Injunctive Relief

Centripetal requests injunctive relief with regard to Cisco's firewall products. In order to merit injunctive relief, Centripetal must prove: "(1) that [they have] suffered an irreparable injury; (2) that remedies available at law, such as monetary damages, are inadequate to compensate for

[23] This was calculated using a simple interest formula - I = P x R x T (27,243,850 = 755,808,545 x .0121 x 3).

that injury; (3) that, considering the balance of hardships between the [Proponents and Opponents], a remedy in equity is warranted; and (4) that the public interest would not be disserved by a permanent injunction." eBay, Inc. v. MercExchange, LLC, 547 U.S. 388, 391 (2006). "[A]n injunction is a drastic and extraordinary remedy, which should not be granted as a matter of course." Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 165 (2010) (citing Weinberger v. Romero–Barcelo, 456 U.S. 305, 311-12 (1982)). "If a less drastic remedy . . . [is] sufficient to redress [Proponents'] injury, no recourse to the additional and extraordinary relief of an injunction [is] warranted." Id. at 165-66. If the Court were to grant an injunction, it would do so on every infringing product and not solely on Cisco's firewalls, as Centripetal originally requested.[24] Moreover, the test for injunctive relief is not met in this case. Cisco's switches, routers, and firewalls make up large portions of the global internet infrastructure. These products are components of both civilian and military networks. Therefore, granting an injunction on the infringing products will likely cause massive adverse effects on the functional capabilities of Cisco's customers and have an adverse ripple effect on national defense and the protection of the global internet.

Therefore, as to factor two, monetary damages are more appropriate to compensate Centripetal for patent infringement. The Keysight license shows that Centripetal is willing to patent its technology to direct competitors. Courts have stated that an injunction is improper where a patent owner has shown that they are willing to accept monetary damages. See EcoServices, LLC v. Certified Aviation Servs., LLC, 340 F. Supp. 3d 1004, 1023 (C.D. Cal. 2018); Cave Consulting Grp., LLC v. Optuminsight, Inc., No. 5:11-CV-00469-EJD, 2016 WL 4658979, at *21 (N.D. Cal. Sept. 7, 2016) (finding that where a patent holder is willing to "forego its patent rights for

[24] Centripetal later expanded its request for injunctive relief to additional products. While EBay factor one has been clearly proven, factor two has clearly not.

compensation," "monetary damages are rarely inadequate"); see also Advanced Cardiovascular Sys., Inc. v. Medtronic Vascular, Inc., 579 F. Supp. 2d 554, 560 (D. Del. 2008) ("The fact that [plaintiff] was selective regarding its licensing compensation—exchanging its technology only for other licenses to competing technology—does not rectify the fact that [plaintiff] was willing, ultimately, to forego its exclusive rights for some manner of compensation. Money damages are rarely inadequate in these circumstances."). As to factor three, the greater hardship would clearly impact Cisco. Factor four, the public interest, does not support injunctive relief for the same reasons outlined as to factor two. Accordingly, for these reasons, the Court **FINDS** that an injunction is not an appropriate legal remedy for Cisco's infringement.

ii. Ongoing Royalty

Rather, the Court **FINDS** that an ongoing royalty is proper in this case. An ongoing royalty is essentially a compulsory license for future use of the patented technology during the life of the patents. Indeed, pre-verdict and post-verdict royalties are "fundamental[ly] differen[t]." XY, LLC v. Trans Ova Genetics, 890 F.3d 1282, 1397 (Fed. Cir. 2018). When setting an ongoing royalty for future use, the district court should consider "the change in the parties' bargaining positions, and the resulting change in economic circumstances." See id., ("When patent claims are held to be not invalid and infringed, this amounts to a 'substantial shift in the bargaining position of the parties."') (quoting ActiveVideo Networks, Inc. v. Verizon Commc'ns, Inc., 694 F.3d 1312, 1342 (Fed. Cir. 2012)). Such differences include a Court's determination that certain of the patents at issue are valid, enforceable, and would be infringed by the accused products. See id.

The Court should analyze future royalties in the context of the Georgia-Pacific factors. Indeed, this is the approach adopted by other district courts, after modifying the Georgia-Pacific analysis to resolve any uncertainty as to whether the accused product will infringe the patent

claims, whether the asserted patents are enforceable, and whether the asserted patent claims are valid. See Creative Internet Advert. Corp. v. Yahoo! Inc., 674 F. Supp. 2d 847, 860 (E.D. Tex. 2009); Paice LLC v. Toyota Motor Corp., 609 F. Supp. 2d 620, 623-24 (E.D. Tex. 2009); Boston Sci. Corp. v. Johnson & Johnson, No. C 02-00790 SI, 2009 WL 975424 (N.D. Cal. Apr. 9, 2009). As discussed supra, this Court has analyzed the Georgia-Pacific factors in the context of past damages. The Court, here, incorporates its analysis of the previous Keysight license but takes into consideration the distinct differences in determining a past damages award as opposed to an ongoing royalty. Therefore, as it did before, the Court **FINDS** the Keysight license as a comparable license for use in determining ongoing royalties. In light of that, the Court **FINDS** an appropriate future royalty is **10% on the APPORTIONED REVENUES OF THE INFRINGING PRODUCTS FOR THREE (3) YEARS**, beginning June 21, 2020 and payable annually beginning June 20, 2021, without interest. The revenues shall be apportioned in the same manner as the pre-judgment damages, and shall apply to the infringing technology as described in the Court's Findings of Fact and Conclusions of Law. Successor products to the infringing product shall pay the same percentage royalty on sales revenue as applied to the current infringing products, so long as the successor products contain any technology found to infringe in this Opinion and Order. As to the four patents infringed, assigning different nomenclature to infringing products, or to Cisco's software technology found to infringe, shall not relieve Cisco of its obligation to pay its royalty. After this three-year term, the Court **FINDS** the royalty should be decreased to **5% FOR ANOTHER THREE (3) YEAR TERM**. Due to Cisco's dominant position in the cyber security software and firewall markets and the resulting damage to Centripetal as the first inventor the Court **FINDS** a six year term is called for in lieu of the three year term agreed upon in Keysight. Similar to the Keysight license, the Court imposes a minimum and maximum on the imposed

ongoing royalty. For the **first three-year term at 10%,** such annual royalty **shall not be less than $167,711,374.10** and **shall not be more than $300,076,834.** For the **second three-year term at 5%,** such annual royalty **shall not be less than $83,855,867.00** and **shall not be more than $150,038,417**. The maximum and minimum of each year is based upon the highest and lowest years of apportioned revenues per a full year of infringement from the 2017-2020 time frame. See Doc. 411 Ex. 7. Similarly, the maximum and minimum is reduced by one-half during the second three year term to reflect the reduced royalty rate. See id. At the conclusion of this second term of three years, there shall be no further monetary payments or other relief for the sale or use of the infringing products or their successors[25].

VII. CONCLUSION

For the reasons stated within, the Court **FINDS** the '856 Patent, the '176 Patent, the '193 Patent, and the '806 Patent claims valid and literally **INFRINGED** and the '205 Patent **NOT INFRINGED**. The Court **FINDS** the actual damages suffered by Centripetal as a result of infringement total $755,808,545; that the infringement was willful and egregious and shall be enhanced by a factor of 2.5x to equal $1,889,521,362.50. The Court awards pre-judgment interest of $13,717,925 applied to the actual damages before enhancement plus its costs. This, accordingly, equals a total award of $1,903,239,287.50 payable in a lump sum due on the judgment date. The Court, additionally, imposes a running royalty of 10% on the apportioned sales of the accused products and their successors for a period of three years followed by a second three year term with a running royalty of 5% on said sales upon the terms described supra. It **DENIES** any further relief to Centripetal at the termination of the second three year term.

[25] The minimums and maximums are based upon the minimum apportioned annual revenue of $167,711,374.10 for the period of June 20, 2017 to June 20, 2018 and the maximum apportioned annual revenue of $300,076,834.00 for the period of June 20, 2018 to June 20, 2019.

The Clerk is **REQUESTED** to electronically deliver a copy of this Opinion and Order to all counsel of record.

It is **SO ORDERED**.

/s/
HENRY COKE MORGAN, JR.
SENIOR UNITED STATES DISTRICT JUDGE

October 5, 2020
Norfolk, Virginia

APPENDIX A
EXPLANATION OF ABBREVIATIONS

Computer engineers use abbreviations to describe basic functionality as well as to describe the specific functionality of individual patented technology. To assist with interpreting their testimony and documents, the Court has compiled a list of the abbreviations used in the testimony and documents cited in this opinion.

ACL	Access Control List
ACE	Access Control Entry
ANC	Adaptive Network Control
ASA	Adaptive Security Appliance
ASDM	Adaptive Security Device Manager
ASR	Aggregation Services Router
ASIC	Application-Specific Integrated Circuit
CLI	Command Line Interface
CPU	Central Processing Unit
CRM	Computer-Readable Media
CSIRT	Computer Security Incident Response Team
CTA	Cognitive Threat Analytics
CTI	Cyber Threat Intelligence
DNA	Digital Network Architecture

DNS	Domain Name Server
DOE	doctrine of equivalents
ETA	Encrypted Traffic Analytics
FC	Flow Collector
FMC	Firepower Management Center
GACL	Group Access Control List
HTTP/HTTPS	HyperText Transfer Protocol (Secure)
ISE	Identity Services Engine
IDP	Initial Data Packet
IDS	Intrusion Detection System
IOS-XE	Internetwork Operating System – XE
IT Manager	Information Technology Manager
ISR	Integrated Services Router
IP	Internet Protocol
IPR	*inter partes* review
IPS	intrusion prevention system
IDS	intrusion detection system

ML	Machine Learning
NAT	network address translation
NSEL	NetFlow Secure Event Logging
PBC	Packet Buffer Complex
PTAB	Patent Trial and Appeals Board
SD-Access	Software Defined Access
SGACL	Security Group Access Control List
SGT	Security Group Tag
SPLT	Sequence of Packet Lengths and Times
SIO	Security Intelligence Operations
SIP	Session Initiation Protocol
Stealthwatch	Stealthwatch Enterprise
SLIC	Stealthwatch Labs Intelligence Center
SMC	Stealthwatch Management Console
SMTP	Simple Mail Transfer Protocol
SNI	Server Name Indication
SSL	Secure Sockets Layer

TID	Threat Intelligence Director
TCAM	Ternary Content-Addressable Memory
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
UADP	Unified Access Data Plane
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VoIP	Voice over Internet Protocol
VMR	Virtual Media Recorder
VPN	Virtual Private Network

APPENDIX B
OUTLINE OF COURT'S PROTOCOLS FOR TRIAL

B. Exhibits

1. Exhibit Lists

The parties have segregated the documents, summaries and other exhibits that may be offered into evidence at trial into exhibit lists. A joint Exhibit List, including documents identified by both parties and not objected to, is attached as Exhibit A; Centripetal's Exhibit List and Defendants' objections thereto are attached as Exhibit B; Defendants' Exhibit List and Centripetal's objections thereto are attached as Exhibit C. The parties reserve the right to object to any additional documents sought to be added to the Exhibit Lists and further reserve the right to object to any additional documents added to the Exhibit Lists under the Federal Rules of Evidence, the Federal Rules of Civil Procedure, or any other appropriate basis.

2. Efforts to Resolve Objections

The parties have been working diligently to resolve or narrow all objections lodged as to their respective exhibits. The parties have successfully resolved many objections and will continue their effo1is to resolve the objections to each other's proposed exhibits.

3. Exhibits to Which No Objections Have Been Made

The parties agree that the documents, summaries and other exhibits listed on their Exhibit Lists to which no objection has been specified may be introduced into evidence, without the necessity of further proof of admissibility through a witness, subject to foundational requirements, provided that a witness offers testimony about the exhibit at trial, either live or by deposition. This is without prejudice to motions in Limine and Daubert motions concerning certain of these documents and related testimony.

4. Cross Examination and Impeachment Exhibits

The Exhibit Lists set forth the parties' exhibits for their respective cases-in-chief; the lists do not include potential cross examination or impeachment exhibits that may or may not be introduced into evidence. The Exhibits Lists also include documents relied upon by experts in rendering opinions which may or may not be introduced into evidence. The parties reserve the right to offer exhibits for purposes of impeachment that are not included in the Exhibit Lists.

5. Authenticity Stipulations For Exhibits

The Parties stipulate to the authenticity of each document that on its face appears to be generated by a party (plaintiff or defendant), including documents generated by its employees during the course of their employment for a party, and produced in this case by that party. Notwithstanding this stipulation, each party preserves its right to object to the document on any ground other than authenticity.

C. Procedures Regarding Witnesses and Exhibits

The parties are required to disclose the expected order in which the witnesses will be called, and use good faith in identifying non-demonstrative exhibits that are intended to be used in the direct testimony of each witness or as part of opening statements. Each party must identify to opposing counsel the identity of any live witnesses to be called at trial (and the order in which they will be called) by no later than 6:30 p.m.[26]three (3) calendar days before the trial day on which that witness is expected to testify (e.g., witnesses to be called on Tuesday must be disclosed by 6:30 p.m. the preceding Saturday).

Except for when a fact witness is testifying during trial, fact witnesses are not permitted to witness or have access to the trial proceedings in any manner until after that fact witness has

[26] All times identified herein are Eastern Time.

completed all testimony that witness will provide at trial. The only exception is the parties' client representative, who will be allowed to witness and have access to the trial proceedings, even if testifying in the case. Expert witnesses may have access to the trial proceedings while other witnesses are testifying.

Any exhibits to be used on direct examination with any live witness must be identified by no later than 7 p.m. two (2) calendar days before the start of the trial day on which that exhibit will be offered (e.g., the exhibit(s) for witnesses to be called on Tuesday must be disclosed by 7 p.m. the preceding Sunday). Objections to exhibits disclosed by a party must be provided by 8 p.m. two (2) calendar days before the start of the trial day on which that exhibit will be offered (e.g., objections to exhibits for witnesses to be called on Tuesday must be provided by 8 p.m. the preceding Sunday). The parties will each designate one or more counsel who shall meet and confer regarding any such objections by 8:30 p.m. on the day when the objections are provided. The notice provisions above shall not apply to illustrative exhibits created in the virtual courtroom during testimony or to the enlargement, highlighting, ballooning, or excerpting of trial exhibits, demonstratives, or testimony, so long as the underlying exhibit is pre-admitted or the party has identified the exhibit or deposition testimony according to the agreed schedule.

The parties will cooperate in seeking to have the Court resolve any objections they are unable to resolve among themselves prior to the proposed testimony. Each party will deliver exhibits to the Court that it anticipates using on direct examination by 9 a.m. ET the day of the direct examination in the form of a witness binder. Each party will deliver exhibits to the Court

that it anticipates using on cross-examination by 9 a.m. ET the day of the cross-examination, and to opposing counsel by e-mail prior to commencing cross-examination.

Any document that on its face appears to have been authored or prepared by an employee, officer, or agent of a party, or was produced from the files of a party, shall be deemed primafacie authentic under F.R.E.901 and 902, subject to the right of the party against whom such a document is offered to introduce evidence to the contrary. The parties reserve the right to add additional deposition designations to establish the foundation and authenticity of an exhibit to the extent the admissibility of a particular document is challenged.

Legible or better quality copies may be offered and received in evidence in lieu of originals thereof, subject to all foundational requirements and other objections which might be made to the admissibility of such originals, and subject to the right of the party against whom they are offered to inspect an original upon request. The parties may use electronic, native versions of exhibits that are spreadsheets or slide presentations to the extent such documents were produced during discovery or otherwise agreed to by both parties.

D. Procedures Regarding Deposition Testimony and Discovery Response Designations

The parties are required to provide opposing counsel the identity of any deposition designations or designations of discovery responses and a list of any exhibits to be introduced along with those designations according to the schedule set forth above for disclosure of witnesses/exhibits. Objections and counter-designations to any such designations disclosed by a party will be provided according to the schedule set forth above for objections to exhibits. For

deposition testimony, the party introducing the deposition testimony shall be responsible for editing the deposition testimony to include the testimony and any counter-designation testimony, and remove any attorney objections, and provide a final version of the deposition testimony excerpts (testimony clip report) to the other party by 6:30 p.m. the day before the testimony is to be submitted, read or played to the Court. The parties will each designate one or more counsel who will meet and confer regarding any objections, including objections to any applicable counter-designations[27], by 8:30 p.m. the same day that such objections are disclosed.

The parties will cooperate in seeking to have the Court resolve any objections they are unable to resolve among themselves prior to the proposed testimony or presentation of a discovery response. Each side is to provide the discovery response or deposition testimony excerpts of the specific portions of the deposition video(s) to be played or read, to opposing counsel and to the Court at the time each such designation is presented to Court.

The parties agree that any counter-designations, to which the other party did not object or to which the Court overruled the objection, will be included in the designation of discovery responses or testimony clip report of deposition designations, and that passages of testimony from a deposition will be presented chronologically. The parties further agree to withdraw any objections or attorney colloquy contained with the deposition designations by both sides to the extent possible. For allocating time between the parties for witnesses presented by deposition, witnesses presented by video or read testimony will be divided by the actual time for designations and counter-designations by each party. For witnesses presented by read testimony, the allocation

[27] The parties agreed not to serve objections to counter-designations as part of this pretrial order, and to raise necessary objections to such counter designations at the time of trial.

of trial time will be determined by the ratio of deposition testimony lines designated by each party to the total number of lines read by that witness. No time will be allocated to the parties for deposition testimony submitted to the Court as an exhibit only, with no video or read testimony. Deposition summaries will be offered at trial as appropriate pursuant to Local Rule 30(G). All testimony clip reports for deposition testimony provided to the Court will be admitted as a trial exhibit. The parties' current deposition designations, objections, and counter-designations are attached as Exhibit D (Centripetal) and Exhibit E (Defendant). The parties' discovery responses designations, objections, and counter-designations are attached as Exhibit F (Centripetal) and Exhibit G (Defendant).

III. Witnesses

The parties agree that for current employees of a party, any such witness that such party expects to call in their case-in-chief will appear live by video. For those non-employee witnesses who will be called in a party's case-in-chief via deposition, the parties agree that any counter-designated testimony will be presented to the Court together with the designated deposition testimony, subject to the resolution of any objections to the designated or counter-designated testimony, as discussed above. The parties also agree that a party who wishes to call an employee of the other party as part of its case-in-chief can do so by deposition, regardless of the availability of that witness to testify live.

The parties agree that all fact and expert witnesses will provide any trial testimony from a location remote from their lawyers or staff working on this matter. A remote location means a home, building or office different from any home, building or office where lawyers or staff working on this matter are present. Furthermore, while providing testimony at trial, no witness

shall access any form of communication other than the Zoom video or audio feed provided by the Court. Once sworn, no witness shall communicate with anyone else regarding the substance of the witness's testimony (absent express permission of the Court) until such time as the witness is excused by the Court from further participation in the trial. The agreement reflected in the foregoing sentence does not apply to fact witnesses or Dr. Medvidovic, Dr. Striegel, and Dr. Almeroth should they be called to testify on more than one occasion during the trial. For such witnesses, the parties agree that they will not communicate or speak with the witness once he begins testimony on the subject matter for which they are in the middle of testimony, as delineated by the Court. Once the witness has completed such testimony and leaves the stand, that witness can speak with counsel before taking the stand to testify at a later time during the trial.

FILED
MAR 17 2021
CLERK, U.S. DISTRICT COURT
NORFOLK, VA

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Norfolk Division

CENTRIPETAL NETWORKS, INC.,	)	
	)	
Plaintiff,	)	
	)	
v.	)	**Civil Action No. 2:18cv94**
	)	
CISCO SYSTEMS, INC.,	)	
	)	
Defendant.	)	

OPINION AND ORDER

Defendant, Cisco Systems, Inc. ("Cisco") filed a Rule 59(a)(2) motion for a new trial regarding the Court's rulings as to the '176 Patent and the '806 Patent as well as a new trial as to willfulness and damages. Cisco simultaneously filed a Rule 52(b) motion regarding direct infringement, damages, and an amended judgment as well as a Rule 54(b) request for partial judgment. There are overlapping findings of fact and conclusions of law applicable to Cisco's several motions and the Court will therefore rule upon all of Cisco's motions in this opinion and order.

For the reasons that follow, the Court **DENIES** each of Cisco's motions.

I. INTRODUCTION

As to infringement and validity, Centripetal and its experts relied on 1) Cisco's technical documents as interpreted by Centripetal's experts, 2) admissions in Cisco's pleadings, and 3) the testimony of Cisco's own engineers, principally Mr. Llewallyn and Mr. Jones, Cisco's

distinguished engineers. Cisco attempts to classify the Court's rulings as sua sponte, however, the most compelling evidence originated in Cisco's own technical documents introduced at trial by Centripetal and thus are anything but sua sponte. Cisco attempted to avoid the impact of its own technical publications by using animations prepared solely for trial as the basis for its expert testimony. The Court found that the animations misrepresented the functionality of the infringing products and found Cisco's retained experts' testimony unpersuasive as to infringement and validity as well as damages.

The four Centripetal patents which the Court found Cisco infringed, when combined, cover a broad spectrum of security software which promoted Cisco's security products from an also ran to a leader in the security marketplace. *See* PTX-1460. Cisco portrays itself as "the largest provider of network infrastructure and services for many years before any of the patents issued." Cisco's Reply Brief in Support of 59(a)(2) at 17[1]. This was probably accurate as to hardware, but not as to the software required to operate it until Cisco began infringing the Centripetal patents on June 20, 2017.

The Centripetal '193 Patent, referred to at trial as the "FORWARD OR DROP EXFILTRATION PATENT," the technology from which is embedded in Cisco's switches and routers, enabled Cisco to proactively search for bad actors attempting to exfiltrate confidential data from the switches and routers which operate its networks. The '856 Patent, referred to at trial as the "ENCRYPTED TRAFFIC PATENT," the technology from which is also embedded in Cisco's switches and routers, enabled Cisco to proactively search for and find bad actors and malware in

[1] The Court is citing to the page numbers listed at the bottom of the briefs, not the page numbers assigned to the document by the Clerk's office.

the unencrypted portion of encrypted packets without decrypting them. Cisco repeatedly claimed that it was the first to possess this technology, but in fact it copied the technology from Centripetal. *See e.g.*, PTX-383; PTX-569; PTX-1009.

The '176 Patent, referred to at trial as the "CORRELATION PATENT," the technology from which is also embedded in its switches and routers, enabled Cisco to correlate its NetFlow intelligence with proxy data from multiple third party sources as well as to correlate intelligence from multiple sources within NetFlow. This enabled Cisco to proactively obtain up to date intelligence data for use in its infringing security software embedded in its switches and routers.

The '806 Patent, referred to at trial as the "RULE SWAP PATENT," the infringing technology from which is also embedded in its switches, routers and firewalls enabled Cisco to more efficiently and proactively transform up to date data and collate this intelligence into rules which are then used to detect and stop malware, bad actors (i.e. hackers) and exfiltration.

Accordingly, the patent claims within Centripetal's patented technology work in combination with one another on Cisco's hardware to transform the obsolete portions of Cisco's software from reactive to proactive. The four infringed patents then work together to furnish Cisco's customers with proactive security software throughout its network hardware, thereby contributing to Cisco's goal of transforming itself from a hardware supplier to a full-service network security supplier.

Although Cisco began infringing on June 20, 2017, it continued its copying of Centripetal's patents through 2019 and later, as is illustrated by its technical documents introduced at trial by Centripetal.

II. JUNE 20, 2017 AS THE DATE OF FIRST INFRINGEMENT AND A BASELINE TO COMPARE SALES

Cisco alleges that the Court ruled sua sponte in fixing the date of Cisco's first infringement. The evidence contradicts this claim. In determining the damages based on a reasonable royalty, the Court employed the hypothetical negotiation approach. Also known as the "willing licensor-willing licensee" approach, this calculation "attempts to ascertain the royalty upon which the parties would have agreed had they successfully negotiated an agreement just before infringement began." *Lucent Techs., Inc. v. Gateway, Inc.*, 580 F. 3d 1301, 1324 (Fed. Cir. 2009). "The date used for the occurrence of the hypothetical negotiation is the date that infringement began." *Centripetal Networks, Inc. v. Cisco Sys., Inc.*, 2:18-CV-94, 2020 WL 5887916, 56 (E.D. VA Oct. 5, 2020) (citing *Wang Labs., Inc. v. Toshiba Corp.*, 993 F. 2d 858, 870 (Fed. Cir. 1993)) [hereinafter October 5, 2020 Opinion]. Cisco stated in its opening statement that Encrypted Traffic Analytics, an infringing technology, came to the marketplace in June of 2017. *See* Trial Transcript [Docket Nos. 496-550] [hereinafter Tr.] at 221:19. As per PTX-1135, Cisco's own press release from June 20, 2017 marked the date of first infringement. Lance Gunderson, Centripetal's damages expert, explained why this date should apply to all four patents:

> "[T]hese patents really work in concert. They work together. They provide this operationalization of threat intelligence, this new concept that was a new and innovative concept brought about by Centripetal. So they really kind of worked together.
>
> . . . [T]hey have equal weight, each of them adds an important element to this operationalization.. . . [I]t seems like that they work in concert, and it's my opinion

> that any negotiation would have negotiated a license to all of the patents. Even some of the patents that actually issued afterwards. My understanding is the patents were actually filed for prior to this hypothetical negotiation, they would have been known, and these reasonable actors would have licensed everything." Tr. 1445:14-1446:2.

Cisco's damages expert, Dr. Stephen Becker, agreed that June 20, 2017 would be about the date of the hypothetical negotiation. *See* Tr. at 2993. Further, Becker agreed that the date of first infringement for at least some of the patents at issue would be June 20, 2017:

> Q: And you agree that the start date of damages for purposes of this case, as it relates to the various [four] patents, begins starting June 20 of 2017; is that right?
> A: Yes. It's not every single patent and every single product, but generally that's when it starts. Tr. 2964:4-8 (cross-examination by Ms. Kobialka).

The Court found the date of first infringement to be June 20, 2017. *See* Tr. 725:3-8 (Dr. Michael Mitzenmacher stating this as the date of first infringement); *see also*, Tr. 1534:17 (Cisco cross-examining Mr. Gunderson and confirming his stated date of first infringement was June 20, 2017). The damages are calculated by positing what would be agreed upon at a hypothetical negotiation. *See Lucent* at 1324. Because all the infringing patents work in concert—and because three of the four infringed patents had been granted and the fourth filed for prior to June 20, 2017 and would have been known—it is reasonable to determine that all four patents would be negotiated for licensing at the same time. *See* Tr. at 1445:14-1446:2. As Mr. Gunderson stated in his testimony:

> You look for the date of first infringement. You have a variety of patents, it's the same month that the '193 Patent was issued. There were also some accused products that were sold that month. So there's not a lot of dispute about this date that I'm aware of. They would negotiate a reasonable royalty for all [four] patents, in my opinion, at this time. Tr. 1444:24-1445:5. (direct examination by Ms. Kobialka).

This date was put forth by Centripetal, based upon a Cisco Publication PTX-1135, acknowledged by Cisco's own damages expert during his trial testimony, and certainly was not a *sua sponte* ruling of the Court as claimed by Cisco.

III. DAMAGES - GENERALLY

In its damages case Centripetal relied upon 1) an apportionment formula approved by the Federal Circuit, 2) the only royalty rate cited by either party previously utilized in an infringement claim relating to the same family of patents, and 3) sales data obtained from Cisco which corroborated the damages claimed by Centripetal and accorded with economic reality.

Cisco presented a damages expert whose theory lacked any precedential or evidentiary support in patent law, and was completely devoid of economic reality.

The Court found Centripetal's evidence on infringement, validity, and damages credible and persuasive. The Court found Cisco's defenses objectively unreasonable and in many areas not credible, as well as finding its conduct willful and egregious in infringing the four patents. The Court found that Centripetal did not prove by a preponderance of the evidence that the '205 Patent was infringed by Cisco. The '205 Patent dealt primarily with a method of 'tapping' telephones and was used mostly by law enforcement to record such calls. This is the opposite of the functionality of the infringing products, Cisco never claimed the ability to make, use or sell products based upon the '205 Patent technology. The '205 Patent had no impact upon the Cisco sales data analyzed by the Court or the Court's computation of any form of damages.

IV. MAKING, SELLING AND USING THE INFRINGING PRODUCTS IN COMBINATION IN THE UNITED STATES AND ELSEWHERE AND DAMAGES

Cisco challenged the Court's calculation of damages in both its Rule 52(b) and 59(a)(2) motions. In the introduction to its brief in support of its Rule 52(b)/54(b) motion, Cisco argued the following: "It is undisputed that the accused products are sold separately and that (for instance) Cisco switches, routers or firewalls may be bought and used without buying the other products in the combined systems found to infringe." Cisco's Brief in Support of its Rule 52(b) Motion [Docket No. 628] at 2. "Centripetal did not show, and the Court did not find, that every one of the accused products would meet claims' limitations when sold or used by themselves." Doc. 628 at 11. The evidence demonstrates that the accused products were made and sold to be used in the United States embedded with and in combination with the infringing technology.

Cisco's hardware - i.e., switches, routers, and firewalls - cannot operate without software, and the software that constituted Cisco's operating systems contained Centripetal's patented technology, which Cisco thereby infringed. Further, Centripetal's experts testified that it was Cisco's post June 20, 2017 infringing software that was embedded in Cisco's switches, routers, and firewalls. Multiple technical documents introduced in evidence by Centripetal, but published and circulated by Cisco itself, illustrated in diagrams and explained in text precisely how the infringing software functioned in the Cisco networks, which operated through its switches, routers, and firewalls. Thus, Centripetal presented credible and persuasive evidence of infringement corroborated by Cisco's own technical publications and the testimony of its own employees; including Mr. Llewallyn and Mr. Jones who were designated "distinguished engineers," as well as by Dr. Schmidt, a retained Cisco expert. Cisco for its noninfringement evidence relied upon

animations created for trial, upon which their independent experts in turn relied in forming their opinions. The Court found the animations misrepresented the functionality of the infringing technology and found the testimony of Cisco's independent experts unpersuasive and in many instances not credible, resulting in a finding that Cisco's defenses were objectively unreasonable.

Cisco did not present any evidence that contradicted its own documents, employees, and Centripetal's experts. In fact, none of the authors or presenters of its technical documents were called as witnesses. Instead, Cisco tried to avoid responding to its own publications by creating misleading animations for use at trial. Cisco presented the testimony of Dr. Becker on its "lack of product combination" defense. Dr. Becker, its damages expert, testified as follows:

> Q. And just to be clear for the record, does that $13.4 billion represent the revenue from Cisco customers who purchased the required combination of products for the '856?
> A. No. No. In fact it's, it is all of the revenue from all 98,800 customers, which we could see from looking at the StealthWatch data we know that the vast, vast majority of those customers just have the switch. They're just using the switches and routers, they're not also using this Cisco security product in the form of this, of StealthWatch.
> Q. Did Mr. Gunderson account for the fact that the accused switches and routers "can" be sold separately from the other products required for these accused combinations?
> A. No.
> Q. Do you know whether Mr. Gunderson had access to the same data that you had with respect to these revenue figures?
> A. He did. He has all the same data that I have and he could have looked at these combinations and didn't.
> Q. If Mr. Gunderson had considered the required combination of products, what would that have done to his royalty base in your view?
> A. Well, I think we know that mathematically his base would have been a very, very small fraction of what it was since well-less than five percent of the customers, the data would indicate, have the combination that's required. Trial Tr. 2879:5-2880:3 (Dr. Stephen Becker's testimony) (emphasis added).

However, testimony from Cisco's first independent expert to testify, Dr. Doug Schmidt, contradicts Dr. Becker's damages theory. Dr. Schmidt's factual testimony confirmed explicitly that ETA was embedded in Cisco's Accused Switches:

> THE COURT: Well, I read something that said ETA was embedded in the switch. What does that mean?
> THE WITNESS: That's correct. That's what it just said here at the bottom. The last sentence that's on the screen right now says that.
> BY MR. GAUDET (Cisco counsel):
> Q. What part of ETA is embedded in the switch?
> A. The part that collects the Initial Data Packet and the Sequence of Packet Length and Times.
> Q. Is that what it says in this document?
> A. That's exactly what it says in this document, yes. Trial Tr. 2131:12-22. See also PTX-963 illustrated.

Cisco Blog > Executive Platform



Share

Executive Platform

Cisco Extends Encrypted Traffic Analytics to Nearly 50,000 Customers



Scott Harrell
January 10, 2018 - 2 Comments

Here. Cisco has solved one of the biggest challenges facing the security industry – and now thousands of Cisco customers can start using this breakthrough new network security technology.

Back in June, Cisco announced Encrypted Traffic Analytics – a breakthrough technology that identifies malware in encrypted traffic, without having to break apart the packets and inspect the contents. This unique solution allows security teams to balance security and privacy – and significantly reduce costs along the way.

Since then, Encrypted Traffic Analytics – or ETA – has been in early field trials with customers around the world. The feedback has been incredibly positive, and we're now moving into general availability. But, as a great man once said, there's one more thing … and we think it's a big deal.

Today, we're also expanding support for ETA beyond campus switching to the majority of our enterprise routing platforms, including our branch office router (the ISR and ASR) and our virtual cloud services routers (CSR).

Plaintiff's Trial Exhibit
PTX-963
Case No. 18-cv-00094-HCM

CENTRIPETAL-CSCO 172783

Dr. Schmidt additionally confirmed in his factual testimony that Cisco's infringing products were sold in combination:

> BY MR. GAUDET (Cisco counsel):
> Q. Let's be clear: Does Cisco have any customers who would only buy this product and not have the other products that are actually designed to prevent malicious packets from coming in?
> MR. ANDRE: Objection. Lacks foundation. He doesn't know.
> THE WITNESS: I do know.
> BY MR. GAUDET:
> Q. Do you know that, Dr. Schmidt?
> A. Yes, of course. Only if those customers are extremely looking forward to having their networks hacked. Good network administration, Your Honor, relies on what's called layered defense, where you have firewalls, you have tools like StealthWatch. This is a comprehensive technique. Comprehensive set of products.
> Trial Tr. 2130:7-20.

While the Court rejected Dr. Schmidt's expert opinion on infringement and invalidity, when reckoning with competing testimony it is within the purview of the Court as the trier of fact to determine which witnesses and what testimony or portions thereof are to be accepted as credible. *See Sartor v. Arkansas Natural Gas Corp.*, 321 U.S. 620, 627 (1944) ("The rule has been stated that if the Court admits the testimony, then it is for the [trier of fact] to decide whether any, and if any what, weight is to be given to the testimony.") (internal quotations removed); *see also, In re Methyl Tertiary Butyl Ether (MTBE) Prod. Liab. Litig.*, 739 F. Supp. 2d 576, 604 (S.D.N.Y. 2010) ("In general, a [factfinder] is not required to choose between adopting or rejecting an expert's testimony wholesale; it is free to accept or reject expert's opinions in whole or in part and to draw its own conclusions from it.")

Of course the software programs, such as StealthWatch, "can" be sold separately, as the sales data twice supplied by Cisco illustrates clearly. Customers who already owned Cisco hardware, as well as the outdated Cisco software such as the older versions of StealthWatch, would

only need to purchase the newer infringing software so long as the customer's existing hardware was compatible. The Court found that the preponderance of the evidence established that the sales data for the switches, routers, and firewalls, produced during pretrial discovery and again in more detail at the damages hearing, listed by Cisco were embedded with software which infringed the four Centripetal patents. Cisco was asked to produce sales data on its "accused products," which Centripetal proved were "embedded with its patented software." Dr. Becker's testimony did not refer to the sales data produced in response to the Plaintiffs and the Court's requests for sales data of the "accused products." Cisco never produced any other evidence that its "accused products," as identified in its pretrial sales data production or its second production at the Court's damages hearing, did not contain the infringing software, while Centripetal presented a preponderance of evidence that it did. The Court inferred that Cisco's failure to produce such evidence, even when Dr. Becker was invited to do so by the Court, is proof that the sales data twice presented by Cisco did contain the infringing software. At no time did the Court request that Cisco produce the sales data for all Cisco's hardware and software, as Dr. Becker's testimony might suggest, but rather sales data relating to the "accused products."

Not only is Dr. Becker's testimony contrary to the preponderance of the evidence in the case, but he also misrepresents the testimony of Centripetal's expert, Mr. Gunderson who stated as follows:

> BY MS. KOBIALKA (Centripetal's counsel):
> Q. And can we go to Slide 45? And can you just provide your key takeaways in terms of your opinion for the hypothetical negotiation?
> A. It's my belief that the Centripetal/Keysight patent license is the best available information we have and it's something that I did use. The asserted functionalities are contained within the switches, the routers, firewalls and the other accused products and they work in concert. And apportionment method needs to measure

value provided to Cisco, and so that's what I believe happened with Dr. Striegel's analysis. The asserted functionalities are of critical importance to Cisco and end-users, and I think we went through a series of schedules that showed that importance. And finally, I believe that Georgia-Pacific factors support the royalty and are consistent with the Keysight license agreed rate.[2] Trial Tr. 1525:10-25 (Lance Gunderson's testimony).

Q. "ETA Impact on Security Bookings." And if you can explain here how this informed your opinion?
A. So it says "We're also embedding it in our products right and you can look at like when we acquire StealthWatch. It's now part of what we're doing at Cat 9000." So this is really talking about the importance of ETA and the fact that it impacts their bookings. And bookings, I think, means their sales, essentially. And it's really a revenue impactor, is what they're saying. Trial Tr. 1472:17-25 (Lance Gunderson's testimony); *see* PTX-31 at Bates No. 006.

Q. Okay. I'd like to turn to the royalty base, and we can go to Slide 36. What did you use for coming up with your royalty base?
A. Well, again, in terms of the royalty base we need to look at what is infringing, and we have to start out with what constitutes infringing. And my understanding of the statute is, making it, using it, importing it, offering it for sell, and selling. Those are the -- that's the way the statute reads. And so I always keep that in the back of our mind as we're looking at what the royalty base is. No. 2, the asserted patents are system claims, and so they're for a system comprising a variety of different things. And they're computer-readable medium claims which, in my mind, is software. It's really software that's on the system that makes the patents go, essentially. And then thirdly, the asserted functionalities are embedded in the switches, routers, and firewalls through this source code. This infringing code that is throughout the system. Trial Tr. 1499:18-1500:10 (Lance Gunderson's testimony).

Q. And the 9300 Series the first -- it looks like it's always included Encrypted Traffic Analytics, and that's the first model to do so?
A. Yep. The way it's sold here is that it's always included, yep.
Q. And in addition there was other evidence at trial, you also saw that ETA was also part of the Catalyst 9000 switches?
A. Yes. Trial Tr. 1461:20-1462:2 (Lance Gunderson's testimony).

---

[2] Centripetal analyzed its damages using the *Georgia-Pacific* factors, and, under those parameters, Keystone was the only license transaction in which Centripetal had been involved. It sought additional licensing information from Cisco, but none was forthcoming. In answering Centripetal's interrogatory, Cisco stated that it was "not presently aware of any patent license agreements that relate to the functionality of accused instrumentalities, nor is Cisco aware of any other license relevant to the evaluation of a reasonable royalty of damages in this case." Trial Tr. 1478:23-1479:2 (Mr. Gunderson quoting Cisco's interrogatory response). However, Cisco's exhibit, DTX-729 at page 5, shows that Cisco had licensed StealthWatch from Lancope for approximately two years before Cisco purchased Lancope in 2015. It is not clear if Cisco was contending that the Old StealthWatch was not comparable to the post-2017 7.0 version of StealthWatch or what the reason was for omitting the StealthWatch license.

MS. KOBIALKA: If we could look at PTX-1507?
BY MS. KOBIALKA:
Q. Mr. Gunderson, can you describe what that document is?
A. It's a very simple -- excuse me --
THE COURT: Let me get to that.
MS. KOBIALKA: Sorry. Maybe we can highlight the date at the bottom.
THE COURT: This is 2017?
MS. KOBIALKA: That's correct.
THE COURT: All right. You may proceed.
BY MS. KOBIALKA:
Q. Mr. Gunderson, could you tell us what this document is?
A. It's very similar to the last document that we had. Last document was talking about switches, this is talking about routers. Integrated Services Router. And it has a couple of different generations of routers, and then it's comparing it to the Cisco 4000 Series of routers. And it's an attempt to upsell, to get the current clients of Cisco to buy this new and innovative router that has this great technology on it.
Q. Okay. And I see a blue button up on top, says "How To Buy". Do you see that as well?
A. Yes.
Q. Okay. So this is evidence of how Cisco offers to sell and sells its routers, right?
A. Yes. They point out the benefits, and they're trying to get their existing customers to upgrade and put in a Cisco 4000 Series router.
MS. KOBIALKA: Okay. Now if we could highlight the second row, which is Cisco IOS XE Open operating system all the way across. Then if we could go down to couple it says Cisco DNA Center[3], Centralized Management.
BY MS. KOBIALKA:
Q. And could you just explain what we're seeing here with the check box under the 4000 Series for these?
A. So it shows no checks on the first two generations and then it had a check box that says that's included. So it's got the new IOS that's being accused here as the DNA Center, Centralized Management System. So there's a check box there. It has – you know, you look further down it says Cisco DNA Assurance Network Monitoring. It has a variety of the accused functionality that is included in the Cisco 4000 Series.
Q. If we could turn to the next page of this document? I'd like to just point out the two rows at the bottom. Says "Cisco StealthWatch Enterprise and Encrypted Traffic Analytics." Does this show that also those things come with the Cisco 4000 Series Integrated Services Router?
A. Yes. You can see that those check boxes are there and they come with it, it appears, automatically.
Q. Is this just one example like the other one with the switches of what you have seen in terms of how Cisco sells and offers to sell these products?

[3] There is a glossary of abbreviations attached as Appendix A of the Court's Opinion and Order dated October 5, 2020.

> A. Yeah. So even though they might have a separate charge, sometimes for StealthWatch, for example, they're selling it as one product. These all work together. And that goes to my point: This is, they're really -- they're really trying to sell everything together and to sell a solution rather than just sell individual products. Even though they might charge differently for them, they're selling them together. Trial Tr. 1462:5-1464:13.

The Court found this testimony presented by Centripetal credible, persuasive, and in accord with the preponderance of the evidence. Mr. Gunderson relied to a great extent upon Cisco's own publications, which corroborated his opinions. There is no equivalent corroboration from any source for Dr. Becker's opinions, which the Court rejected. In addition to the evidence Centripetal presented relative to the accused technology being embedded in Cisco's switches, routers and firewalls, Cisco effectively admitted as much in its discovery responses. When asked to produce data regarding its sales of accused products it included specific amounts for its switches, routers, and firewalls through December 31, 2019 in response to Centripetal's pretrial discovery. In its attempt to tailor its damage awards to the evidence, the Court requested that Cisco refine its sales data to a month to month outline and update it to begin in July of 2016 and extend it through the trial which began on May 8, 2020. The Court also invited Cisco's damage witness, Dr. Becker, to furnish any data supporting his damage theory, where at one point he stated that less than five percent of all sales involved sales in infringing combinations. The Court rejected his five percent figure since Cisco offered no sales data to support it, and it conflicted with Centripetal's evidence to the contrary that the Court found reliable. Cisco's sales data produced for pretrial discovery was the same data produced when the Court requested updated sales records. Cisco merely updated the sales records. At no point did Cisco dispute which accused products should have been included or excluded, nor did they at trial contradict with evidence to Centripetal's characterizations that the accused products contained in the sales data infringed.

With regard to damages, the Court accepted Centripetal's theory of damage calculations which was based upon Dr. Striegel's apportionment and Mr. Gunderson's and Mr. Malackowski's application of the financial data. The Court did not base its damages calculations upon the comparative sales data before and after June 20, 2017 produced at the June 25, 2020 Court hearing on damages, but upon the *Finjan* and *Ericsson* cases in which the Federal Circuit expressly approved the damages theory employed by Centripetal. *See Finjan, Inc. v. Blue Coat Sys., Inc.*, 879 F. 3d 1299, 1310 (Fed. Cir. 2018); *Ericsson, Inc. v. D-Link Sys., Inc.*, 773 F. 3d 1291, 1266 (Fed. Cir. 2014). The Court also analyzed the *Georgia-Pacific* factors in its opinion. *See* October 5, 2020 Opinion at 126-49; 164-65.

The Court did seek further evidence supporting damages from both parties in an attempt to resolve the vast difference in the approaches and results presented by the opposing parties. The request by the Court to Dr. Becker began on Trial Tr. 2968:1 and continued through Trial Tr. 2979:5. The Court only had six (6) months of sales data, beginning January 1, 2017, preceding the June 20, 2017 date of first infringement. The Court found that an additional six (6) months of sales data would assist it in determining whether the data would support Centripetal's theory of damages or that of Cisco. The key portions of the Court's request for additional data is set forth as follows:

> THE COURT: All right, Dr. Becker. With respect to that data, what the Court needs, to try to figure out what's going on between these various opinions, is the sales of the products in the '176, the '193, the '205, and the '806. I need the monthly sales of those products beginning in 2016, June of 2016. You can't begin them in the middle of a month, so let's say you'll begin them July '16, July of 2016, with those four patents. I want the monthly sales of the predecessor products for the period of one year prior to June 20, 2017, so that would include the entire month of June, for the predecessors of the accused products because the products are accused beginning June 20th. And when I say, "the accused products," I want to include the sales of all products after that date, on a month-to-month basis, which included the products – all the features accused by the plaintiff. Trial Tr. 2968:17-2969:7.

The Court then asked Dr. Becker to furnish the sales figures based upon his damages theory:

> THE COURT: ...Then I'd like for you to do the same thing with what you considered to be the relevant products, which -- and you didn't consider, for example, in some cases, the routers and switches to be relevant products, so I just want the sales of what you considered to be the relevant products, which included, for example, StealthWatch in some instances, but it didn't include the routers and switches. Trial Tr. 2970:23-2971:4.

Cisco only produced one set of documents in response to the Court's request. It did not produce any compilation of sales figures to support Dr. Becker's theory of damages.

The Court dealt specifically with the '856 Patent because it was granted after June 20, 2017.

> THE COURT: All right. And for the '856 Patent, that patent -- well, I would really just ask for the same data on the '856 Patent, but the patent wasn't granted until after the relevant date. It was granted in '18, and the relevant date is June 20 of '17, so just get me the same figures for that patent on a monthly basis.
> THE WITNESS: Right. I think, to the extent that -- the data that's collected for these other four patents will -- just glancing at the list, I think it will overlap with the '856, and I think, to the extent that we are able to collect the data and get it to you related to the other four, it will cover everything you're asking for on the '856. Trial Tr. 2973:5-16 (Dr. Stephen Becker's testimony).

In its Reply (Rebuttal) brief in support of its Rule 59(a)(2) motion on Doc. 635 p. 15, Cisco stated:

> Likewise, the Court put strict limits on this follow-up testimony from Dr. Becker, instructing Dr. Becker that he was "not to discuss your testimony with anyone between now and the time that you're prepared to deliver the data to the Court," and cautioning Cisco's counsel that it was "to use good faith in limiting themselves to just furnishing the source of the data." Trial Tr. 2978:4-25.

What Cisco describes as "strict limits" applied to barring new damages theories (models). There were no limits on the data to be supplied.

> THE WITNESS: Yes. There's a particular model, for example, that I think the record would show doesn't actually -- won't work with any of the security products, but I think I have an understanding of what you want, and we will work to get that done.
> THE COURT: Well, and you're not limited by what I ask for.
> THE WITNESS: I understand.
> THE COURT: If there's something else along these lines -- you know what I'm thinking about -- that you think would be helpful, go ahead and include it. But I've got to resolve this tremendous difference in --
> THE WITNESS: I understand.
> THE COURT: -- what each side is coming up with, and I'm trying to think how I can best do that. Trial Tr. 2977:2-17 (Dr. Stephen Becker's testimony).

What the Court requested and received was updated sales data through June 2020 plus comparative data for the year preceding the date of the alleged first infringement on June 20, 2017. The sales data, if any, which Dr. Becker used in his damages calculations was not furnished. The Court already had the total sales of the accused products from January 1, 2017 to December 31, 2019.

On page 9 of Doc. 626, its initial memorandum in support of its Rule 59(a)(2) motion, Cisco states:

> In its Opinion and Order, the Court used the sales data from June 2016-June 2017 in a way that Centripetal never had. The Court set forth a table summarizing "Centripetal's estimates regarding Cisco's revenue increase for the infringing products, after the date of first infringement, as compared to the predecessor products sales for the fiscal year before June 20, 2017." Order at 139-140.

And further stated on page 10 of Doc. 626:

> Comparing product sales from June 2016 – June 2017 to product sales over the subsequent three-year period was not a damages model that Centripetal presented to the Court. Nor was it a model that Centripetal (via its damages experts Mr. Gunderson or Mr. Malackowski) had ever suggested would be appropriate.
>
> These allegations are not supported by the evidence.

As previously noted, comparative sales before and after June 20, 2017 was not the damages model the Court utilized. It was evidence, which along with Cisco's marketing documents, corroborated the enormous increase in sales resulting from Cisco embedding Centripetal's software in its switches, routers, and firewalls. The Court also considered sales data as corroborating evidence in accord with *Georgia-Pacific* factor number 11, the comparison which originated with Centripetal's damages expert, James Malackowski, who stated:

> I calculated the averages sales for the predecessor products; I set that as the baseline; and then I calculated everything that was above the baseline for the accused sales to show you the rate of growth. Trial Tr. 3437:16-19

Centripetal electronically filed a group of seven (7) exhibits outlining the data which was the basis for his above quoted testimony at the damages hearing. Mr. Malackowski received the underlying data from Cisco on June 18th and 19th, 2020. Cisco never objected to the Court's request for this data at trial, nor did it object to the manner in which the data was utilized during the damages hearing at which Centripetal compared the dollar amounts of sales of the predecessor products with the dollar amounts of the alleged sales of infringing products. Cisco's only objection to the data was the manner in which the sales of the predecessor switch products were computed.

> BY MR. JAMESON (Cisco counsel):
> Q. And, Dr. Becker, was there daylight between you and Mr. Malackowski with respect to what constituted the predecessor products to the 9000 series one?
> A. Yes. There's substantial -- there's a substantial difference. Set aside this question of the update between June 18th and June 19th, the slides that Mr. Malackowski just presented, which have the updated data in them, are comparisons that only treat the Cisco 3000 series switches as predecessors to the Catalyst accused 9000 series switches, and that is just -- frankly, it's inconsistent with the facts and, I think, creates a very significant difference in the picture that is painted with respect to the sales of the predecessor switches versus the accused switches. Trial Tr. 3441:14-3442:1.

As the Court noted in its opinion, the technical predecessor issue may have been caused by Cisco arguing at trial that the 3000 series of switches, not the 6000 series, was the "design"

predecessor to the 9000 series. However, as to damages, the 6000 series should be treated as a predecessor product. The Court reduced the differential by approximately $200,000, but the differential in sales of the infringing Cisco products was nonetheless $5,575.4 billion, which corroborates Centripetal's apportionment theory and royalty rate for damages. The $5,575.4 billion is not an exact figure, but it was only used to corroborate the multi-billion dollar damages figure claimed by Centripetal, not to actually compute damages.

Dr. Becker's bottom line was to value all five (5) patents then in issue at $3,014,561.00. It is instructive to compare this number with PTX-584, a Cisco technical document from 2018 that states the average cost of a single data breach is $3.86 million, which is more than Dr. Becker's value for all of the patents combined. However, the cost of a data breach helps to explain why Cisco's customers paid it over twenty (20) billion dollars for its infringing security products for the period from June of 2017 to June of 2020.

Very shortly before the Court's damages hearing on June 25, 2020, Cisco filed sales data separating sales in the United States from overseas sales in an effort to reduce the royalty base. This deepens the enigma Cisco created by its tactics in producing sales data in the United States and overseas while denying that any sales of accused products have been proven by Centripetal.

Cisco took similarly inconsistent positions during the trial regarding infringement and validity attempting to use the case of *01 Communique Lab., Inc. v. Citrix Sys., Inc.*, 889 F. 3d 735, 742-43 (Fed. Cir. 2018) to support its arguments. The *01 Communique* case did not support Cisco's inconsistent positions on infringement and invalidity then or on damages now. Cisco has cited no

other authority that supports the inconsistent positions regarding its sales data and making, using, and selling the accused products which it attempts to argue.

The authority cited by Cisco in support of its defense to damages based upon the worldwide sales of the accused products is inapposite. In fact, the case relied upon by Cisco (*Power Integrations, Inc. v. Fairchild Semiconductor Int'l., Inc.*, 711 F. 3d 1348, 1371 (Fed. Cir. 2013)) makes clear that where products are made in the United States, the patent owner is entitled to damages for direct infringement based on overseas sales. *Power Integrations* discusses whether a party is entitled to damages for infringement that occurs outside of the United States. *See* 711 F. 3d at 1371 ("[T]he underlying question here remains whether Power Integrations is entitled to compensatory damages for injury caused by infringing activity that occurred outside the territory of the United States."). As the court in *Power Integrations* notes, infringement cannot happen entirely outside of the United States: "[T]he entirely extraterritorial *production*, use, or sale of an invention patented in the United States is an independent, intervening act that, under almost all circumstances, cuts off the chain of causation initiated by an act of domestic infringement." *Id.* (emphasis added). Centripetal, however, did not seek damages for extraterritorial products. Thus, *Power Integrations*' only value in this instance would be to show that the sales for infringing products *produced* in the United States but used or sold extraterritorially do indeed infringe.

There is support for the Centripetal's damages award for worldwide sales due to direct infringement under § 271(a). The Supreme Court's decision in *WesternGeco LLC v. ION Geophysical Corp* allowed damages for foreign sales when there is infringement under subsection § 271(f)(2). 138 S.Ct. 2129, 2139 (2018). As the Supreme Court states, "Taken together, §

271(f)(2) and § 284 allow the patent owner to recover for lost foreign profits . . . when the patent owner proves infringement under § 271(f)(2)." *Id. WesternGeco* suggests that a similar act of infringement under § 271(a), where an infringing product was made in the United States but sold internationally, would qualify a plaintiff to the same damages for foreign sales set forth under § 271(f)(2). *See, e.g., Plastronics Socket Partners, Ltd. v. Dong Weon Hwang*, No. 218CV00014JRGRSP, 2019 WL 4392525, at *5 (E.D. Tex. June 11, 2019) ("[T]hese instances would constitute infringement under § 271(a), and thus, under the reasoning of *WesternGeco*, would be compensable even if the sale causing damage ultimately occurred abroad.").

Cisco never offered any persuasive evidence to counter Centripetal's proffered testimony and its own response to requests for admissions evidencing that the accused products were made, used, and sold in the United States and the Court found for Centripetal on this issue. *See* Opinion at 32, 86, and 100; *see also*, PTX-1409 at 5-6; PTX-1932. Further Cisco never offered evidence to rebut Centripetal's preponderance of the evidence that its infringing software was not embedded in its traditional hardware and sold in combination with it and when it was asked in pre-trial discovery and later by the Court to produce the data explaining the sales of its "accused products" it produced sales data which included "accused products" containing the infringing technology. Cisco's only response to Centripetal's evidence was to say it's hardware "can" be sold separately, which is insufficient to challenge Centripetal's comprehensive presentation.

Accordingly, the Court **FINDS** that Centripetal has proven that the sales data of the "accused products" which it produced was embedded with and sold in combination with the infringing technology continued Centripetal's Patents '806, '856, '176 and '193. The Court further

FINDS that Centripetal accurately computed its damages based upon the correct data supplied by Cisco using a proper model including apportionment and the *Georgia-Pacific* factors approved by the Federal Circuit, and that Centripetal is entitled to damages based upon worldwide sales as Centripetal proved direct infringement of the four patents remaining in issue. Insofar as Cisco's Rule 59(a) and 52(b) and 54(b) motions relied upon arguments to the contrary they are denied.

V. MR. LLEWALLYN'S AFFIDAVIT AND PATENT '856

Cisco's motion pursuant to Rules 52(b) and 54(b) challenged the Court's finding that the '856 Patent was directly infringed. Cisco attached affidavits from Mr. Daniel Llewallyn and Mr. Peter Jones, its distinguished engineers, to its initial Rule 59(a)(2) motion for a new trial. Llewallyn's affidavit and its attachments were marked as Exhibit A to Doc. 625. Cisco presented Mr. Llewallyn at trial in its defense of the claimed infringement of the '856 Patent. Centripetal relied on Llewallyn's trial testimony in its infringement case particularly regarding Patent '856 referred to at trial as the Encrypted Traffic Patent. In its post-trial Rule 59(a)(2) motion Cisco seeks to use Llewallyn's affidavit to support its noninfringement argument with regard to the '176 Patent which was referred to at trial as the Correlation Patent. Trial Tr.884:25.

However, Llewallyn's expertise was related primarily to the old StealthWatch which he helped develop while employed by Lancope, which was purchased by Cisco. Cognitive Threat Analysis (CTA) was later integrated with an updated version of StealthWatch in 2017, and Mr. Llewallyn had only a basic familiarity with Encrypted Traffic Analysis (ETA) or CTA at the time of his trial testimony.

BY MR. BAIRD (Cisco counsel):

Q. Okay. Now we're showing this with Cognitive Threat Analytics integrated with StealthWatch. When did that happen?
A. The Cognitive Threat Analytics integration was in 2017. It was in version 6.10.3.
THE COURT: This represents Version 10.3 of StealthWatch?
THE WITNESS: 6.10.3, I'm sorry.
THE COURT: 6.10.3?
THE WITNESS: That's correct.
BY MR. BAIRD:
Q. So this is --
THE COURT: What do all those numbers stand for?
THE WITNESS: Oh, that's just our numbering system.
We have like our release levels. We'll call it 6.10, 6.11 as we move on. But if you have a minor release in between the bigger releases, that's where the third number comes in. So we had a 6.10.1, a 6.10.2. That's just our numbering system for our releases.
THE COURT: And each of those, the last number would be a minor release; the one before that would be a major release, is that it?
THE WITNESS: Exactly. Exactly. And if it's a really, really big change we would change this to 7.0.
THE COURT: Okay. When did you get to level 6?
THE WITNESS: That was in around 2012 I think it is when we started shipping 6.0.
THE COURT: And when did you get to 6.10?
THE WITNESS: That was in the 2017 time frame.
THE COURT: Okay. You may proceed. Trial Tr. 2148:8–2149:11.

Mr. Llewallyn testified that he had never heard of Centripetal:

BY MR. BAIRD:
Q. Okay. Last question or set of questions:
Had you ever heard of a company called Centripetal
Networks before this lawsuit?
A. I had not.
Q. In developing StealthWatch, have you ever referred to or relied on anything in any way, shape, or form from Centripetal?
A. I have not. Trial Tr. 2196:2-9.

Therefore he would not have been involved in the exchange of technology between Cisco and Centripetal which resulted in integrating the new version of StealthWatch with CTA. He confirmed this on his cross examination by Centripetal:

BY MR. ANDRE (Centripetal counsel):
Q. You don't know what goes on over in Cognitive Threat

Analytics, do you?
A. I do not, just the big picture. Trial Tr. 2205:20-22.

Cisco continued to improve its security software after the June 20, 2017 transformation from manual after the fact security software to Centripetal's patented proactive machine learning security software. Llewallyn's testimony and PTX-569 illustrate the transition:

BY MR. ANDRE:
Q. I'm not asking about automatic. I'm just saying can the switches and routers -- and particularly the Catalyst 9000 switches and the same routers -- can they block bad traffic from coming in based on StealthWatch intelligence that it gives to them via the ISE?
A. That's correct. If the manual quarantine is fired, then the result is those switches or routers do initiate the rerouting of this IP address's traffic into a quarantined area, yeah.
Q. And so the switches and routers would not let this bad website get to the host, right, if StealthWatch gives it the information?
A. Well, yes. It's more like the host is quarantined, so it won't be able to reach that host anymore. The host is kind of segmented off into an area that can do no harm.
Q. And in that way, StealthWatch is being proactive in prohibiting the attack, correct?
A. I don't know about the word "proactive." It's just -- it's the result of the manual operation of the ISE quarantine. You can call that proactive, I guess, but it's in response, though, to me. You're implying to me that it's -- "proactive" to me means before, you know. This is after the fact. Trial Tr. 2202:5-2203:2.

and:

BY MR. ANDRE:
Q. Now, you talked about how StealthWatch works to monitor internal in the network, correct?
A. That's correct.
Q. You also mentioned how it is integrated with Cisco's Identity Services Engine, right?
A. That's correct.
Q. Okay. Let's go to Page Bates number 803 of this document. And in the left-hand column, there's a paragraph next-from-the-last on the bottom. It says, "Integration of Cisco StealthWatch with Cisco's Identity Services Engine." Do you see that?
A. Yes, sir.
Q. It says, "Helps organizations get 360-degree view of their extended network." Now, what I want to focus on is at the bottom, where it says, "Simplify segmentation throughout your network with centralized control and policy enforcement and address threats faster, both proactively with threat detection and

retroactively via advanced forensics." Now, StealthWatch, working with other products in Cisco's Security Suite, in this case the Identity Services Engine, can proactively protect against threats, correct?
A. Well, it's based on a manual operation, though. Trial Tr. 2198:15-2199:13.

Llewallyn describes a manual operation and he also states that there is no correlation between StealthWatch alarms and CTA alarms. However, Cisco examined Mr. Llewallyn regarding PTX-569, a 2018 Cisco technical document, as follows:

BY MR. BAIRD (Cisco counsel):
Q. And so, Mr. Llewallyn, is it true that this is a 2018 document?
A. Yes, it is.
Q. Okay. And what is this document? Is the document still used today for -- by Cisco?
A. Yes, it is. It's on the Cisco website in the public area.
Q. Okay. And what is this document?
A. It's basically how to configure your switches or routers and exporting devices to work more effectively with StealthWatch. And it also has some troubleshooting issues that you can refer to when working with StealthWatch if you see problems. Trial Tr. 2178:8-21.

Exhibit PTX-569 contains the following language:

"Cisco StealthWatch Enterprise

Cisco StealthWatch is a security analytics solution that leverages enterprise telemetry from the existing network or public cloud infrastructure. It provides advanced threat detection, accelerated threat responses and simplified network segmentation using multi-layer machine learning and entity modeling. With a single, agentless solution, you get visibility across the extended network including endpoints, branch, data center and cloud. And it is the only product that can detect malware in encrypted traffic and ensure policy compliance, without decryption.

It consumes information about the traffic that is passing through the devices in the network such as routers, switches, and firewalls. StealthWatch can analyze enterprise telemetry from any source (NetFlow, IPFIC, sFlow, other Layer 7 protocols) across the extended network, to provide real time visibility into assets that are using the network, while profiling each of these assets. It provides visibility into the east-west traffic in an enterprise network (in addition to north-south traffic) and analyzes network behavior to detect policy violations, anomalies as well as data consumption in the network. This document covers StealthWatch configuration for NetFlow enabled network devices.

Aggregation and correlation

The flow or telemetry represents unidirectional accounting information about the traffic that is passing through a network device and is stored at the level of the flow capable device for a period of time until timeout or until flow ends. This flow will them be exported into StealthWatch that will correlate flows from multiple devices and interfaces and perform stitching and de-duplication action to provide a single bidirectional flow of the traffic end-to-end." PTX-569 at Bates No. 270.

Cisco's counsel did not identify the foregoing language from PTX-569, but they did question Llewallyn about certain other language.

"The Flow Collector usually only needs ingress export from all interfaces on the exporter to create interface traffic data for inbound and outbound traffic. For devices that use logical interfaces enabling both may cause the Flow Collector to double report traffic stats in noninterface documents. We usually ask the Customer to choose which data set is most important." PTX-569 at Bates No. 282.

However, Llewallyn also testified:

BY MR. BAIRD:
Q. Okay. Have you done anything in the code to deal with that problem?
A. I have. Some customers do export ingress/egress for their own reasons, and I've added the ability to configure the StealthWatch Flow Collector to ignore the egress side. Trial Tr. 2173:4-8.

The above testimony confirms that the egress portion of the infringing technology is also used by his customers.

Paragraph 9 of the Llewallyn affidavit is troublesome. It describes proxy as a device and a different type of equipment, when in reality proxy is more correctly classified as a software feature achieved by combining StealthWatch and CTA. The proxy sources are identified as Cisco USA, Bluecoat proxy, Squid and McAfee Web Gateway which are sources of intelligence transmitted over the internet by subscription. The Cisco product described in PTX-569 does not require any additional device or equipment to consume this data as the capability is contained in the Centripetal software embedded in Cisco's hardware as shown in the Cisco diagram in PTX-1065 attached to

Llewallyn's affidavit. *See* PTX-1065, Attachment 1 to exhibit A of Cisco's Motion for a New Trial, Doc. 625. This Cisco diagram is also cited by the Court on p.76 of the October 5, 2020 Opinion.

Paragraph 11 of the Llewallyn affidavit says the third party intelligence data does not originate in the switches and routers, which is true, but misleading. Instead this outside the network third party data enters as proxy data which is then forwarded via the switches and routers which utilize Centripetal software to correlate the proxy data with the NetFlow data thereby creating the data to be analyzed by cognitive (threat) analysis as shown in the diagram on page 5 of the Llewallyn affidavit. Llewallyn described the diagramed process in his trial testimony:

> BY MR. BAIRD:
> Q. Okay. Mr. Llewallyn, can you just briefly orient the Court about how this relates to the demonstrative that we were using earlier? Let's just start on the left side. What's this client server and this switch-router?
> A. The client server equates to computer A and computer B and the other screens. So the client is sending a request to the server above, and it's going through a switch or router to do that. As it passes through the switch or router, the NetFlow is exported to the Flow Collector to make StealthWatch flow out of it, like we were saying, and that copy of the StealthWatch flow is sent to CTA in the cloud for analysis, and then the same copy is sent to the database below for the Flow Collector, and CTA analyzes it, and it reports back to the StealthWatch Management Console anything that it discovered in terms of maliciousness.
> The StealthWatch user on the right, Adam the Analyst, he's using the user interface provided by the StealthWatch Management Console. Trial Tr. 2189:10-2090:4.

By 2018 Cisco had replaced Adam the Analyst with Centripetal's machine learning as previously explained by PTX-569.

The balance of the Llewallyn affidavit repeats Cisco's contentions that it didn't make, use, offer to sell or sell infringing products from 2017 through June of 2020. In their invalidity evidence

Cisco nonetheless claimed they possessed and offered for sale the infringing technology in 2014 and earlier which conflicts with Mr. Llewallyn's and Mr. Jones' trial testimony as well as with multiple Cisco technical and marketing documents. In its Rule 52(b)/54(b) motion alleges that Centripetal did not prove that Cisco directly infringed the '856 Patent. For the reasons stated in this Section V and in Section IV supra the Court **FINDS** that Cisco did so infringe and **DENIES** this portion of Cisco's motions based upon its claimed noninfringement of the '856 Patent.

VI. MR. JONES AFFIDAVIT AND PATENT '806

The conflict between Cisco distinguished engineer Mr. Peter Jones' trial testimony and Cisco's presentation of its expert trial testimony was a subject of the "Overview of the Evidence" beginning on page 22 of the October 5, 2020 Opinion. Cisco now seeks to supplement or perhaps to change or obfuscate his trial testimony through one of its sua sponte arguments in both its Rule 52(b)/54(b) and 59(a) motions. Initially, the Court observes there is no persuasive authority presented in support of supplementing his testimony posttrial via affidavits. However, an examination of the Jones affidavit's content discloses that it did not change his description of the functionality of Cisco's accused products, which infringe the claims in the '806 Patent referred to at trial as the "Rule Swap Patent." As the Court noted in its opinion, at trial Cisco attempted to contradict its own distinguished engineer Jones' testimony through its retained expert, Dr. Reddy. However, the Court rejected Reddy's testimony and accepted Jones' explanation, which was in accord with the other evidence introduced by Centripetal and its experts.

Jones defines the Access Control List (ACL) as a set of rules:

BY MR. POWERS (Cisco counsel):
Q. Okay. Could you briefly explain to the Court what an Access Control List is?

A. An Access Control List is basically a set of rules. Each rule contains criteria to compare a packet against and an [sic] action. Something to do. Simple actions are either to permit or deny, allow a packet to proceed forward or to throw it away. Trial Tr. 2549:24-2550:4.

The UADP is the Cisco diagram illustrated on page 28 of the October 5, 2020 Opinion (DTX-562 at Bates No. 043). Mr. Jones thoroughly explained this Cisco software which the Court found infringed the '806 Patent in DTX-562 as follows:

By MR. POWERS (Cisco counsel):
Q. Okay. Now, just to the left, there's something called the egress forwarding controller. Please tell the Court what the forwarding controller is.
A. It looks at the headers of the packets, applies the rules to them. It decides the fate of the packets.
Q. And just above that, there's something called the PBC, packet buffers complex. Do you see that?
A. I do.
Q. And could you give the Court an overview of what that component is and how it's used during packet processing?
A. That is where the packets stay, waiting for the results from the ingress forwarding controller.
Q. Do all packets pass through that buffer complex?
A. They do.
Q. Please explain any relationship between the packet buffers complex and the hitless ACL rule update technique that we talked about yesterday.
A. There is no relationship.
Q. Now, if we go to the bottom left-hand corner, there is something called ingress FIFO.
THE COURT: What is that packet buffers complex? What is that?
THE WITNESS: It is a storage place. So as packets arrive in from ports, the packet headers are sent to the ingress forwarding controller. The packet itself goes into the packet buffers complex.
THE COURT: What goes there?
THE WITNESS: I'm sorry. Could you repeat yourself, Your Honor?
THE COURT: What goes from the ingress forwarding controller to the packet buffers complex? What goes there?
THE WITNESS: The results of all the rule settings, so the instructions for what to do with the packet. A simple case would be throw the packet away. Another one would be send it to the stack interface or the ingress forwarding controller.
THE COURT: The second one would be what, now?

THE WITNESS: A very simple answer would be if the rule set at the ACL says to discard the packet, the instruction would go from the ingress forwarding controller to the packet buffer to discard the packet.
THE COURT: And you said the second alternative was what?
THE WITNESS: It would be to send the packet forward, to send it out to a different forwarder or switch so it could leave.
THE COURT: So it could what?
THE WITNESS: A way to describe this would be the results of like a -- of an ACL could be either to admit or deny. The ingress forwarding controller processes those rules. It may send an instruction to the packet buffers complex to discard the packet, or it may send an instruction to tell the packet buffers complex where that packet should leave the system.
THE COURT: So if it goes to the packet buffers complex, it's not going to reach its destination --
THE WITNESS: Let me clarify.
THE COURT: -- its original destination; is that right?
THE WITNESS: Let me clarity. The packet buffers complex is where the packet stays waiting for results from the ingress forwarding controller. It may be dropped, or it may be sent on to its destination. For instance, you will see on the right-hand side there's links from the packet buffers complex to the egress forwarding controller. This is the part in which the packet can leave the system.
THE COURT: Well, when you say, "leave the system," that means it's been blocked; is that right?
THE WITNESS: No, that does not mean it's been blocked. If it has been blocked, it is discarded. If we forward the packet, it will leave out another port on the system. It's an example of the path on which it would leave.
THE COURT: But there might be different paths that it would follow. Is that right?
THE WITNESS: So we have a number of these complexes inside the system. This would describe when the ingress port and the egress port were on the same UADP. The block at the top -- you see it's called "stack interface" -- this is how we link together multiple UADPs inside the system. So the results of the ingress forwarding controller can include a set of destinations that the packet needs to leave the system.
THE COURT: Well, suppose it was going to go to its destination, initial destination. Where would it go from the packet buffers complex? Would it go through the ingress forwarding controller?
THE WITNESS: No. If you see, it would not – it would leave through the egress forwarding controller. We tend to have -- the ingress forwarding controller is the processing we do on packets as they arrive. The egress forwarding controller is the process we do on the packets as they leave the system.
THE COURT: Well, maybe I'm not understanding what it means to leave the system. When you say, "leave the system," where does it go when it leaves the system?
THE WITNESS: It will go out one of the ports. On the front of the switch, you'll see a whole set of ports. So packets arrive through a port and are processed. While they're waiting for the result, they sit in the packet buffers complex. Once we have

the results, which could either be throw the packet away or forward the packet, it will leave out through one of our egress forwarding controllers out to a port.
THE COURT: And will it go from the egress forwarding controller to the original destination?
THE WITNESS: Yes. Trial Tr. 2563:2-2567:8.

Jones repeated this same explanation a second time in his direct testimony:

By MR. POWERS(Cisco counsel):
Q. And, Mr. Jones, could you just remind us what FIFO is?
A. It's called a first-in-first-out buffer. It's a small queue.
The packet is then sent into the PBC for storage.
Q. What is the PBC?
A. Yes.
Q. Could you -- packet buffers complex?
A. Packet buffers complex.
Q. Thank you.
A. At the same time, the packet headers, the addresses of the packets, are sent into the ingress forwarding controller. The ingress forwarding controller processes the packet according to the rules that are in the lookup tables. The result is then sent to the packet buffers complex, and it instructs the packet buffers complex what to do with the packet. A simple example would be to throw the packet away. Another example would be to send it out a port. If the packet is to be sent out a port, it's sent from the packet buffers complex to the egress forwarding controller. The egress forwarding controller also runs rules, including Access Control Lists. When the packet is finished going through the egress forwarding controller, it could also be dropped, or it could be sent out a port. It goes via the rewrite engine, which makes modifications to the packets. It goes through the egress FIFO, again, a small shallow buffer, the block level MACSec, Media Access Control Security -- it's an encryption block -- and the packet would leave the front panel port. So it comes in on the left side, circles around, and goes out on the right side. Trial Tr. 2568:1-2569:9.

And again repeated the same explanation during his very brief cross examination by Centripetal:

BY MR. HANNAH (Centripetal counsel):
Q. Thank you, Your Honor. Good morning, Mr. Jones.
A. Good morning.
Q. My name is James Hannah. I'll be asking you some questions this morning. I want to talk about the Catalyst switches that
you've been discussing and, in particular, the 9000 series of
switches, okay?
A. Yes.
Q. Now, the Catalyst switches, they can receive rule sets from a variety of sources; isn't that right?

A. That is correct.
Q. And one of those sources can be the DNA center; isn't that right?
A. Yes, they may receive rules from the DNA center.
Q. And, now, the way the Catalyst processes these rules, in order to process these rules, the Catalyst switch must compile them, right, in order to implement the rules?
A. That is correct.
Q. And in doing this compiling, it compiles these rules while the old rule set is still processing packets, while the old rules are still being applied to packets; isn't that right?
A. That is correct.
Q. Now, once the compilation is complete, a signal is sent to the processor to stop processing packets with the old rule set and to start processing packets with the new rule set; isn't that right?
A. That is correct.
Q. And then during the two to four clock periods that you mentioned yesterday, when there's no processing of packets, the rules are swapped; isn't that right?
A. That is correct. There is -- the processing of packets continues. Packets are processed at a maximum frequency of two to four clock periods. So we don't stop processing the packets, there's just an idle period between two packets.
Q. But there's a signal that's sent to say, stop processing packets with the old rule set and start processing packets with the new rule set, correct?
A. Yes, we swap from the old to the new.
Q. And you do that swap in between -- in that two to four clock cycles that you mentioned yesterday, correct?
A. Right.
Q. Now, once that process is complete, the system signals that the swap has been complete, and then the new rule set will be applied to any subsequent packet; isn't that right?
A. We don't -- we don't signal that a swap is complete, we just instruct the swap to happen.
Q. Well, there's a return success that happens after the swap is complete, correct?
A. There's really not. We just do a write of the new value.
So it's a memory write.
Q. A memory write, okay. But in the document, it actually says that you return success. That's how you represent that memory write, correct?
A. Yes.
MR. HANNAH: No further questions, Your Honor. Trial Tr. 2571:2-2573:9

Mr. Jones affidavit in paragraphs 8-12 outlines what "he could have testified to." While no persuasive authority is cited for such content to be considered, there is nothing in paragraphs 8-12 to contradict what "he did testify to" at trial. As it did during trial with its expert witness, Dr. Reddy, Cisco is attempting to contradict or obfuscate Jones' trial testimony upon which the Court

relied. Cisco's principal defense to infringement of the '806 Patent during the trial was that it's accused products neither cached (stored) the packets nor subjected them to two sets of rules during processing. Jones' trial testimony, which is not contradicted in his affidavit, confirms that Cisco's accused products "store packets in the buffer" (the same function is referred to in the trial as "caches") between subjecting each packet to a first set of rules on ingress and a second on egress.

As is explained in more detail in its October 5, 2020 Opinion, Jones' testimony corroborated Centripetal's own expert testimony and the Court accordingly DENIES both Cisco's Rule 52b/54b and its 59(a)(2) motion insofar as they are based upon its alleged noninfringement of the '806 Patent.

VII. CISCO'S ADDITIONAL EVIDENCE

Centripetal has cited multiple circuits and other federal courts that have refused to accept additional evidence of the nature proffered by Cisco before this Court in post-trial motions, and Cisco has not cited any applicable authority to the contrary. Nonetheless, the Court has reviewed and considered the affidavits of Mr. Llewallyn and Mr. Jones and finds that there is no content therein or content in the attachments to Mr. Llewallyn's affidavit that would change the Court's interpretation of their trial testimony and the inferences to be drawn therefrom. Cisco has also cited testimony from the trial in its briefs, much of which the Court rejected and instead adopted testimony presented by Centripetal to the contrary. In addition, in numerous portions of their opening and Reply (Rebuttal) briefs, Cisco presents testimonial statements, without reference to trial testimony or exhibits that the Court admitted. Such testimonial statements are given no weight by the Court, as there are no evidentiary references to support the same.

As Centripetal argued, with supporting authorities, in its brief: Cisco cannot simply add evidence that was not introduced at trial. *See Goldblum v. Klem*, 510 F.3d 204, 226 n.14 (3d Cir. 2007) ("Evidence is not 'new' if it was available at trial, but a petitioner merely chose not to present it to the jury."); *see also*, *Amrine v. Bowersox*, 238 F.3d 1023, 1029 (8th Cir. 2001), cert. denied, 534 U.S. 963 (2001) (approving district court's determination on remand that "evidence is new only if it was not available at trial and could not have been discovered earlier through the exercise of due diligence"); *United States v. Starr*, 275 F. App'x 788, 790 (10th Cir. 2008) ("[T]he district court correctly found that this evidence was available before trial, and in fact had been discovered by defense counsel. Thus Starr's claim is not based on 'new' evidence, but rather on evidence that could have been presented at trial.").

Numerous federal trial courts cited by Centripetal have come to the same conclusion. *See, e.g.*, *Berlinger v. Wells Fargo*, N.A., No. 2:11-cv-459-FtM-29CM, 2016 WL 11423815, at *1 (M.D. Fla. Sept. 6, 2016); *Guisao v. Secretary, Dep't of Corr.*, No. 8:15-cv-9-T35AAS, 2018 WL 10883771, at *2 (M.D. Fla. Mar. 26, 2018); *Lorme v. Delta Air Lines, Inc.*, No. 03-cv-5239 (GBD), 2005 WL 1653871, at *5 n.6 (S.D.N.Y. July 13, 2005); *Watkins v. Casiano*, No. CCB-07-2419, 2009 WL 2578984, at *3 (D. Md. Aug. 17, 2009), aff'd, 413 F. App'x 568 (4th Cir. 2011); *Connelly v. Blot*, No. 1:16-cv-1282 (AJT/JFA), 2017 WL 11501501, at *3 (E.D. Va. Oct. 18, 2017). Cisco has not provided any authority to the contrary. The one case cited by Cisco, *Twigg v. Norton Co.*, 894 F.2d 672, 675-676 (4th Cir. 1990), does not support the admissibility of the Llewallyn affidavit or its attachments, the Jones affidavit, or the testimonial statements in Cisco memoranda, and accordingly this Court **FINDS** that such evidence is not admissible for purposes of the Cisco motions ruled upon in this opinion and order. In its October 5, 2020 Opinion the Court

found direct infringement of the four (4) patents based upon Centripetal's evidence. It further found that the functionality explained in Cisco's own evidence as to the '806 Patent based upon Mr. Jones' testimony and Cisco's documents would also support infringement under Centripetal's evidence. It was not a sua sponte finding as Cisco's purported defense amounted to an admission of infringement set forth by its own distinguished engineer, Mr. Jones and corroborated by Cisco's technical publications.

In its other motion under Rules 52(b) and 54(b), Cisco claims that Centripetal did not prove Cisco's hardware was embedded with Centripetal's technology or sold in combination with same. Interestingly, Cisco states in its Reply (Rebuttal) brief in support of its Rule 52(b)/54(b) motion "… but Cisco only admitted that it loaded software onto "some" of the accused firewalls in the United States," which is, of course, all Centripetal has to prove in the making, using, and selling factor of its infringement case against the firewalls. The factor of sales of the accused products embedded and used in combination as for damages is analyzed in Section IV of this opinion. Accordingly, the Court **DENIES** Cisco's motion insofar as it is based upon the noninfringement of the '806 Patent as argued in both Rule 59(a)(2) and 53(b)/54(b) motions.

VIII. THE '193 PATENT

Cisco challenges the Court's finding that the accused products directly infringed the '193 Patent in its Rule 52(b)/54(b) motion. It alleges in its motion that the Court's finding of direct infringement depends upon the theory that the Identity Services Engine (ISE) device must be found to infringe. The use of the word engine may suggest that ISE is a "device," but in reality it is a

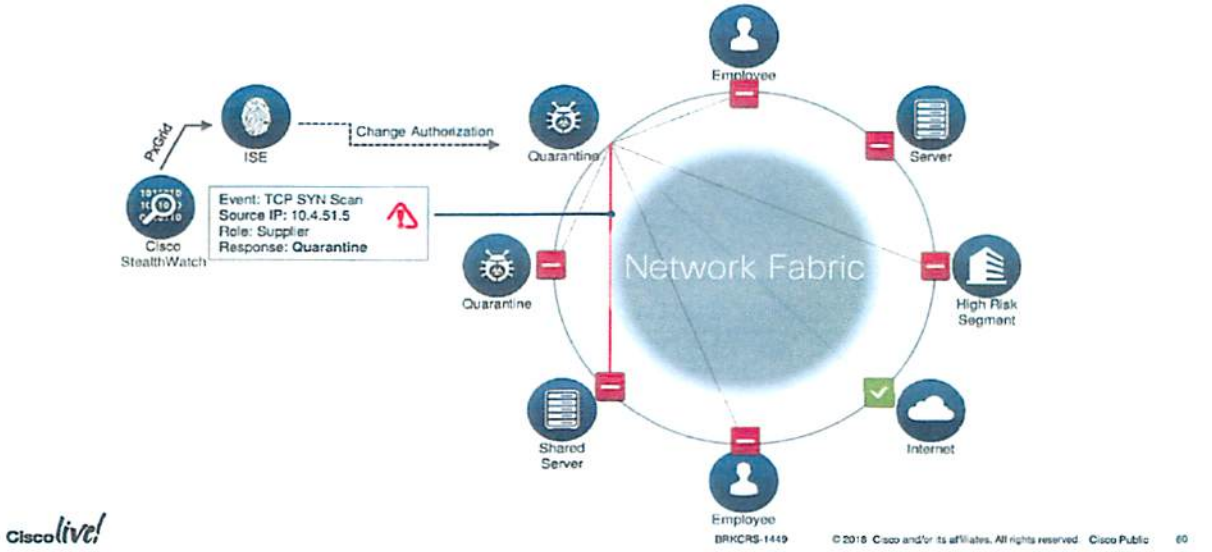
part of Cisco's infringing software. The Court did describe ISE as a "device" in patent jargon on Page 19 of the October 5, 2020 Opinion.

Cisco states "However, Centripetal's infringement proof also relied extensively on ISE to establish infringement of the '193 Patent." Doc 628 at 9. Actually, Centripetal's expert Dr. Mitzenmacher's testimony was to the contrary.

> BY MR. GAUDET (Cisco counsel):
> Q. Dr. Mitzenmacher, you didn't undertake any analysis to figure out how many of Cisco's router and switch customers also buy StealthWatch or also buy Cognitive Threat Analytics or also buy the Identity Services Engine. You don't know any of those numbers. Is that fair?
> A. I certainly couldn't recite them to you. Off the top of my head, I don't know them, but, again, since these are both system claims and computer-readable medium claims, which relate to the code on the switches and the performance of the switches and all our end routers, and all of these devices have the code there to do these things, as I've described, I just am not clear why that would specifically be relevant for me, but... Trial Tr. 804:11-23.

Cisco also states: "Again, the Court did not find that Cisco's switches and routers are only ever used with ISE, and the record would not support such a finding." Doc. 628 at 9.

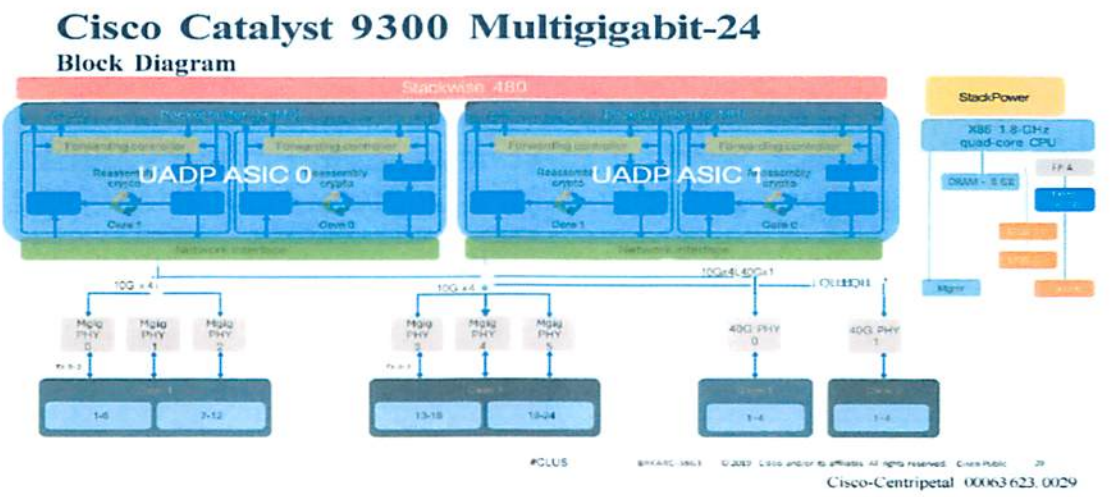
While it is not clear to the Court precisely what this sentence means, Ex. PTX-563, a Cisco technical document introduced by Centripetal during the testimony of Dr. Mitzenmacher (Tr. at 500) at Page Bates No. 415, diagrams StealthWatch forwarding data to ISE which in turn forwards data to the switches and routers in which the infringing software is embedded as explained by Dr. Mitzenmacher.

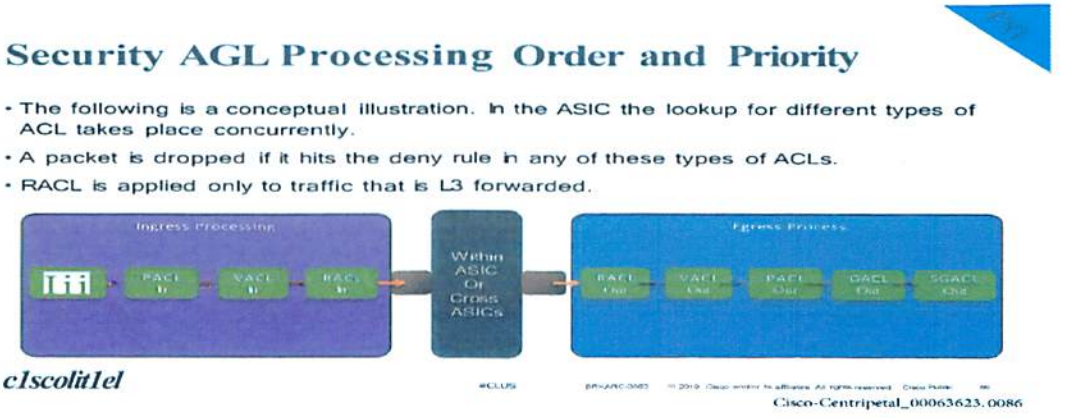


The language from PTX-1280, also a 2018 Cisco technical document introduced by Centripetal during the testimony of Dr. Mitzenmacher, contains the following language confirming that the switches and routers perform a two stage process as opposed to only one stage which was Cisco's defense to infringement at trial:

> "Notice above that rapid threat containment is seamless in SD-Access fabric, as the endpoint continues to be operational in the employee VLAN and the IP address remains unchanged. However, the SGT assignment has changed from 4 to 255, which is the quarantine SGT.
>
> Fabric edge devices will then download SGACL permissions specific to SGT 255, which will limit the endpoint's network address access until a successful remediation is performed." PTX-1280 at Bates No. 21.

Exhibit PTX-1390, a 2019 Cisco technical document, introduced by Centripetal, illustrates at Bates No. 029 how the packets are buffered between being subjected to the two-step process and at Bates No. 086 how the packets are subjected to one set of ACLs (rules) at stage one and, after being placed in the buffer, another set of ACLs on egress at stage two. As to the '193 Patent, this exhibit corroborates the infringing software embedded in Cisco's switches and routers processes the data sent to them by ISE and StealthWatch via a two stage process.





As it did at trial, Cisco attempts to ignore the content of its technical documents that Centripetal introduced in evidence as well as the clear inferences to be drawn from them. In its Reply (Rebuttal) brief in support of its 59(a)(2) motion, Cisco argues that "… Cisco also would have offered factual testimony from the many Cisco technical witnesses that were the original architects of the relevant products." Doc. 635 at 15, line 20. The Court repeatedly observed in the October 5, 2020 Opinion that Cisco failed to call such technical witnesses to respond to its technical documents which Centripetal presented as exhibits. The Court inferred in its October 5,

2020 Opinion on page 159 that Cisco wished to protect such witnesses from Centripetal's cross examination. Cisco goes on to argue in its Reply (Rebuttal) brief in Doc. 635 page 15 line 22, "For example, Cisco would have elicited testimony confirming that – contrary to the Court's findings (Order at 140-141) the increase in sales was impacted by the addition of numerous non-accused features, and had nothing to do with Centripetal's claimed technology." Cisco's marketing documents raved about its increased sales based upon the functionality of the accused products. If Cisco actually had evidence of such new and non-accused features in its hardware or in its own software, why would it not present it at trial?

FRCP 52(b) motions should not attempt to relitigate a theory available at trial. The rule states that a party may make a motion requesting the Court "amend its findings—or make additional findings—and . . . amend the judgment accordingly." "The purpose of motions to amend is to correct manifest errors of law or fact or, in some limited situations, to present newly discovered evidence." *Fontenot v. Mesa Petroleum Co.*, 791 F. 2d 1207, 1219 (5th Cir. 1986) (quoting *Evans, Inc. v. Tiffany & Co.*, 416 F. Supp. 224, 244 (N.D.Ill.1976)). "This is not to say, however, that a motion to amend should be employed to introduce evidence that was available at trial but was not proffered, to relitigate old issues, to advance new theories, or to secure a rehearing on the merits." *Id.* (citing *Evans, Inc. v. Tiffany & Co.*, 416 F. Supp. 224, 244 (N.D.Ill.1976)). Additionally, as Centripetal argues in its opposition brief, a Rule 52(b) motion should not be granted when it "constitute[s] nothing more than an invitation to the district court to reverse itself." *Weatherchem Corp. v. J.L. Clark, Inc.*, 163 F.3d 1326, 1336 (Fed. Cir. 1998) (denying motion). Doc. 630 at 4. Accordingly insofar as its Rule 52(b)/54(b) motion relies on Centripetal's alleged failure to prove direct infringement of the '193 Patent, such motion is **DENIED**.

IX. THE '176 PATENT

Cisco challenged the Court's ruling that the '176 Patent was infringed by the accused products in both its Rule 52(b)/Rule 54(b) motion and its Rule 59(a)(2) motion. The '176 Patent was referred to during the trial as the "Correlation Patent."

In its Rule 52(b) / 54(b) Reply (Rebuttal) brief there is only a single paragraph referencing the '176 Patent. The argument is based upon Cisco's made, used, or sold in combination argument which the Court analyzed in Section IV of this opinion. Again, Cisco begins its argument in its Rule 59(a)(2) opening brief by stating "The Court sua sponte adopted a new claim construction and infringement theory with regard to the '176 Patent." Doc. 626 at 2. Cisco argues that Dr. Cole limited his infringing testimony to a single switch or router. Dr. Cole's cross examination testimony does not support Cisco's claim; indeed it may suggest exactly the opposite:

> BY MR. JAMESON (Cisco counsel):
> Q: Now Dr. Cole, this is claim 11 [of the '176 Patent], all right?
> A: Once again we have the same caveat that this is the exact wording from the patent and nothing's been altered or modified.
> Q: Okay. And if you look at the elements B1 through B4, there is a reference to a network device in each of those elements, right?
> A: That is correct. There is a network device listed in each of those elements.
> Q: And the network device is the router or switch, right?
> A: Once again, we're not infringing individual components, it's the entire system, but the *component* in this case that's receiving and transmitting those packets is the router or switch. Trial Tr. 1101:1-13 (emphasis added).

In any event Centripetal dealt directly with this point when Cisco's expert witness on the '176 Patent, Dr. Almeroth testified during his cross examination as follows:

> BY MR. KASTENS (Centripetal counsel):
> Q. And then you said this had to be a single network device, correct?

A. Not quite. It says a network device here, and then later it's the network device. So it's the same network device across the limitations.
Q. But you do understand that in a patent, when it says A, it can mean one or more; is that correct?
A. That's my understanding.
Q. So this could be more than one network device, correct?
A. It could be. Trial Tr. 2278:11-20.

Mr. Llewallyn also corroborated Centripetal's claim that multiple switches and routers are utilized in Cisco's infringing network:

BY MR. BAIRD:
Q. Now, this slide just showed one router or switch. Mr. Llewallyn, is it correct that the flow collector could be getting NetFlow records from other switches and routers along the path between the two computers that aren't shown here?
A. That's correct. And it's also most common. It's very rare to get it from just one. Trial Tr. 2149:12-18.

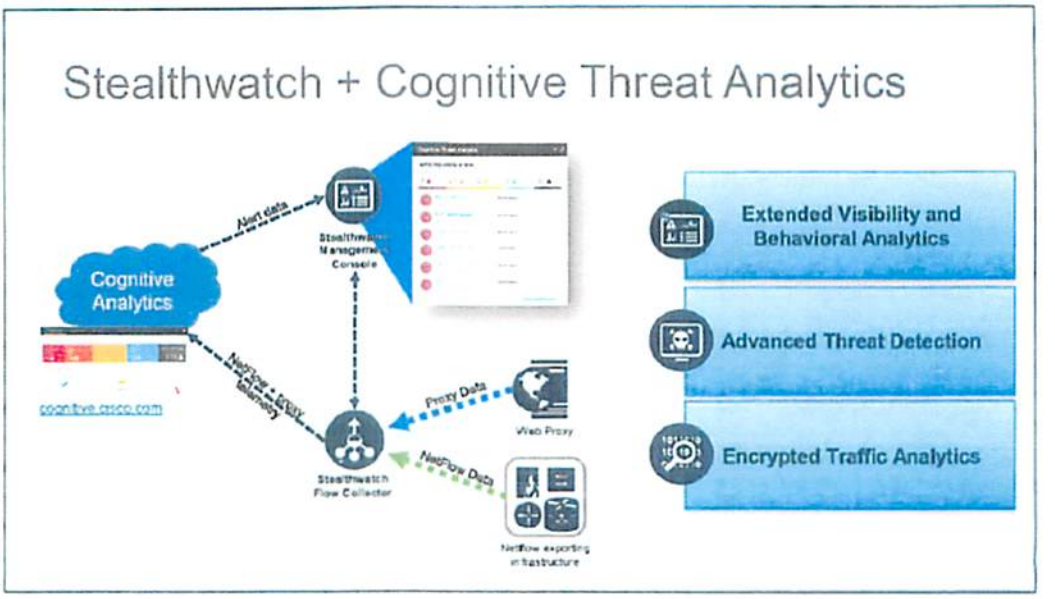
The multiple device language also appears in the patent specification. *See* '176 Patent col.2 l.58-63 (filed Jan. 31, 2017) ("Network device(s) **120** may include one or more devices (e.g., servers, routers, gateways, switches, access points, or the like) that interface hosts **108**, **110**, and **112** with network **106**. Similarly, network device(s) **122** may include one or more devices that interface hosts **114**, **116**, and **118** with network **106**."). Therefore, it was Centripetal and its exhibits that introduced the multiple device argument, not the Court sua sponte. Notably "devices" as used in the patent means; servers, routers, gateways, switches, access points (another name for firewalls) or the like, all expressed in the plural.

Cisco's repeated references to sua sponte seems to suggest that the Court must somehow limit its analysis to the testimony of Centripetal's experts. The Court again observes that Cisco's own documents contradict its arguments, in particular PTX-1065 a November 2017 Cisco

technical document which is Exhibit A to Mr. Llewallyn's affidavit Doc. 635, Ex. A, Attachment 1.

Compare Cisco's argument in its "Reply" (Rebuttal) brief:

> "Had Centripetal or its infringement expert relied on a "one or more" construction of the phrase "a network device," then Dr. Almeroth would have explained why that theory breaks down as well—namely that the claims would still require correlation of packets received into a set of switches or routers with packets transmitted by the *same* set of devices; not just any "correlation" generically with other data. Finding a document with the word "correlation" in it is not good enough; the claims requires correlation of packets entering with packets exiting the same thing. Had Centripetal accused a group of switches or routers, Dr. Almeroth could have responded accordingly. But because Centripetal did not raise the Court's new theory, Cisco had no notice of it and no opportunity to present responsive evidence at trial.
>
> Finally, Centripetal's suggestion that its expert Dr. Cole testified regarding correlation of logs from multiple devices is incorrect. *See* Opp. at 10. Centripetal cites a brief discussion of Syslog data in Dr. Cole's redirect examination, which contains no suggestion that StealthWatch can correlate logs from multiple switches or routers. Trial Tr. 1114:24-1116:20. More importantly, the cited testimony actually shows that Dr. Cole *does not* use Syslog as evidence of infringement. Dr. Cole testified: So customers can just use NetFlow by itself to do that correlation. It does not need to use the proxy data." *Id.* at 1116:12-13. When asked what this means for infringement, Dr. Cole testified "This shows that the claim language says *it must be able to correlate the two NetFlows*. So this is confirming that it can correlate NetFlow by itself which would consist of ingress and egress NetFlow." *Id.* at 1116:23-1117:1 (emphasis added). In sum, Dr. Cole never opined that correlation of Syslogs is infringing; his infringement theory relied entirely on correlation of NetFlow data." Doc. 635 at 6.



Stealthwatch integrates with Cognitive Analytics ("CA" - aka Cognitive Threat Analytics). This involves the addition of a new information panel on the SMC's WebUI, and enhances Stealthwatch further by leveraging CA's cloud based analytics engine, that correlates threat behaviors seen in the enterprise with those seen globally. It uses machine learning and statistical modeling to learn from what it sees and adapt to changing network behavior over time.

Compare the foregoing argument by Cisco with its 2017 technical document PTX-1065. The explanatory text contains the following language which explains the functionality of the diagrammed Cisco network which infringes as made, used, and sold by Cisco and contradicts its arguments:

> "…and enhances StealthWatch further by leveraging CA's cloud based analytics engine, that correlates threat behaviors seen in the enterprise with those seen globally. It uses machine learning and statistical modeling to learn from what it sees and adapt to changing network behavior over time…
>
> …This solution uses the Proxy ingestion feature to consume Syslog information sent from proxy sources, integrating it into StealthWatch's flow visibility…
>
> …This Syslog information contains details similar to what a flow record contains: Source IP, destination IP, Source Port, Destination Port, URL, Username…

> …StealthWatch will then correlate the received Syslog and relates it to the flows collected from network devices before and after the proxy, providing deeper visibility into customers web traffic…
>
> …Customer may use either NetFlow or Proxy data, or both…" PTX-1065 at Bates No. 005.

In support of its arguments Cisco attacks a part of PTX-1065 in the text of Mr. Llewallyn's affidavit at Paragraph 11 on Page 5, Doc. 626-1. The explanatory language which appears immediately below the diagram in PTX-1065 as it was introduced at trial contains the foregoing explanatory language that directly contradicts both Mr. Llewallyn's affidavit and Cisco's argument in its Reply (Rebuttal) brief as well as the testimony of Dr. Almeroth, Cisco's expert witness on the '176 Patent. (Exhibit 1065 in its entirety is attached to Cisco's brief Doc. 626-1 as Exhibit A).

Attachments 2 and 3 of Mr. Llewallyn's affidavit amount to no more than a play on words. These exhibits use the term "de-duplicated," which is a function performed by a previous form of StealthWatch when Lancope was still a separate company, as if it described the accused technology, which it does not. De-duplication is only one of the many functions of the post June 20, 2017 infringing software. The term de-duplication does not even appear in the diagram or the text explaining the diagram. Likewise, the Llewallyn affidavit states that "proxy data" in PTX-1065 is not "generated" by Cisco's switches and routers, which is correct, but, again, misleading. The proxy data, which is intelligence data usually generated by third parties, arrives at Cisco's network via the internet whereupon Cisco switches and routers (single as shown in the diagram, or multiple), embedded with Centripetal's infringing technology, feed it to StealthWatch which correlates it and sends it to Cognitive Analysis (aka Cognitive Threat Analysis) and the correlated intelligence data generate rules which are utilized to process such data in its infringing network of

switches, routers and, in some instances, firewalls as well. Clearly there is more going on in Cisco's post June 20, 2017 network than "de-duplicating" as described in attachments 2 and 3.

The diagram's explanatory text demonstrate that the StealthWatch and Cognitive Threat Analysis contain either correlation from a single source through a single router (i.e. NetFlow Data to StealthWatch Flow Collector) which processes ingress, correlation and egress through a single switch (i.e. NetFlow to StealthWatch Flow Collector to Cognitive Analysis) or multiple switches, Proxy Data (such as Syslog and NetFlow Data to StealthWatch Flow Collector or Collectors to Cognitive Analysis). *See* PTX-1060.

However, PTX-1060, a Cisco technical document introduced by Centripetal during Dr, Cole's testimony, demonstrates that as of December 2017 Cisco was having scalability issues which indicate the need for multiple StealthWatch Flow Collectors describing multiple switches as follows:

> "The Catalyst 9400 series of switches supports analysis of up to 3500 flows per second for ETA and are capable of up to 384,000 NetFlow entries per switch (128K per ASIC); 192,000 ingress and 192,000 egress based on the installed supervisor regardless of the number of linecards installed. At 3500 FPS for ETA, it is recommended that it only be configured when the Catalyst 9400 is used as an access switch and not in distribution or core of the network. As with the Catalyst 9300, ETA on the 9400 when exceeding 3500 flows per second may miss exporting ETA records for some flows, causing incomplete ETA fields in flow analysis.
>
> In addition to the Catalyst 9300 and 9400 specification, you need to carefully consider the number of StealthWatch Flow Collectors required to support the Catalyst 9300s with ETA configured and the flows per second reaching the Flow Collectors." PTX-1060 p. 23.

Centripetal's demonstrative exhibit PTX-547 explains that its software technology solves Cisco's speed and reliability problems. PTX-547, page 141 of the October 5, 2020 Opinion.

Cisco argues that "Finding "a" document with the word correlation is not good enough." (emphasis added) In addition to PTX-1065, which both diagrams and explains in depth how the '176 Patent is infringed through correlation, the following Cisco technical publications post June 20, 2017 explain the correlation feature in whole or in part; PTX-584 at Bates No. 402, PTX-1009 at Bates No. 409, PTX-591 at Bates No. 522, PTX-202, PTX-569 at Bates No. 272 and PTX-1893 at Bates 011. Pre June 20, 2017 older versions of StealthWatch also used the term "correlate" (DTX-343 Bates No. 002), however, the technology at that time relied upon manual responses from Adam the Analyst and therefore operated only retroactively;

> "The StealthWatch System quickly zooms in on any unusual behavior, immediately sending an alarm to the SMC with the contextual information necessary for security personnel to take quick, decisive action to mitigate any potential damage." DTX-343 at Bates No. 001 (a 2014 document).

Cisco technical documents also illustrate that Cisco's products continued to rely on manual software referred to as "Adam the Analyst" until it copied Centripetal's machine learning software. PTX-1089 at Bates No. 239.

Cisco did not successfully copy all of Centripetal's technology at one time, rather it did so over a period of years. It now claims the ability to process billions of packets, where it formerly claimed hundreds of thousands.

Cisco cannot credibly argue that it was taken by surprise (i.e. sua sponte) by its own technical documents or by the patent itself, both of which refer to multiple devices and both of

which were introduced by Centripetal during trial. Accordingly what Cisco attempts to classify as sua sponte originated in the patent itself, was the subject of cross examination of Cisco's retained expert Dr. Almeroth as well as Cisco's direct examination of its distinguished engineer, Mr. Llewallyn, and was corroborated by Cisco's own published documents and explanatory text. The Court **DENIES** both Cisco's Rule 59(a)(2) motion and its Rule 52(b)/54(b) motion insofar as each motion relies upon its claim that Centripetal failed to prove infringement of the '176 Patent.

X. WILLFULNESS

While Cisco did not directly address willfulness in its brief in support of its Rule 59(a)(2) motion, it did argue the point in its Reply (Rebuttal) brief. The Court addressed willfulness in its October 5, 2020 Opinion in Pages 149-161 as well as on Page 166.

Cisco is particularly critical of the Court's analysis of *Read* factor four, Cisco's "size and financial condition." Cisco does not dispute the significance of its "size and financial condition, as it portrays itself as "the largest provider of network infrastructure and services for many years before any of the patents issued." Doc. 635 at Page 17.

In reviewing Cisco's marketing documents, the Court observes the repeated claims that it had "solve[d] a network security challenge previously thought to be unsolvable" (PTX-452 at Page 648) and was the "Industry's first network with the ability to find threats in encrypted traffic without decryption." (PTX-989 at Page 4); *see also*, PTX-383 ("Stealthwatch is the first and only solution in the industry that can detect malware in encrypted traffic without any decryption using Encrypted Traffic Analysis."); PTX-561; PTX-963; PTX-1004; PTX-1010; PTX-1136; PTX-1417. All the while Cisco knew that Centripetal had solved the challenge and was providing the

software needed to deal with encrypted traffic, based upon information it obtained from Centripetal during the Nondisclosure Period. The Nondisclosure Agreement was signed and effective on January 26, 2016 (PTX-99) and confidential information was shared for approximately one and a half years thereafter. Thus, Cisco utilized its footprint in the marketplace and financial prowess to the detriment of Centripetal and its conduct was willful and egregious.

XI. FINAL ORDER

The Court has undertaken to analyze each issue raised by Cisco in both of its motions individually and collectively. The Court **DENIES** the relief sought in Cisco's Rule 59(a) as it **FINDS** no merit in any of the grounds upon which Cisco relies. The Court also **FINDS** no merit in any of the grounds raised in support of its Rule 52(b)/54(b) motion when considered individually and collectively and accordingly **DENIES** that motion.

With regard to Cisco's motion as it separately relates to Rule 54(b) the Court **FINDS** that Cisco's request is mooted by the Court's Order of November 19, 2020 **GRANTING** the joint motion of the parties to dismiss, without prejudice, all remaining claims not addressed in its Order of October 5, 2020.

Therefore the Court enters **FINAL JUDGMENT** in favor of Centripetal Networks, Inc. against Cisco Systems, Inc. for the reasons and upon the terms set forth in its October 5, 2020 Order as well as in this Order.

The Clerk is **REQUESTED** to electronically deliver a copy of this Opinion and Order to all counsel of record.

It is **SO ORDERED**.

/s/
Henry Coke Morgan, Jr.
Senior United States District Judge

HENRY COKE MORGAN, JR.
SENIOR UNITED STATES DISTRICT JUDGE

March 17, 2021
Norfolk, Virginia

US009203806B2

(12) **United States Patent**
Ahn et al.

(10) **Patent No.: US 9,203,806 B2**
(45) **Date of Patent: Dec. 1, 2015**

(54) **RULE SWAPPING IN A PACKET NETWORK**

(71) Applicant: **Centripetal Networks, Inc.**, Leesburg, VA (US)

(72) Inventors: **David K. Ahn**, Winston-Salem, NC (US); **Steven Rogers**, Leesburg, VA (US); **Sean Moore**, Hollis, NH (US)

(73) Assignee: **Centripetal Networks, Inc.**, Herndon, VA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 333 days.

(21) Appl. No.: **13/739,178**

(22) Filed: **Jan. 11, 2013**

(65) **Prior Publication Data**

US 2014/0201123 A1 Jul. 17, 2014

(51) **Int. Cl.**

H04L 29/00	(2006.01)
H04L 29/06	(2006.01)
G06N 5/02	(2006.01)

(52) **U.S. Cl.**

CPC ***H04L 63/0263*** (2013.01); ***G06N 5/02*** (2013.01)

(58) **Field of Classification Search**

CPC H04L 63/0263; G06N 5/02

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,226,372	B1	5/2001	Beebe et al.	
6,317,837	B1	11/2001	Kenworthy	
6,611,875	B1 *	8/2003	Chopra et al.	709/245
7,478,429	B2	1/2009	Lyon	
7,539,186	B2	5/2009	Aerrabotu et al.	
7,684,400	B2	3/2010	Govindarajan et al.	
7,710,885	B2	5/2010	Ilnicki et al.	
7,721,084	B2	5/2010	Salminen et al.	
7,818,794	B2	10/2010	Wittman	
8,004,994	B1	8/2011	Darisi et al.	
8,306,994	B2	11/2012	Kenworthy	
8,806,638	B1 *	8/2014	Mani	726/24
8,856,926	B2	10/2014	Narayanaswamy et al.	
8,935,785	B2	1/2015	Pandrangi	
2001/0039624	A1	11/2001	Kellum	
2002/0049899	A1	4/2002	Kenworthy	
2003/0035370	A1	2/2003	Brustoloni	
2003/0097590	A1 *	5/2003	Syvanne	713/201
2003/0123456	A1	7/2003	Denz et al.	

(Continued)

FOREIGN PATENT DOCUMENTS

EP	1313290	A1	5/2003
EP	1677484	A2	7/2006

(Continued)

OTHER PUBLICATIONS

International Search Report off International Application No. PCT/US2014/023286, dated Jun. 24, 2014.

(Continued)

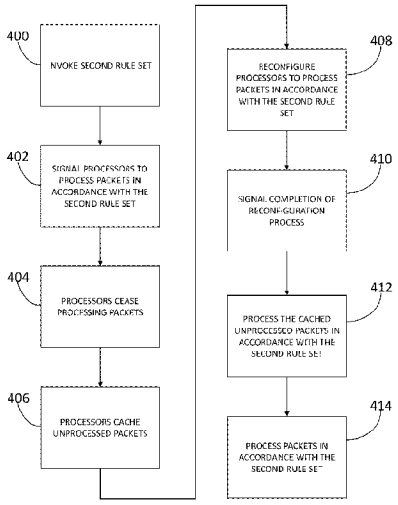
Primary Examiner — Michael Pyzocha

(74) *Attorney, Agent, or Firm* — Banner & Witcoff, Ltd.

(57) **ABSTRACT**

In some variations, first and second rule sets may be received by a network protection device. The first and second rule sets may be preprocessed. The network protection device may be configured to process packets in accordance with the first rule set. Packets may be received by the network protection device. A first portion of the packets may be processed in accordance with the first rule set. The network protection device may be reconfigured to process packets in accordance with the second rule set. A second portion of the packets may be processed in accordance with the second rule set.

24 Claims, 9 Drawing Sheets



Joint Trial Exhibit
JTX-2
Case No. 18-cv-00094-HCM

(56) **References Cited**

U.S. PATENT DOCUMENTS

2003/0142681	A1	7/2003	Chen et al.	
2003/0145225	A1	7/2003	Bruton et al.	
2003/0154297	A1	8/2003	Suzuki et al.	
2003/0188192	A1	10/2003	Tang et al.	
2003/0212900	A1	11/2003	Liu et al.	
2004/0088542	A1	5/2004	Daude et al.	
2004/0151155	A1	8/2004	Jouppi	
2005/0117576	A1	6/2005	McDysan et al.	
2005/0138204	A1	6/2005	Iyer et al.	
2005/0141537	A1	6/2005	Kumar et al.	
2006/0048142	A1	3/2006	Roese et al.	
2006/0114899	A1	6/2006	Toumura et al.	
2006/0136987	A1	6/2006	Okuda	
2006/0146879	A1	7/2006	Anthias et al.	
2006/0195896	A1	8/2006	Fulp et al.	
2006/0212572	A1	9/2006	Afek et al.	
2006/0248580	A1*	11/2006	Fulp et al.	726/11
2007/0083924	A1	4/2007	Lu	
2007/0240208	A1	10/2007	Yu et al.	
2008/0005795	A1	1/2008	Acharya et al.	
2008/0072307	A1	3/2008	Maes	
2008/0235755	A1	9/2008	Blaisdell et al.	
2009/0172800	A1	7/2009	Wool	
2009/0328219	A1*	12/2009	Narayanaswamy	726/23
2010/0011434	A1	1/2010	Kay	
2010/0082811	A1	4/2010	Van Der Merwe et al.	
2010/0132027	A1	5/2010	Ou	
2010/0211678	A1	8/2010	McDysan et al.	
2010/0242098	A1	9/2010	Kenworthy	
2010/0296441	A1	11/2010	Barkan	
2011/0055916	A1	3/2011	Ahn	
2011/0088092	A1	4/2011	Nguyen et al.	
2011/0185055	A1	7/2011	Nappier et al.	
2011/0270956	A1	11/2011	McDysan et al.	
2012/0113987	A1	5/2012	Riddoch et al.	
2012/0240135	A1*	9/2012	Risbood et al.	719/328
2012/0264443	A1	10/2012	Ng et al.	
2012/0314617	A1*	12/2012	Erichsen et al.	370/254
2012/0331543	A1	12/2012	Bostrom et al.	
2013/0059527	A1	3/2013	Hasesaka et al.	
2013/0061294	A1	3/2013	Kenworthy	
2013/0254766	A1	9/2013	Zuo et al.	

FOREIGN PATENT DOCUMENTS

EP	2385676	A1	11/2011
EP	2498442	A1	9/2012
WO	2005046145	A1	5/2005

OTHER PUBLICATIONS

"Build Security Into Your Network's DNA: The Zero Trust Network Architecture"; John Kindervag; Forester Research Inc.; Nov. 5, 2010.

"Designing a Zero Trust Network With Next-Generation Firewalls"; Palo Alto Networks: Technology Brief; last viewed on Oct. 21, 2012.

Reumann, John et al., "Adaptive Packet Filters," Department of Electrical Engineering and Computer Science, The University of Michigan, Ann Arbor, MI, IEEE, 2001.

Greenwald, Michael et al., "Designing an Academic Firewall: Policy, Practice, and Experience with SURF," Department of Computer Science, Stanford University, Stanford, CA, IEEE, Proceedings of SNDSS, 1996.

ISR off International Application No. PCT/US2014/027723, dated Jun. 26, 2014.

"SBIR Case Study: Centripetal Networks Subtitle: How CNI Leveraged DIIS S&T SBIR Funding to Launch a Successful Cyber Security Company, Cyber Security Division, 2012 Principal Investigators' Meeting"; Sean Moore, Oct. 10, 2012.

"Control Plane Policing Implementation Best Practices"; Cisco Systems; Mar. 13, 2013; <https://web.archive.org/web/20130313135143/http:www.cisco.com/web/about/security/intelligence/coppwp_gs.html>.

International Search Report off PCT Application No. PCT/US2013/072566, mailed Mar. 24, 2014.

ISR for PCT/US2013/057502 dated Nov. 7, 2013.

Mizuno et al., A New Remote Configurable Firewall System for Home-use Gateways, NTT Information Sharing Platform Laboratories, IEEE, 2004.

Communication Relating to the Results of the Partial International Search for International App. No. PCT/US2015/024691, dated Jul. 10, 2015.

International Preliminary Report on Patentability for International App. No. PCT/US2013/072566, dated Jul. 23, 2015.

International Search Report and Written Opinion for International App. No. PCT/US2015/024691, dated Sep. 16, 2015.

International Preliminary Report on Patentability for International App. No. PCT/US2014/023286, dated Sep. 24, 2015.

International Preliminary Report on Patentability for International App. No. PCT/US2014/027723, dated Sep. 24, 2015.

* cited by examiner

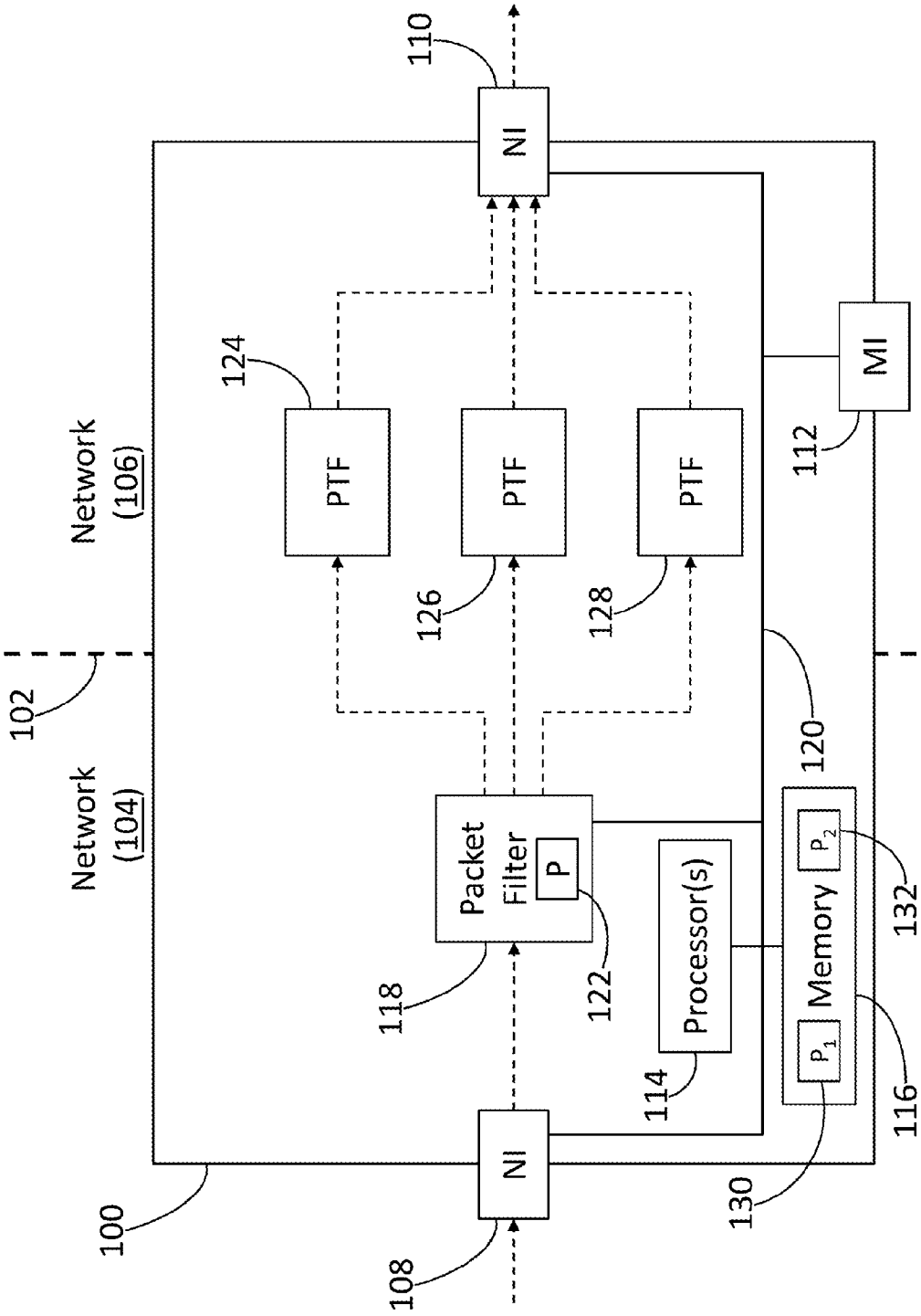


FIG. 1

Keysight, EX-1028
Page 358
CENTRIPETAL-SSCG 001252

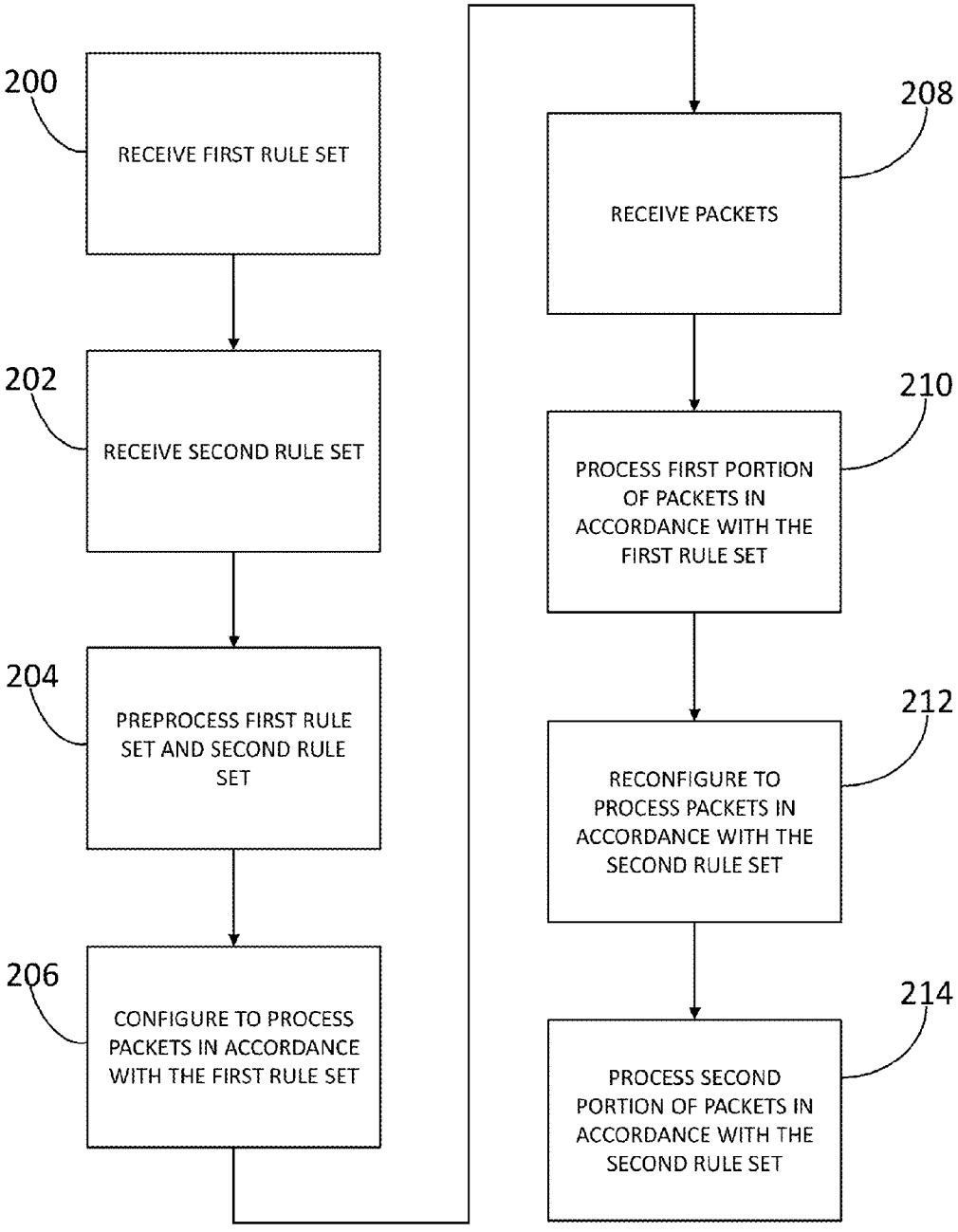


FIG. 2

Keysight, EX-1028
CENTRIPETAL-0001253

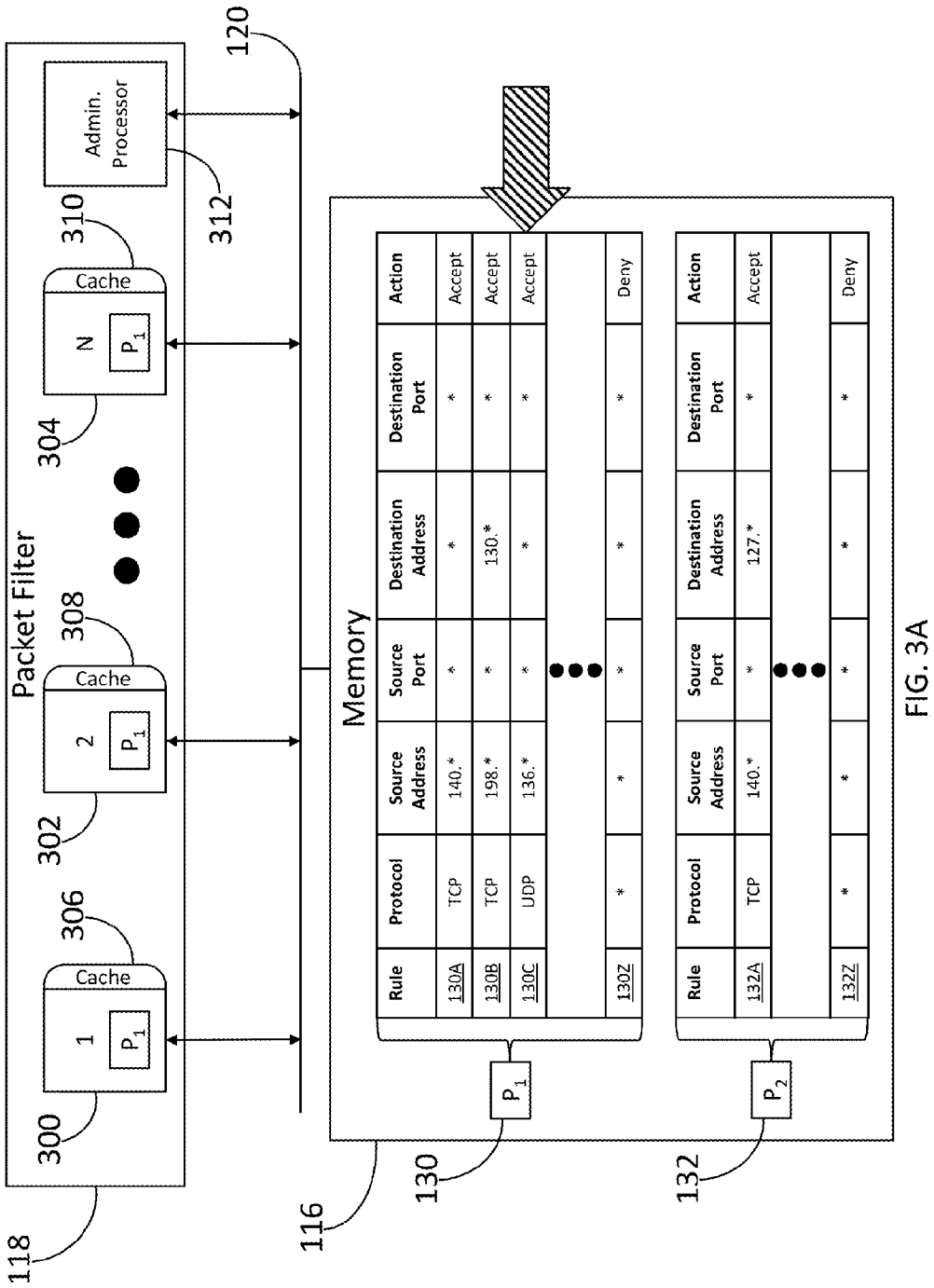


FIG. 3A

Keysight, EX-1028
CENTRIPETAL-SCO 001254

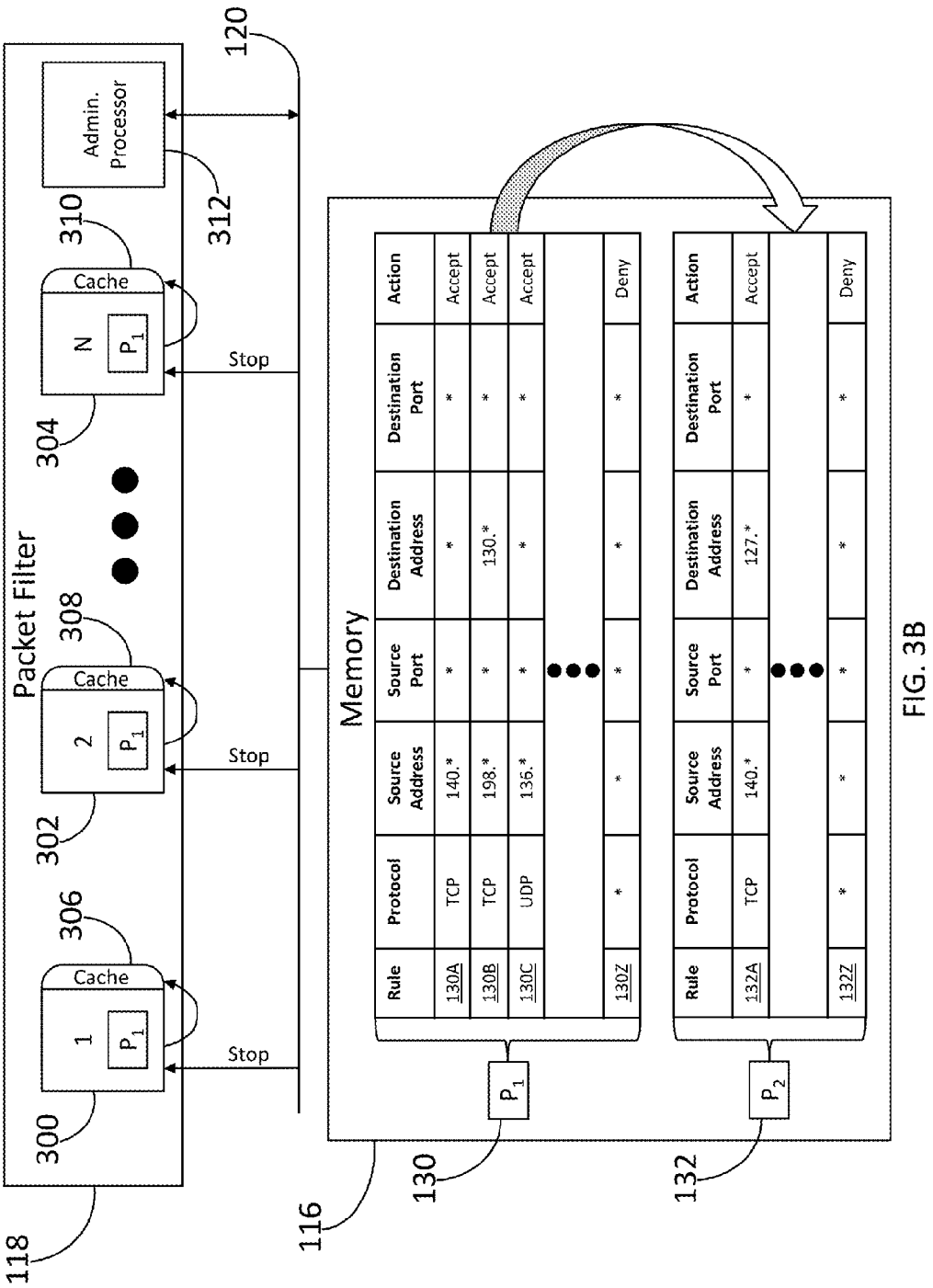


FIG. 3B

Keysight, EX-1028
CENTRIPETAL-SSO 001255

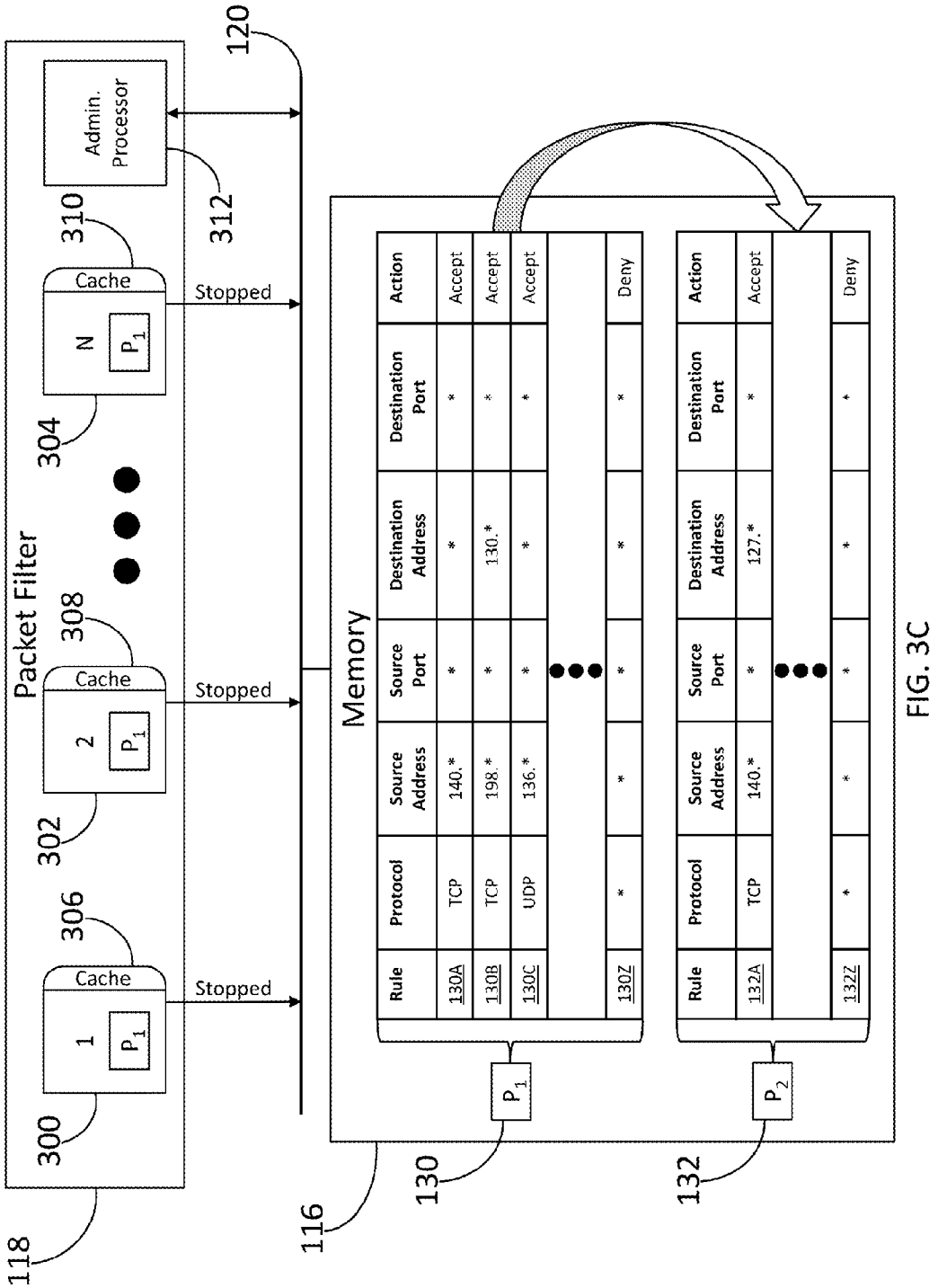


FIG. 3C

Keysight, EX-1028
CENTRIPETAL-SOC 001256

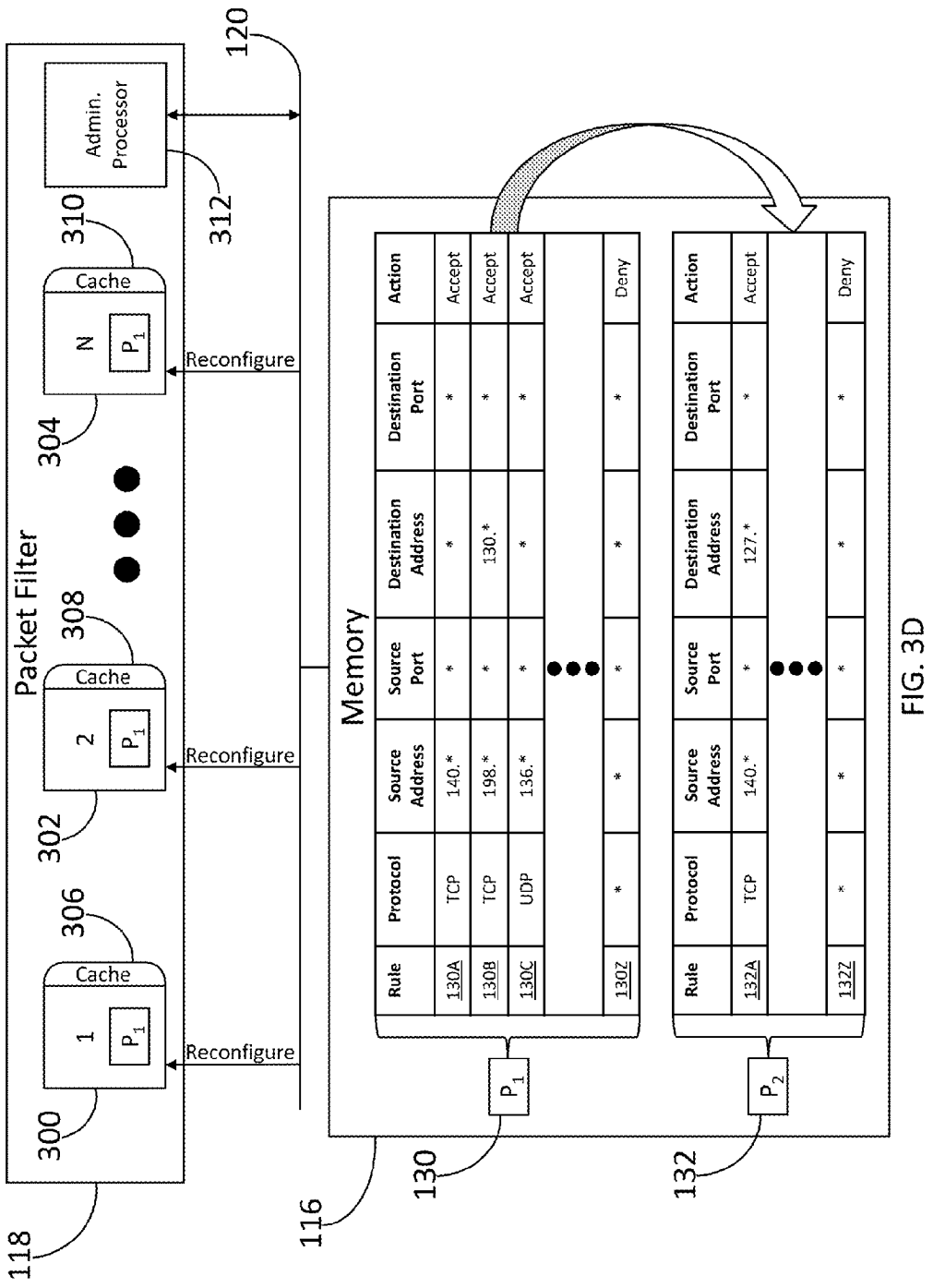


FIG. 3D

Keysight, EX-1028
CENTRIPETAL-0003 001257

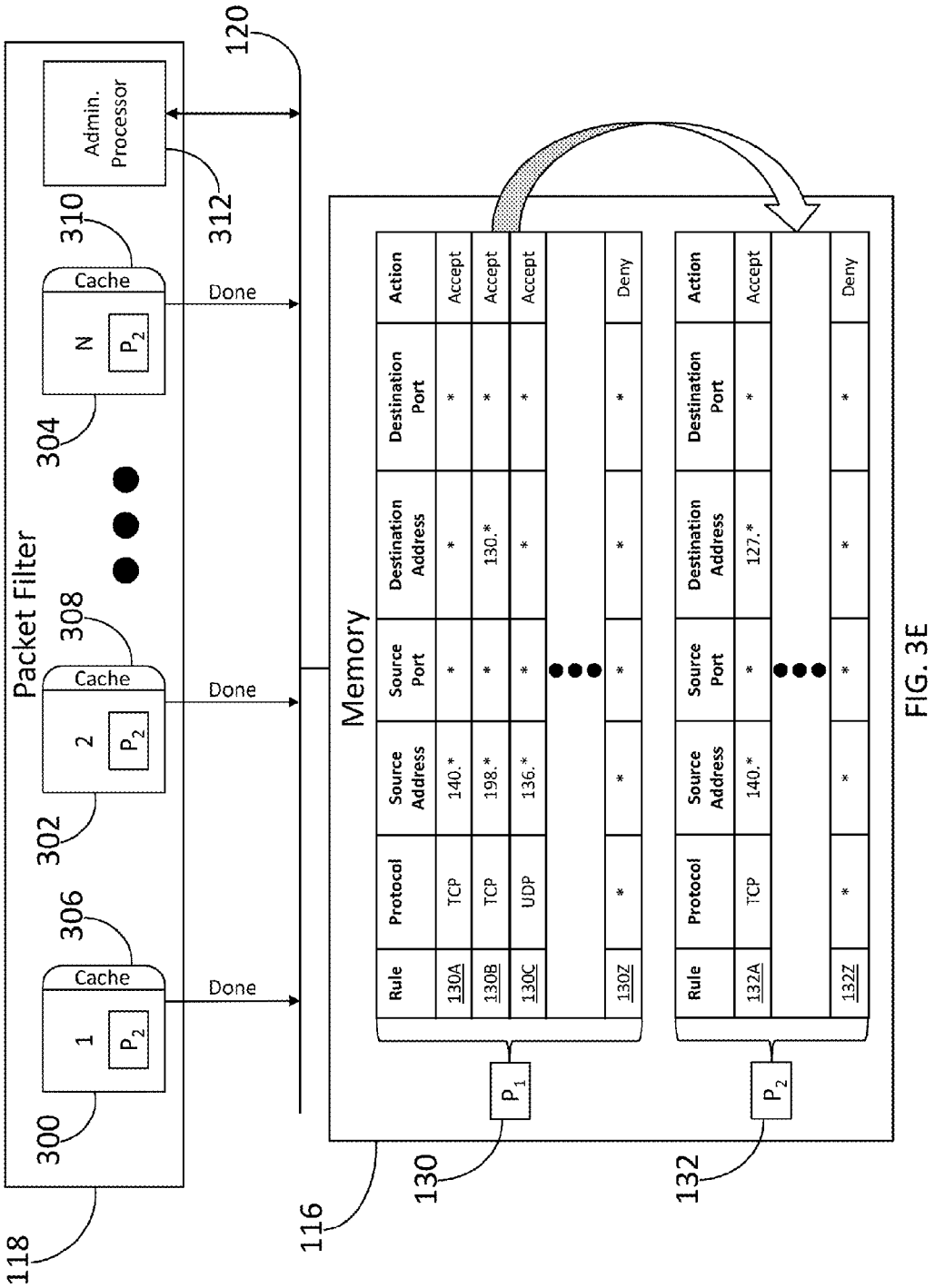


FIG. 3E

Keysight, EX-1028
CENTRIPETAL-SOC-001258

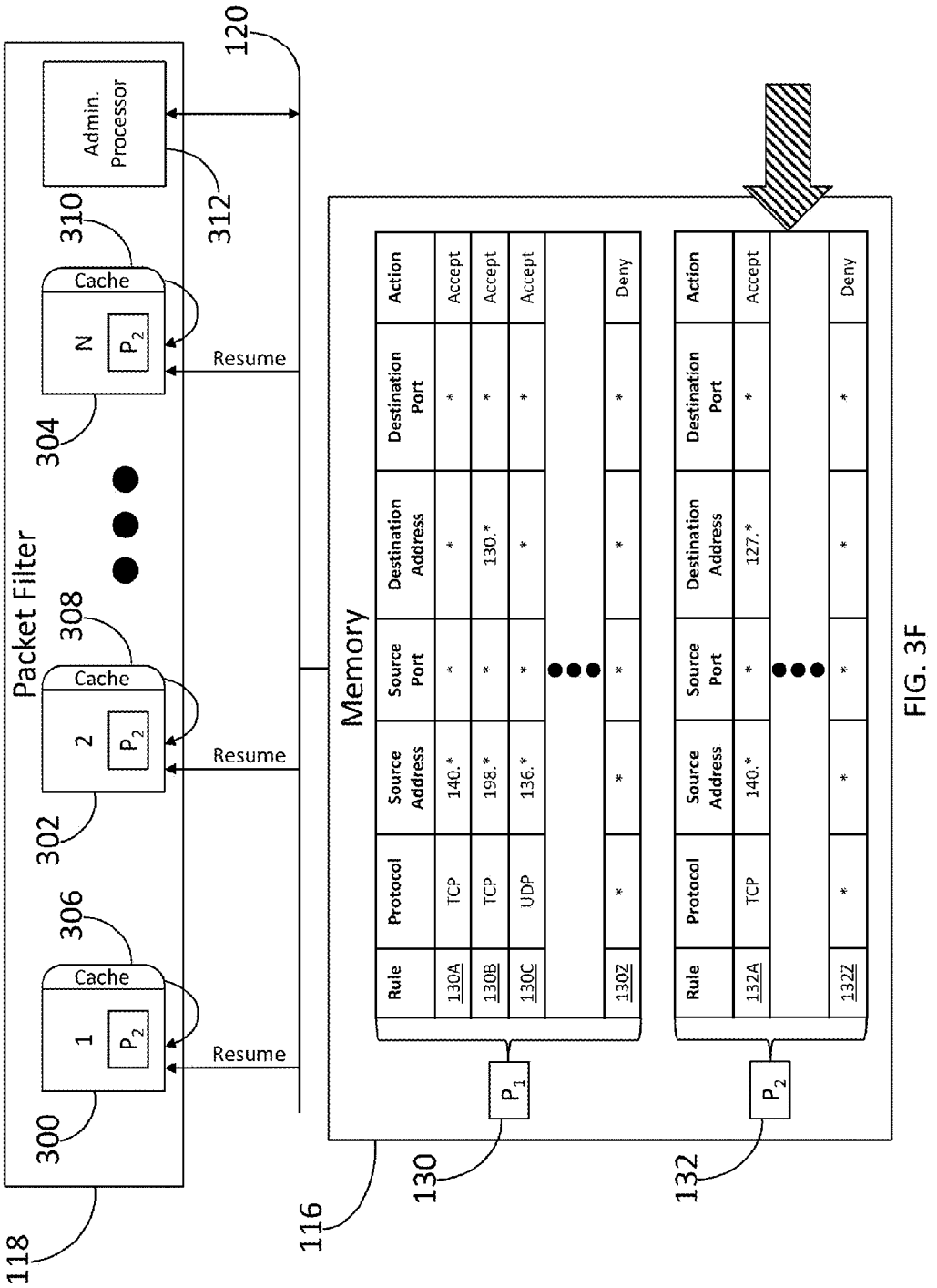


FIG. 3F

Keysight, EX-1028
CENTRIPETAL-SCG 001259

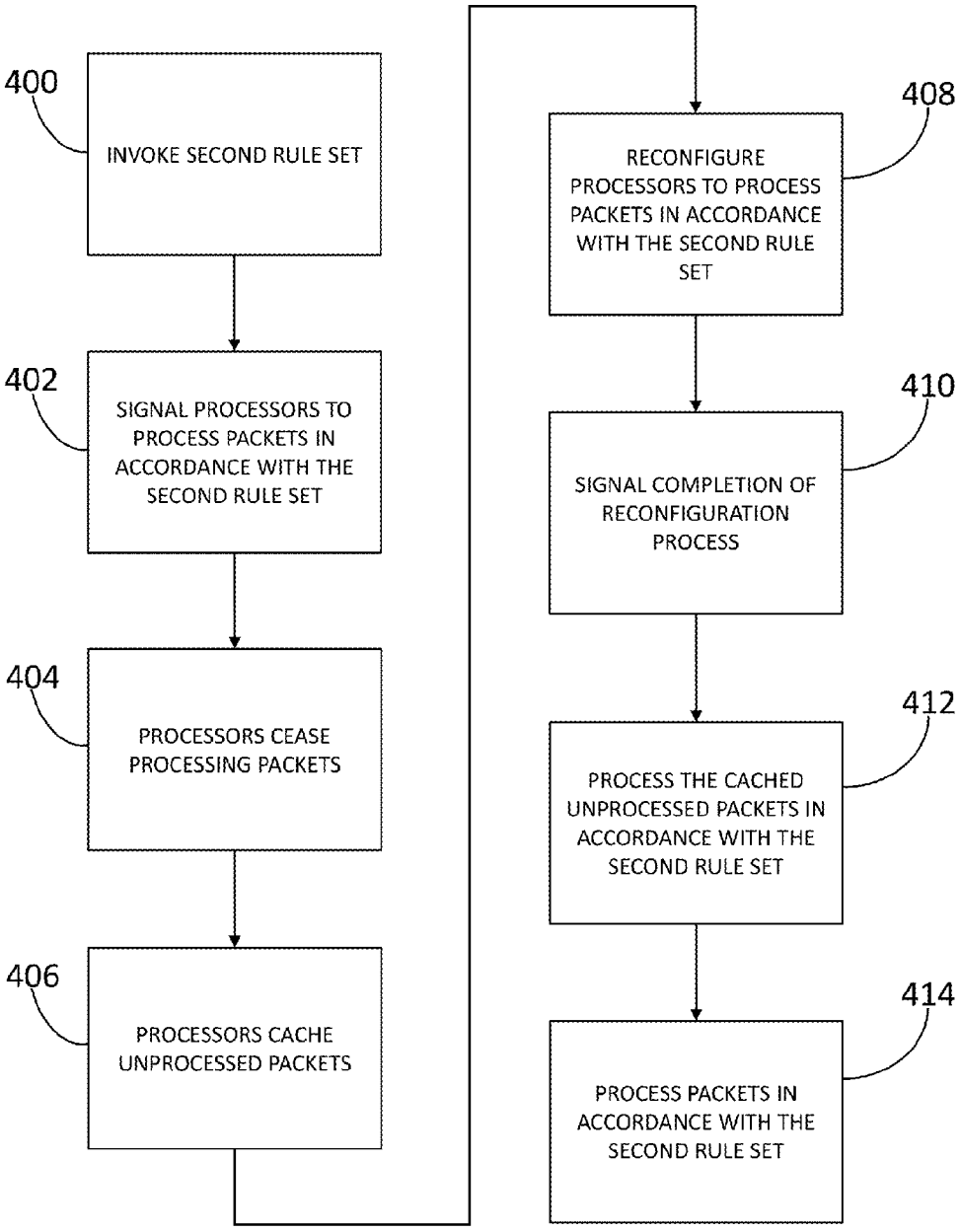

400
INVOKE SECOND RULE SET
402
SIGNAL PROCESSORS TO PROCESS PACKETS IN ACCORDANCE WITH THE SECOND RULE SET
404
PROCESSORS CEASE PROCESSING PACKETS
406
PROCESSORS CACHE UNPROCESSED PACKETS
408
RECONFIGURE PROCESSORS TO PROCESS PACKETS IN ACCORDANCE WITH THE SECOND RULE SET
410
SIGNAL COMPLETION OF RECONFIGURATION PROCESS
412
PROCESS THE CACHED UNPROCESSED PACKETS IN ACCORDANCE WITH THE SECOND RULE SET
414
PROCESS PACKETS IN ACCORDANCE WITH THE SECOND RULE SET

FIG. 4

RULE SWAPPING IN A PACKET NETWORK

BACKGROUND

Network protection devices (e.g., firewalls) implement rules with respect to packet-switched network traffic entering or leaving the networks they protect. Such devices compare the rules with the traffic. If a match is found, then the devices apply the actions associated with the rules to the traffic, e.g., the traffic may be allowed to cross the network boundary, or the traffic may be prevented from crossing the boundary. Such rules are often grouped into rule sets, which may form one or more network policies. As networks increase in complexity, the number of rules in a rule set may correspondingly increase. Similarly, the number of rules in a rule set may increase due to a desire on the part of an administrator to manage network traffic with a high level of granularity.

Network protection devices may require time to switch between rule sets. As rule sets increase in complexity, the time required for switching between them presents obstacles for effective implementation. For example, a network protection device may be unable to process network traffic while switching between rule sets due to the utilization of resources for implementing the new rule set. Additionally, while implementing a new rule set, a network protection device may continue processing packets in accordance with an outdated rule set. In certain circumstances (e.g., in the event of a network attack), such processing may exacerbate rather than mitigate the impetus for the rule set switch (e.g., the effect of the network attack).

SUMMARY

The following presents a simplified summary in order to provide a basic understanding of some aspects of the disclosure. It is neither intended to identify key or critical elements of the disclosure nor to delineate the scope of the disclosure. The following summary merely presents some concepts in a simplified form as a prelude to the description below.

In some variations, first and second rule sets may be received by a network protection device. The first and second rule sets may be preprocessed. For example, the first and second rule sets may be optimized to improve performance. The network protection device may be configured to process packets in accordance with the first rule set. Packets may be received by the network protection device. A first portion of the packets may be processed in accordance with the first rule set. The network protection device may be reconfigured to process packets in accordance with the second rule set. A second portion of the packets may be processed in accordance with the second rule set.

In some embodiments, the network protection device may include multiple processors. The processors, or a portion thereof, may be utilized for processing the first portion of the packets in accordance with the first rule set. Reconfiguring the network protection device to process packets in accordance with the second rule set may include synchronizing the processors. Synchronizing the processors may include signaling the processors to process packets in accordance with the second rule set. Responsive to signaling the processors to process packets in accordance with the second rule set, the processors may cease processing packets and may cache any unprocessed packets. The processors may be reconfigured to process packets in accordance with the second rule set. Once reconfigured, the processors may signal completion of the reconfiguration process. Responsive to signaling completion of the reconfiguration process, the processors may process the cached unprocessed packets in accordance with the second rule set.

In some embodiments, configuration information for configuring the network protection device to process packets in accordance with the first rule set may be stored. The stored configuration information may be utilized to reconfigure the network protection device to process packets in accordance with the first rule set, and a third portion of the packets may be processed in accordance with the first rule set.

In some embodiments, the first rule set may specify a set of network addresses for which packets should be forwarded and the second rule set may specify a set of network addresses for which packets should be forwarded. The second set of network addresses may include fewer network addresses than the first set. Alternatively, the second set of network addresses may include more network addresses than the first set.

In some embodiments, the first rule set may specify a set of network addresses for which packets should be dropped and the second rule set may specify a set of network addresses for which packets should be dropped. The second set of network addresses may include fewer network addresses than the first set. Alternatively, the second set of network addresses may include more network addresses than the first set.

In some embodiments, reconfiguring the network protection device to process packets in accordance with the second rule set may be performed in response to the network protection device receiving a message invoking the second rule set. Additionally or alternatively, reconfiguring the network protection device to process packets in accordance with the second rule set may be performed in response to one or more detected network conditions indicating a network attack.

Other details and features will be described in the sections that follow.

BRIEF DESCRIPTION OF THE DRAWINGS

Some features herein are illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings, in which like reference numerals refer to similar elements.

FIG. **1** illustrates an exemplary network protection device in which one or more aspects of the disclosure may be implemented.

FIG. **2** illustrates an exemplary method for performing fast rule swapping.

FIGS. **3A-3F** illustrate aspects of an exemplary network protection device synchronizing multiple processors performing fast rule swapping.

FIG. **4** illustrates an exemplary method for synchronizing multiple processors performing fast rule swapping.

DETAILED DESCRIPTION

In the following description of various illustrative embodiments, reference is made to the accompanying drawings, which form a part hereof, and in which is shown, by way of illustration, various embodiments in which aspects of the disclosure may be practiced. It is to be understood that other embodiments may be utilized, and structural and functional modifications may be made, without departing from the scope of the present disclosure.

Various connections between elements are discussed in the following description. These connections are general and, unless specified otherwise, may be direct or indirect, wired or wireless, physical or logical. In this respect, the specification is not intended to be limiting.

Keysight, EX-1028
CENTRIPETAL-SOC 001261

FIG. 1 illustrates an exemplary network protection device in which one or more aspects of the disclosure may be implemented. Referring to FIG. **1**, network protection device **100** may be located at boundary **102** between networks **104** and **106**. As used herein, a network protection device includes any computing device having a processor, a memory, and a communication interface. Optionally, a network protection device may be configured to perform one or more additional functions as described herein. For example, network protection device **100** may be a firewall, gateway, router, or switch that interfaces networks **104** and **106**. Network protection device **100** may include one or more network interfaces. For example, network protection device **100** may include network interface **108** for communicating with network **104**, and network interface **110** for communicating with network **106**. In some embodiments, network protection device **100** may include a management interface for providing an administrator with configuration access or provisioning network protection device **100** with one or more rule sets. For example, network protection device **100** may include management interface **112**.

Network protection device **100** may also include one or more processors **114**, memory **116**, and packet filter **118**. Network interfaces **108** and **110**, management interface **112**, processor(s) **114**, memory **116**, and packet filter **118** may be interconnected via data bus **120**. Packet filter **118** may be configured to examine information specified by policy **122** with respect to packets received by network protection device **100** and forward the packets to one or more packet transformation functions specified by policy **122** based on the examined information. As used herein, a policy includes any combination of rules, rule sets, messages, instructions, files, data structures, 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. Optionally, a policy may further specify one or more additional parameters as described herein.

Packet filter **118** may examine information specified by policy **122** with respect to packets received by network protection device **100** (e.g., packets received from network **104** via network interface **108**) and forward the packets to one or more of packet transformation functions **124**, **126**, or **128** specified by policy **122** based on the examined information. Packet transformation functions **124**, **126**, and **128** may be configured to perform one or more functions on packets they receive from packet filter **118**. For example, one or more of packet transformation functions **124**, **126**, and **128** may be configured to forward packets received from packet filter **118** into network **106**, forward packets received from packet filter **118** to an Internet Protocol Security (IPsec) stack having an IPsec security association corresponding to the packets, or drop packets received from packet filter **118**. Additionally or alternatively, one or more of packet transformation functions **124**, **126**, and **128** may be configured to forward one or more packets they receive to one or more other packet transformation functions (e.g., packet transformation function **124**, **126**, or **128**), which may, in turn, perform one or more additional functions on the packets (e.g., log the packets, forward the packets into network **106**, drop the packets, or forward the packets to one or more additional packet transformation functions for further processing). In some embodiments, one or more of packet transformation functions **124**, **126**, and **128** may be configured to drop packets by sending the packets to a local "infinite sink" (e.g., the /dev/null device file in a UNIX/LINUX system). U.S. patent application Ser. No. 13/657,010, filed Oct. 22, 2012, describes the use of packet transformation functions and is incorporated by reference herein in its entirety.

As indicated above, network protection devices (e.g., network protection device **100**) may require time to switch between rule sets, and, as rule sets increase in complexity, the time required for switching between them may present obstacles for effective implementation. For example, memory **116** may include policies **130** and **132**. Each of policies **130** and **132** may include a rule set. In some embodiments, memory **116** may store policies **130** and **132**'s rule sets in one or more buffers. The buffers may be statically sized to one or more predetermined sizes or the size of the buffers may be dynamically adjusted based on the size of policies **130** and **132**'s rule sets. In order to optimize network protection device **100**'s implementation of policies **130** and **132** the rule set contained within policy **130** or policy **132** may be preprocessed prior to its implementation by network protection device **100**. For example, recent advances in packet filtering technology have reduced the time required to apply large rule sets to network traffic. United States Patent Application Publication Nos. 2006/0195896 and 2006/0248580 to Fulp et al., and United States Patent Application Publication No. 2011/0055916 to Ahn, describe such advanced packet filtering technologies, and are each incorporated by reference herein in their entireties. In some embodiments, preprocessing policies **130** and **132**'s rule sets may include merging two or more rules within the rule sets into one rule, separating one or more rules within the rule sets into two or more rules, or reordering one or more rules within the rule sets.

While preprocessing a rule set prior to its implementation may optimize its application to packets, preprocessing a rule set may be a resource intensive process that may require a substantial period of time. In certain contexts (e.g., initial setup) the time required for preprocessing may be of little moment; however, in other contexts (e.g., when rule sets are being swapped live), the time required for preprocessing a rule set may adversely affect the performance of network protection device **100**. For example, network protection device **100** may preprocess policy **130**'s rule set and then implement the preprocessed rule set with respect to network traffic flowing between networks **104** and **106**. Later, it may be desired to reconfigure network protection device **100** to implement policy **132**'s rule set with respect to network traffic flowing between networks **104** and **106**. Accordingly, policy **132**'s rule set may be preprocessed and network protection device **100** may be reconfigured to implement the preprocessed rule set with respect to network traffic flowing between networks **104** and **106**. Utilizing such an approach, however, may result in network protection device **100** having to devote resources to preprocessing policy **132**'s rule set while simultaneously implementing policy **130**'s rule set with respect to traffic flowing between networks **104** and **106**. Thus, network protection device **100** may have to wait until preprocessing of policy **132**'s rule set is completed before switching to policy **132**. Moreover, this period may be extended due to network protection device **100**'s ongoing implementation of policy **130**'s rule set with respect to traffic flowing between networks **104** and **106**.

In accordance with aspects of the disclosure, network protection device **100** may be configured to preprocess multiple rule sets prior to their implementation and thereby enable network protection device **100** to perform fast rule swapping between rule sets. FIG. **2** illustrates an exemplary method for performing fast rule swapping. Referring to FIG. **2**, the steps may be performed by a network protection device, such as network protection device **100**. At step **200**, a first rule set may

be received. For example, network protection device **100** may receive policy **130** via management interface **112**. At step **202**, a second rule set may be received. For example, network protection device **100** may receive policy **132** via management interface **112**. At step **204**, the first and second rule sets may be preprocessed. For example, network protection device **100** may preprocess both policy **130**'s rule set and policy **132**'s rule set. At step **206**, the network protection device may be configured to process packets in accordance with the first rule set. For example, network protection device **100** may be configured to process packets flowing between networks **104** and **106** in accordance with policy **130**'s preprocessed rule set. At step **208**, packets may be received. For example, network protection device **100** may receive packets from network **104** via network interface **108**. At step **210**, a first portion of the packets may be processed in accordance with the first rule set. For example, network protection device **100** may perform one or more packet transformation functions specified by policy **130**'s preprocessed rule set on a first portion of the packets received from network **104**. At step **212**, the network protection device may be reconfigured to process packets in accordance with the second rule set. For example, network protection device **100** may be reconfigured to process packets flowing between networks **104** and **106** in accordance with policy **132**'s preprocessed rule set. At step **214**, a second portion of the packets may be processed in accordance with the second rule set. For example, network protection device **100** may perform one or more packet transformation functions specified by policy **132**'s preprocessed rule set on a second portion of the packets received from network **104**.

It will be appreciated that by preprocessing both policy **130**'s rule set and policy **132**'s rule set prior to processing packets flowing between networks **104** and **106** in accordance with either of policy **130**'s rule set or policy **132**'s rule set, network protection device **100** may swap or switch between policy **130**'s rule set and policy **132**'s rule set more efficiently. For example, because policy **132**'s rule set is preprocessed prior to network protection device **100** being reconfigured to process packets in accordance with policy **132**'s rule set, network protection device **100** is not required to preprocess policy **132**'s rule set at the time network protection device **100** is switching between policy **130**'s rule set and policy **132**'s rule set. Moreover, network protection device **100** may be able to preprocess policy **132**'s rule set more efficiently because it may not be required to simultaneously process packets in accordance with policy **130**'s rule set.

In some embodiments, network protection device **100** may be configured to store configuration information associated with policy **130**'s rule set or policy **132**'s rule set. Such configuration information may later be utilized to reconfigure network protection device **100** to process packets in accordance with policy **130**'s rule set or policy **132**'s rule set (e.g., to swap or switch back to processing packets in accordance with a rule set network protection device **100** has previously processed packets in accordance with).

Due to the large number of rules a rule set may contain and the high volume of traffic a network protection device may be required to efficiently process, a network protection device may include multiple processors for processing packets in accordance with a rule set. Such a multi-processor network protection device may distribute packets amongst its processors for processing in accordance with a rule set.

FIGS. **3**A-**3**F illustrate aspects of an exemplary network protection device synchronizing multiple processors performing fast rule swapping. Referring to FIG. **3**A, as indicated above, network protection device **100** may include packet filter **118**. Packet filter **118** may include one or more processor(s). For example, packet filter **118** may include processors **300**, **302**, and **304**. Each of processors **300**, **302**, and **304** may be associated with a memory cache. For example, processor **300** may be associated with cache **306**. Similarly, processor **302** may be associated with cache **308** and processor **304** may be associated with cache **310**. Packet filter **118** may further include one or more administrative processors for controlling or coordinating its processors. For example, packet filter **118** may include administrative processor **312** for controlling or coordinating processors **300**, **302**, and **304**. As indicated above, network protection device **100** may be configured to swap or switch between processing packets in accordance with one rule set to processing packets in accordance with a different rule set. In multi-processor embodiments, it may be advantageous to synchronize the processors involved in processing packets in accordance with the rule sets. For example, policy **130**'s rule set may include rules **130**A, **130**B, and **130**C-**130**Z; and policy **132**'s rule set may include rules **132**A-**132**Z. It will be appreciated, that either or both of policies **130** and **132**'s rule sets may include more than the number of rules illustrated (e.g., either or both of policies **130** and **132**'s rule sets may include hundreds of thousands or millions of individual rules).

Each of the individual rules within either of policies **130** or **132**'s rule sets may specify criteria (e.g., a set of network addresses) and an action (e.g., accept or deny) to be performed on packets matching the specified criteria. For example, rule **130**A may specify that packets containing TCP packets, originating from a source IP address that begins with **140**, having any source port, destined for any IP address, and destined for any port should have an accept packet transformation function performed on them. Similarly, rule **130**B may specify that packets containing TCP packets, originating from a source IP address that begins with **198**, having any source port, destined for an IP address that begins with **130**, and destined for any port should have an accept packet transformation function performed on them; rule **130**C may specify that packets containing UDP packets, originating from a source IP address that begins with **136**, having any source port, destined for any IP address, and destined for any port should have an accept packet transformation function performed on them; rule **130**Z may specify that packets containing packets of any protocol, originating from any IP source address, having any source port, destined for any IP address, and destined for any port should have a deny packet transformation function performed on them; rule **132**A may specify that packets containing TCP packets, originating from a source IP address that begins with **140**, having any source port, destined for any IP address than begins with **127**, and destined for any port should have an accept packet transformation function performed on them; and rule **132**Z may specify that packets containing packets of any protocol, originating from any IP source address, having any source port, destined for any IP address, and destined for any port should have a deny packet transformation function performed on them.

The individual rules of policies **130** and **132**'s rule sets may execute in a linear fashion. That is, a packet being processed in accordance with policy **130**'s rule set may first be compared to the criteria specified by rule **130**A. If the packet matches the criteria specified by rule **130**A, the corresponding action may be performed on the packet and packet filter **118**'s processor(s) may move on to the next packet. If the packet does not match the criteria specified by rule **130**A, then the packet is compared to the criteria specified by the next rule (e.g., rule **130**B), and so on, until the packet matches

the criteria specified by a rule and the corresponding action is performed on the packet. Thus, for a multi-processor network protection device, individual processors may be comparing different individual packets to different rules within a given rule set when it is determined that the network protection device should swap or switch the rule set the packets are being processed in accordance with.

For example, at a time when it is determined that network protection device **100** should swap or switch from processing packets in accordance with policy **130**'s rule set to processing packets in accordance with policy **132**'s rule set, processor **300** may be beginning to process a packet than does not match the criteria of any of policy **130**'s rule set's rules other than rule **130**Z. Thus, processor **300** may be required to compare the packet being processed to a large number of additional rules potentially millions before reaching the rule whose criteria the packet will match (e.g., rule **130**Z). In contrast, at the time it is determined that network protection device **100** should swap or switch from processing packets in accordance with policy **130**'s rule set to processing packets in accordance with policy **132**'s rule set, processor **302** may be beginning to process a packet that matches the criteria specified by rule **130**A, and will therefore process the packet relatively quickly compared to processor **300**. Thus, if processors **300** and **302** each reconfigure to process packets in accordance with policy **132**'s rule set upon completion of processing their respective packets, processor **302** may begin processing packets in accordance with policy **132**'s rule set while processor **300** continues to process packets in accordance with policy **130**'s rule set. Accordingly, it may be advantageous to synchronize processors **300**, **302**, and **304**'s implementation of policy **132**'s rule set.

Referring to FIG. **3**B, when it is determined that network protection device **100** should swap or switch from processing packets in accordance with policy **130**'s rule set to processing packets in accordance with policy **132**'s rule set, each of processors **300**, **302**, and **304** may be signaled by administrative processor **312** (e.g., via data bus **120**) to stop processing packets. In some embodiments, processors **300**, **302**, and **304** may be signaled via the same channel over which they receive packets (e.g., data bus **120**). For example, a control packet, indicting the policy swap, may be sent to each of processors **300**, **302**, and **304**. In some embodiments, such a control packet may comprise a header value (e.g., a negative integer) that would not exist in a real network packet (e.g., a packet received from network **104**). Additionally or alternatively, packets sent to processors **300**, **302**, and **304** may be encapsulated within meta packets and the meta packets may include information indicating whether they are control packets (e.g., packets indicating that processors **300**, **302**, and **304** should swap from processing packets in accordance with policy **130**'s rule set to processing packets in accordance with policy **132**'s rule set) or packets containing real network packets (e.g., packets received from network **104**).

In some embodiments, each of processors **300**, **302**, and **304** may finish processing the packet they are currently processing and then cease processing packets. In other embodiments, each of processors **300**, **302**, and **304** may cease processing packets and cache the packet they are currently processing for future processing in accordance with policy **132**'s rule set. In any of the aforementioned embodiments, once a processor has ceased processing packets, it may cache any additional packets for future processing in accordance with policy **132**'s rule set. For example, processor **300** may cache any unprocessed packets in cache **306**. Similarly, processor **302** may cache any unprocessed packets in cache **308** and processor **304** may cache any unprocessed packets in cache **310**.

Referring to FIG. **3**C, upon ceasing to process packets (e.g., when a current packet has been examined against the rules in policy **130**'s rule set), each of processors **300**, **302**, and **304** may signal administrative processor **312** that they have stopped processing packets. Referring to FIG. **3**D, once each of processors **300**, **302**, and **304** have signaled that they have stopped processing packets, each of processors **300**, **302**, and **304** may be reconfigured to process packets in accordance with policy **132**'s rule set. Referring to FIG. **3**E, once reconfigured to process packets in accordance with policy **132**'s rule set, each of processors **300**, **302**, and **304** may signal administrative processor **312** that they have been successfully reconfigured. Referring to FIG. **3**F, once each of processors **300**, **302**, and **304** have signaled that they have been successfully reconfigured, each of processors **300**, **302**, and **304** may resume processing packets. For example, processors **300**, **302**, and **304** may begin by processing any packets respectively stored in caches **306**, **308**, and **310**, and then may process additional packets received from network **104** via network interface **108**.

By synchronizing the implementation of policy **132**'s rule set across processors **300**, **302**, and **304**, packets processed by network protection device **100** at any given time may receive uniform treatment irrespective of the particular processor which handles them. Because both policy **130**'s rule set and policy **132**'s rule set may be preprocessed prior to processing any packets in accordance with either of policies **130** or **132**'s rule sets, the time required to reconfigure network protection device **100** to process packets in accordance with policy **132**'s rule set may be reduced. Reducing the time required to swap or switch between processing packets in accordance with policy **130**'s rule set and policy **132**'s rule set may be particularly advantageous in certain contexts. For example, policy **130**'s rule set may specify a set of network address for which packets should be accepted (e.g., a set of network addresses corresponding to devices for which communications should be supported under normal network conditions) and that all other packets should be denied. Policy **132**'s rule set may specify a smaller set of network addresses for which packets should be accepted than that specified by policy **130**'s rule set (e.g., a set of network addresses corresponding to devices for which communications should be supported under demanding network conditions), and may further specify that all other packets should be denied. In the event of a network attack (e.g., a Distributed Denial-of-Service (DDoS) attack) or detection of one or more network conditions indicating a network attack, network protection device **100** may switch from processing packets in accordance with policy **130**'s rule set to processing packets in accordance with policy **132**'s rule set (e.g., in an effort to mitigate the effects of the attack). Accordingly, the faster network protection device **100** can switch from processing packets in accordance with policy **130**'s rule set to processing packets in accordance with policy **132**'s rule set, the greater the likelihood that the effects of the attack may be mitigated.

FIG. **4** illustrates an exemplary method for synchronizing multiple processors performing fast rule swapping. Referring to FIG. **4**, the steps may be performed by a network protection device, such as network protection device **100**. At step **400**, the second rule set may be invoked. For example, network protection device **100** may receive a message invoking policy **132**'s rule set or one or more network conditions indicating a network attack may be detected. At step **402**, one or more of the network protection device's processors responsible for

processing packets may be signaled to process packets in accordance with the second rule set. For example, processors **300**, **302**, and **304** may be signaled to process packets in accordance with policy **132**'s rule set. At step **404**, the one or more processors of the network protection device responsible for processing packets may cease processing packets. For example, each of processors **300**, **302**, and **304** may cease processing packets in accordance with policy **300**'s rule set. At step **406**, the one or more processors of the network protection device responsible for processing packets may cache any unprocessed packets. For example, each of processors **300**, **302**, and **304** may respectively cache any unprocessed packets in caches **306**, **308**, and **310**. At step **408**, the one or more processors of the network protection device responsible for processing packets may be reconfigured to process packets in accordance with the second rule set. For example, each of processors **300**, **302**, and **304** may be reconfigured to process packets in accordance with policy **132**'s rule set. At step **410**, the one or more processors of the network protection device responsible for processing packets may signal completion of the reconfiguration process. For example, each of processors **300**, **302**, and **304** may signal completion of their respective reconfiguration processes. At step **412**, the one or more processors of the network protection device responsible for processing packets may process any cached unprocessed packets in accordance with the second rule set. For example, each of processors **300**, **302**, and **304** may respectively process any unprocessed packets previously cached in caches **306**, **308**, and **310** in accordance with policy **132**'s rule set. At step **414**, additional packets may be processed in accordance with the second rule set. For example, each of processors **300**, **302**, and **304** may process additional packets received from network **104** in accordance with policy **132**'s rule set.

The functions and steps described herein may be embodied in computer-usable data or computer-executable instructions, such as in one or more program modules, executed by one or more computers or other devices to perform one or more functions described herein. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types when executed by one or more processors in a computer or other data processing device. The computer-executable instructions may be stored on a computer-readable medium such as a hard disk, optical disk, removable storage media, solid state memory, RAM, etc. As will be appreciated, the functionality of the program modules may be combined or distributed as desired in various embodiments. In addition, the functionality may be embodied in whole or in part in firmware or hardware equivalents, such as integrated circuits, application-specific integrated circuits (ASICs), field programmable gate arrays (FPGA), and the like. Particular data structures may be used to more effectively implement one or more aspects of the disclosure, and such data structures are contemplated to be within the scope of computer executable instructions and computer-usable data described herein.

Although not required, one of ordinary skill in the art will appreciate that various aspects described herein may be embodied as a method, an apparatus, or as one or more computer-readable media storing computer-executable instructions. Accordingly, those aspects may take the form of an entirely hardware embodiment, an entirely software embodiment, an entirely firmware embodiment, or an embodiment combining software, hardware, and firmware aspects in any combination.

As described herein, the various methods and acts may be operative across one or more computing servers and one or more networks. The functionality may be distributed in any manner, or may be located in a single computing device (e.g., a server, a client computer, etc.).

Aspects of the disclosure have been described in terms of illustrative embodiments thereof. Numerous other embodiments, modifications, and variations within the scope and spirit of the appended claims will occur to persons of ordinary skill in the art from a review of this disclosure. For example, one of ordinary skill in the art will appreciate that the steps illustrated in the illustrative figures may be performed in other than the recited order, and that one or more steps illustrated may be optional.

What is claimed is:

1. A method comprising:

receiving, by a network protection device, a first rule set and a second rule set;

preprocessing, by the network protection device, the first rule set and the second rule set to optimize performance of the network protection device for processing packets in accordance with at least one of the first rule set or the second rule set;

configuring at least two processors of the network protection device to process packets in accordance with the first rule set;

after the preprocessing and the configuring, receiving, by the network protection device, a plurality of packets;

processing, by the network protection device and in accordance with the first rule set, a portion of the plurality of packets;

signaling, each processor of the at least two processors, to process packets in accordance with the second rule set; and

configuring, each processor of the at least two processors, to responsive to the signaling to process packets in accordance with the second rule set:

cease processing of one or more packets;

cache the one or more packets;

reconfigure to process packets in accordance with the second rule set;

signal completion of reconfiguration to process packets in accordance with the second rule set; and

responsive to receiving signaling that each other processor of the at least two processors has completed reconfiguration to process packets in accordance with the second rule set, process, in accordance with the second rule set, the one or more packets.

2. The method of claim **1**, comprising:

storing, by the network protection device, configuration information for processing packets in accordance with the first rule set;

utilizing, by the network protection device, the configuration information to reconfigure to process packets in accordance with the first rule set; and

after the utilizing, processing, by the network protection device and in accordance with the first rule set, an additional portion of the plurality of packets.

3. The method of claim **1**, comprising:

storing, by the network protection device, the first rule set and the second rule set in a memory buffer; and

dynamically adjusting, by the network protection device and based on at least one of a size of the first rule set or a size of the second rule set, a size of the memory buffer.

4. The method of claim **1**, wherein the signaling to process packets in accordance with the second rule set is performed in

response to the network protection device receiving a message invoking the second rule set.

5. The method of claim **1**, wherein the signaling to process packets in accordance with the second rule set is performed in response to one or more detected network conditions indicating a network attack.

6. The method of claim **1**, wherein the preprocessing comprises merging two or more rules included in at least one of the first rule set or the second rule set into a single rule.

7. The method of claim **1**, wherein the preprocessing comprises separating a rule included in at least one of the first rule set or the second rule set into two or more rules.

8. The method of claim **1**, wherein the preprocessing comprises reordering one or more rules included in at least one of the first rule set or the second rule set.

9. A system comprising:

a plurality of processors; and

a memory comprising instructions that when executed by at least one processor of the plurality of processors cause the system to:

receive a first rule set and a second rule set;

preprocess the first rule set and the second rule set to optimize performance of the system for processing packets in accordance with at least one of the first rule set or the second rule set;

configure at least two processors of the plurality of processors to process packets in accordance with the first rule set;

after preprocessing the first rule set and the second rule set and configuring the at least two processors to process packets in accordance with the first rule set, receive a plurality of packets;

process, in accordance with the first rule set, a portion of the plurality of packets;

signal, each processor of the at least two processors, to process packets in accordance with the second rule set; and

configure, each processor of the at least two processors to, responsive to being signaled to process packets in accordance with the second rule set:

cease processing of one or more packets;

cache the one or more packets;

reconfigure to process packets in accordance with the second rule set;

signal completion of reconfiguration to process packets in accordance with the second rule set; and

responsive to receiving signaling that each other processor of the at least two processors has completed reconfiguration to process packets in accordance with the second rule set, process, in accordance with the second rule set, the one or more packets.

10. The system of claim **9**, wherein the instructions, when executed by the at least one processor, cause the system to:

store configuration information for processing packets in accordance with the first rule set;

utilize the configuration information to reconfigure to process packets in accordance with the first rule set; and

after utilizing the configuration information to reconfigure to process packets in accordance with the first rule set, process, in accordance with the first rule set, an additional portion of the plurality of packets.

11. The system of claim **9**, wherein the instructions, when executed by the at least one processor, cause the system to:

store the first rule set and the second rule set in a memory buffer; and

dynamically adjust, based on at least one of a size of the first rule set or a size of the second rule set, a size of the memory buffer.

12. The system of claim **9**, wherein the instructions, when executed by the at least one processor, cause the system to signal to process packets in accordance with the second rule set in response to the system receiving a message invoking the second rule set.

13. The system of claim **9**, wherein the instructions, when executed by the at least one processor, cause the system to signal to process packets in accordance with the second rule set in response to one or more detected network conditions indicating a network attack.

14. The system of claim **9**, wherein the instructions, when executed by the at least one processor, cause the system to, prior to configuring the at least two processors to process packets in accordance with the first rule set, merge two or more rules included in at least one of the first rule set or the second rule set into a single rule.

15. The system of claim **9**, wherein the instructions, when executed by the at least one processor, cause the system to, prior to configuring the at least two processors to process packets in accordance with the first rule set, separate a rule included in at least one of the first rule set or the second rule set into two or more rules.

16. The system of claim **9**, wherein the instructions, when executed by the at least one processor, cause the system to, prior to configuring the at least two processors to process packets in accordance with the first rule set, reorder one or more rules included in at least one of the first rule set or the second rule set.

17. One or more non-transitory computer-readable media comprising instructions that when executed by a computing system cause the computing system to:

receive a first rule set and a second rule set:

preprocess the first rule set and the second rule set to optimize performance of the computing system for processing packets in accordance with at least one of the first rule set or the second rule set;

configure at least two processors of the computing system to process packets in accordance with the first rule set;

after preprocessing the first rule set and the second rule set and configuring the at least two processors to process packets in accordance with the first rule set, receive a plurality of packets;

process, in accordance with the first rule set, a portion of the plurality of packets;

signal, each processor of the at least two processors, to process packets in accordance with the second rule set; and

configure, each processor of the at least two processors to, responsive to being signaled to process packets in accordance with the second rule set:

cease processing of one or more packets;

cache the one or more packets;

reconfigure to process packets in accordance with the second rule set;

signal completion of reconfiguration to process packets in accordance with the second rule set; and

responsive to receiving signaling that each other processor of the at least two processors has completed reconfiguration to process packets in accordance with the second rule set, process, in accordance with the second rule set, the one or more packets.

18. The one or more non-transitory computer-readable media of claim **17**, wherein the instructions, when executed by the computing system, cause the computing system to:

store configuration information for processing packets in accordance with the first rule set;

utilize the configuration information to reconfigure to process packets in accordance with the first rule set; and

after utilizing the configuration information to reconfigure to process packets in accordance with the first rule set, process, in accordance with the first rule set, an additional portion of the plurality of packets.

19. The one or more non-transitory computer-readable media of claim **17**, wherein the instructions, when executed by the computing system, cause the computing system to:

store the first rule set and the second rule set in a memory buffer; and

dynamically adjust, based on at least one of a size of the first rule set or a size of the second rule set, a size of the memory buffer.

20. The one or more non-transitory computer-readable media of claim **17**, wherein the instructions, when executed by the computing system, cause the computing system to signal to process packets in accordance with the second rule set in response to the computing system receiving a message invoking the second rule set.

21. The one or more non-transitory computer-readable media of claim **17**, wherein the instructions, when executed by the computing system, cause the computing system to signal to process packets in accordance with the second rule set in response to one or more detected network conditions indicating a network attack.

22. The one or more non-transitory computer-readable media of claim **17**, wherein the instructions, when executed by the computing system, cause the computing system to, prior to configuring the at least two processors to process packets in accordance with the first rule set, merge two or more rules included in at least one of the first rule set or the second rule set into a single rule.

23. The one or more non-transitory computer-readable media of claim **17**, wherein the instructions, when executed by the computing system, cause the computing system to, prior to configuring the at least two processors to process packets in accordance with the first rule set, separate a rule included in at least one of the first rule set or the second rule set into two or more rules.

24. The one or more non-transitory computer-readable media of claim **17**, wherein the instructions, when executed by the computing system, cause the computing system to, prior to configuring the at least two processors to process packets in accordance with the first rule set, reorder one or more rules included in at least one of the first rule set or the second rule set.

* * * * *

US009560176B2

(12) **United States Patent**
Ahn et al.

(10) **Patent No.: US 9,560,176 B2**
(45) **Date of Patent: Jan. 31, 2017**

(54) **CORRELATING PACKETS IN COMMUNICATIONS NETWORKS**

(71) Applicant: **Centripetal Networks, Inc.**, Herndon, VA (US)

(72) Inventors: **David K. Ahn**, Winston-Salem, NC (US); **Peter P. Geremia**, Portsmouth, NH (US); **Pierre Mallett, III**, Herndon, VA (US); **Sean Moore**, Hollis, NH (US); **Robert T. Perry**, Ashburn, VA (US)

(73) Assignee: **Centripetal Networks, Inc.**, Herndon, VA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **14/714,207**

(22) Filed: **May 15, 2015**

(65) **Prior Publication Data**

US 2016/0234083 A1 Aug. 11, 2016

Related U.S. Application Data

(63) Continuation of application No. 14/618,967, filed on Feb. 10, 2015, now Pat. No. 9,264,370.

(51) **Int. Cl.**
H04L 29/06 (2006.01)
H04L 12/851 (2013.01)
(Continued)

(52) **U.S. Cl.**
CPC ***H04L 69/22*** (2013.01); ***H04L 43/026*** (2013.01); ***H04L 43/04*** (2013.01); ***H04L 43/12*** (2013.01);
(Continued)

(58) **Field of Classification Search**
CPC H04L 69/22; H04L 12/2605; H04L 43/04; H04L 45/745; H04L 43/12; H04L 63/0263; H04L 43/026; H04L 47/2483; H04L 47/32; H04L 61/2567; H04L 43/16; H04L 43/087; H04L 43/106
(Continued)

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,098,172 A 8/2000 Coss et al.
6,226,372 B1 5/2001 Beebe et al.
(Continued)

FOREIGN PATENT DOCUMENTS

AU 2005328336 B2 9/2011
AU 2006230171 B2 6/2012
(Continued)

OTHER PUBLICATIONS

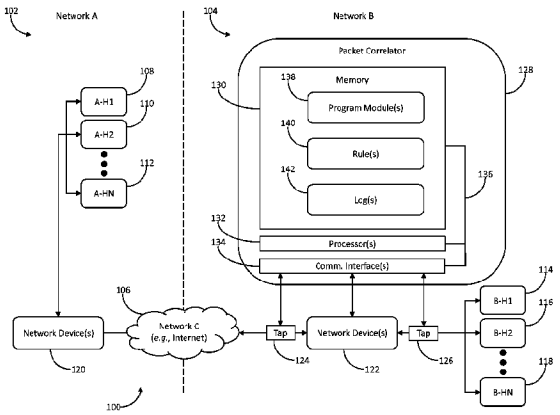
Greenwald et al., Designing an Academic Firewall: Policy, Practice, and Experience With SURF, Proceedings of SNDSS '96, IEEE, 1996, Department of Computer Science, Stanford University, Stanford, CA.
(Continued)

Primary Examiner — Obaidul Huq
(74) *Attorney, Agent, or Firm* — Banner & Witcoff, Ltd.

(57) **ABSTRACT**

A computing system may identify packets received by a network device from a host located in a first network and may generate log entries corresponding to the packets received by the network device. The computing system may identify packets transmitted by the network device to a host located in a second network and may generate log entries corresponding to the packets transmitted by the network device. Utilizing the log entries corresponding to the packets received by the network device and the log entries corresponding to the packets transmitted by the network device, the computing system may correlate the packets transmitted by the network device with the packets received by the network device.

30 Claims, 7 Drawing Sheets



Joint Trial Exhibit
JTX-3
Case No. 18-cv-00094-HCM

(51) **Int. Cl.**

H04L 12/26	(2006.01)
H04L 12/741	(2013.01)
H04L 29/12	(2006.01)
H04L 12/823	(2013.01)

(52) **U.S. Cl.**

CPC ***H04L 45/745*** (2013.01); ***H04L 47/2483*** (2013.01); ***H04L 47/32*** (2013.01); ***H04L 61/2567*** (2013.01); ***H04L 63/0263*** (2013.01); *H04L 43/087* (2013.01); *H04L 43/106* (2013.01); *H04L 43/16* (2013.01)

(58) **Field of Classification Search**

USPC 370/241, 351, 352, 356, 389, 395.1, 370/395.3, 395.31, 464, 474

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,317,837	B1	11/2001	Kenworthy	
6,484,261	B1	11/2002	Wiegel	
6,611,875	B1	8/2003	Chopra et al.	
6,662,235	B1	12/2003	Callis et al.	
7,089,581	B1	8/2006	Nagai et al.	
7,107,613	B1	9/2006	Chen et al.	
7,215,637	B1	5/2007	Ferguson et al.	
7,227,842	B1	6/2007	Ji et al.	
7,237,267	B2	6/2007	Rayes et al.	
7,263,099	B1	8/2007	Woo et al.	
7,299,353	B2	11/2007	Le Pennec et al.	
7,331,061	B1	2/2008	Ramsey et al.	
7,478,429	B2	1/2009	Lyon	
7,539,186	B2	5/2009	Aerrabotu et al.	
7,684,400	B2	3/2010	Govindarajan et al.	
7,710,885	B2	5/2010	Ilnicki et al.	
7,721,084	B2	5/2010	Salminen et al.	
7,818,794	B2	10/2010	Wittman	
7,954,143	B2	5/2011	Aaron	
8,004,994	B1 *	8/2011	Darisi et al.	370/241
3,042,167	A1	10/2011	Fulp et al.	
8,037,517	B2	10/2011	Fulp et al.	
8,117,655	B2	2/2012	Spielman	
8,176,561	B1	5/2012	Hurst et al.	
8,306,994	B2	11/2012	Kenworthy	
8,495,725	B2	7/2013	Ahn	
8,726,379	B1	5/2014	Stiansen et al.	
8,806,638	B1	8/2014	Mani	
8,856,926	B2	10/2014	Narayanaswamy et al.	
8,935,785	B2	1/2015	Pandrangi	
9,094,445	B2	7/2015	Moore et al.	
9,124,552	B2	9/2015	Moore	
9,137,205	B2	9/2015	Rogers et al.	
9,160,713	B2	10/2015	Moore	
2001/0039579	A1	11/2001	Trcka et al.	
2001/0039624	A1	11/2001	Kellum	
2002/0016858	A1	2/2002	Sawada et al.	
2002/0038339	A1	3/2002	Xu	
2002/0049899	A1	4/2002	Kenworthy	
2002/0165949	A1	11/2002	Na et al.	
2002/0186683	A1	12/2002	Buck et al.	
2002/0198981	A1	12/2002	Corl et al.	
2003/0035370	A1	2/2003	Brustoloni	
2003/0097590	A1	5/2003	Syvanne	
2003/0105976	A1	6/2003	Copeland	
2003/0120622	A1	6/2003	Nurmela et al.	
2003/0123456	A1	7/2003	Denz et al.	
2003/0142681	A1	7/2003	Chen et al.	
2003/0145225	A1	7/2003	Bruton, III et al.	
2003/0154297	A1 *	8/2003	Suzuki et al.	709/229
2003/0154399	A1	8/2003	Zuk et al.	
2003/0188192	A1	10/2003	Tang et al.	
2003/0212900	A1	11/2003	Liu et al.	
2004/0010712	A1	1/2004	Hui et al.	
2004/0073655	A1	4/2004	Kan	
2004/0088542	A1	5/2004	Daude et al.	
2004/0093513	A1	5/2004	Cantrell et al.	
2004/0098511	A1	5/2004	Lin et al.	
2004/0151155	A1	8/2004	Jouppi	
2004/0177139	A1	9/2004	Schuba et al.	
2004/0193943	A1	9/2004	Angelino et al.	
2004/0205360	A1	10/2004	Norton et al.	
2004/0250124	A1	12/2004	Chesla et al.	
2005/0010765	A1	1/2005	Swander et al.	
2005/0114704	A1	5/2005	Swander	
2005/0117576	A1	6/2005	McDysan et al.	
2005/0125697	A1	6/2005	Tahara	
2005/0138204	A1	6/2005	Iyer et al.	
2005/0141537	A1	6/2005	Kumar et al.	
2005/0183140	A1	8/2005	Goddard	
2005/0229246	A1	10/2005	Rajagopal et al.	
2005/0251570	A1	11/2005	Heasman et al.	
2005/0286522	A1	12/2005	Paddon et al.	
2006/0048142	A1	3/2006	Roese et al.	
2006/0053491	A1	3/2006	Khuti et al.	
2006/0070122	A1	3/2006	Bellovin	
2006/0104202	A1	5/2006	Reiner	
2006/0114899	A1 *	6/2006	Toumura et al.	370/389
2006/0136987	A1	6/2006	Okuda	
2006/0137009	A1	6/2006	Chesla	
2006/0146879	A1	7/2006	Anthias et al.	
2006/0195896	A1	8/2006	Fulp et al.	
2006/0212572	A1	9/2006	Afek et al.	
2006/0248580	A1	11/2006	Fulp et al.	
2006/0262798	A1	11/2006	Joshi et al.	
2007/0083924	A1	4/2007	Lu	
2007/0211644	A1	9/2007	Ottamalika et al.	
2007/0240208	A1	10/2007	Yu et al.	
2008/0005795	A1	1/2008	Acharya et al.	
2008/0043739	A1	2/2008	Suh et al.	
2008/0072307	A1	3/2008	Maes	
2008/0077705	A1	3/2008	Li et al.	
2008/0163333	A1	7/2008	Kasralikar	
2008/0229415	A1	9/2008	Kapoor et al.	
2008/0235755	A1	9/2008	Blaisdell et al.	
2008/0279196	A1	11/2008	Friskney et al.	
2008/0301765	A1	12/2008	Nicol et al.	
2009/0138938	A1	5/2009	Harrison et al.	
2009/0172800	A1	7/2009	Wool	
2009/0222877	A1	9/2009	Diehl et al.	
2009/0240698	A1	9/2009	Shukla et al.	
2009/0328219	A1	12/2009	Narayanaswamy	
2010/0011433	A1	1/2010	Harrison et al.	
2010/0011434	A1	1/2010	Kay	
2010/0082811	A1	4/2010	Van Der Merwe et al.	
2010/0095367	A1	4/2010	Narayanaswamy	
2010/0107240	A1	4/2010	Thaler et al.	
2010/0132027	A1	5/2010	Ou	
2010/0199346	A1	8/2010	Ling et al.	
2010/0211678	A1	8/2010	McDysan et al.	
2010/0232445	A1	9/2010	Bellovin	
2010/0242098	A1	9/2010	Kenworthy	
2010/0268799	A1	10/2010	Maestas	
2010/0296441	A1	11/2010	Barkan	
2010/0303240	A1	12/2010	Beachem et al.	
2011/0055916	A1	3/2011	Ahn	
2011/0055923	A1	3/2011	Thomas	
2011/0088092	A1	4/2011	Nguyen et al.	
2011/0185055	A1 *	7/2011	Nappier et al.	709/224
2011/0270956	A1	11/2011	McDysan et al.	
2012/0023576	A1	1/2012	Sorensen et al.	
2012/0106354	A1 *	5/2012	Pleshek	H04L 43/12 370/241
2012/0113987	A1	5/2012	Riddoch et al.	
2012/0240135	A1	9/2012	Risbood et al.	
2012/0264443	A1	10/2012	Ng et al.	
2012/0314617	A1	12/2012	Erichsen et al.	
2012/0331543	A1 *	12/2012	Bostrom et al.	726/13
2013/0047020	A1	2/2013	Hershko et al.	
2013/0059527	A1	3/2013	Hasesaka et al.	
2013/0061294	A1	3/2013	Kenworthy	
2013/0117852	A1	5/2013	Stute	
2013/0254766	A1 *	9/2013	Zuo et al.	718/1
2013/0305311	A1	11/2013	Puttaswamy Naga et al.	

Keysight, EX-1028
CENTRIPETAL-SCO 001832

(56) **References Cited**

U.S. PATENT DOCUMENTS

2014/0075510	A1	3/2014	Sonoda et al.
2014/0115654	A1	4/2014	Rogers et al.
2014/0201123	A1	7/2014	Ahn et al.
2014/0215574	A1	7/2014	Erb et al.
2014/0281030	A1	9/2014	Cui
2014/0283004	A1	9/2014	Moore
2014/0283030	A1	9/2014	Moore et al.
2014/0366132	A1	12/2014	Stiansen et al.
2015/0237012	A1	8/2015	Moore
2015/0304354	A1	10/2015	Rogers et al.
2015/0334125	A1	11/2015	Bartos et al.

FOREIGN PATENT DOCUMENTS

CA	2600236	A1	10/2006
EP	1006701	A2	6/2000
EP	1313290	A1	5/2003
EP	1484884	A2	12/2004
EP	1677484	A2	7/2006
EP	2385676	A1	11/2011
EP	2498442	A1	9/2012
EP	1864226	B1	5/2013
KR	20010079361	A	8/2001
WO	2005046145	A1	5/2005
WO	2006093557	A2	9/2006
WO	2006105093	A2	10/2006
WO	2011038420	A2	3/2011
WO	20120146265	A1	11/2012

OTHER PUBLICATIONS

Reumann et al., Adaptive Packet Filters, IEEE, 2001, Department of Electrical Engineering and Computer Science, The University of Michigan, Ann Arbor, MI.

Mizuno et al., A New Remote Configurable Firewall System for Home-use Gateways, IEEE, 2004, NTT Information Sharing Platform Laboratories.

Kindervag et al., Build Security Into Your Network's DNA: The Zero Trust Network Architecture, Nov. 5, 2010, Forrester Research, Inc., Cambridge MA.

Moore, SBIR Case Study: Centripetal Networks, How CNI Leveraged DHS S&T SBIR Funding to Launch a Successful Cyber Security Company, Cyber Security Division, 2012 Principal Investigators' Meeting, Oct. 10, 2012, Centripetal Networks, Inc.

Designing A Zero Trust Network With Next-Generation Firewalls, Palo Alto Networks: Technology Brief, viewed Oct. 21, 2012, Palo Alto Networks, Santa Clara, CA.

Control Plane Policing Implementation Best Practices, Mar. 13, 2013, Cisco Systems.

International Search Report and Written Opinion for International App. No. PCT/US2013/057502, dated Nov. 7, 2013.

International Search Report and Written Opinion for International App. No. PCT/US2013/072566, dated Mar. 24, 2014.

International Search Report and Written Opinion for International App. No. PCT/US2014/023286, dated Jun. 24, 2014.

International Search Report and Written Opinion for International App. No. PCT/US2014/027723, dated Jun. 26, 2014.

Communication Relating to the Results of the Partial International Search for International App. No. PCT/US2015/024691, dated Jul. 10, 2015.

International Preliminary Report on Patentability for International App. No. PCT/US2013/072566, dated Jul. 23, 2015.

International Search Report and Written Opinion for International App. No. PCT/US2015/024691, dated Sep. 16, 2015.

International Preliminary Report on Patentability for International App. No. PCT/US2013/057502, dated May 7, 2015.

International Preliminary Report on Patentability for International App. No. PCT/US2014/023286, dated Sep. 24, 2015.

International Preliminary Report on Patentability for International App. No. PCT/US2014/027723, dated Sep. 24, 2015.

Statement RE: Related Application, dated Sep. 30, 2015.

Apr. 15, 2016—(US) Notice of Allowance—U.S. Appl. No. 14/855,374.

Jan. 28, 2016—(WO) International Search Report and Written Opinion—App PCT/US2015/062691.

Jan. 11, 2016—(US) Non Final Rejection—U.S. Appl. No. 14/698,560.

Apr. 27, 2011—(WO) International Search Report and Written Opinion—App PCT/US2010/054520.

Mar. 4, 2011—(US) Notice of Allowance—U.S. Appl. No. 11/316,331.

Mar. 3, 2011—(EP) Communication Pursuant to Rules 70(2) and 70a(2)—App 06758213.0.

Feb. 14, 2011—(EP) Search Report—App 06758213.0.

Fulp, Errin: "Errin Fulp," XP002618346, www.cs.wfu.edu/fulp/ewfPub.html. pp. 1-5 (Copyright 2010).

Sep. 30, 2010—(US) Office Action—U.S. Appl. No. 11/390,976.

Sep. 10, 2010—(AU) Office Action—App 2006230171.

Aug. 20, 2010—(AU) Office Action—App 2005328336.

Jun. 23, 2010—(US) Final Rejection—U.S. Appl. No. 11/316,331.

Apr. 29, 2010—(US) Interview Summary—U.S. Appl. No. 11/390,976.

Mar. 26, 2010—(US) Final Rejection—U.S. Appl. No. 11/390,976.

Sep. 14, 2009 (US) Office Action—U.S. Appl. No. 11/316,331.

Jun. 24, 2009—(US) Office Action—U.S. Appl. No. 11/390,976.

Jul. 3, 2008—(WO) Written Opinion of the International Searching Authority—App PCT/US06/11291.

Aug. 31, 2007—(EP) Communication Pursuant to Rules 109 and 110—App 05857614.1.

Acharya et al, "OPTWALL: A Hierarchical Traffic-Aware Firewall," Department of Computer Science, Telecommunications Program, University of Pittsburgh, pp. 1-11 (2007).

Sep. 11, 2006—(WO) Written Opinion of the International Searching Authority—App PCT/US05/47008.

Tarsa et al., "Balancing Trie-Based Policy representations for Network Firewalls," Department of Computer Science, Vake Forest University, pp. 1-6 (2006).

Fulp, "Trie-Based Policy Representations for Network Firewalls," Proceedings of the IEEE International Symposium on computer Communications (2005).

E. Fulp, "Optimization of Network Firewall Policies Using Ordered Sets and Directed Acyclical Graphs", Technical Report, Computer Scient Department, Wake Forest University, Jan. 2004.

E. Fulp et al., "Network Firewall Policy Tries", Technical Report, Computer Science Department, Wake Forest University, 2004.

E. Al-Shaer et al., "Modeling and Management of Firewall Policies", IEEE Transactions on Network and Service Management, 1(1): 2004.

E.W. Fulp, "Firewall Architectures for High Speed Networks", U.S. Department of Energy Grant Application, Funded Sep. 2003.

E. Al-Shaer et al., "Firewall Policy Advisor for Anomaly Discovery and Rule Editing", Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management, 2003.

V.P. Ranganath, "A Set-Based Approach to Packet Classification", Proceedings of the IASTED International Conference on Parallel and Distributed Computing and Systems, 889-894, 2003.

M. Christiansen et al., "Using IDDsfor Packet Filtering", Technical Report, BRICS. Oct. 2002.

Lee et al., "Development Framework for Firewall Processors," IEEE, pp. 352-355 (2002).

L. Qui et al., "Fast Firewall Implementations for Software and Hardware-Based Routers", Proceedings of ACM Sigmetrics, Jun. 2001.

D. Eppstein et al., "Internet Packet Filter Management and Rectangle Geometry", Proceedings of the Symposium on Discrete Algorithms, 827-835, 2001.

E. Fulp, "Preventing Denial of Service Attacks on Quality of Service", Proceedings of the 2001 DARPA Information Survivability Conference and Exposition II, 2001.

S. Goddard et al., "An Unavailability Analysis of Firewall Sandwich Configurations", Proceedings of the 6th IEEE Symposium on High Assurance Systems Engineering, 2001.

(56) **References Cited**

OTHER PUBLICATIONS

G.V. Rooij, "Real Stateful TCP Packet Filtering in IP Filter", Proceedings of the 10th USENIX Security Symposium, 2001.
P. Warkhede et al., "Fast Packet Classification for Two-Dimensional Conflict-Free Filters", Proceedings of IEEE INFOCOM, 1434-1443, 2001.
D. Decasper et al., "Router Plugins: A Software Architecture for Next-Generation Routers", IEEE/ACM Transactions on Networking, 8(1): Feb. 2000.
A. Feldmann et al., "Tradeoffs for Packet Classification", Proceedings of the IEEE INFOCOM, 397-413, 2000.
X. Gan et al., "LSMAC vs. LSNAT: Scalable Cluster-based Web servers", Journal of Networks, Software Tools, and Applications, 3(3): 175-185, 2000.
A. Hari et al., "Detecting and Resolving Packet Filter Conflicts", Proceedings of IEEE INFOCOM, 1203-1212, 2000.
O. Paul et al., "A full Bandwidth ATM Firewall", Proceedings of the 6th European Symposium on Research in Computer Security ESORICS'2000, 2000.
J. Xu et al., "Design and Evaluation of a High-Performance ATM Firewall Switch and Its Applications", IEEE Journal on Selected Areas in Communications, 17(6): 1190-1200, Jun. 1999.
C. Benecke, "A Parallel Packet Screen for High Speed Networks", Proceedings of the 15th Annual Computer Security Applications Conference, 1999.
R. Funke et al., "Performance Evaluation of Firewalls in Gigabit-Networks", Proceedings of the Symposium on Performance Evaluation of Computer and Telecommunication Systems, 1999.
S. Suri et al., "Packet Filtering in High Speed Networks", Proceedings of the Symposium on Discrete Algorithms, 969-970, 1999.
J. Ellermann et al., "Firewalls for ATM Networks", Proceedings of INFOSEC'COM, 1998.
V. Srinivasan et al., "Fast and Scalable Layer Four Switching", Proceedings of ACM SIGCOMM, 191-202, 1998.
M. Degermark et al., "Small Forwarding Tables for Fast Routing Lookups", Proceedings of ACM SIGCOMM, 4-13, 1997.
S,M. Bellovin et al., "Network Firewalls", IEEE Communications Magazine, 50-57, 1994.
W.E. Leland et al., "On the Self-Similar Nature of Ethernet Traffic", IEEE Transactions on Networking, 2(1); 15, 1994.
G. Brightwell et al., "Counting Linear Extensions is #P-Complete", Proceedings of the Twenty-Third Annual ACM Symposium on Theory of Computing, 1991.
M. Al-Suwaiyel et al., "Algorithms for Trie Compaction", ACM Transactions on Database Systems, 9(2): 243-263, Jun. 1984.
D. Corner, "Analysis of a Heuristic for Full Trie Minimization", ACM Transactions on Database Systems, 6(3): 513-537, Sep. 1981.
R.L. Graham et al., "Optimization and Approximation in Deterministic Sequencing and Scheduling: A Survey", Annals of Discrete Mathematics, 5: 287-326, 1979.
E.L. Lawler, "Sequencing Jobs to Minimize Total Weighted Completion oTime Subject to Precedence Constraints", Annals of Discrete Mathematics, 2: 75-90, 1978.
J.K. Lenstra et al., "Complexity of Scheduling Under Precedence Constraints", Operations Research, 26(1): 22-35,1978.
R. Rivest, "On Self-Organizing Sequential Search Heuristics", Communications of the ACM, 19(2): 1976.
W.E. Smith, "Various Optimizers for Single-Stage Productions", Naval Research Logistics Quarterly, 3: 59-66, 1956.
Bellion, "High Performance Packet Classification", http://www.hipac.org (Publication Date Unknown).
Oct. 18, 2011—(EP) Communication Pursuant to Article 94(3)—App 06 758 213.0.
Jun. 9, 2011—(US) Notice of Allowance—U.S. Appl. No. 11/390,976.
Jun. 26, 2012—(EP) Extended Search Report—App 05857614.1.
Jun. 9, 2012—(AU) Notice of Acceptance—App 2006230171.
Nov. 11, 2011—(AU) Second Office Action—App 2006230171.
Jan. 17, 2013—(CA) Office Action—App 2,600,236.
Jan. 16, 2013—(CA) Office Action—App 2,594,020.
Nov. 20, 2012—(EP) Communication under rule 71(3)—App 06 758 213.0.
Apr. 18, 2013—(EP) Decision to Grant a European Patent—App 06758212.0.
Aug. 25, 2011—(US) Non Final Rejection—U.S. Appl. No. 12/871,806.
Feb. 6, 2012—(US) Final Rejection—U.S. Appl. No. 12/871,806.
Aug. 7, 2012—(US) Non Final Rejection—U.S. Appl. No. 12/871,806.
Nov. 26, 2012—(US) Final Rejection—U.S. Appl. No. 12/871,806.
Apr. 4, 2013—(US) Notice of Allowance—U.S. Appl. No. 12/871,806.
Jan. 14, 2015—(EP) Extended Search Report—App 10819667.6.
May 26, 2014—(CA) Office Action—App 2010297968.
May 25, 2015—(AU) Notice of Acceptance—App 2010297968.
May 14, 2015—(US) Non Final Rejection—U.S. Appl. No. 13/940,240.
Nov. 27, 2015—(US) Final Rejection—U.S. Appl. No. 13/940,240.
Statement RE: Related Application, dated Jul. 24, 2015.
Feb. 26, 2016—(US) Non Final Office Action—U.S. Appl. No. 14/253,992.
Nov. 2, 2015—(AU) Office Action—App 2013372879.
Apr. 26, 2016—(US) Office Action—U.S. Appl. No. 14/745,207.
May 13, 2016—(US) Office Action—U.S. Appl. No. 13/940,240.
Jun. 14, 2016—(US) Office Action—U.S. Appl. No. 14/625,486.
Feb. 25, 2016—(AU) Office Action—App 2014249055.
Feb. 24, 2016—(AU) Office Action—App 2014228257.
Jun. 9, 2016—(WO) International Search Report—PCT/US2016/026339.
Jun. 16, 2016—(CA) Office Action—App 2,888,935.
Jul. 11, 2016—(EP) Office Action—App 14720824.3.
Jul. 22, 2016—(US) Office Action—U.S. Appl. No. 14/921,718.
Jul. 20, 2016—(AU) Office Action—App 2013335255.

* cited by examiner

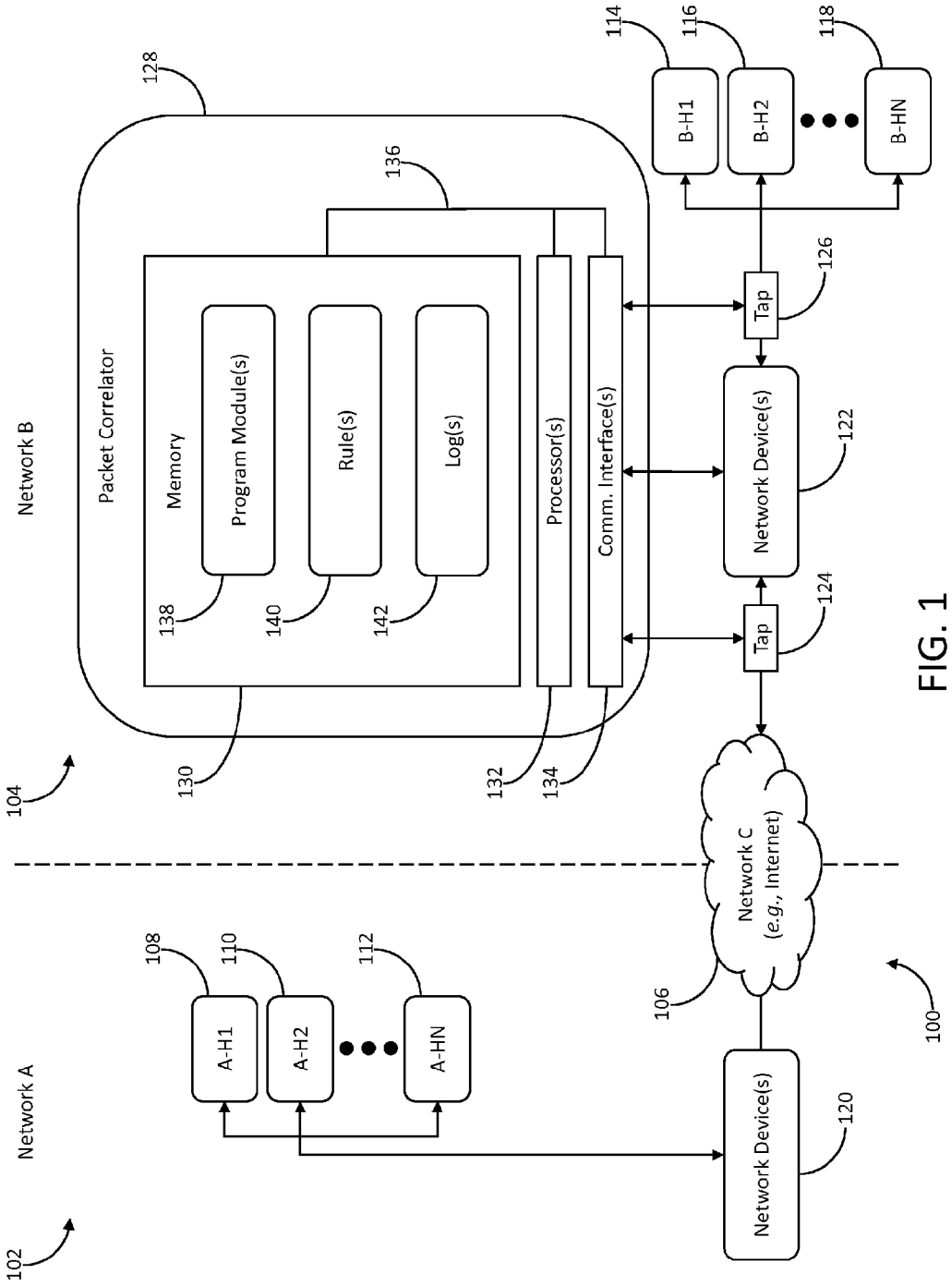

Network B
Packet Correlator
Memory
Program Module(s)
Rule(s)
Log(s)
Processor(s)
Comm. Interface(s)
Network Device(s)
Tap
Tap
B-H1
B-H2
B-HN
Network C
(e.g., Internet)
Network A
A-H1
A-H2
A-HN
Network Device(s)
128
136
138
140
142
130
132
134
104
114
116
118
126
122
124
108
110
112
106
120
102
100

FIG. 1

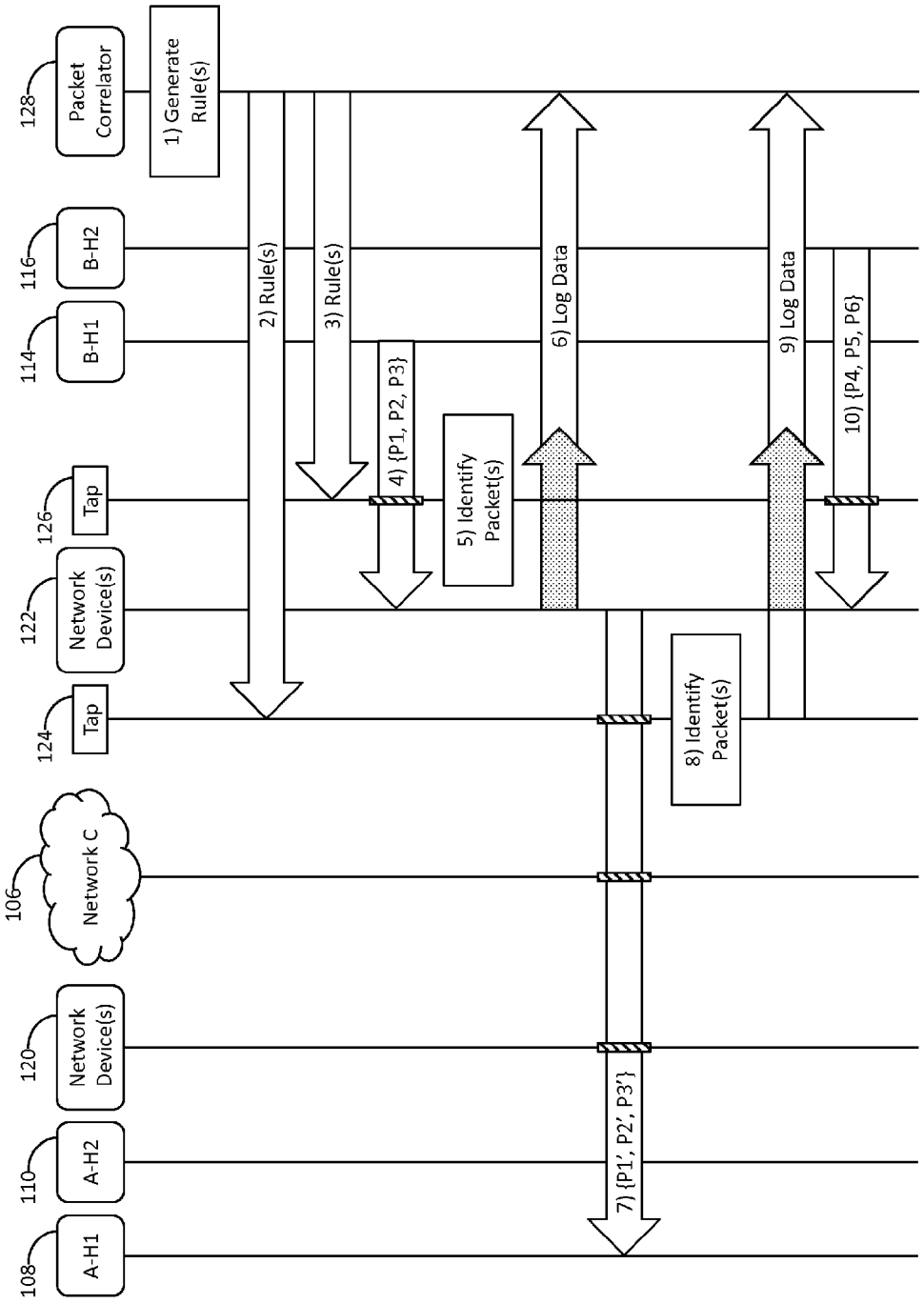


FIG. 2A

Keysight, EX-1028
CENTRIPETAL-SCG 001836

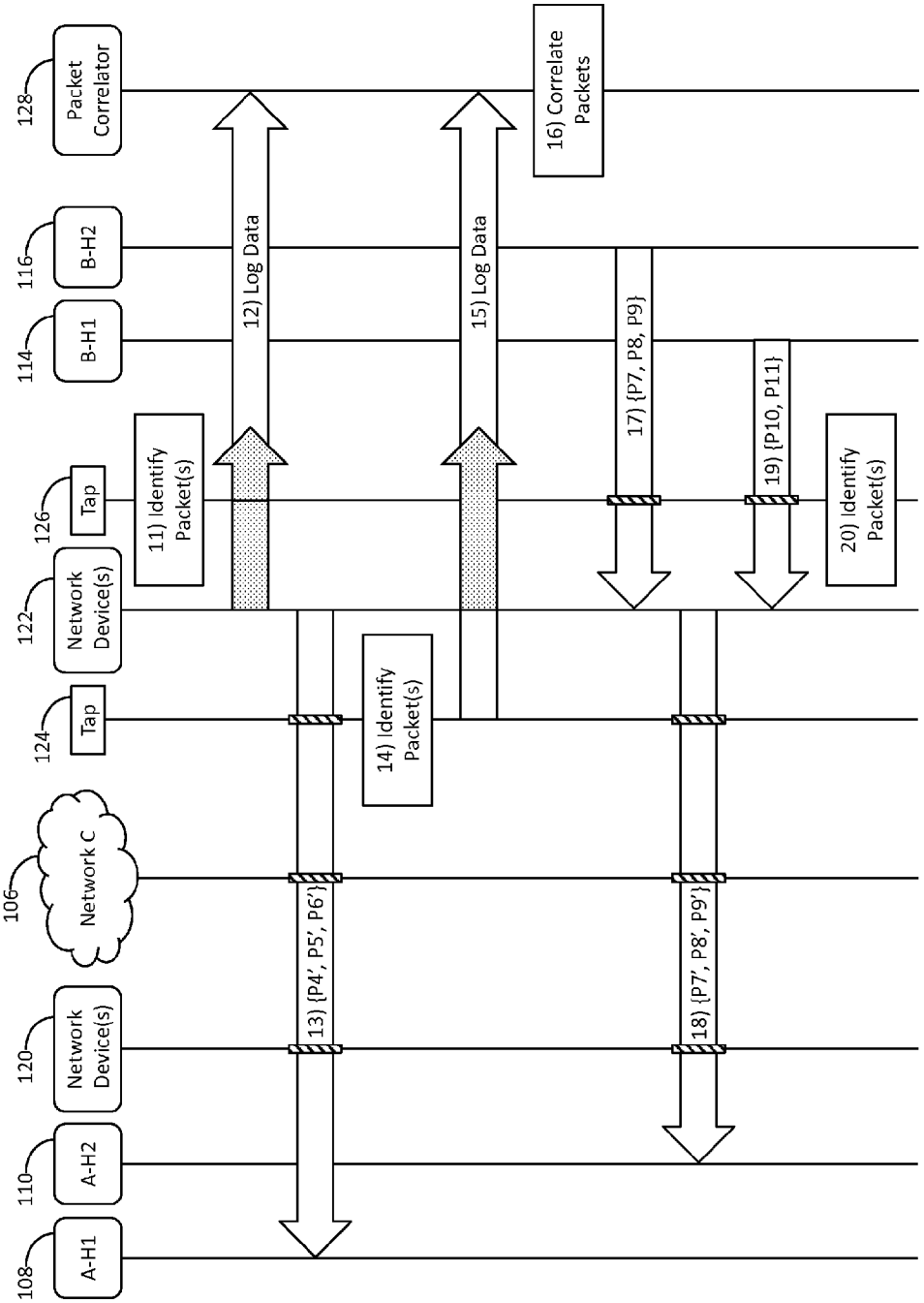


FIG. 2B

Keysight, EX-1028
CENTRIPETAL-SCO 001837

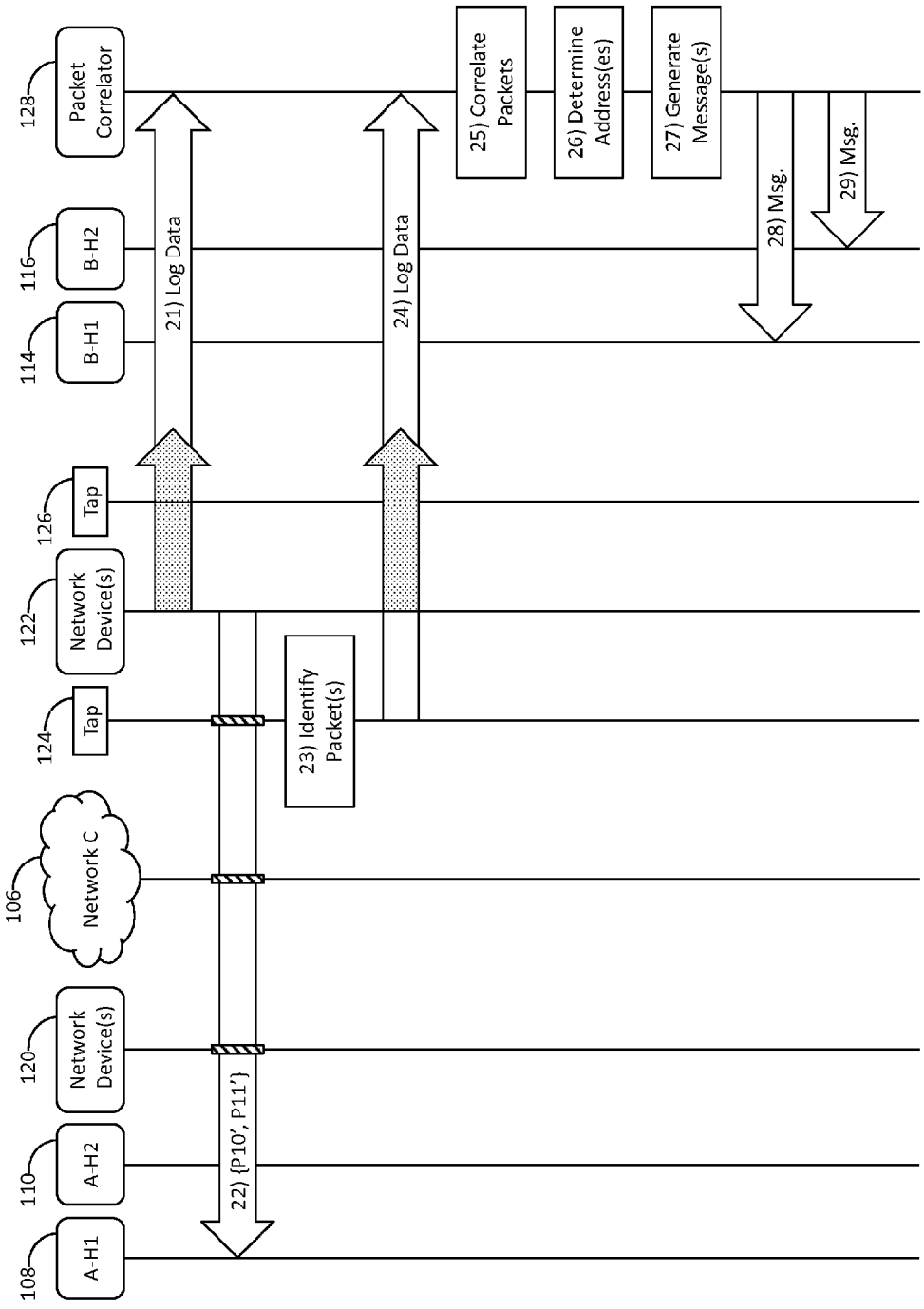


FIG. 2C

Keysight, EX-1028
CENTRIPETAL-SSC 001838

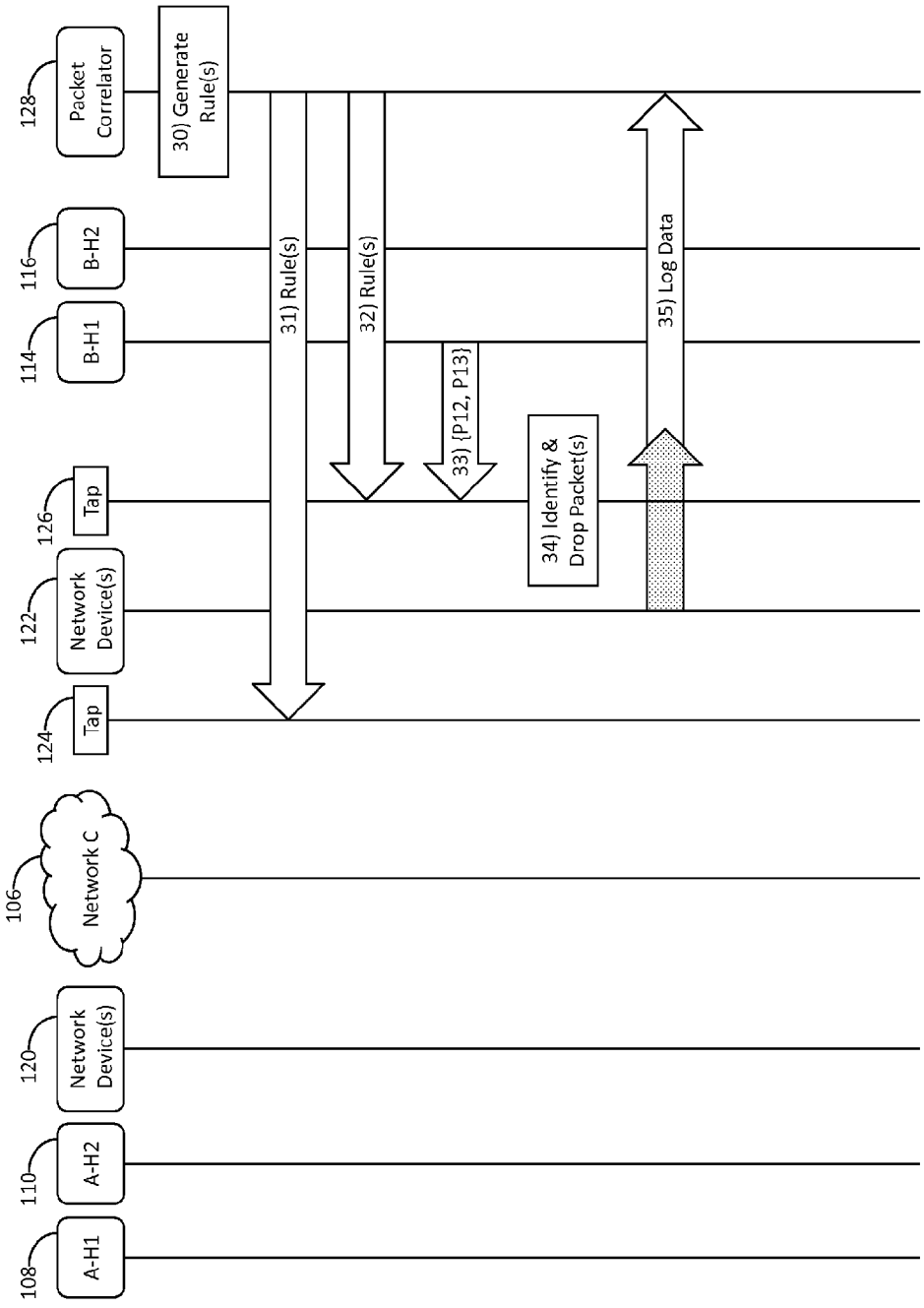

128
Packet Correlator
30) Generate Rule(s)
116
B-H2
114
B-H1
31) Rule(s)
32) Rule(s)
33) {P12, P13}
35) Log Data
126
Tap
34) Identify & Drop Packet(s)
122
Network Device(s)
124
Tap
106
Network C
120
Network Device(s)
110
A-H2
108
A-H1

FIG. 2D

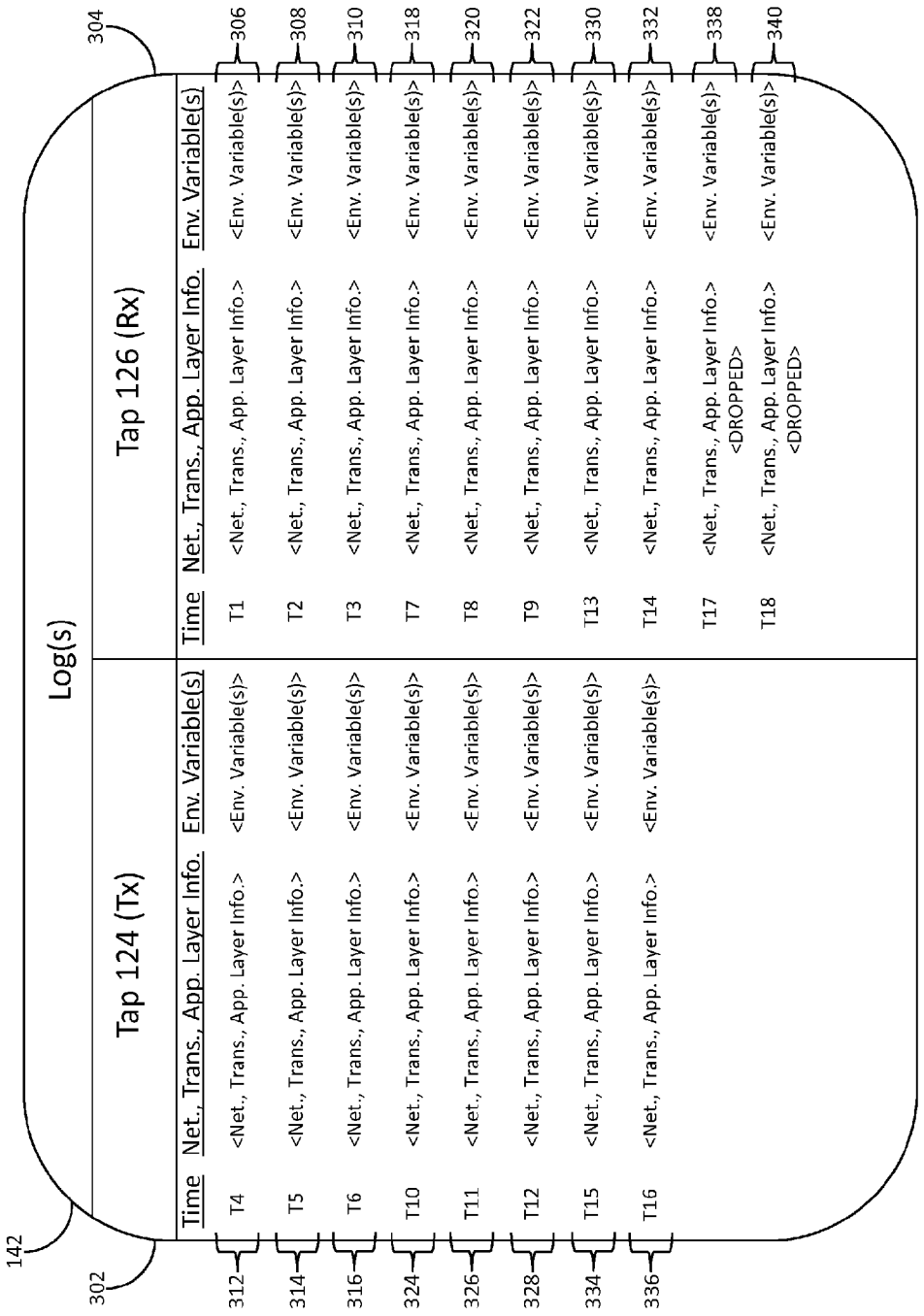


FIG. 3

Keysight, EX-1028
CENTRIPETAL-0003 001840

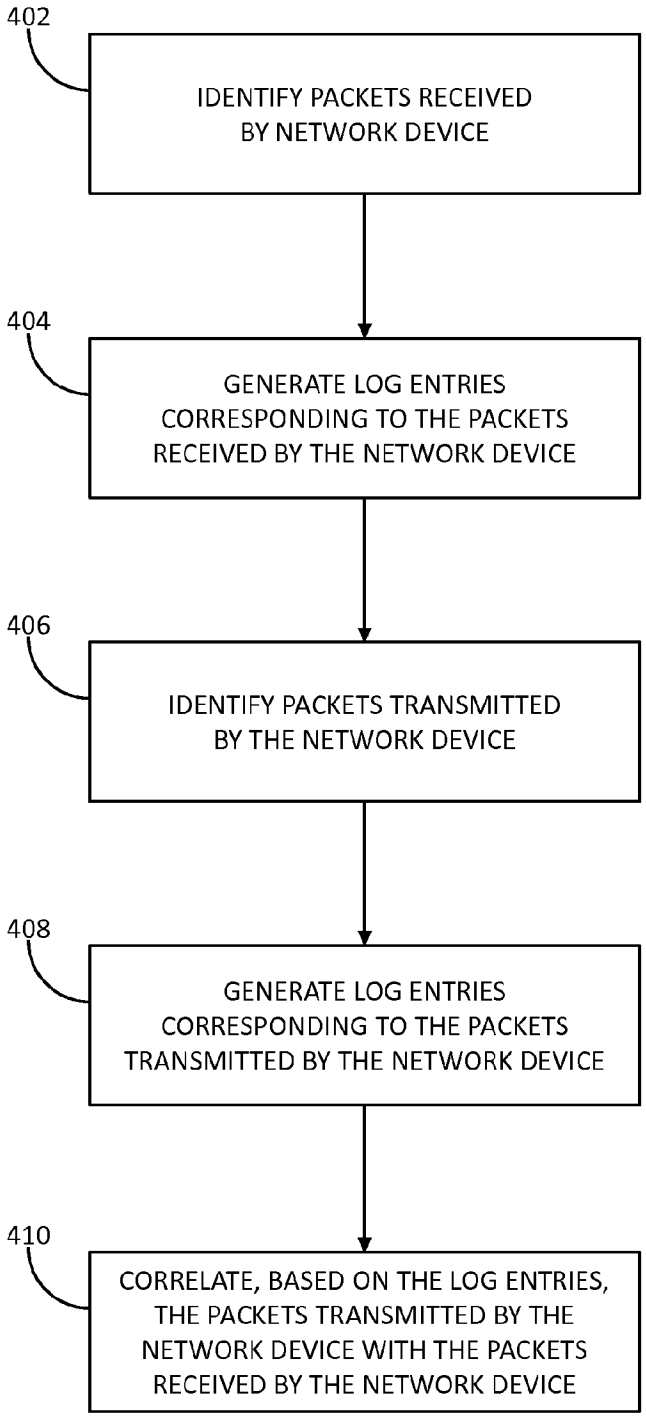


FIG. 4

Keysight, EX-1028
CENTRIPETAL-SSC-001841

CORRELATING PACKETS IN COMMUNICATIONS NETWORKS

CROSS-REFERENCE TO RELATED APPLICATION

This application is a continuation of and claims priority to U.S. patent application Ser. No. 14/618,967, filed Feb. 10, 2015, and entitled "CORRELATING PACKETS IN COMMUNICATIONS NETWORKS," the disclosure of which is incorporated by reference herein in its entirety and made part hereof.

BACKGROUND

Communications between endpoints of packet-switched networks may be characterized as flows of associated packets. A particular flow may include packets containing information (e.g., within headers of the packets) that distinguishes the packets from packets associated with other flows. Network devices located between endpoints may alter packets associated with a flow and in doing so may potentially obfuscate the flow with which a particular packet is associated from other network devices. Accordingly, there is a need for correlating packets in communications networks.

SUMMARY

The following presents a simplified summary in order to provide a basic understanding of some aspects of the disclosure. It is intended neither to identify key or critical elements of the disclosure nor to delineate the scope of the disclosure. The following summary merely presents some concepts of the disclosure in a simplified form as a prelude to the description below.

Aspects of this disclosure relate to correlating packets in communications networks. In accordance with embodiments of the disclosure, a computing system may identify packets received by a network device from a host located in a first network and may generate log entries corresponding to the packets received by the network device. The computing system may identify packets transmitted by the network device to a host located in a second network and may generate log entries corresponding to the packets transmitted by the network device. Utilizing the log entries corresponding to the packets received by the network device and the log entries corresponding to the packets transmitted by the network device, the computing system may correlate the packets transmitted by the network device with the packets received by the network device.

In some embodiments, the packets received by the network device may be associated with one or more flows (e.g., distinct end-to-end communication sessions); however, the network device may alter the packets in a way that obscures their association with the flow(s) from the computing system. Correlating the packets transmitted by the network device with the packets received by the network device may enable the computing system to determine that the packets transmitted by the network device are associated with the flow(s).

BRIEF DESCRIPTION OF THE DRAWINGS

The present disclosure is pointed out with particularity in the appended claims. Features of the disclosure will become more apparent upon a review of this disclosure in its entirety, including the drawing figures provided herewith.

Some features herein are illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings, in which like reference numerals refer to similar elements, and wherein:

FIG. **1** depicts an illustrative environment for correlating packets in communications networks in accordance with one or more aspects of the disclosure;

FIGS. **2**A, **2**B, **2**C, and **2**D depict an illustrative event sequence for correlating packets in communications networks in accordance with one or more aspects of the disclosure;

FIG. **3** depicts illustrative log entries for correlating packets in communications networks in accordance with one or more aspects of the disclosure; and

FIG. **4** depicts an illustrative method for correlating packets in communications networks in accordance with one or more aspects of the disclosure.

DETAILED DESCRIPTION

In the following description of various illustrative embodiments, reference is made to the accompanying drawings, which form a part hereof, and in which is shown, by way of illustration, various embodiments in which aspects of the disclosure may be practiced. It is to be understood that other embodiments may be utilized, and structural and functional modifications may be made, without departing from the scope of the disclosure.

Various connections between elements are discussed in the following description. These connections are general and, unless specified otherwise, may be direct or indirect, wired or wireless. In this respect, the specification is not intended to be limiting.

FIG. **1** depicts an illustrative environment for correlating packets in communications networks in accordance with one or more aspects of the disclosure. Referring to FIG. **1**, environment **100** may include networks **102**, **104**, and **106**. Networks **102** and **104** may comprise one or more networks (e.g., Local Area Networks (LANs), Wide Area Networks (WANs), Virtual Private Networks (VPNs), or combinations thereof) associated with one or more individuals or entities (e.g., governments, corporations, service providers, or other organizations). Network **106** may comprise one or more networks (e.g., LANs, WANs, VPNs, or combinations thereof) that interface networks **102** and **104**. For example, network **106** may be the Internet, a similar network, or portions thereof. Networks **102** and **104** may include one or more hosts. For example, network **102** may include hosts **108**, **110**, and **112**. Similarly, network **104** may include hosts **114**, **116**, and **118**. Hosts **108**, **110**, **112**, **114**, **116**, and **118** may be one or more computing or network devices (e.g., servers, desktop computers, laptop computers, tablet computers, mobile devices, smartphones, routers, gateways, switches, access points, or the like). or a communication interface thereof. Networks **102** and **104** may include one or more network devices. For example, network **102** may include network device(s) **120**, and network **104** may include network device(s) **122**. Network device(s) **120** may include one or more devices (e.g., servers, routers, gateways, switches, access points, or the like) that interface hosts **108**, **110**, and **112** with network **106**. Similarly, network device(s) **122** may include one or more devices that interface hosts **114**, **116**, and **118** with network **106**.

Network **104** may include tap devices **124** and **126** and packet correlator **128**. Tap device **124** may be located on or have access to a communication path that interfaces network device(s) **122** and network **106**. Tap device **126** may be

Keysight, EX-1028
CENTRIPETAL-0001842

located on or have access to a communication path that interfaces network device(s) **122** and network **104** (e.g., one or more of hosts **114**, **116**, and **118**). Packet correlator **128** may comprise one or more devices and may include memory **130**, processor(s) **132**, communication interface(s) **134**, and data bus **136**. Data bus **136** may interface memory **130**, processor(s) **132**, and communication interface(s) **134**. Communication interface(s) **134** may interface packet correlator **128** with network device(s) **122** and tap devices **124** and **126**. Memory **130** may comprise program module(s) **138**, rule(s) **140**, and log(s) **142**. Program module(s) **138** may comprise instructions that when executed by processor(s) **132** cause packet correlator **128**, tap device **124**, or tap device **126** to perform one or more of the functions described herein. Rule(s) **140** may be generated by packet correlator **128** and may be configured to cause tap device(s) **124** and **126** to identify packets meeting criteria specified by rule(s) **140** and to perform one or more functions specified by rule(s) **140** on the identified packets (e.g., forward (or route) the packets toward their respective destinations, drop the packets, log information associated with or contained in the packets, copy the packets (or data contained therein), or the like). For example, tap devices **124** and **126** may comprise one or more packet-filtering devices and may be provisioned with rule(s) **140**, which may configure tap device(s) **124** and **126** to identify packets meeting criteria specified by rule(s) **140** and to communicate data associated with the identified packets to packet correlator **128** (e.g., via communication interface(s) **134**), which may utilize the data to generate one or more log entries corresponding to the identified packets in log(s) **142**.

FIGS. **2**A, **2**B, **2**C, and **2**D depict an illustrative event sequence for correlating packets in communications networks in accordance with one or more aspects of the disclosure. Referring to FIG. **2**A, at step **1**, packet correlator **128** may generate rule(s) **140**. As indicated above, rule(s) **140** may comprise criteria and may be configured to cause tap devices **124** and **126** to identify packets meeting the criteria and to perform one or more functions specified by rule(s) **140** on the identified packets. For example, rule(s) **140** may comprise criteria specifying a set of destination network addresses that includes an address associated with host **108** and may be configured to cause tap devices **124** and **126** to identify packets meeting the criteria (e.g., destined for host **108**) and to communicate data associated with the identified packets to packet correlator **128**. At step **2**, packet correlator **128** may provision tap device **124** with rule(s) **140**. At step **3**, packet correlator **128** may provision tap device **126** with rule(s) **140**.

At step **4**, host **114** may generate packets (e.g., P**1**, P**2**, and P**3**) destined for host **108** and may communicate the packets to network device(s) **122**. As indicated by the shaded box overlaying the communication of the packets and the line extending downward from tap device **126**, the packets may be routed through tap device **126**, or tap device **126** may have access to a communication path that interfaces network device(s) **122** and host **114** (e.g., tap device **126** may receive copies of or information associated with or contained in packets traversing the communication path that interfaces network device(s) **122** and host **114**). At step **5**, tap device **126** may identify the packets (e.g., P**1**, P**2**, and P**3**) by determining that the packets are destined for the network address associated with host **108** (e.g., based on network-layer information contained in their headers) and determining that the network address associated with host **108** is in the set of destination network addresses specified by the criteria included in rule(s) **140**. At step **6**, tap device **126** may generate log data associated with the packets received by network device(s) **122** from host **114** (e.g., P**1**, P**2**, and P**3**) and may communicate the log data to packet correlator **128**. As indicated by the shaded communication emanating from network device(s) **122**, the log data may include data from network device(s) **122**, which may be requested (e.g., by tap device **126**) and communicated via communication interface(s) **134**.

Packet correlator **128** may receive the log data and may utilize the log data to generate one or more entries corresponding to the packets in log(s) **142**. For example, referring to FIG. **3**, log(s) **142** may include log(s) **302** (e.g., for entries associated with packets transmitted by network device(s) **122**) and log(s) **304** (e.g., for entries associated with packets received by network device(s) **122**), and, responsive to receiving the log data from tap device **126**, packet correlator **128** may utilize the log data to generate entries **306**, **308**, and **310** (e.g., corresponding to P**1**, P**2**, and P**3**, respectively). Each of entries **306**, **308**, and **310** may include data associated with their respective corresponding packet, including, for example, network-layer information (e.g., information derived from one or more network-layer header fields of the packet, such as a protocol type, a destination network address, a source network address, a signature or authentication information (e.g., information from an Internet Protocol Security (IPsec) Encapsulating Security Payload (ESP)), or the like), transport-layer information (e.g., a destination port, a source port, a checksum or similar data (e.g., error detection or correction values, such as those utilized by the transmission control protocol (TCP) and the user datagram protocol (UDP)), or the like), application-layer information (e.g., information derived from one or more application-layer header fields of the packet, such as a domain name, a uniform resource locator (URL), a uniform resource identifier (URI), an extension, a method, state information, media-type information, a signature, a key, a timestamp, an application identifier, a session identifier, a flow identifier, sequence information, authentication information, or the like), other data in the packet (e.g., data in a payload of the packet), or one or more environmental variables (e.g., information associated with but not solely derived from the packet itself, such as an arrival time (e.g., at network device(s) **122** or tap device **126**), an ingress or egress identifier of network device(s) **122** (e.g., an identifier associated with a physical or logical network interface or port of network device(s) **122** via which the packet was received), a communication-media type of network device(s) **122**, an identifier associated with tap device **126**, or the like). For example, entries **306**, **308**, and **310** may include data indicating that P**1**, P**2**, and P**3** were received from host **114** and destined for host **108** (e.g., data derived from network- or application-layer header fields of P**1**, P**2**, and P**3**).

Packet correlator **128** may generate timestamps for each of entries **306**, **308**, and **310**. For example, packet correlator **128** may generate a timestamp for entry **306** indicating a time (e.g., T**1**) corresponding to receipt of P**1** by network device(s) **122** (e.g., a time corresponding to when network device(s) **122** received P**1**, a time corresponding to when tap device **126** identified P**1**, a time corresponding to generation of entry **306**, or the like). Similarly, packet correlator **128** may generate a timestamp for entry **308** indicating a time (e.g., T**2**) corresponding to receipt of P**2** by network device(s) **122** and generate a timestamp for entry **310** indicating a time (e.g., T**3**) corresponding to receipt of P**3** by network device(s) **122**.

Returning to FIG. **2**A, at step **7**, network device(s) **122** may generate one or more packets (e.g., P**1**', P**2**', and P**3**') corresponding to the packets received from host **114** and may communicate (or transmit) (e.g., via network **106** and network device(s) **120**) the corresponding packets (or data contained therein) to host **108**. The packets received by network device(s) **122** from host **114** (e.g., P**1**, P**2**, and P**3**) may be associated with one or more flows (e.g., distinct end-to-end communication sessions between host **114** and host **108**), and the corresponding packets generated by network device(s) **122** and communicated to host **108** (e.g., P**1**', P**2**', and P**3**') may thus also be associated with the flow(s). Network device(s) **122**, however, may include one or more devices that alter one or more aspects of the packets (e.g., a flow-transforming device) in a way that obfuscates the association of the packets received from host **114** (e.g., P**1**, P**2**, and P**3**) with the corresponding packets generated by network device(s) **122** (e.g., P**1**', P**2**', and P**3**'), at least from the perspective of devices other than network device(s) **122**.

For example, in some embodiments, network device(s) **122** may be configured to perform network address translation (NAT) for network addresses associated with network **104** (e.g., network addresses associated with hosts **114**, **116**, and **118**). In such embodiments, the packets received from host **114** (e.g., P**1**, P**2**, and P**3**) may comprise network- or transport-layer header information identifying their source as a network address associated with host **114** (e.g., a network address associated with network **104** (or a private network address)), and the corresponding packets generated by network device(s) **122** (e.g., P**1**', P**2**', and P**3**') may comprise network- or transport-layer header information identifying their source as a network address associated with network device(s) **122** (e.g., a network address associated with network **106** (or a public network address)).

Additionally or alternatively, network device(s) **122** may comprise a proxy (e.g., a web proxy, a domain name system (DNS) proxy, a session initiation protocol (SIP) proxy, or the like) configured to receive requests and generate corresponding requests. For example, the packets received by network device(s) **122** from host **114** (e.g., P**1**, P**2**, and P**3**) may comprise requests for data from host **108** configured to cause host **108** to transmit the requested data to host **114**, and the corresponding packets generated by network device(s) **122** (e.g., P**1**', P**2**', and P**3**') may comprise corresponding requests for the data from host **108** configured to cause host **108** to transmit the requested data to network device(s) **122**.

In some embodiments, network device(s) **122** may comprise a gateway (e.g., a bridge, intermediary, VPN, or tunneling gateway). For example, the packets received from host **114** (e.g., P**1**, P**2**, and P**3**) may comprise data destined for host **108**, and the corresponding packets generated by network device(s) **122** (e.g., P**1**', P**2**', and P**3**') may comprise packets that encapsulate, encrypt, or otherwise transform the packets received from host **114** (e.g., P**1**, P**2**, and P**3**) (or the data destined for host **108** included therein). For example, network device(s) **122** may comprise a tunneling gateway, and network device(s) **120** may comprise a paired tunneling gateway configured to decapsulate, decrypt, or otherwise inverse transform P**1**', P**2**', and P**3**' (or data included therein) to produce, reproduce, or replicate P**1**, P**2**, and P**3** (or the data destined for host **108** included therein). In such embodiments, there may not be a one-to-one correspondence between the packets received by network device(s) **122** and the corresponding packets generated by network device(s) **122**. For example, data associated with the encapsulation may cause network device(s) **122** to generate more corresponding packets (e.g., due to one or more protocol size constraints).

While such obfuscation may be done without malice, it may also be performed with malicious intent. For example, network device(s) **122** may be employed by a malicious entity to attempt to obfuscate, spoof, or proxy for the identity or location of host **114** (e.g., network device(s) **122** may be employed as part of a man-in-the-middle attack).

At step **8**, tap device **124** may identify the corresponding packets generated by network device(s) **122** (e.g., P**1**', P**2**', and P**3**') by determining that the packets meet the criteria included in rule(s) **140**. The criteria may include any combination of the network-layer information, transport-layer information, application-layer information, or environmental variable(s), as described above with respect to FIG. **3**. For example, tap device **124** may identify the corresponding packets generated by network device(s) **122** (e.g., P**1**', P**2**', and P**3**') by determining that the corresponding packets are destined for the network address associated with host **108** (e.g., based on network-layer information contained in their headers) and determining that the network address associated with host **108** is in the set of destination network addresses specified by the criteria included in rule(s) **140**. At step **9**, tap device **124** may generate log data associated with the corresponding packets generated by network device(s) **122** (e.g., P**1**', P**2**', and P**3**') and may communicate the log data to packet correlator **128**. As indicated by the shaded communication emanating from network device(s) **122**, the log data may include data from network device(s) **122**, which may be requested (e.g., by tap device **124**) and communicated via communication interface(s) **134**.

Packet correlator **128** may receive the log data and may utilize the log data to generate one or more entries corresponding to the packets in log(s) **142**. For example, responsive to receiving the log data from tap device **124**, packet correlator **128** may utilize the log data to generate entries **312**, **314**, and **316** (e.g., corresponding to P**1**', P**2**', and P**3**', respectively) in log(s) **302**. Each of entries **312**, **314**, and **316** may include data associated with their respective corresponding packet (e.g., network-layer information, transport-layer information, application-layer information, or environmental variable(s)). For example, entries **312**, **314**, and **316** may include data indicating that P**1**', P**2**', and P**3**' were destined for host **108** (e.g., data derived from application-layer header fields of P**1**', P**2**', and P**3**').

Packet correlator **128** may generate timestamps for each of entries **312**, **314**, and **316**. For example, packet correlator **128** may generate a timestamp for entry **312** indicating a time (e.g., T**4**) corresponding to transmission of P**1**' by network device(s) **122** (e.g., a time corresponding to when network device(s) **122** transmitted P**1**', a time corresponding to when tap device **124** identified P**1**', a time corresponding to generation of entry **312**, or the like). Similarly, packet correlator **128** may generate a timestamp for entry **314** indicating a time (e.g., T**5**) corresponding to transmission of P**2**' by network device(s) **122** and generate a timestamp for entry **316** indicating a time (e.g., T**6**) corresponding to transmission of P**3**' by network device(s) **122**.

At step **10**, host **116** may generate packets (e.g., P**4**, P**5**, and P**6**) destined for host **108** and may communicate the packets to network device(s) **122**. Referring to FIG. **2**B, at step **11**, tap device **126** may identify the packets (e.g., P**4**, P**5**, and P**6**) by determining that the packets are destined for the network address associated with host **108** (e.g., based on network-layer information contained in their headers) and determining that the network address associated with host

108 is in the set of destination network addresses specified by the criteria included in rule(s) 140. At step 12, tap device 126 may generate log data associated with the packets received by network device(s) 122 from host 116 (e.g., P4, P5, and P6) and may communicate the log data to packet correlator 128.

Packet correlator 128 may receive the log data and may utilize the log data to generate one or more entries corresponding to the packets in log(s) 142. For example, responsive to receiving the log data from tap device 126, packet correlator 128 may utilize the log data to generate entries 318, 320, and 322 (e.g., corresponding to P4, P5, and P6, respectively) in log(s) 304. Each of entries 318, 320, and 322 may include data associated with their respective corresponding packet (e.g., network-layer information, transport-layer information, application-layer information, or environmental variable(s)). For example, entries 318, 320, and 322 may include data indicating that P4, P5, and P6 were received from host 116 and destined for host 108 (e.g., data derived from application-layer header fields of P4, P5, and P6).

Packet correlator 128 may generate timestamps for each of entries 318, 320, and 322. For example, packet correlator 128 may generate a timestamp for entry 318 indicating a time (e.g., T7) corresponding to receipt of P4 by network device(s) 122 (e.g., a time corresponding to when network device(s) 122 received P4, a time corresponding to when tap device 126 identified P4, a time corresponding to generation of entry 318, or the like). Similarly, packet correlator 128 may generate a timestamp for entry 320 indicating a time (e.g., T8) corresponding to receipt of P5 by network device(s) 122 and generate a timestamp for entry 322 indicating a time (e.g., T9) corresponding to receipt of P6 by network device(s) 122.

At step 13, network device(s) 122 may generate one or more packets (e.g., P4', P5', and P6') corresponding to the packets received from host 116 and may communicate (or transmit) (e.g., via network 106 and network device(s) 120) the corresponding packets (or data contained therein) to host 108. The packets received by network device(s) 122 from host 116 (e.g., P4, P5, and P6) may be associated with one or more flows (e.g., distinct end-to-end communication sessions between host 116 and host 108), and the corresponding packets generated by network device(s) 122 and communicated to host 108 (e.g., P4', P5', and P6') may thus also be associated with the flow(s). As indicated above, however, network device(s) 122 may include one or more devices that alter one or more aspects of the packets (e.g., a device configured to perform NAT for network addresses associated with network 104, a proxy, a gateway (e.g., a VPN or tunneling gateway), or one or more other flow-transforming devices) in a way that obfuscates the association of the packets received from host 116 (e.g., P4, P5, and P6) with the corresponding packets generated by network device(s) 122 (e.g., P4', P5', and P6'), at least from the perspective of devices other than network device(s) 122.

For example, as indicated above, network device(s) 122 may be configured to perform NAT for network addresses associated with network 104. The packets received from host 116 (e.g., P4, P5, and P6) may comprise network- or transport-layer header information identifying their source as a network address associated with host 116 (e.g., a network address associated with network 104 (or a private network address)), and the corresponding packets generated by network device(s) 122 (e.g., P4', P5', and P6') may comprise network- or transport-layer header information identifying their source as a network address associated with network device(s) 122 (e.g., a network address associated with network 106 (or a public network address)).

At step 14, tap device 124 may identify the corresponding packets generated by network device(s) 122 (e.g., P4', P5', and P6') by determining that the packets meet the criteria included in rule(s) 140. For example, tap device 124 may identify the corresponding packets generated by network device(s) 122 (e.g., P4', P5', and P6') by determining that the corresponding packets are destined for the network address associated with host 108 (e.g., based on network- or transport-layer information contained in their headers) and determining that the network address associated with host 108 is in the set of destination network addresses specified by the criteria included in rule(s) 140. At step 15, tap device 124 may generate log data associated with the corresponding packets generated by network device(s) 122 (e.g., P4', P5', and P6') and may communicate the log data to packet correlator 128.

Packet correlator 128 may receive the log data and may utilize the log data to generate one or more entries corresponding to the packets in log(s) 142. For example, responsive to receiving the log data from tap device 124, packet correlator 128 may utilize the log data to generate entries 324, 326, and 328 (e.g., corresponding to P4', P5', and P6', respectively) in log(s) 302. Each of entries 324, 326, and 328 may include data associated with their respective corresponding packet (e.g., network-layer information, transport-layer information, application-layer information, or environmental variable(s)). For example, entries 324, 326, and 328 may include data indicating that P4', P5', and P6' were destined for host 108 (e.g., data derived from application-layer header fields of P4', P5', and P6').

Packet correlator 128 may generate timestamps for each of entries 324, 326, and 328. For example, packet correlator 128 may generate a timestamp for entry 324 indicating a time (e.g., T10) corresponding to transmission of P4' by network device(s) 122 (e.g., a time corresponding to when network device(s) 122 transmitted P4', a time corresponding to when tap device 124 identified P4', a time corresponding to generation of entry 324, or the like). Similarly, packet correlator 128 may generate a timestamp for entry 326 indicating a time (e.g., T11) corresponding to transmission of P5' by network device(s) 122 and generate a timestamp for entry 328 indicating a time (e.g., T12) corresponding to transmission of P6' by network device(s) 122.

At step 16, packet correlator 128 may utilize log(s) 142 to correlate the packets transmitted by network device(s) 122 with the packets received by network device(s) 122. For example, packet correlator 128 may compare data in entry 306 with data in entry 312 (e.g., network-layer information, transport-layer information, application-layer information, or environmental variable(s)) to correlate P1' with P1 (e.g., by determining that a portion of the data in entry 306 corresponds with data in entry 312). Similarly, packet correlator 128 may compare data in entry 308 with data in entry 314 to correlate P2' with P2, packet correlator 128 may compare data in entry 310 with data in entry 316 to correlate P3' with P3, packet correlator 128 may compare data in entry 318 with data in entry 324 to correlate P4' with P4, packet correlator 128 may compare data in entry 320 with data in entry 326 to correlate P5' with P5, and packet correlator 128 may compare data in entry 322 with data in entry 328 to correlate P6' with P6.

In some embodiments, packet correlator 128 may compare data in one or more entries of log(s) 142 with data in one or more other entries of log(s) 142 to determine correlation scores for each of multiple possible correlations. For

example, for each entry in log(s) **302** (or a portion thereof (e.g., a portion of the entries comprising data matching one or more criteria)), packet correlator **128** may compare data in the entry with data in each of the entries in log(s) **304** (or a portion thereof (e.g., a portion of the entries comprising data matching the one or more criteria)) to determine correlation scores corresponding to multiple possible correlations (e.g., based on the amount (e.g., percentage) of information in the data that corresponds) and may select the correlation corresponding to the correlation score indicating the strongest correlation (e.g., indicating the greatest amount of corresponding information in the data of the entries). For example, for entry **312**, packet correlator **128** may compare the data in entry **312** (e.g., network-layer information, transport-layer information, application-layer information, or environmental variable(s)) (or a portion thereof) with the data in entries **306**, **308**, and **310** (or corresponding portions thereof), may determine that the amount (e.g., percentage) of data in entry **312** that corresponds to data in entry **306** is greater than the amount of data in entry **312** that corresponds to data in entry **308** and the amount of data in entry **312** that corresponds to data in entry **310**, and, based on such a determination, may correlate P**1**' with P1.

In some embodiments, packet correlator **128** may correlate the packets transmitted by network device(s) **122** with the packets received by network device(s) **122** by comparing one or more timestamps of the entries in log(s) **142** with one or more other timestamps of the entries in log(s) **142**. For example, for each entry in log(s) **302** (or a portion thereof (e.g., a portion of the entries comprising data matching one or more criteria)), packet correlator **128** may compare the timestamp of the entry with the timestamps of the entries in log(s) **304** (or a portion thereof (e.g., a portion of the entries comprising data matching the one or more criteria)) to determine a difference between the times indicated by the timestamps and may correlate the packet corresponding to the entry in log(s) **302** with a packet corresponding to an entry in log(s) **304** having the smallest difference in time indicated by the timestamps. For example, for entry **312**, packet correlator **128** may compute a difference between T**4** and T**1**, T**2**, and T**3**, may determine that |T**4**−T**1**|<|T**4**−T**2**|<|T**4**−T**3**|, and, based on such a determination, may correlate P**1**' with P**1**.

At step **17**, host **116** may generate packets (e.g., P**7**, P**8**, and P**9**) destined for host **110** and may communicate the packets to network device(s) **122**. Tap device **126** may determine that the packets (e.g., P**7**, P**8**, and P**9**) are destined for a network address associated with host **110** (e.g., based on network-layer information contained in their headers), may determine that the network address associated with host **110** is not in the set of destination network addresses specified by the criteria included in rule(s) **140**, and, based on these determinations, may fail to generate log data associated with the packets received by network device(s) **122** from host **116** (e.g., P**7**, P**8**, and P**9**). At step **18**, network device(s) **122** may generate one or more packets (e.g., P**7**', P**8**', and P**9**') corresponding to the packets received from host **116** and may communicate (or transmit) (e.g., via network **106** and network device(s) **120**) the corresponding packets (or data contained therein) to host **110**. Tap device **124** may determine that the corresponding packets (e.g., P**7**', P**8**', and P**9**') are destined for the network address associated with host **110** (e.g., based on network-layer information contained in their headers), may determine that the network address associated with host **110** is not in the set of destination network addresses specified by the criteria included in rule(s) **140**, and, based on these determinations, may fail to generate log data associated with the packets generated by network device(s) **122** (e.g., P**7**', P**8**', and P**9**'). For example, packet correlator **128** may be configured to correlate packets destined for the network address associated with host **108** but not packets destined for the network address associated with host **110**, and rule(s) **140** may be configured to cause tap devices **124** and **126** to generate log data for packets destined for the network address associated with host **108** but not for packets destined for the network address associated with host **110** (e.g., host **108** may be associated with a malicious entity or host **110** may be associated with a trusted entity).

At step **19**, host **114** may generate packets (e.g., P**10** and P**11**) destined for host **108** and may communicate the packets to network device(s) **122**. At step **20**, tap device **126** may identify the packets (e.g., P**10** and P**11**) by determining that the packets are destined for the network address associated with host **108** (e.g., based on network-layer information contained in their headers) and determining that the network address associated with host **108** is in the set of destination network addresses specified by the criteria included in rule(s) **140**. Referring to FIG. **2**C, at step **21**, tap device **126** may generate log data associated with the packets received by network device(s) **122** from host **114** (e.g., P**10** and P**11**) and may communicate the log data to packet correlator **128**.

Packet correlator **128** may receive the log data and may utilize the log data to generate one or more entries corresponding to the packets in log(s) **142**. For example, responsive to receiving the log data from tap device **126**, packet correlator **128** may utilize the log data to generate entries **330** and **332** (e.g., corresponding to P**10** and P**11**, respectively) in log(s) **304**. Each of entries **330** and **332** may include data associated with their respective corresponding packet (e.g., network-layer information, transport-layer information, application-layer information, or environmental variable(s)). For example, entries **330** and **332** may include data indicating that P**10** and P**11** were received from host **114** and destined for host **108** (e.g., data derived from application-layer header fields of P**10** and P**11**).

Packet correlator **128** may generate timestamps for each of entries **330** and **332**. For example, packet correlator **128** may generate a timestamp for entry **330** indicating a time (e.g., T**13**) corresponding to receipt of P**10** by network device(s) **122** (e.g., a time corresponding to when network device(s) **122** received P**10**, a time corresponding to when tap device **126** identified P**10**, a time corresponding to generation of entry **330**, or the like). Similarly, packet correlator **128** may generate a timestamp for entry **332** indicating a time (e.g., T**14**) corresponding to receipt of P**11** by network device(s) **122**.

At step **22**, network device(s) **122** may generate one or more packets (e.g., P**10**' and P**11**') corresponding to the packets received from host **114** and may communicate (or transmit) (e.g., via network **106** and network device(s) **120**) the corresponding packets (or data contained therein) to host **108**. The packets received by network device(s) **122** from host **114** (e.g., P**10** and P**11**) may be associated with one or more flows (e.g., distinct end-to-end communication sessions between host **114** and host **108**), and the corresponding packets generated by network device(s) **122** and communicated to host **108** (e.g., P**10**' and P**11**') may thus also be associated with the flow(s). As indicated above, however, network device(s) **122** may include one or more devices that alter one or more aspects of the packets (e.g., a device configured to perform NAT for network addresses associated with network **104**, a proxy, a gateway (e.g., a VPN or

tunneling gateway), or one or more other flow-transforming devices) in a way that obfuscates the association of the packets received from host **114** (e.g., P**10** and P**11**) with the corresponding packets generated by network device(s) **122** (e.g., P**10'** and P**11'**), at least from the perspective of devices other than network device(s) **122**.

For example, as indicated above, network device(s) **122** may be configured to perform NAT for network addresses associated with network **104**. The packets received from host **114** (e.g., P**10** and P**11**) may comprise network-layer header information identifying their source as a network address associated with host **114** (e.g., a network address associated with network **104** (or a private network address)), and the corresponding packets generated by network device(s) **122** (e.g., P**10'** and P**11'**) may comprise network-layer header information identifying their source as a network address associated with network device(s) **122** (e.g., a network address associated with network **106** (or a public network address)).

At step **23**, tap device **124** may identify the corresponding packets generated by network device(s) **122** (e.g., P**10'** and P**11'**) by determining that the packets meet the criteria included in rule(s) **140**. For example, tap device **124** may identify the corresponding packets generated by network device(s) **122** (e.g., P**10'** and P**11'**) by determining that the corresponding packets are destined for the network address associated with host **108** (e.g., based on network-layer information contained in their headers) and determining that the network address associated with host **108** is in the set of destination network addresses specified by the criteria included in rule(s) **140**. At step **24**, tap device **124** may generate log data associated with the corresponding packets generated by network device(s) **122** (e.g., P**10'** and P**11'**) and may communicate the log data to packet correlator **128**.

Packet correlator **128** may receive the log data and may utilize the log data to generate one or more entries corresponding to the packets in log(s) **142**. For example, responsive to receiving the log data from tap device **124**, packet correlator **128** may utilize the log data to generate entries **334** and **336** (e.g., corresponding to P**10'** and P**11'**, respectively) in log(s) **302**. Each of entries **334** and **336** may include data associated with their respective corresponding packet (e.g., network-layer information, transport-layer information, application-layer information, or environmental variable(s)). For example, entries **334** and **336** may include data indicating that P**10'** and P**11'** were destined for host **108** (e.g., data derived from application-layer header fields of P**10'** and P**11'**).

Packet correlator **128** may generate timestamps for each of entries **334** and **336**. For example, packet correlator **128** may generate a timestamp for entry **334** indicating a time (e.g., T**15**) corresponding to transmission of P**10'** by network device(s) **122** (e.g., a time corresponding to when network device(s) **122** transmitted P**10'**, a time corresponding to when tap device **124** identified P**10'**, a time corresponding to generation of entry **334**, or the like). Similarly, packet correlator **128** may generate a timestamp for entry **336** indicating a time (e.g., T**16**) corresponding to transmission of P**11'** by network device(s) **122**.

At step **25**, packet correlator **128** may utilize log(s) **142** to correlate the packets transmitted by network device(s) **122** with the packets received by network device(s) **122**. For example, packet correlator **128** may compare data in entry **330** with data in entry **334** (e.g., network-layer information, transport-layer information, application-layer information, or environmental variable(s)) to correlate P**10'** with P**10** (e.g., by determining that a portion of the data in entry **330** corresponds with data in entry **334**). Similarly, packet correlator **128** may compare data in entry **332** with data in entry **336** to correlate P**11'** with P**11**. In some embodiments, packet correlator **128** may compare data from one or more requests included in the packets transmitted by network device(s) **122** with data from one or more requests included in the packets received by network device(s) **122** and may correlate one or more of the packets transmitted by network device(s) **122** with one or more of the packets received by network device(s) **122** by determining that the data from the request(s) included in the packet(s) transmitted by network device(s) **122** corresponds to the data from the request(s) included in the packet(s) received by network device(s) **122** (e.g., where network device(s) **122** include a proxy). Additionally or alternatively, packet correlator **128** may compare data encapsulated in one or more of the packets transmitted by network device(s) **122** with data from one or more of the packets received by network device(s) **122** and may correlate one or more of the packets transmitted by network device(s) **122** with one or more of the packets received by network device(s) **122** by determining that the data encapsulated in the packet(s) transmitted by network device(s) **122** corresponds to the data in the packet(s) received by network device(s) **122** (e.g., where network device(s) **122** include a gateway (e.g., a VPN or tunneling gateway)).

In some embodiments, packet correlator **128** may correlate the packets transmitted by network device(s) **122** with the packets received by network device(s) **122** by comparing one or more timestamps of the entries in log(s) **142** with one or more other timestamps of the entries in log(s) **142**. For example, packet correlator **128** may compare the timestamp of an entry in log(s) **302** with the timestamps of one or more entries in log(s) **304** (e.g., a portion of the entries comprising data matching one or more criteria)) to determine a difference between the times indicated by the timestamps and may compare the difference between the times indicated by the timestamps with a threshold latency value associated with network device(s) **122** (e.g., a predetermined value representing the time it takes for a packet to be communicated from tap device **126** to tap device **124**, an estimated maximum latency associated with a communication path spanning from tap device **126** to tap device **124** (e.g., a communication path comprising network device(s) **122**), or the like). For example, for entry **334**, packet correlator **128** may compute a difference between T**15** and T**13**, may determine that 0<T**15**−T**13**<THRESHOLD, and, based on such a determination, may correlate P**10'** with P**10**. In some embodiments, the threshold latency value may be determined based on one or more previously determined differences between timestamps of entries corresponding to previously correlated packets. For example, the threshold latency value with which the difference between T**15** and T**13** is compared may have been determined based on the differences between T**4** and T**1**, T**5** and T**2**, or T**6** and T**3**.

Responsive to correlating the packets transmitted by network device(s) **122** with the packets received by network device(s) **122**, at step **26**, packet correlator **128** may determine, based on one or more of the entries in log(s) **142**, a network address associated with a host located in network **104** that is associated with a packet transmitted by network device(s) **122**. For example, responsive to correlating P**10'** with P**10**, packet correlator **128** may determine, based on data in entry **330** (e.g., network-layer information comprising the network address associated with host **114**) that the network address associated with host **114** is associated with P**10'** (e.g., a communication with host **108**). At step **27**, packet correlator **128** may generate one or more messages

identifying host **114**. For example, host **108** may be associated with a malicious entity, packet correlator **128** may determine (e.g., based on network-layer information in entry **334**) that P**10'** was transmitted to host **108**, and the message (s) may indicate that host **114** communicated with host **108** (e.g., the malicious entity). At step **28**, packet correlator **128** may communicate one or more of the message(s) to host **114** (e.g., to notify a user of host **114** of the communication with the malicious entity), and, at step **29**, packet correlator **128** may communicate one or more of the message(s) to host **116**, which may be associated with an administrator of network **104** (e.g., to notify the administrator of the communication of host **114** with the malicious entity).

Referring to FIG. **2**D, at step **30**, packet correlator **128** may generate or update rule(s) **140** (e.g., generate one or more new rules or update one or more existing rules) to configure tap devices **124** and **126** to identify and drop packets received from host **114**. At step **31**, packet correlator **128** may provision tap device **124** with rule(s) **140**, and, at step **32**, packet correlator **128** may provision tap device **126** with rule(s) **140**. At step **33**, host **114** may communicate one or more packets (e.g., P**12**, which may be destined for host **112**, and P**13**, which may be destined for host **118**). At step **34**, tap device **126** may identify and drop the packets (e.g., P**12** and P**13**) communicated by host **114** (e.g., based on rule(s) **140** and network-layer information contained in the headers of P**12** and P**13**). For example, one or more of the communications between host **108** and **114** (e.g., P**1** and P**1'**, P**2** and P**2'**, P**3** and P**3'**, P**10** and P**10'**, or P**11** and P**11'**) may be indicative of malware installed by a computing device associated with host **108** (e.g., the malicious entity) on a computing device associated with host **114**, and rule(s) **140** may be configured to prevent the spread of the malware.

At step **35**, tap device **126** may generate log data associated with the packets communicated by host **114** (e.g., P**12** and P**13**) and may communicate the log data to packet correlator **128**, which may receive the log data and may utilize the log data to generate one or more entries corresponding to the packets in log(s) **142**. For example, responsive to receiving the log data from tap device **126**, packet correlator **128** may utilize the log data to generate entries **338** and **340** (e.g., corresponding to P**12** and P**13**, respectively) in log(s) **304**. Each of entries **338** and **340** may include data associated with their respective corresponding packet (e.g., network-layer information, transport-layer information, application-layer information, or environmental variable(s)). For example, entry **338** may include data indicating that P**12** was received from host **114** and destined for host **112** (e.g., data derived from application-layer header fields of P**12**), and entry **340** may include data indicating that P**13** was received from host **114** and destined for host **118** (e.g., data derived from application-layer header fields of P**13**). Entries **338** and **340** may indicate that tap device **126** dropped their respective corresponding packets. Packet correlator **128** may generate timestamps for each of entries **338** and **340**. For example, packet correlator **128** may generate a timestamp for entry **338** indicating a time (e.g., T**17**) corresponding to when tap device **126** identified P**12**, generation of entry **338**, or the like. Similarly, packet correlator **128** may generate a timestamp for entry **340** indicating a time (e.g., T**18**) corresponding to when tap device **126** identified P**13**, generation of entry **340**, or the like.

FIG. **4** depicts an illustrative method for correlating packets in communications networks in accordance with one or more aspects of the disclosure. Referring to FIG. **4**, at step **402**, a computing system may identify packets received by a network device from a host located in a first network. For example, tap device **126** may identify P**1**, P**2**, and P**3**. At step **404**, the computing system may generate log entries corresponding to the packets received by the network device. For example, packet correlator **128** may generate entries **306**, **308**, and **310**. At step **406**, the computing system may identify packets transmitted by the network device to a host located in a second network. For example, tap device **124** may identify P**1'**, P**2'**, and P**3'**. At step **408**, the computing system may generate log entries corresponding to the packets transmitted by the network device. For example, packet correlator **128** may generate entries **312**, **314**, and **316**. At step **410**, the computing system may correlate, based on the log entries corresponding to the packets received by the network device and the log entries corresponding to the packets transmitted by the network device, the packets transmitted by the network device with the packets received by the network device. For example, packet correlator **128** may correlate, based on entries **306**, **308**, **310**, **312**, **314**, and **316**, P**1'** with P**1**, P**2'** with P**2**. and P**3'** with P**3**.

In some embodiments, the packets received by the network device may be associated with one or more flows (e.g., distinct end-to-end communication sessions); however, the network device may alter the packets in a way that obscures their association with the flow(s) from the computing system. For example, P**1**, P**2**, and P**3** may be associated with a common flow; however, network device(s) **122** may alter P**1**, P**2**, and P**3** (e.g., by generating P**1'**, P**2'**, and P**3'**) in a way that obscures their association with the common flow from packet correlator **128**. Correlating the packets transmitted by the network device with the packets received by the network device may enable the computing system to determine that the packets transmitted by the network device are associated with the flow(s). For example, correlating P**1'** with P**1**, P**2'** with P**2**, and P**3'** with P**3** may enable packet correlator **128** to determine that P**1'**, P**2'**, and P**3'** are associated with the common flow.

The functions and steps described herein may be embodied in computer-usable data or computer-executable instructions, such as in one or more program modules, executed by one or more computers or other devices to perform one or more functions described herein. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types when executed by one or more processors in a computer or other data-processing device. The computer-executable instructions may be stored on a computer-readable medium such as a hard disk, optical disk, removable storage media, solid-state memory, RAM, etc. As will be appreciated, the functionality of the program modules may be combined or distributed as desired. In addition, the functionality may be embodied in whole or in part in firmware or hardware equivalents, such as integrated circuits, application-specific integrated circuits (ASICs), field-programmable gate arrays (FPGA), and the like. Particular data structures may be used to more effectively implement one or more aspects of the disclosure, and such data structures are contemplated to be within the scope of computer-executable instructions and computer-usable data described herein.

Although not required, one of ordinary skill in the art will appreciate that various aspects described herein may be embodied as a method, system, apparatus, or one or more computer-readable media storing computer-executable instructions. Accordingly, aspects may take the form of an entirely hardware embodiment, an entirely software embodi-

ment, an entirely firmware embodiment, or an embodiment combining software, hardware, and firmware aspects in any combination.

As described herein, the various methods and acts may be operative across one or more computing devices and networks. The functionality may be distributed in any manner or may be located in a single computing device (e.g., a server, client computer, or the like).

Aspects of the disclosure have been described in terms of illustrative embodiments thereof. Numerous other embodiments, modifications, and variations within the scope and spirit of the appended claims will occur to persons of ordinary skill in the art from a review of this disclosure. For example, one of ordinary skill in the art will appreciate that the steps illustrated in the illustrative figures may be performed in other than the recited order and that one or more illustrated steps may be optional. Any and all features in the following claims may be combined or rearranged in any way possible.

What is claimed is:

1. A method comprising:

identifying, by a computing system, a plurality of packets received by a network device from a host located in a first network;

generating, by the computing system, a plurality of log entries corresponding to the plurality of packets received by the network device;

identifying, by the computing system, a plurality of packets transmitted by the network device to a host located in a second network;

generating, by the computing system, a plurality of log entries corresponding to the plurality of packets transmitted by the network device;

correlating, by the computing system and based on the plurality of log entries corresponding to the plurality of packets received by the network device and the plurality of log entries corresponding to the plurality of packets transmitted by the network device, the plurality of packets transmitted by the network device with the plurality of packets received by the network device; and

responsive to correlating the plurality of packets transmitted by the network device with the plurality of packets received by the network device:

generating, by the computing system and based on the correlating, one or more rules configured to identify packets received from the host located in the first network; and

provisioning a packet-filtering device with the one or more rules configured to identify packets received from the host located in the first network.

2. The method of claim **1**, wherein a communication path that interfaces the network device and the first network comprises a first tap, wherein a communication path that interfaces the network device and the second network comprises a second tap, the method comprising:

provisioning, by the computing system, the first tap with one or more rules configured to identify the plurality of packets received by the network device; and

provisioning, by the computing system, the second tap with one or more rules configured to identify the plurality of packets transmitted by the network device.

3. The method of claim **1**, wherein correlating the plurality of packets transmitted by the network device with the plurality of packets received by the network device comprises comparing one or more ports indicated by the plurality of log entries corresponding to the plurality of packets received by the network device with one or more ports indicated by the plurality of log entries corresponding to the plurality of packets transmitted by the network device.

4. The method of claim **1**, wherein correlating the plurality of packets transmitted by the network device with the plurality of packets received by the network device comprises correlating one or more protocol types indicated by the plurality of log entries corresponding to the plurality of packets received by the network device with one or more protocol types indicated by the plurality of log entries corresponding to the plurality of packets transmitted by the network device.

5. The method of claim **1**, wherein correlating the plurality of packets transmitted by the network device with the plurality of packets received by the network device comprises comparing application-layer data indicated by the plurality of log entries corresponding to the plurality of packets received by the network device with application-layer data indicated by the plurality of log entries corresponding to the plurality of packets transmitted by the network device.

6. The method of claim **1**, wherein correlating the plurality of packets transmitted by the network device with the plurality of packets received by the network device comprises comparing one or more network-interface identifiers of the network device indicated by the plurality of log entries corresponding to the plurality of packets received by the network device with one or more network-interface identifiers of the network device indicated by the plurality of log entries corresponding to the plurality of packets transmitted by the network device.

7. The method of claim **1**, wherein correlating the plurality of packets transmitted by the network device with the plurality of packets received by the network device comprises comparing one or more times indicated by the plurality of log entries corresponding to the plurality of packets received by the network device with one or more times indicated by the plurality of log entries corresponding to the plurality of packets transmitted by the network device.

8. The method of claim **7**, wherein:

generating the plurality of log entries corresponding to the plurality of packets received by the network device comprises generating a plurality of timestamps indicating times corresponding to receipt, by the network device, of the plurality of packets received by the network device;

generating the plurality of log entries corresponding to the plurality of packets transmitted by the network device comprises generating a plurality of timestamps indicating times corresponding to transmission, by the network device, of the plurality of packets transmitted by the network device; and

comparing the one or more times comprises comparing one or more times indicated by the plurality of timestamps indicating times corresponding to receipt with one or more times indicated by the plurality of timestamps indicating times corresponding to transmission.

9. The method of claim **1**, comprising:

determining, by the computing system, that the host located in the second network is associated with a malicious entity; and

generating, by the computing system, one or more rules configured to cause the first network to drop packets transmitted by the host located in the first network.

10. The method of claim **1**, comprising:

generating, by the computing system, a message identifying the host located in the first network; and

communicating, by the computing system and to at least one of the host located in the first network or a computing device associated with an administrator of the first network, the message identifying the host located in the first network.

11. A system comprising:

at least one processor; and

a memory storing instructions that when executed by the at least one processor cause the system to:

identify a plurality of packets received by a network device from a host located in a first network;

generate a plurality of log entries corresponding to the plurality of packets received by the network device;

identify a plurality of packets transmitted by the network device to a host located in a second network;

generate a plurality of log entries corresponding to the plurality of packets transmitted by the network device;

correlate, based on the plurality of log entries corresponding to the plurality of packets received by the network device and the plurality of log entries corresponding to the plurality of packets transmitted by the network device, the plurality of packets transmitted by the network device with the plurality of packets received by the network device; and

responsive to correlating the plurality of packets transmitted by the network device with the plurality of packets received by the network device:

generate, based on the correlating, one or more rules configured to identify packets received from the host located in the first network; and

provision a device located in the first network with the one or more rules configured to identify packets received from the host located in the first network.

12. The system of claim **11**, wherein the instructions, when executed by the at least one processor, cause the system to:

provision a device in a communication path that interfaces the network device and the first network with one or more rules configured to identify the plurality of packets received by the network device; and

provision a device in a communication path that interfaces the network device and the second network with one or more rules configured to identify the plurality of packets transmitted by the network device.

13. The system of claim **11**, wherein the instructions, when executed by the at least one processor, cause the system to correlate the plurality of packets transmitted by the network device with the plurality of packets received by the network device based on a comparison of one or more ports indicated by the plurality of log entries corresponding to the plurality of packets received by the network device with one or more ports indicated by the plurality of log entries corresponding to the plurality of packets transmitted by the network device.

14. The system of claim **11**, wherein the instructions, when executed by the at least one processor, cause the system to correlate one or more protocol types indicated by the plurality of log entries corresponding to the plurality of packets received by the network device with one or more protocol types indicated by the plurality of log entries corresponding to the plurality of packets transmitted by the network device.

15. The system of claim **11**, wherein the instructions, when executed by the at least one processor, cause the system to correlate the plurality of packets transmitted by the network device with the plurality of packets received by the network device based on a comparison of application-layer data indicated by the plurality of log entries corresponding to the plurality of packets received by the network device with application-layer data indicated by the plurality of log entries corresponding to the plurality of packets transmitted by the network device.

16. The system of claim **11**, wherein the instructions, when executed by the at least one processor, cause the system to correlate the plurality of packets transmitted by the network device with the plurality of packets received by the network device based on a comparison of one or more network-interface identifiers of the network device indicated by the plurality of log entries corresponding to the plurality of packets received by the network device with one or more network-interface identifiers of the network device indicated by the plurality of log entries corresponding to the plurality of packets transmitted by the network device.

17. The system of claim **11**, wherein the instructions, when executed by the at least one processor, cause the system to correlate the plurality of packets transmitted by the network device with the plurality of packets received by the network device based on a comparison of one or more times indicated by the plurality of log entries corresponding to the plurality of packets received by the network device with one or more times indicated by the plurality of log entries corresponding to the plurality of packets transmitted by the network device.

18. The system of claim **11**, wherein the instructions, when executed by the at least one processor, cause the system to:

generate a plurality of timestamps indicating times corresponding to receipt, by the network device, of the plurality of packets received by the network device;

generate a plurality of timestamps indicating times corresponding to transmission, by the network device, of the plurality of packets transmitted by the network device; and

correlate the plurality of packets transmitted by the network device with the plurality of packets received by the network device based on a comparison of one or more times indicated by the plurality of timestamps indicating times corresponding to receipt with one or more times indicated by the plurality of timestamps indicating times corresponding to transmission.

19. The system of claim **11**, wherein the instructions, when executed by the at least one processor, cause the system to:

determine that the host located in the second network is associated with a malicious entity; and

generate one or more rules configured to cause the first network to drop packets transmitted by the host located in the first network.

20. The system of claim **11**, wherein the instructions, when executed by the at least one processor, cause the system to:

generate a message identifying the host located in the first network; and

communicate, to at least one of the host located in the first network or a computing device associated with an administrator of the first network, the message identifying the host located in the first network.

21. One or more non-transitory computer-readable media comprising instructions that when executed by a computing system cause the computing system to:

identify a plurality of packets received by a network device from a host located in a first network;

generate a plurality of log entries corresponding to the plurality of packets received by the network device;

identify a plurality of packets transmitted by the network device to a host located in a second network;

generate a plurality of log entries corresponding to the plurality of packets transmitted by the network device;

correlate, based on the plurality of log entries corresponding to the plurality of packets received by the network device and the plurality of log entries corresponding to the plurality of packets transmitted by the network device, the plurality of packets transmitted by the network device with the plurality of packets received by the network device; and

responsive to correlating the plurality of packets transmitted by the network device with the plurality of packets received by the network device:

generate, based on the correlating, one or more rules configured to identify packets received from the host located in the first network; and

provision a device located in the first network with the one or more rules configured to identify packets received from the host located in the first network.

22. The one or more non-transitory computer-readable media of claim **21**, wherein the instructions, when executed by the computing system, cause the computing system to:

provision a device in a communication path that interfaces the network device and the first network with one or more rules configured to identify the plurality of packets received by the network device; and

provision a device in a communication path that interfaces the network device and the second network with one or more rules configured to identify the plurality of packets transmitted by the network device.

23. The one or more non-transitory computer-readable media of claim **21**, wherein the instructions, when executed by the computing system, cause the computing system to correlate the plurality of packets transmitted by the network device with the plurality of packets received by the network device based on a comparison of one or more ports indicated by the plurality of log entries corresponding to the plurality of packets received by the network device with one or more ports indicated by the plurality of log entries corresponding to the plurality of packets transmitted by the network device.

24. The one or more non-transitory computer-readable media of claim **21**, wherein the instructions, when executed by the computing system, cause the computing system to correlate one or more protocol types indicated by the plurality of log entries corresponding to the plurality of packets received by the network device with one or more protocol types indicated by the plurality of log entries corresponding to the plurality of packets transmitted by the network device.

25. The one or more non-transitory computer-readable media of claim **21**, wherein the instructions, when executed by the computing system, cause the computing system to correlate the plurality of packets transmitted by the network device with the plurality of packets received by the network device based on a comparison of application-layer data indicated by the plurality of log entries corresponding to the plurality of packets received by the network device with application-layer data indicated by the plurality of log entries corresponding to the plurality of packets transmitted by the network device.

26. The one or more non-transitory computer-readable media of claim **21**, wherein the instructions, when executed by the computing system, cause the computing system to correlate the plurality of packets transmitted by the network device with the plurality of packets received by the network device based on a comparison of one or more network-interface identifiers of the network device indicated by the plurality of log entries corresponding to the plurality of packets received by the network device with one or more network-interface identifiers of the network device indicated by the plurality of log entries corresponding to the plurality of packets transmitted by the network device.

27. The one or more non-transitory computer-readable media of claim **21**, wherein the instructions, when executed by the computing system, cause the computing system to correlate the plurality of packets transmitted by the network device with the plurality of packets received by the network device based on a comparison of one or more times indicated by the plurality of log entries corresponding to the plurality of packets received by the network device with one or more times indicated by the plurality of log entries corresponding to the plurality of packets transmitted by the network device.

28. The one or more non-transitory computer-readable media of claim **21**, wherein the instructions, when executed by the computing system, cause the computing system to:

generate a plurality of timestamps indicating times corresponding to receipt, by the network device, of the plurality of packets received by the network device;

generate a plurality of timestamps indicating times corresponding to transmission, by the network device, of the plurality of packets transmitted by the network device; and

correlate the plurality of packets transmitted by the network device with the plurality of packets received by the network device based on a comparison of one or more times indicated by the plurality of timestamps indicating times corresponding to receipt with one or more times indicated by the plurality of timestamps indicating times corresponding to transmission.

29. The one or more non-transitory computer-readable media of claim **21**, wherein the instructions, when executed by the computing system, cause the computing system to:

determine that the host located in the second network is associated with a malicious entity; and

generate one or more rules configured to cause the first network to drop packets transmitted by the host located in the first network.

30. The one or more non-transitory computer-readable media of claim **21**, wherein the instructions, when executed by the computing system, cause the computing system to:

generate a message identifying the host located in the first network; and

communicate, to at least one of the host located in the first network or a computing device associated with an administrator of the first network, the message identifying the host located in the first network.

* * * * *

US009686193B2

(12) **United States Patent**
Moore

(10) **Patent No.: US 9,686,193 B2**
(45) **Date of Patent: Jun. 20, 2017**

(54) **FILTERING NETWORK DATA TRANSFERS**

(71) Applicant: **Centripetal Networks, Inc.**, Herndon, VA (US)

(72) Inventor: **Sean Moore**, Hollis, NH (US)

(73) Assignee: **Centripetal Networks, Inc.**, Herndon, VA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **14/625,486**

(22) Filed: **Feb. 18, 2015**

(65) **Prior Publication Data**

US 2016/0072709 A1 Mar. 10, 2016

Related U.S. Application Data

(63) Continuation of application No. 13/795,822, filed on Mar. 12, 2013, now Pat. No. 9,124,552.

(51) **Int. Cl.**

H04L 12/741	(2013.01)
H04L 29/06	(2006.01)
H04L 29/08	(2006.01)

(52) **U.S. Cl.**

CPC ***H04L 45/74*** (2013.01); ***H04L 63/0254*** (2013.01); ***H04L 63/0263*** (2013.01);
(Continued)

(58) **Field of Classification Search**

None

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,098,172 A 8/2000 Coss et al.
6,147,976 A 11/2000 Shand et al.
(Continued)

FOREIGN PATENT DOCUMENTS

AU 2005328336 B2 9/2011
AU 2006230171 B2 6/2012
(Continued)

OTHER PUBLICATIONS

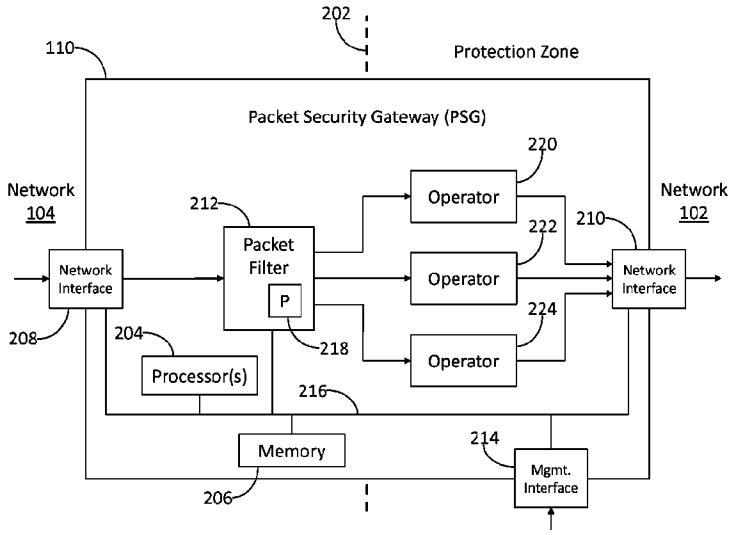
Greenwald et al., Designing an Academic Firewall: Policy, Practice, and Experience With SURF, Proceedings of SNDSS '96, IEEE, 1996, Department of Computer Science, Stanford University, Stanford, CA.
(Continued)

Primary Examiner — Anh Ngoc Nguyen
(74) *Attorney, Agent, or Firm* — Banner & Witcoff, Ltd.

(57) **ABSTRACT**

Aspects of this disclosure relate to filtering network data transfers. In some variations, multiple packets may be received. A determination may be made that a portion of the packets have packet header field values corresponding to a packet filtering rule. Responsive to such a determination, an operator specified by the packet filtering rule may be applied to the portion of packets having the packet header field values corresponding to the packet filtering rule. A further determination may be made that one or more of the portion of the packets have one or more application header field values corresponding to one or more application header field criteria specified by the operator. Responsive to such a determination, at least one packet transformation function specified by the operator may be applied to the one or more of the portion of the packets.

20 Claims, 4 Drawing Sheets



Joint Trial Exhibit
JTX-4
Case No. 18-cv-00094-HCM

(52) **U.S. Cl.**
CPC ***H04L 63/1466*** (2013.01); ***H04L 67/02*** (2013.01); ***H04L 69/22*** (2013.01)

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,226,372 B1 5/2001 Beebe et al.
6,317,837 B1 11/2001 Kenworthy
6,484,261 B1 11/2002 Wiegel
6,611,875 B1 8/2003 Chopra et al.
6,662,235 B1 12/2003 Callis et al.
7,089,581 B1 8/2006 Nagai et al.
7,107,613 B1 9/2006 Chen et al.
7,215,637 B1 5/2007 Ferguson et al.
7,227,842 B1 6/2007 Ji et al.
7,237,267 B2 6/2007 Rayes et al.
7,263,099 B1 8/2007 Woo et al.
7,299,353 B2 11/2007 Le Pennec et al.
7,331,061 B1 2/2008 Ramsey et al.
7,478,429 B2 1/2009 Lyon
7,539,186 B2 5/2009 Aerrabotu et al.
7,610,621 B2 10/2009 Turley et al.
7,684,400 B2 3/2010 Govindarajan et al.
7,710,885 B2 5/2010 Ilnicki et al.
7,721,084 B2 5/2010 Salminen et al.
7,818,794 B2 10/2010 Wittman
7,954,143 B2 5/2011 Aaron
8,004,994 B1 8/2011 Darisi et al.
3,042,167 A1 10/2011 Fulp et al.
8,037,517 B2 10/2011 Fulp et al.
8,117,655 B2 * 2/2012 Spielman H04L 12/2602 726/12
8,176,561 B1 5/2012 Hurst et al.
8,306,994 B2 11/2012 Kenworthy
8,495,725 B2 7/2013 Ahn
8,726,379 B1 5/2014 Stiansen et al.
8,806,638 B1 8/2014 Mani
8,856,926 B2 10/2014 Narayanaswamy et al.
8,935,785 B2 1/2015 Pandrangi
9,094,445 B2 7/2015 Moore et al.
9,124,552 B2 9/2015 Moore
9,137,205 B2 9/2015 Rogers et al.
9,154,446 B2 10/2015 Gemelli et al.
9,160,713 B2 10/2015 Moore
2001/0039579 A1 11/2001 Trcka et al.
2001/0039624 A1 11/2001 Kellum
2002/0016858 A1 2/2002 Sawada et al.
2002/0038339 A1 3/2002 Xu
2002/0049899 A1 4/2002 Kenworthy
2002/0164962 A1 11/2002 Mankins et al.
2002/0165949 A1 11/2002 Na et al.
2002/0186683 A1 * 12/2002 Buck H04L 63/029 370/352
2002/0198981 A1 12/2002 Corl et al.
2003/0035370 A1 2/2003 Brustoloni
2003/0097590 A1 5/2003 Syvanne
2003/0105976 A1 6/2003 Copeland
2003/0120622 A1 6/2003 Nurmela et al.
2003/0123456 A1 7/2003 Denz et al.
2003/0142681 A1 7/2003 Chen et al.
2003/0145225 A1 7/2003 Bruton. III et al.
2003/0154297 A1 8/2003 Suzuki et al.
2003/0154399 A1 8/2003 Zuk et al.
2003/0188192 A1 10/2003 Tang et al.
2003/0212900 A1 11/2003 Liu et al.
2004/0010712 A1 1/2004 Hui et al.
2004/0073655 A1 4/2004 Kan et al.
2004/0088542 A1 5/2004 Daude et al.
2004/0093513 A1 5/2004 Cantrell et al.
2004/0098511 A1 * 5/2004 Lin H04L 69/329 709/249
2004/0151155 A1 8/2004 Jouppi
2004/0177139 A1 9/2004 Schuba et al.
2004/0193943 A1 9/2004 Angelino et al.
2004/0199629 A1 10/2004 Bomer et al.
2004/0205360 A1 10/2004 Norton et al.
2004/0250124 A1 12/2004 Chesla et al.
2005/0010765 A1 1/2005 Swander et al.
2005/0024189 A1 2/2005 Weber
2005/0114704 A1 5/2005 Swander
2005/0117576 A1 6/2005 McDysan et al.
2005/0125697 A1 6/2005 Tahara
2005/0138204 A1 6/2005 Iyer et al.
2005/0138353 A1 6/2005 Spies et al.
2005/0141537 A1 6/2005 Kumar et al.
2005/0183140 A1 8/2005 Goddard
2005/0229246 A1 10/2005 Rajagopal et al.
2005/0251570 A1 11/2005 Heasman et al.
2005/0286522 A1 12/2005 Paddon et al.
2006/0048142 A1 3/2006 Roese et al.
2006/0053491 A1 3/2006 Khuti et al.
2006/0070122 A1 3/2006 Bellovin
2006/0104202 A1 5/2006 Reiner
2006/0114899 A1 6/2006 Toumura et al.
2006/0136987 A1 6/2006 Okuda
2006/0137009 A1 6/2006 Chesla
2006/0146879 A1 7/2006 Anthias et al.
2006/0195896 A1 8/2006 Fulp et al.
2006/0212572 A1 9/2006 Afek et al.
2006/0248580 A1 11/2006 Fulp et al.
2006/0262798 A1 11/2006 Joshi et al.
2007/0083924 A1 4/2007 Lu
2007/0211644 A1 9/2007 Ottamalika et al.
2007/0240208 A1 10/2007 Yu et al.
2008/0005795 A1 1/2008 Acharya et al.
2008/0043739 A1 2/2008 Suh et al.
2008/0072307 A1 3/2008 Maes
2008/0077705 A1 3/2008 Li et al.
2008/0163333 A1 7/2008 Kasralikar
2008/0229415 A1 9/2008 Kapoor et al.
2008/0235755 A1 9/2008 Blaisdell et al.
2008/0279196 A1 11/2008 Friskney et al.
2008/0301765 A1 12/2008 Nicol et al.
2009/0138938 A1 5/2009 Harrison et al.
2009/0172800 A1 7/2009 Wool
2009/0222877 A1 * 9/2009 Diehl H04L 63/1416 726/1
2009/0240698 A1 * 9/2009 Shukla G06F 17/30286
2009/0328219 A1 12/2009 Narayanaswamy
2010/0011433 A1 1/2010 Harrison et al.
2010/0011434 A1 1/2010 Kay
2010/0082811 A1 * 4/2010 Van Der Merwe G06F 17/30867 709/225
2010/0095367 A1 4/2010 Narayanaswamy
2010/0107240 A1 * 4/2010 Thaler H04L 63/20 726/15
2010/0132027 A1 5/2010 Ou
2010/0199346 A1 8/2010 Ling et al.
2010/0211678 A1 8/2010 McDysan et al.
2010/0232445 A1 * 9/2010 Bellovin H04L 45/02 370/410
2010/0242098 A1 9/2010 Kenworthy
2010/0268799 A1 10/2010 Maestas
2010/0296441 A1 11/2010 Barkan
2010/0303240 A1 12/2010 Beachem et al.
2011/0055916 A1 * 3/2011 Ahn H04L 63/0227 726/13
2011/0055923 A1 3/2011 Thomas
2011/0088092 A1 4/2011 Nguyen et al.
2011/0141900 A1 6/2011 Jayawardena et al.
2011/0185055 A1 7/2011 Nappier et al.
2011/0270956 A1 11/2011 McDysan et al.
2012/0023576 A1 1/2012 Sorensen et al.
2012/0106354 A1 5/2012 Pleshek et al.
2012/0113987 A1 5/2012 Riddoch et al.
2012/0240135 A1 9/2012 Risbood et al.
2012/0264443 A1 10/2012 Ng et al.
2012/0314617 A1 12/2012 Erichsen et al.
2012/0331543 A1 12/2012 Bostrom et al.
2013/0047020 A1 * 2/2013 Hershko H04L 67/02 713/323
2013/0059527 A1 3/2013 Hasesaka et al.
2013/0061294 A1 3/2013 Kenworthy
2013/0117852 A1 5/2013 Stute

Keysight, EX-1028
CENTRIPETAL-USCG 003291

(56) **References Cited**

U.S. PATENT DOCUMENTS

2013/0254766	A1	9/2013	Zuo et al.
2013/0305311	A1*	11/2013	Puttaswamy Naga H04L 63/0263 726/1
2014/0075510	A1	3/2014	Sonoda et al.
2014/0115654	A1	4/2014	Rogers et al.
2014/0201123	A1	7/2014	Ahn et al.
2014/0215574	A1	7/2014	Erb et al.
2014/0281030	A1	9/2014	Cui et al.
2014/0283004	A1	9/2014	Moore
2014/0283030	A1	9/2014	Moore et al.
2014/0366132	A1	12/2014	Stiansen et al.
2015/0237012	A1	8/2015	Moore
2015/0304354	A1	10/2015	Rogers et al.
2015/0334125	A1	11/2015	Bartos et al.

FOREIGN PATENT DOCUMENTS

CA	2600236	A1	10/2006
EP	1006701	A2	6/2000
EP	1313290	A1	5/2003
EP	1484884	A2	12/2004
EP	1677484	A2	7/2006
EP	2385676	A1	11/2011
EP	2498442	A1	9/2012
EP	1864226	B1	5/2013
KR	20010079361	A	8/2001
WO	2005046145	A1	5/2005
WO	2006093557	A2	9/2006
WO	2006105093	A2	10/2006
WO	2007109541	A2	9/2007
WO	2011038420	A2	3/2011
WO	2012146265	A1	11/2012

OTHER PUBLICATIONS

Reumann et al., Adaptive Packet Filters, IEEE, 2001, Department of Electrical Engineering and Computer Science, The University of Michigan, Ann Arbor, MI.

Mizuno et al., A New Remote Configurable Firewall System for Home-use Gateways, IEEE, 2004, NTT Information Sharing Platform Laboratories.

Kindervag et al., Build Security Into Your Network's DNA: The Zero Trust Network Architecture, Nov. 5, 2010, Forrester Research, Inc., Cambridge MA.

Moore, SBIR Case Study: Centripetal Networks, How CNI Leveraged DHS S&T SBIR Funding to Launch a Successful Cyber Security Company, Cyber Security Division, 2012 Principal Investigators' Meeting, Oct. 10, 2012, Centripetal Networks, Inc.

Designing a Zero Trust Network With Next-Generation Firewalls, Palo Alto Networks: Technology Brief, viewed Oct. 21, 2012, Palo Alto Networks, Santa Clara, CA.

Control Plane Policing Implementation Best Practices, Mar. 13, 2013, Cisco Systems.

International Search Report and Written Opinion for International App. No. PCT/US2013/057502, dated Nov. 7, 2013.

International Search Report and Written Opinion for International App. No. PCT/US2013/072566, dated Mar. 24, 2014.

International Search Report and Written Opinion for International App. No. PCT/US2014/023286, dated Jun. 24, 2014.

International Search Report and Written Opinion for International App. No. PCT/US2014/027723, dated Jun. 26, 2014.

International Search Report and Written Opinion for International App. No. PCT/US2015/024691, dated Sep. 16, 2015.

International Preliminary Report on Patentability for International App. No. PCT/US2013/057502, dated May 7, 2015.

International Preliminary Report on Patentability for International App. No. PCT/US2014/023286, dated Sep. 24, 2015.

International Preliminary Report on Patentability for International App. No. PCT/US2014/027723, dated Sep. 24, 2015.

Communication Relating to the Results of the Partial International Search for International App. No. PCT/US2015/024691, dated Jul. 10, 2015.

International Preliminary Report on Patentability for International App. No. PCT/US2013/072566, dated Jul. 23, 2015.

Statement RE: Related Application, dated Jul. 24, 2015.

Mizuno et al., A New Remote Configurable Firewall System for Home-use Gateways, Jan. 2005. Second IEEE Consumer Communications and Networking Conference, pp. 599-601.

John Kindervag; "Build Security Into Your Network's DNA: The Zero Trust Network Architecture", Forrester Research Inc.; Nov. 5, 2010, pp. 1-26.

Palo Alto Networks; "Designing a Zero Trust Network With Next-Generation Firewalls"; pp. 1-10; last viewed on Oct. 21, 2012.

Jan. 11, 2016—(US) Non Final Rejection—U.S. Appl. No. 14/698,560.

Apr. 27, 2011—(WO) International Search Report and Written Opinion—App PCT/US2010/054520.

Mar. 4, 2011—(US) Notice of Allowance—U.S. Appl. No. 11/316,331.

Mar. 3, 2011—(EP) Communication Pursuant to Rules 70(2) and 70a(2)—App 06758213.0.

Feb. 14, 2011—(EP) Search Report—App 06758213.0.

Fulp, Errin: "Errin Fulp," XP002618346, www.cs.wfu.edu/fulp/ewfPub.html. pp. 1-5 (Copyright 2010).

Sep. 30, 2010—(US) Office Action—U.S. Appl. No. 11/390,976.

Sep. 10, 2010—(AU) Office Action—App 2006230171.

Aug. 20, 2010—(AU) Office Action—App 2005328336.

Jun. 23, 2010—(US) Final Rejection—U.S. Appl. No. 11/316,331.

Apr. 29, 2010—(US) Interview Summary—U.S. Appl. No. 11/390,976.

Mar. 26, 2010—(US) Final Rejection—U.S. Appl. No. 11/390,976.

Sep. 14, 2009 (US) Office Action—U.S. Appl. No. 11/316,331.

Jun. 24, 2009—(US) Office Action—U.S. Appl. No. 11/390,976.

Jul. 3, 2008—(WO) Written Opinion of the International Searching Authority—App PCT/US06/11291.

Aug. 31, 2007—(EP) Communication Pursuant to Rules 109 and 110—App 05857614.1.

Acharya et al, "OPTWALL: A Hierarchical Traffic-Aware Firewall," Department of Computer Science, Telecommunications Program, University of Pittsburgh, pp. 1-11 (2007).

Sep. 11, 2006—(WO) Written Opinion of the International Searching Authority—App PCT/US05/47008.

Tarsa et al., "Balancing Trie-Based Policy representations for Network Firewalls." Department of Computer Science, Wake Forest University, pp. 1-6 (2006).

Fulp, "Trie-Based Policy Representations for Network Firewalls," Proceedings of the IEEE International Symposium on Computer Communications (2005).

E. Fulp, "Optimization of Network Firewall Policies Using Ordered Sets and Directed Acyclical Graphs", Technical Report, Computer Scient Department, Wake Forest University, Jan. 2004.

E. Fulp et al., "Network Firewall Policy Tries", Technical Report, Computer Science Department, Wake Forest University, 2004.

E. Al-Shaer et al., "Modeling and Management of Firewall Policies", IEEE Transactions on Network and Service Management, 1(1): 2004.

E.W. Fulp, "Firewall Architectures for High Speed Networks", U.S. Department of Energy Grant Application, Funded Sep. 2003.

E. Al-Shaer et al., "Firewall Policy Advisor for Anomaly Discovery and Rule Editing", Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management, 2003.

V.P. Ranganath, "A Set-Based Approach to Packet Classification", Proceedings of the IASTED International Conference on Parallel and Distributed Computing and Systems, 889-894, 2003.

M. Christiansen et al., "Using IDDsfor Packet Filtering", Technical Report, BRICS. Oct. 2002.

Lee et al., "Development Framework for Firewall Processors," IEEE, pp. 352-355 (2002).

L. Qui et al., "Fast Firewall Implementations for Software and Hardware-Based Routers", Proceedings of ACM Sigmetrics, Jun. 2001.

(56) **References Cited**

OTHER PUBLICATIONS

D. Eppstein et al., "Internet Packet Filter Management and Rectangle Geometry", Proceedings of the Symposium on Discrete Algorithms, 827-835, 2001.
E. Fulp, "Preventing Denial of Service Attacks on Quality of Service", Proceedings of the 2001 DARPA Information Survivability Conference and Exposition II, 2001.
S. Goddard et al., "An Unavailability Analysis of Firewall Sandwich Configurations", Proceedings of the 6th IEEE Symposium on High Assurance Systems Engineering, 2001.
G.V. Rooij, "Real Stateful TCP Packet Filtering in IP Filter", Proceedings of the 10th USENIX Security Symposium, 2001.
P. Warkhede et al., "Fast Packet Classification for Two-Dimensional Conflict-Free Filters", Proceedings of IEEE INFOCOM, 1434-1443, 2001.
D. Decasper et al., "Router Plugins: A Software Architecture for Next-Generation Routers", IEEE/ACM Transactions on Networking, 8(1): Feb. 2000.
A. Feldmann et al., "Tradeoffs for Packet Classification", Proceedings of the IEEE INFOCOM, 397-413, 2000.
X. Gan et al., "LSMAC vs. LSNAT: Scalable Cluster-based Web servers", Journal of Networks, Software Tools, and Applications, 3(3): 175-185, 2000.
A. Hari et al., "Detecting and Resolving Packet Filter Conflicts", Proceedings of IEEE INFOCOM, 1203-1212, 2000.
O. Paul et al., "A full Bandwidth ATM Firewall", Proceedings of the 6th European Symposium on Research in Computer Security ESORICS'2000, 2000.
J. Xu et al., "Design and Evaluation of a High-Performance ATM Firewall Switch and Its Applications", IEEE Journal on Selected Areas in Communications, 17(6): 1190-1200, Jun. 1999.
C. Benecke, "A Parallel Packet Screen for High Speed Networks", Proceedings of the 15th Annual Computer Security Applications Conference, 1999.
R. Funke et al., "Performance Evaluation of Firewalls in Gigabit-Networks", Proceedings of the Symposium on Performance Evaluation of Computer and Telecommunication Systems, 1999.
S. Suri et al., "Packet Filtering in High Speed Networks", Proceedings of the Symposium on Discrete Algorithms, 969-970, 1999.
J. Ellermann et al., "Firewalls for ATM Networks", Proceedings of INFOSEC'COM, 1998.
V. Srinivasan et al., "Fast and Scalable Layer Four Switching", Proceedings of ACM SIGCOMM, 191-202, 1998.
M. Degermark et al., "Small Forwarding Tables for Fast Routing Lookups", Proceedings of ACM SIGCOMM, 4-13, 1997.
S,M. Bellovin et al., "Network Firewalls", IEEE Communications Magazine, 50-57, 1994.
W.E. Leland et al., "On the Self-Similar Nature of Ethernet Traffic", IEEE Transactions on Networking, 2(1); 15, 1994.
G. Brightwell et al., "Counting Linear Extensions is #P-Complete", Proceedings of the Twenty-Third Annual ACM Symposium on Theory of Computing, 1991.
M. Al-Suwaiyel et al., "Algorithms for Tile Compaction", ACM Transactions on Database Systems, 9(2): 243-263, Jun. 1984.
D. Corner, "Analysis of a Heuristic for Full Tile Minimization", ACM Transactions on Database Systems, 6(3): 513-537, Sep. 1981.
R.L. Graham et al., "Optimization and Approximation in Deterministic Sequencing and Scheduling: A Survey", Annals of Discrete Mathematics, 5: 287-326, 1979.
E.L. Lawler, "Sequencing Jobs to Minimize Total Weighted Completion oTime Subject to Precedence Constraints", Annals of Discrete Mathematics, 2: 75-90, 1978.
J.K. Lenstra et al., "Complexity of Scheduling Under Precedence Constraints", Operations Research, 26(1): 22-35,1978.
R. Rivest, "On Self-Organizing Sequential Search Heuristics", Communications of the ACM, 19(2): 1976.
W.E. Smith, "Various Optimizers for Single-Stage Productions", Naval Research Logistics Quarterly, 3: 59-66, 1956.
Bellion, "High Performance Packet Classification", http://www.hipac.org (Publication Date Unknown).
Oct. 18, 2011—(EP) Communication Pursuant to Article 94(3)—App 06 758 213.0.
Jun. 9, 2011—(US) Notice of Allowance—U.S. Appl. No. 11/390,976.
Jun. 26, 2012—(EP) Extended Search Report—App 05857614.1.
Jun. 9, 2012—(AU) Notice of Acceptance—App 2006230171.
Nov. 11, 2011—(AU) Second Office Action—App 2006230171.
Jan. 17, 2013—(CA) Office Action—App 2,600,236.
Jan. 16, 2013—(CA) Office Action—App 2,594,020.
Nov. 20, 2012—(EP) Communication under rule 71(3)—App 06 758 213.0.
Apr. 18, 2013—(EP) Decision to Grant a European Patent—App 06758212.0.
Aug. 25, 2011—(US) Non Final Rejection—U.S. Appl. No. 12/871,806.
Feb. 6, 2012—(US) Final Rejection—U.S. Appl. No. 12/871,806.
Aug. 7, 2012—(US) Non Final Rejection—U.S. Appl. No. 12/871,806.
Nov. 26, 2012—(US) Final Rejection—U.S. Appl. No. 12/871,806.
Apr. 4, 2013—(US) Notice of Allowance—U.S. Appl. No. 12/871,806.
Jan. 14, 2015—(EP) Extended Search Report—App 10819667.6.
May 26, 2014—(CA) Office Action—App 2010297968.
May 25, 2015—(AU) Notice of Acceptance—App 2010297968.
May 14, 2015—(US) Non Final Rejection—U.S. Appl. No. 13/940,240.
Nov. 27, 2015—(US) Final Rejection—U.S. Appl. No. 13/940,240.
Jul. 10, 2015—(WO) Communication Relating to the Results of the Partial International Search for International App—PCT/US2015/024691.
Jul. 23, 2015—(WO) International Preliminary Report on Patentability—App PCT/US2013/072566.
Jan. 28, 2016 (WO) International Search Report and Written Opinion—App PCT/US2015/062691.
Dec. 22, 2015—(US) Final Office Action—U.S. Appl. No. 14/714,207.
Feb. 26, 2016—(US) Non Final Office Action—U.S. Appl. No. 14/253,992.
Apr. 15, 2016—(US) Notice of Allowance—U.S. Appl. No. 14/855,374.
Nov. 2, 2015—(AU) Office Action—App 2013372879.
Apr. 26, 2016—(US) Office Action—U.S. Appl. No. 14/745,207.
May 6, 2016—(US) Office Action—U.S. Appl. No. 14/714,207.
May 13, 2016—(US) Office Action—U.S. Appl. No. 13/940,240.
Feb. 25, 2016—(AU) Office Action—App 2014249055.
Feb. 24, 2016—(AU) Office Action—App 2014228257.
Jun. 9, 2016—(WO) International Search Report—PCT/US2016/026339.
Jun. 16, 2016—(CA) Office Action—App 2,888,935.
Jul. 11, 2016—(EP) Office Action—App 14720824.3.
Jul. 22, 2016—(US) Office Action—U.S. Appl. No. 14/921,718.
Jul. 20, 2016—(AU) Office Action—App 2013335255.
Oct. 5, 2016—(US) Notice of Allowance—U.S. Appl. No. 14/698,560.
Sep. 13, 2016—(CA) Office Action—App 2,902,206.
Sep. 14, 2016—(CA) Office Action—App 2,897,737.
Sep. 26, 2016—(CA) Office Action—App 2,902,158.
Oct. 26, 2016—(US) Office Action—U.S. Appl. No. 13/940,240.
Nov. 21, 2016—(US) Office Action—U.S. Appl. No. 14/745,207.
Dec. 5, 2016—(US) Notice of Allowance—U.S. Appl. No. 14/714,207.
Feb. 15, 2017—(US) Notice of Allowance—U.S. Appl. No. 14/921,718.
Apr. 12, 2017—(US) Office Action—U.S. Appl. No. 14/757,638.

* cited by examiner

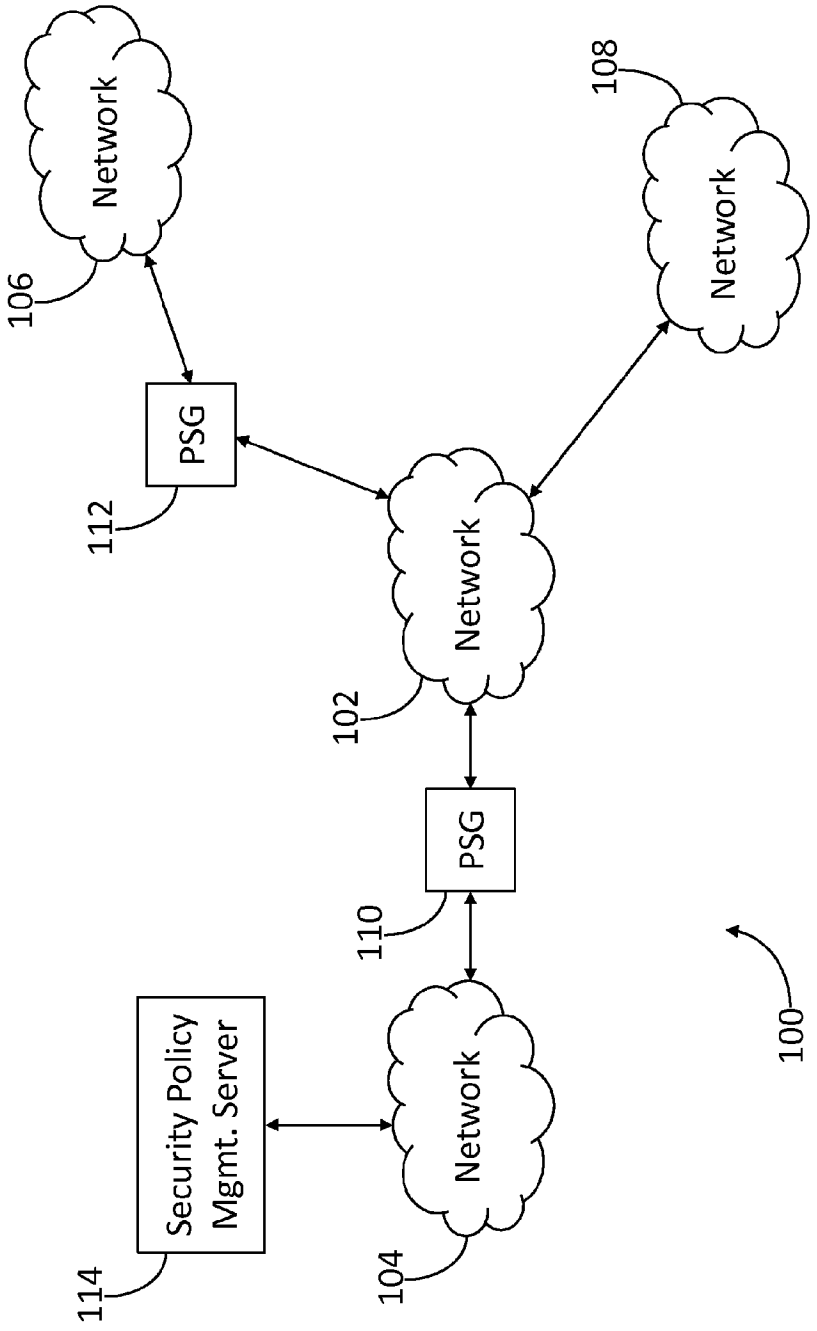

Network
106
PSG
112
Network
102
108
Network
PSG
110
Security Policy
Mgmt. Server
114
Network
104
100

FIG. 1

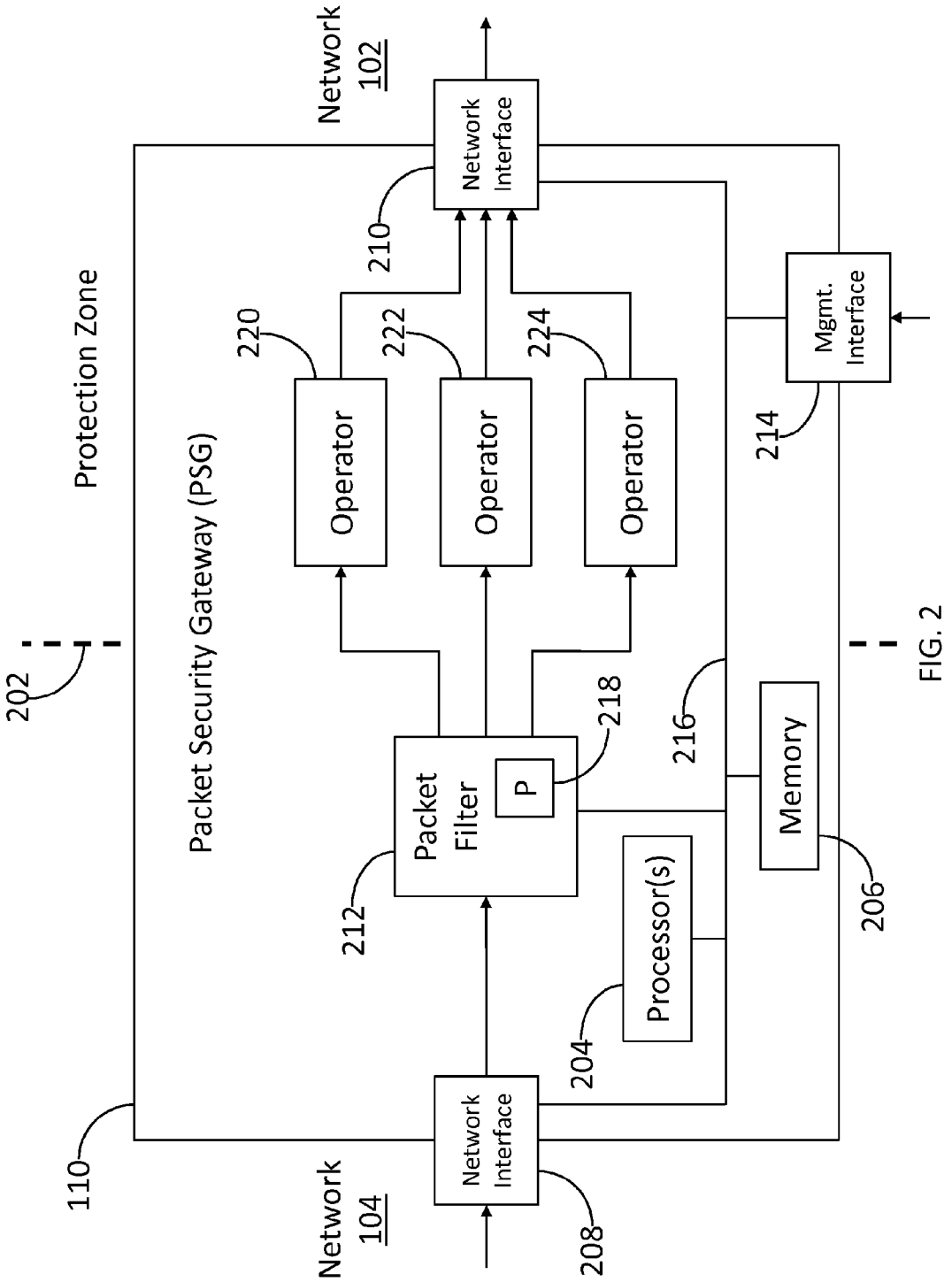
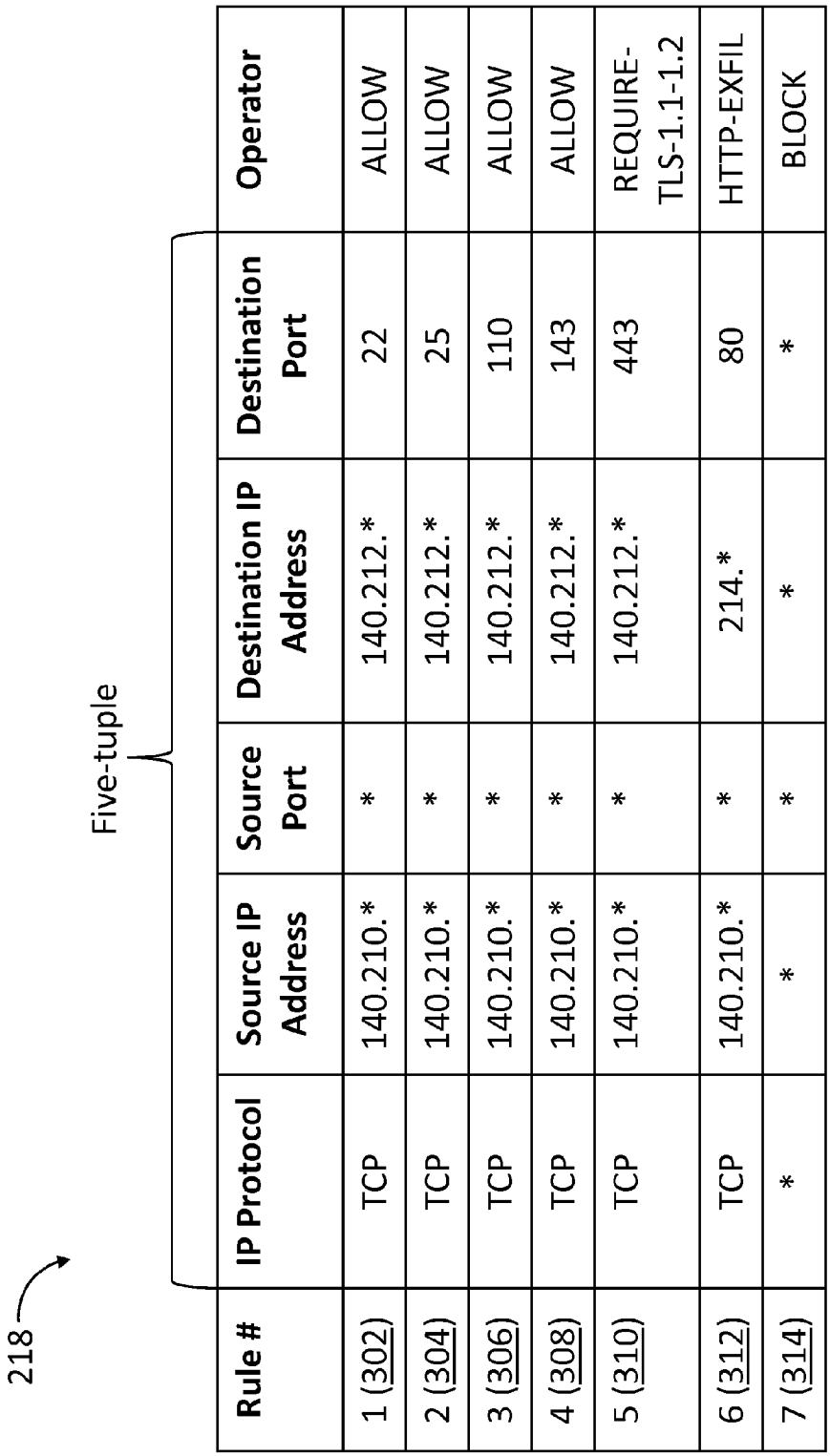

Network
102
Network Interface
210
Protection Zone
Packet Security Gateway (PSG)
220
222
224
Operator
Operator
Operator
Mgmt. Interface
214
202
218
216
Packet Filter
P
Memory
212
206
Processor(s)
204
Network Interface
110
Network
104
208

FIG. 2



Rule #	IP Protocol	Source IP Address	Source Port	Destination IP Address	Destination Port	Operator
1 (302)	TCP	140.210.*	*	140.212.*	22	ALLOW
2 (304)	TCP	140.210.*	*	140.212.*	25	ALLOW
3 (306)	TCP	140.210.*	*	140.212.*	110	ALLOW
4 (308)	TCP	140.210.*	*	140.212.*	143	ALLOW
5 (310)	TCP	140.210.*	*	140.212.*	443	REQUIRE-TLS-1.1-1.2
6 (312)	TCP	140.210.*	*	214.*	80	HTTP-EXFIL
7 (314)	*	*	*	*	*	BLOCK

FIG. 3

Keysight, EX-1028
CENTRIPETAL-SSCO 003296

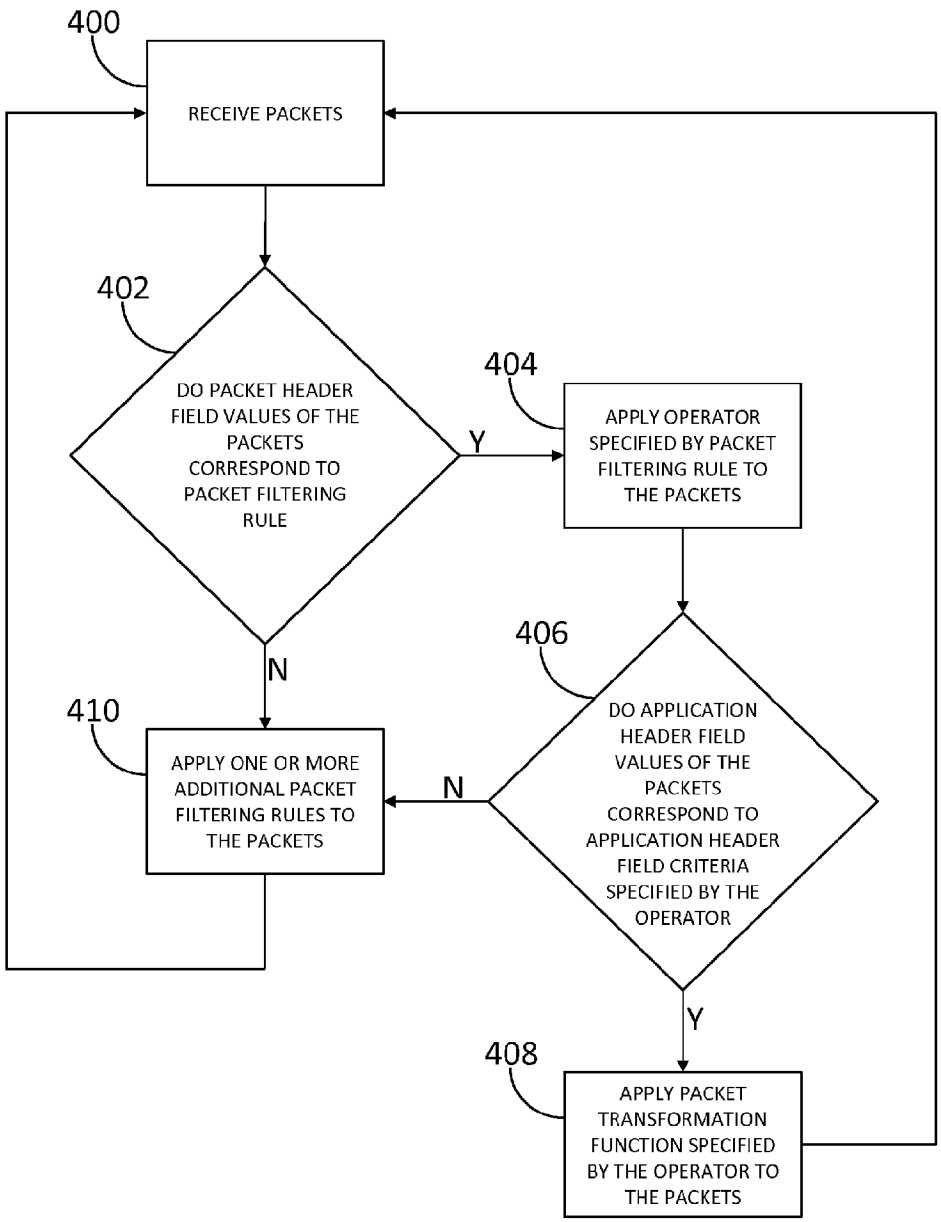


FIG. 4

Keysight, EX-1028
CENTRIPETAL-SSC-003297

FILTERING NETWORK DATA TRANSFERS

CROSS-REFERENCE TO RELATED APPLICATION

This application is a continuation of and claims priority to U.S. patent application Ser. No. 13/795,822, filed Mar. 12, 2013, and entitled "FILTERING NETWORK DATA TRANSFERS," the disclosure of which is incorporated by reference herein in its entirety and made part hereof.

BACKGROUND

The TCP/IP network protocols (e.g., the Transmission Control Protocol (TCP) and the Internet Protocol (IP)) were designed to build large, resilient, reliable, and robust networks. Such protocols, however, were not originally designed with security in mind. Subsequent developments have extended such protocols to provide for secure communication between peers (e.g., Internet Protocol Security (IPsec)), but the networks themselves remain vulnerable to attack (e.g., Distributed Denial-of-Service (DDoS) attacks, phishing attacks, and the like).

A category of cyber attack known as exfiltrations (e.g., stealing sensitive data or credentials via the Internet) has proven to be especially difficult for conventional cyber defense systems to prevent. A first cause is that many exfiltrations are facilitated by using popular network data transfer protocols, such as the Hypertext Transfer Protocol (HTTP) used by the World Wide Web, that often appear to an observer (e.g., a conventional cyber defense system) as normal network behavior. A second cause is that typical network trust models, such as those used by network firewalls, interpret exfiltrations as trusted operations. A third cause is that human users often knowingly or unknowingly engage in network activities that are vulnerable to attack. A fourth cause is the general inability of conventional cyber defense systems to scale sufficiently to counter a cyber threat; for example, with respect to traffic volumes, network link speeds, network performance (e.g., latency and packet loss requirements), network usage policy enforcement, etc. Accordingly, many cyber attacks (e.g., DDoS attacks and exfiltrations) leverage Internet-scale characteristics to achieve their goals. Moreover, beyond those enumerated here, there are other causes for the failure of conventional, state-of-the-art cyber defense systems to prevent cyber attacks, such as exfiltrations.

SUMMARY

The following presents a simplified summary in order to provide a basic understanding of some aspects of the disclosure. It is neither intended to identify key or critical elements of the disclosure nor to delineate the scope of the disclosure. The following summary merely presents some concepts in a simplified form as a prelude to the detailed description below.

Aspects of this disclosure relate to filtering network data transfers. In some variations, multiple packets may be received. A determination may be made that a portion of the packets have packet header field values corresponding to a packet filtering rule. Responsive to such a determination, an operator specified by the packet filtering rule may be applied to the portion of packets having the packet header field values corresponding to the packet filtering rule. A further determination may be made that one or more of the portion of the packets have one or more application header field values corresponding to one or more application header field criteria specified by the operator. Responsive to such a determination, at least one packet transformation function specified by the operator may be applied to the one or more of the portion of the packets.

In some embodiments, a network packet filter may be located at a boundary between a secured network and an unsecured network (e.g., the Internet). The filter may observe packets traversing the network link between the secured network and the unsecured network. The filter may be capable of comparing certain packet header information (e.g., source and destination IP address(s), source and destination port(s), and protocol type(s)) with one or more packet filtering rules, which may define a network usage policy or network security policy. One or more of the rules may be associated with an operator that may be applied to a packet that matches one or more criteria specified by the rule.

Such packet filters may implement at least two operators: an identity operator, which may allow the packet to continue towards its destination, and a null operator which may prevent, or block, the packet from continuing towards its destination. In some embodiments, the network packet filter may implement one or more additional operators having the capability to determine if a packet contains an application-level header that specifies a particular method associated with a data transfer protocol; and, if so, whether to apply an identity operator or null operator to the packet. To distinguish a network packet filter that implements said additional operators from network packet filters that do not, a network packet filter that implements such additional operators will be referred to hereinafter as a packet security gateway (PSG).

For example, such an operator may be able to perform one or more of the following functions: (1) determine if an IP packet traversing a boundary contains an HTTP packet (e.g., an application-level HTTP packet) that specifies one or more specific HTTP methods (e.g., GET, PUT, POST, etc.), and (2) allow the packet (e.g., if a GET method is specified), or block the packet (e.g., if a PUT or POST method is specified). One or more administrators of the secured network may associate such an operator with one or more rules in a network security policy in order to enforce, via the PSG, a Web usage policy that may, for example, allow users to surf (e.g., GET) to one or more web sites attached to the Internet, but may prevent such user(s) from one or more of writing (e.g., PUT) data files or posting (e.g., POST) forms to one or more web sites. For example, administrator(s) may utilize such functionality to prevent one or more exfiltrations (e.g., file transfers containing sensitive information, posting of login credentials (usernames and passwords), etc.) to network nodes (e.g., web sites) that they may not trust.

Other details and features will be described in the sections that follow.

BRIEF DESCRIPTION OF THE DRAWINGS

The present disclosure is pointed out with particularity in the appended claims. Features of the disclosure will become more apparent upon a review of this disclosure in its entirety, including the drawing figures provided herewith.

Some features herein are illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings, in which like reference numerals refer to similar elements.

Keysight, EX-1028
CENTRIPETAL-SCC 003298

FIG. **1** illustrates an exemplary network environment in which one or more aspects of the disclosure may be implemented.

FIG. **2** illustrates an exemplary packet security gateway.

FIG. **3** illustrates an exemplary dynamic security policy with operators that filter on data transfer protocol, or application-layer protocol, header information.

FIG. **4** illustrates an exemplary method for protecting a secured network by enforcing one or more network usage policies or network security policies.

DETAILED DESCRIPTION

In the following description of various illustrative embodiments, reference is made to the accompanying drawings, which form a part hereof, and in which is shown, by way of illustration, various embodiments in which aspects of the disclosure may be practiced. It is to be understood that other embodiments may be utilized, and structural and functional modifications may be made, without departing from the scope of the present disclosure.

Various connections between elements are discussed in the following description. These connections are general and, unless specified otherwise, may be direct or indirect, wired or wireless, physical or logical. In this respect, the specification is not intended to be limiting.

FIG. **1** illustrates an exemplary network environment **100** in which one or more aspects of the disclosure may be implemented. Referring to FIG. **1**, network **102** may function as an interconnect between networks **104**, **106**, and **108**. For example, network **102** may be the public Internet, or some other large TCP/IP network functioning as an interconnect between one or more Local Area Networks (LANs) or Wide-Area Networks (WANs), (e.g., the Non-classified Internet Protocol (IP) Router Network (NIPRNet), operated by the United States Defense Information Systems Agency (DISA)). Networks **104**, **106**, and **108** may be LANs or WANs operated by or otherwise associated with various organizations (e.g., one or more commercial enterprises, companies, universities, military commands, government agencies, or cyber criminal organizations).

For example, a geographically distributed commercial enterprise X may own and operate networks **104** and **106**, and use network **102** (e.g., the Internet) to interconnect networks **104** and **106**, and to access other networks (e.g., other networks not owned or operated by enterprise X) attached to network **102**. One or more computing devices (e.g., workstations, servers, etc.) of enterprise X may be attached to network **104** or **106**. Network **108** may be owned and operated by a cyber criminal organization Z, which may attempt to steal information (e.g., sensitive data) from enterprise X, for example, via network **102**. Members of organization Z may attach one or more computing devices (e.g., workstations or servers) to network **108**, and may use these workstation(s) or server(s) to attack or collect data from one or more networks affiliated with enterprise X (e.g., network **104** or **106**).

As used herein, a packet security gateway (PSG) may include one or more computing devices configured to receive packets, and apply one or more filters or operators, including an identity (e.g., allow) or null (e.g., block) operator, to the packets. In some embodiments, a packet security gateway may be configured to apply one or more additional operators as described herein. As used herein, a security policy management server may include one or more computing devices configured to communicate a dynamic security policy to a packet security gateway. In some

embodiments, a security policy management server may be configured to perform one or more additional functions as described herein. As used herein, a dynamic security policy may include one or more rules, messages, instructions, files, data structures, or the like specifying criteria corresponding to one or more packets and may identify one or more operators to be applied to packets corresponding to the specified criteria. In some embodiments, a dynamic security policy may specify one or more additional parameters as described herein.

Network environment **100** may include one or more packet security gateways and one or more security policy management servers. For example, network environment **100** may include packet security gateways **110** and **112**, and security policy management server **114**. One or more security policy management servers may be associated with a protected network. For example, networks **104** and **106** may each be distinct LANs associated with a common enterprise X, and may each form part of a protected or secured network associated with security policy management server **114**. Enterprise X may desire to prevent cyber attacks (e.g., exfiltrations) from one or more of its networks (e.g., network **104** or **106**). Accordingly, it may locate one or more packet security gateways at each boundary between its networks and one or more public interconnect networks (e.g., network **102**), which may be utilized by a cyber criminal, such as organization Z, to attempt to remotely access its networks (e.g., network **104** or **106**), and which may, for example, potentially be used to attempt to transfer data from one or more of its networks (e.g., network **104** or **106**) to one or more networks affiliated with organization Z (e.g., network **108**). For example, packet security gateway **110** may protect network **104** from one or more cyber attacks (e.g., exfiltrations) mediated by network **102** (e.g., the Internet), and packet security gateway **112** may protect network **106** from one or more cyber attacks (e.g., exfiltrations) mediated by network **102**.

As will be described in greater detail below, each of one or more packet security gateways associated with a security policy management server may be configured to receive a dynamic security policy from a security policy management server, receive packets associated with a network protected by the packet security gateway, and perform one or more operations specified by the dynamic security policy on the packets. For example, each of packet security gateways **110** and **112** may be configured to receive a dynamic security policy from security policy management server **114**. Each of packet security gateways **110** and **112** may also be configured to receive packets associated with networks **104**, **106**, or **108**. Each of packet security gateways **110** and **112** may further be configured to apply one or more rules or operators specified by the dynamic security policy received from security policy management server **114** to packets associated with networks **104**, **106**, or **108**.

FIG. **2** illustrates an exemplary packet security gateway according to one or more aspects of the disclosure. Referring to FIG. **2**, as indicated above, packet security gateway **110** may be located at network boundary **202** between networks **104** and **102**. Packet security gateway **110** may include one or more processors **204**, memory **206**, network interfaces **208** and **210**, packet filter **212**, and management interface **214**. Processor(s) **204**, memory **206**, network interfaces **208** and **210**, packet filter **212**, and management interface **214** may be interconnected via data bus **216**. Network interface **208** may connect packet security gateway **110** to network **104**. Similarly, network interface **210** may connect packet security gateway **110** to network **102**. Memory **206** may

Keysight, EX-1028
CENTRIPETAL SCC 003299

include one or more program modules that when executed by processor(s) **204**, may configure packet security gateway **110** to perform one or more of various functions described herein.

Packet security gateway **110** may be configured to receive a dynamic security policy from security policy management server **114**. For example, packet security gateway **110** may receive dynamic security policy **218** from security policy management server **114** via management interface **214** (e.g., via out-of-band signaling) or network interface **208** (e.g., via in-band signaling). Packet security gateway **110** may include one or more packet filters or packet discriminators, or logic for implementing one or more packet filters or packet discriminators. For example, packet security gateway **110** may include packet filter **212**, which may be configured to examine information associated with packets received by packet security gateway **110** and forward such packets to one or more of operators **220**, **222**, or **224** based on the examined information. For example, packet filter **212** may examine information associated with packets received by packet security gateway **110** (e.g., packets received from network **104** via network interface **208**) and forward the packets to one or more of operators **220**, **222**, or **224** based on the examined information.

As will be described in greater detail below, dynamic security policy **218** may include one or more rules and the configuration of packet filter **212** may be based on one or more of the rules included in dynamic security policy **218**. For example, dynamic security policy **218** may include one or more rules specifying that packets having specified information should be forwarded to operator **220**, that packets having different specified information should be forwarded to operator **222**, and that all other packets should be forwarded to operator **224**. Operators **220**, **222**, and **224** may be configured to perform one or more functions on packets they receive from packet filter **212**. For example, one or more of operators **220**, **222**, or **224** may be configured to forward packets received from packet filter **212** into network **102**, forward packets received from packet filter **212** to an IPsec stack (not illustrated) having an IPsec security association corresponding to the packets, or drop packets received from packet filter **212**. In some embodiments, one or more of operators **220**, **222**, or **224** may be configured to drop packets by sending the packets to a local "infinite sink" (e.g., the /dev/null device file in a UNIX/LINUX system).

FIG. **3** illustrates an exemplary dynamic security policy in accordance with one or more embodiments. Referring to FIG. **3**, dynamic security policy **218** may include rules 1 **302**, 2 **304**, 3 **306**, 4 **308**, 5 **310**, 6 **312**, and 7 **314**. Each of these rules may specify criteria and one or more operators that may be applied to packets associated with (e.g., matching) the specified criteria. The specified criteria may take the form of a five-tuple, which may, for example, comprise one or more values selected from, packet header information, specifying a protocol type of the data section of an IP packet (e.g., TCP, User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), or one or more other protocols), one or more source IP addresses, one or more source port values, one or more destination IP addresses, and one or more destination ports.

For example, rule 1 **302** may specify that IP packets containing one or more TCP packets, originating from a source IP address that begins with 140.210, having any source port, destined for an IP address that begins with 140.212, and destined for port **22** (e.g., associated with the Secure Shell (SSH) protocol) should have an ALLOW operator (e.g., an identity operator) applied to them. Similarly, rule 2 **304** may specify that IP packets containing one or more TCP packets, originating from a source IP address that begins with 140.210, having any source port, destined for an IP address that begins with 140.212, and destined for port **25** (e.g., associated with the Simple Mail Transfer Protocol (SMTP)) should have an ALLOW operator applied to them.

Rule 3 **306** may specify that IP packets containing one or more TCP packets, originating from a source IP address that begins with 140.210, having any source port, destined for an IP address that begins with 140.212, and destined for port **110** (e.g., associated with Post Office Protocol version 3 (POP3)) should have an ALLOW operator applied to them.

Rule 4 **308** may specify that IP packets containing one or more TCP packets, originating from a source IP address that begins with 140.210, having any source port, destined for an IP address that begins with 140.212, and destined for port **143** (e.g., associated with the Internet Message Access Protocol (IMAP)) should have an ALLOW operator applied to them.

Rule 5 **310** may specify that IP packets containing one or more TCP packets, originating from a source IP address that begins with 140.210, having any source port, destined for an IP address that begins with 140.212, and destined for port **443** (e.g., associated with the port for the Hypertext Transfer Protocol Secure (HTTPS) protocol) should have a specified Transport Layer Security (TLS) protocol (e.g., REQUIRE-TLS 1.1-1.2) operator (as described in greater detail below) applied to them.

Rule 7 **314** may be a "wildcard" rule and may apply a BLOCK operator (e.g., a null operator which "drops" any packets it is applied to) to any packets that do not match the criteria of any of Rules 1 **302**, 2 **304**, 3 **306**, 4 **308**, 5 **310**, or 6 **312** (e.g., when rules 1 **302**, 2 **304**, 3 **306**, 4 **308**, 5 **310**, 6 **312**, and 7 **314** are applied to packets in a linear fashion).

As described above with respect to FIG. **1**, networks **104** and **106** may be owned or operated by enterprise X. Enterprise X may have allocated IPv4 addresses 140.210.0.0/16 to network **104**, and IPv4 addresses 140.212.0.0/16 to network **106**. Enterprise X may have loaded PSG **110** with dynamic security policy **218**, and may utilize PSG **110** to enforce one or more network security policies embodied in one or more rules of dynamic security policy **218** to restrict network communications between networks **104** and **106** (e.g., to secure system logins, e-mail, encrypted web sessions, and the like). For example, based on standard usage of ports, rule 1 **302** may allow any hosts attached to network **104** to conduct Secure Shell (SSH) sessions (e.g., system logins) with any hosts attached to network **106**; rule 2 **304** may allow any e-mail servers attached to network **104** to conduct SMTP sessions (e.g., e-mail transfer sessions) with any e-mail servers attached to network **106**; rule 3 **306** and rule 4 **308**, may respectively allow e-mail clients attached to network **104** to conduct POP3 and IMAP sessions (e.g., e-mail download sessions into a webmail browser application) with any e-mail servers attached to network **106**; and rule 5 **310** may allow web browsers attached to network **104** to conduct HTTPS sessions (e.g., secure web sessions) with any web servers attached to network **106**, but may, as described in greater detail below, utilize the REQUIRE-TLS-1.1-1.2 operator to ensure that only HTTPS secure web sessions using version 1.1 or 1.2 of the Transport Layer Security (TLS) protocol to secure such HTTPS sessions are allowed (e.g., because the popular TLS version 1.0 protocol has a known security vulnerability that attackers may exploit to decrypt HTTPS sessions).

Rule 6 **312** may specify that IP packets containing one or more TCP packets, originating from a source IP address that begins with 140.210., having any source port, destined for an IP address that begins with 200.214, and destined for port **80** (e.g., associated with the HTTP protocol) should have an HTTP-EXFIL operator applied to them. As described in greater detail below, an HTTP-EXFIL operator may allow HTTP packets containing a GET method, but may block HTTP packets containing other HTTP methods (e.g., PUT, POST, CONNECT, etc.). Such an operator may thus allow a web browser to "surf the web" (e.g., download web pages hosted by web servers), but may prevent the web browser from writing files to a web server (e.g., using the PUT method), posting forms (e.g., forms that might contain login credentials, such as usernames or passwords) to a web server (e.g., using the POST method), or otherwise communicating with a web server (e.g., using any HTTP method except GET). Because attackers may often use HTTP PUT or POST methods to exfiltrate sensitive data, operators such as HTTP-EXFIL may be used to stop such exfiltrations.

Returning to the example described above, organization Z may own or operate network **108**, and may have allocated network IP addresses 214.0.0.0/8 to network **108**. Enterprise X may not have a business relationship with organization Z, and may therefore not consider network **108** to be trusted. While enterprise X could simply block all communications to networks that are owned or operated by organizations it does not fully trust, this would likely result in enterprise X blocking access to most of the Internet. Enterprise X's employees, therefore, could not freely surf the Web, which may restrict the employees' ability to conduct business on behalf of enterprise X. By enforcing sets of rules similar to rule 6 **312** that may apply operators like or similar to HTTP-EXFIL, enterprise X may enable its employees to freely surf the web and conduct company business, but may prevent one or more cyber attacks (e.g., HTTP-mediated exfiltrations).

One function of operators like HTTP-EXFIL and REQUIRE-TLS-1.1-1.2 may be to inspect fields in the headers of application packets contained in IP packets, determine field values, and depending on the field values, decide to allow, block, or otherwise apply a packet transformation function (e.g., encapsulate the packet into a tunnel, alter one or more header field values, etc.) to the packets. The logic for this function may be executed by one or more of operators **220**, **222**, or **224**. The logic may be developed in a high-level programming language such as C. An example of such programmatic logic, written in pseudocode, for the HTTP-EXFIL operator, is as follows:

```
Operator HTTP-EXFIL(ip-packet):
    Inspect app-pkt(ip-packet) match GET return ALLOW;
    Inspect app-pkt(ip-packet) match POST return BLOCK;
    Inspect app-pkt(ip-packet) match PUT return BLOCK;
    Inspect app-pkt(ip-packet) match DELETE return BLOCK;
    Inspect app-pkt(ip-packet) match CONNECT return BLOCK;
    Return BLOCK;
End Operator HTTP-EXFIL;
```

Referring to the above-example, Operator HTTP-EXFIL may accept as input an IP packet that matches a rule, such as rule 6 **312** of dynamic security policy **218**. If the application packet contained in the IP packet is an HTTP packet, the value of the HTTP method field in the HTTP packet header may be compared to the values that encode the GET, POST, PUT, DELETE, and CONNECT methods. If a match is found, then the HTTP-EXFIL operator may return either ALLOW or BLOCK, depending on the method value. If no match is found, then the HTTP-EXFIL operator may return BLOCK.

An example of programmatic logic, written in pseudocode, for a REQUIRE-TLS-1.1-1.2 operator is provided below. The REQUIRE-TLS-1.1-1.2 operator may be associated with filter rules for HTTPS sessions, such as rule 5 **310** of dynamic security policy **218**. HTTPS may be used to encrypt HTTP sessions. HTTPS is not a protocol per se, but rather the result of layering the HTTP protocol on top of the TLS protocol. For an HTTPS session composed of IP packets, the application packets contained in the IP packets may be TLS Record Protocol packets. The header fields of TLS Record Protocol packets may not be encrypted. One of the header fields may contain a value indicating the TLS version.

Exemplary programmatic logic for a REQUIRE-TLS-1.1-1.2 operator, written in pseudocode, is as follows:

```
Operator REQUIRE-TLS-1.1-1.2(ip-packet):
    Inspect app-pkt(ip-packet) match 1.0 return BLOCK;
    Inspect app-pkt(ip-packet) match 1.1 return ALLOW;
    Inspect app-pkt(ip-packet) match 1.2 return ALLOW;
    Return BLOCK;
End Operator REQUIRE-TLS-1.1-1.2;
```

Referring to the above-example, Operator REQUIRE-TLS-1.1-1.2 may accept as input an IP packet that matches a rule, such as rule 5 **310** of dynamic security policy **218**. If the application packet contained in the IP packet is a TLS Record Protocol packet, the value of the version field in the TLS Record Protocol packet header may be compared to the values that encode version numbers 1.0, 1.1, and 1.2. If a match is found, then the REQUIRE-TLS-1.1-1.2 operator may return either ALLOW or BLOCK, depending on the version number value. If no match is found, then the REQUIRE-TLS-1.1-1.2 operator may return BLOCK.

The filtering process described herein may be viewed as having two (2) stages: A first stage in which the "5-tuple" of IP packet header field values and transport protocol (e.g., TCP, UDP, etc.) packet header field values may be filtered; and, a second stage in which application packet header field values may be filtered (e.g., by applying operator logic similar to that described above). Conceptually, the first stage may determine if the network policy allows any communications between the resources identified in the 5-tuple rule; if so, the second stage may determine if the policy allows the specific method or type of communication (e.g., file read, file write, encrypted communication, etc.) between the resources. Such a method may, however, be used in other conceptual models.

The methods described above may be modified to achieve different functionality and may be extended to other data transfer protocols or to other application-layer protocols. These methods may provide network administrators with capabilities to enforce network usage policies and network security policies that have capabilities and functionalities beyond those described above. For example, these methods may provide network administrators with capabilities to prevent exfiltrations that are mediated by other data transfer protocols besides HTTP and HTTPS. Examples of such protocols include File Transfer Protocol (FTP) and messaging protocols such as eXtensible Messaging and Presence Protocol (XMPP). Moreover, new network applications may emerge in the future which may use new data transfer protocols or application-layer protocols to which the present

methods may be applied. These methods may also be used for purposes other than network policy enforcement and exfiltration prevention. For example, it may be useful for a packet filter to rapidly detect if an IP packet contains a Real-time Transport Protocol (RTP) application packet used to deliver audio or video information (e.g., if a cyber attack based on RTP has yet to be discovered, network administrators may choose to not process RTP packets through the cyber security defense systems that may be protecting their networks).

FIG. **4** illustrates an exemplary method for protecting a secured network in accordance with one or more embodiments of the present disclosure. The steps may be performed at one or more packet security gateways associated with a security policy management server. For example, each of packet security gateways **110** and **112** may be associated with security policy management server **114**, and the steps may be performed at packet security gateway **110** or **112**. At step **400**, packets may be received. For example, packet security gateway **110** may receive packets from network **104** via network interface **208** that are destined for network **106**. At step **402**, a determination may be made as to whether a portion of the received packets have packet header field values corresponding to a packet filtering rule. For example, a determination may be made as to whether a portion of the packets received from network **104** have packet header field values (e.g., one or more of one or more data section protocols, one or more source IP addresses, one or more source ports, one or more destination IP addresses, or one or more destination ports) corresponding to rule 5 **310**. At step **404**, responsive to determining that one or more of the portion of received packets have packet header field values corresponding to the packet filtering rule, an operator specified by the packet filtering rule may be applied to the portion of the received packets. For example, the REQUIRE TLS-1.1-1.2 operator specified by rule 5 **310** may be applied to the portion of the received packets.

At step **406**, a determination may be made as to whether one or more application header field values of one or more of the portion of the received packets correspond to one or more application header field criteria specified by the operator. For example, a determination may be made as to whether one or more of the portion of the received packets have application header field values corresponding to one or more application header field criteria of the REQUIRE TLS-1.1-1.2 operator specified by rule 5 **310** (e.g., application header field values corresponding to TLS version 1.1 or 1.2). At step **408**, responsive to determining that one or more of the portion of received packets have application header field values corresponding to one or more application header field criteria specified by the operator, a packet transformation function specified by the operator may be applied to the one or more of the portion of the received packets. For example, an ALLOW packet transformation function specified by the REQUIRE TLS-1.1-1.2 operator may be applied to the one or more of the portion of the received packets having application header field values corresponding to one or more application header field criteria of the REQUIRE TLS-1.1-1.2 operator specified by rule 5 **310** (e.g., each of the one or more of the portion of the received packets may be allowed to continue toward their respective destinations). The method may then return to step **400** and await receipt of one or more additional packets (e.g., one or more additional packets from network **104** received via network interface **208** that are destined for network **106**).

Returning to step **406**, a determination may be made as to whether one or more application header field values of one or more of the portion of the received packets correspond to one or more application header field criteria specified by the operator. For example, a determination may be made as to whether one or more of the portion of the received packets have application header field values corresponding to one or more application header field criteria of the REQUIRE TLS-1.1-1.2 operator specified by rule 5 **310** (e.g., application header field values corresponding to TLS version 1.1 or 1.2). Responsive to determining that one or more of the portion of received packets have application header field values that do not correspond to one or more application header field criteria specified by the operator, one or more additional packet filtering rules may be applied to the one or more of the portion of the received packets. For example, rule 7 **314** may be applied to the one or more of the portion of the received packets having application header field values that do not correspond to one or more application header field criteria of the REQUIRE TLS-1.1-1.2 operator specified by rule 5 **310** (e.g., each of the one or more of the portion of the received packets may be blocked from continuing toward their respective destinations). The method may then return to step **400** and await receipt of one or more additional packets (e.g., one or more additional packets from network **104** received via network interface **208** that are destined for network **106**).

Returning to step **402**, a determination may be made as to whether a portion of the received packets have packet header field values corresponding to a packet-filtering rule. For example, a determination may be made as to whether a portion of the packets received from network **104** have packet header field values (e.g., one or more of one or more data section protocols, one or more source IP addresses, one or more source ports, one or more destination IP addresses, or one or more destination ports) corresponding to rule 5 **310**. Responsive to determining that the portion of received packets have packet header field values that do not correspond to the packet filtering rule, one or more additional packet filtering rules may be applied to the one or more of the portion of the received packets. For example, rule 7 **314** may be applied to the portion of received packets that do not have packet header field values that correspond to rule 5 **310** (e.g., each of the portion of the received packets may be blocked from continuing toward their respective destinations). The method may then return to step **400** and await receipt of one or more additional packets (e.g., one or more additional packets from network **104** received via network interface **208** that are destined for network **106**).

The functions and steps described herein may be embodied in computer-usable data or computer-executable instructions, such as in one or more program modules, executed by one or more computers or other devices to perform one or more functions described herein. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types when executed by one or more processors in a computer or other data processing device. The computer-executable instructions may be stored on a computer-readable medium such as a hard disk, optical disk, removable storage media, solid-state memory, RAM, etc. As will be appreciated, the functionality of the program modules may be combined or distributed as desired in various embodiments. In addition, the functionality may be embodied in whole or in part in firmware or hardware equivalents, such as integrated circuits, application-specific integrated circuits (ASICs), field programmable gate arrays (FPGA), and the like. Particular data structures may be used to more effectively implement one or more aspects of the disclosure,

and such data structures are contemplated to be within the scope of computer executable instructions and computer-usable data described herein.

Although not required, one of ordinary skill in the art will appreciate that various aspects described herein may be embodied as a method, an apparatus, or as one or more computer-readable media storing computer-executable instructions. Accordingly, those aspects may take the form of an entirely hardware embodiment, an entirely software embodiment, an entirely firmware embodiment, or an embodiment combining software, hardware, and firmware aspects in any combination.

As described herein, the various methods and acts may be operative across one or more computing devices and one or more networks. The functionality may be distributed in any manner, or may be located in a single computing device (e.g., a server, a client computer, etc.).

Aspects of the disclosure have been described in terms of illustrative embodiments thereof. Numerous other embodiments, modifications, and variations within the scope and spirit of the appended claims will occur to persons of ordinary skill in the art from a review of this disclosure. For example, one of ordinary skill in the art will appreciate that the steps illustrated in the illustrative figures may be performed in other than the recited order, and that one or more steps illustrated may be optional.

What is claimed is:

1. A method comprising:

receiving, by a computing system and from a computing device located in a first network, a plurality of packets, wherein the plurality of packets comprises a first portion of packets and a second portion of packets;

responsive to a determination by the computing system that the first portion of packets comprises data corresponding to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network, wherein the data indicates that the first portion of packets is destined for the second network:

applying, by the computing system and to each packet in the first portion of packets, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and

dropping, by the computing system, each packet in first portion of packets; and

responsive to a determination by the computing system that the second portion of packets comprises data that does not correspond to the criteria wherein the data indicates that the second portion of packets is destined for a third network:

applying, by the computing system and to each packet in the second portion of packets, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, a second operator configured to forward packets not associated with the particular type of data transfer toward the third network; and

forwarding, by the computing system, each packet in the second portion of packets toward the third network.

2. The method of claim **1**, wherein

the first portion of packets comprises data indicating: a protocol type associated with the particular type of data transfer, and corresponding to the criteria specified by the one or more packet-filtering rules; and

the second portion of packets comprises data indicating a protocol type not associated with the particular type of data transfer.

3. The method of claim **1**, wherein:

the first portion of packets comprises data indicating a first destination port number associated with the particular type of data transfer, and corresponding to the criteria specified by the one or more packet-filtering rules; and

the second portion of packets comprises data indicating a second destination port number not associated with the particular type of data transfer.

4. The method of claim **1**, wherein:

the first portion of packets comprises data associated with hypertext transfer protocol (HTTP), and corresponding to the criteria specified by the one or more packet-filtering rules; and

the second portion of packets does not comprise data associated with HTTP.

5. The method of claim **1**, wherein:

the first portion of packets comprises data associated with hypertext transfer protocol secure (HTTPS), and corresponding to the criteria specified by the one or more packet-filtering rules; and

the second portion of packets does not comprise data associated with HTTPS.

6. The method of claim **1**, wherein:

the first portion of packets comprises data associated with file transfer protocol (FTP), and corresponding to the criteria specified by the one or more packet-filtering rules; and

the second portion of packets does not comprise data associated with FTP.

7. The method of claim **1**, wherein:

the first portion of packets comprises data associated with real-time transport protocol (RTP), and corresponding to the criteria specified by the one or more packet-filtering rules; and

the second portion of packets does not comprise data associated with RTP.

8. A method comprising:

receiving, by a computing system and from a computing device located in a first network, a plurality of packets;

responsive to a determination by the computing system that a first packet of the plurality of packets comprises data associated with eXtensible messaging and presence protocol (XMPP) and the data corresponds to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network;

applying, by the computing system and to the first packet, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and

dropping, by the computing system, the first packet; and

responsive to a determination by the computing system that a second packet of the plurality of packets does not comprise data associated with XMPP:

applying, by the computing system, to the second packet, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, a second operator configured to forward packets not associated with the particular type of data transfer toward the second network; and

forwarding, by the computing system, the second packet toward the second network.

9. The method of claim **1**, wherein:

receiving the plurality of packets comprises receiving packets comprising data associated with hypertext transfer protocol (HTTP);

the first portion of packets comprises a first type of data associated with HTTP;

the second portion of packets comprises a second type of data associated with HTTP; and

applying the first operator configured to drop packets associated with the particular type of data transfer is performed responsive to a determination by the computing system that the first portion of packets comprises the first type of data.

10. The method of claim **9**, wherein applying the first operator configured to drop packets associated with the particular type of data transfer is performed responsive to a determination by the computing system that the first portion of packets comprises data corresponding to an HTTP POST method.

11. The method of claim **9**, wherein applying the first operator configured to drop packets associated with the particular type of data transfer is performed responsive to a determination by the computing system that the first portion of packets comprises data corresponding to an HTTP PUT method.

12. The method of claim **9**, wherein applying the first operator configured to drop packets associated with the particular type of data transfer is performed responsive to a determination by the computing system that the first portion of packets comprises data corresponding to an HTTP DELETE method.

13. The method of claim **9**, wherein applying the first operator configured to drop packets associated with the particular type of data transfer is performed responsive to a determination by the computing system that the first portion of packets comprises data corresponding to an HTTP CONNECT method.

14. The method of claim **9**, wherein applying the first operator configured to forward packets not associated with the particular type of data transfer toward the second network is performed responsive to a determination by the computing system that the second portion of packets comprises the second type of data.

15. The method of claim **9**, wherein applying the first operator configured to forward packets not associated with the particular type of data transfer toward the second network is performed responsive to a determination by the computing system that the second portion of packets comprises data corresponding to an HTTP GET method.

16. The method of claim **1**, wherein applying the first operator configured to drop packets associated with the particular type of data transfer is performed responsive to a determination by the computing system that the first portion of packets comprises data corresponding to a particular transport layer security (TLS) version value.

17. The method of claim **1**, wherein applying the first operator configured to forward packets not associated with the particular type of data transfer toward the second network is performed responsive to a determination by the computing system that the second portion of packets comprises data corresponding to a particular transport layer security (TLS) version value.

18. A system comprising:

at least one processor; and

a memory storing instructions that when executed by the at least one processor cause the system to:

receive, from a computing device located in a first network, a plurality of packets wherein the plurality of packets comprises a first portion of packets and a second portion of packets;

responsive to a determination that the first portion of packets comprises data corresponding to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network, wherein the data indicates that the first portion of packets is destined for the second network:

apply, to each packet in the first portion of packets, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and

drop each packet in the first portion of packets; and

responsive to a determination that the second portion of packets comprises data that does not correspond to the criteria, wherein the data indicates that the second portion of packets is destined for a third network:

apply, to each packet in the second portion of packets, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, a second operator configured to forward packets not associated with the particular type of data transfer toward the third network; and

forward each packet in the second portion of packets toward the third network.

19. One or more non-transitory computer-readable media comprising instructions that when executed by one or more computing devices cause the one or more computing devices to:

receive, from a computing device located in a first network, a plurality of packets wherein the plurality of packets comprises a first portion of packets and a second portion of packets;

responsive to a determination that the first portion of packets comprises data corresponding to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network, wherein the data indicates that the first portion of packets is destined for the second network:

apply, to each packet in the first portion of packets, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and

drop each packet in the first portion of packets; and

responsive to a determination that the second portion of packets comprises data that does not correspond to the criteria, wherein the data indicates that the second portion of packets is destined for a third network:

apply, to each packet in the second portion of packets, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, a second operator, configured to forward packets not associated with the particular type of data transfer toward the third network; and

forward each packet in the second portion of packets toward the third network.

20. The method of claim **1**, wherein:

the first portion of packets comprises data indicating: a first source port number associated with the particular type of data transfer, and corresponding to the criteria specified by the one or more packet-filtering rules; and

the second portion of packets comprises data indicating a second source port number not associated with the particular type of data transfer.

* * * * *

US009917856B2

(12) **United States Patent**
Ahn et al.

(10) **Patent No.: US 9,917,856 B2**
(45) **Date of Patent: Mar. 13, 2018**

(54) **RULE-BASED NETWORK-THREAT DETECTION FOR ENCRYPTED COMMUNICATIONS**

(71) Applicant: **Centripetal Networks, Inc.**, Herndon, VA (US)

(72) Inventors: **David K. Ahn**, Winston-Salem, NC (US); **Sean Moore**, Hollis, NH (US); **Douglas M. DiSabello**, Leesburg, VA (US)

(73) Assignee: **Centripetal Networks, Inc.**, Portsmouth, NH (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **14/757,638**

(22) Filed: **Dec. 23, 2015**

(65) **Prior Publication Data**

US 2017/0187733 A1 Jun. 29, 2017

(51) **Int. Cl.**
H04L 29/06 (2006.01)
H04L 29/12 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/1425*** (2013.01); ***H04L 61/1511*** (2013.01); ***H04L 63/0263*** (2013.01); ***H04L 63/0281*** (2013.01); ***H04L 63/1416*** (2013.01); ***H04L 63/20*** (2013.01); ***H04L 69/22*** (2013.01)

(58) **Field of Classification Search**
USPC 713/153
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,098,172	A	8/2000	Coss et al.
6,147,976	A	11/2000	Shand et al.
6,226,372	B1	5/2001	Beebe et al.
6,317,837	B1	11/2001	Kenworthy
6,484,261	B1	11/2002	Wiegel
6,611,875	B1	8/2003	Chopra et al.
6,662,235	B1	12/2003	Callis et al.
7,089,581	B1	8/2006	Nagai et al.

(Continued)

FOREIGN PATENT DOCUMENTS

AU	2005328336 B2	9/2011
AU	2006230171 B2	6/2012

(Continued)

OTHER PUBLICATIONS

Apr. 15, 2016—(US) Notice of Allowance—U.S. Appl. No. 14/855,374.

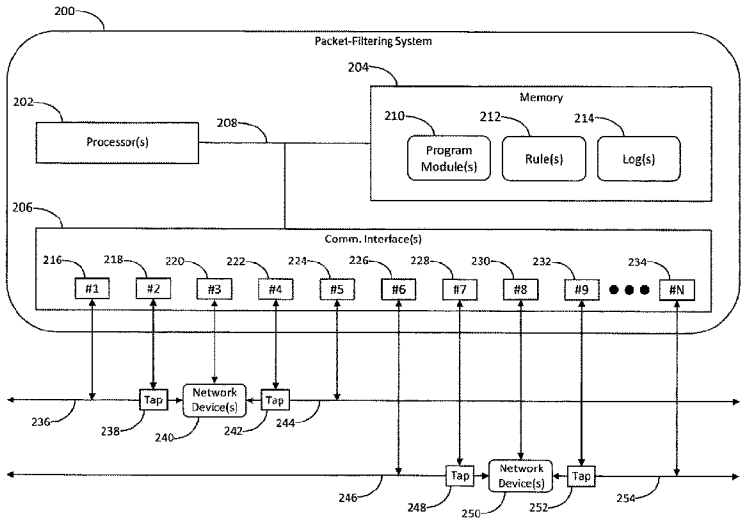
(Continued)

Primary Examiner — Jason Lee
(74) *Attorney, Agent, or Firm* — Banner & Witcoff, Ltd.

(57) **ABSTRACT**

A packet-filtering system configured to filter packets in accordance with packet-filtering rules may receive data indicating network-threat indicators and may configure the packet-filtering rules to cause the packet-filtering system to identify packets comprising unencrypted data, and packets comprising encrypted data. A portion of the unencrypted data may correspond to one or more of the network-threat indicators, and the packet-filtering rules may be configured to cause the packet-filtering system to determine, based on the portion of the unencrypted data, that the packets comprising encrypted data correspond to the one or more network-threat indicators.

25 Claims, 13 Drawing Sheets



Joint Trial Exhibit
JTX-5
Case No. 18-cv-00094-HCM

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,107,613 B1 9/2006 Chen et al.
7,215,637 B1 5/2007 Ferguson et al.
7,227,842 B1 6/2007 Ji et al.
7,237,267 B2 6/2007 Rayes et al.
7,263,099 B1 8/2007 Woo et al.
7,299,353 B2 11/2007 Le Pennec et al.
7,331,061 B1 2/2008 Ramsey et al.
7,478,429 B2 1/2009 Lyon
7,539,186 B2 5/2009 Aerrabotu et al.
7,610,621 B2 10/2009 Turley et al.
7,684,400 B2 3/2010 Govindarajan et al.
7,710,885 B2 5/2010 Ilnicki et al.
7,721,084 B2 5/2010 Salminen et al.
7,818,794 B2 10/2010 Wittman
7,954,143 B2 5/2011 Aaron
8,004,994 B1 8/2011 Darisi et al.
8,037,517 B2 10/2011 Fulp et al.
8,042,167 B2 10/2011 Fulp et al.
8,117,655 B2 2/2012 Spielman
8,176,561 B1 5/2012 Hurst et al.
8,306,994 B2 11/2012 Kenworthy
8,495,725 B2 7/2013 Ahn
8,726,379 B1 5/2014 Stiansen et al.
8,806,638 B1 8/2014 Mani
8,856,926 B2 10/2014 Narayanaswamy et al.
8,935,785 B2 1/2015 Pandrangi
9,094,445 B2 7/2015 Moore et al.
9,124,552 B2 9/2015 Moore
9,137,205 B2 9/2015 Rogers et al.
9,154,446 B2 10/2015 Gemelli et al.
9,160,713 B2 10/2015 Moore
2001/0039579 A1 11/2001 Trcka et al.
2001/0039624 A1 11/2001 Kellum
2002/0016858 A1 2/2002 Sawada et al.
2002/0038339 A1 3/2002 Xu
2002/0049899 A1 4/2002 Kenworthy
2002/0164962 A1 11/2002 Mankins et al.
2002/0165949 A1 11/2002 Na et al.
2002/0186683 A1 12/2002 Buck et al.
2002/0198981 A1 12/2002 Corl et al.
2003/0035370 A1 2/2003 Brustoloni
2003/0097590 A1 5/2003 Syvanne
2003/0105976 A1 6/2003 Copeland
2003/0120622 A1 6/2003 Nurmela et al.
2003/0123456 A1 7/2003 Denz et al.
2003/0142681 A1 7/2003 Chen et al.
2003/0145225 A1 7/2003 Bruton et al.
2003/0154297 A1 8/2003 Suzuki et al.
2003/0154399 A1 8/2003 Zuk et al.
2003/0188192 A1 10/2003 Tang et al.
2003/0212900 A1 11/2003 Liu et al.
2004/0010712 A1 1/2004 Hui et al.
2004/0073655 A1 4/2004 Kan et al.
2004/0088542 A1 5/2004 Daude et al.
2004/0093513 A1 5/2004 Cantrell et al.
2004/0098511 A1 5/2004 Lin et al.
2004/0151155 A1 8/2004 Jouppi
2004/0177139 A1 9/2004 Schuba et al.
2004/0193943 A1 9/2004 Angelino et al.
2004/0199629 A1* 10/2004 Bomer G06F 11/362 709/224
2004/0205360 A1 10/2004 Norton et al.
2004/0250124 A1 12/2004 Chesla et al.
2005/0010765 A1 1/2005 Swander et al.
2005/0024189 A1 2/2005 Weber
2005/0108557 A1 5/2005 Kayo et al.
2005/0114704 A1 5/2005 Swander
2005/0117576 A1 6/2005 McDysan et al.
2005/0125697 A1 6/2005 Tahara
2005/0138204 A1 6/2005 Iyer et al.
2005/0138353 A1* 6/2005 Spies H04L 63/0442 713/153
2005/0141537 A1 6/2005 Kumar et al.
2005/0183140 A1 8/2005 Goddard
2005/0229246 A1 10/2005 Rajagopal et al.
2005/0251570 A1 11/2005 Heasman et al.
2005/0286522 A1 12/2005 Paddon et al.
2006/0048142 A1 3/2006 Roese et al.
2006/0053491 A1 3/2006 Khuti et al.
2006/0070122 A1 3/2006 Bellovin
2006/0104202 A1 5/2006 Reiner
2006/0114899 A1 6/2006 Toumura et al.
2006/0136987 A1 6/2006 Okuda
2006/0137009 A1 6/2006 Chesla
2006/0146879 A1 7/2006 Anthias et al.
2006/0195896 A1 8/2006 Fulp et al.
2006/0212572 A1 9/2006 Afek et al.
2006/0248580 A1 11/2006 Fulp et al.
2006/0262798 A1 11/2006 Joshi et al.
2007/0083924 A1 4/2007 Lu
2007/0211644 A1 9/2007 Ottamalika et al.
2007/0240208 A1 10/2007 Yu et al.
2008/0005795 A1 1/2008 Acharya et al.
2008/0043739 A1 2/2008 Suh et al.
2008/0072307 A1 3/2008 Maes
2008/0077705 A1 3/2008 Li et al.
2008/0163333 A1 7/2008 Kasralikar
2008/0229415 A1 9/2008 Kapoor et al.
2008/0235755 A1 9/2008 Blaisdell et al.
2008/0279196 A1 11/2008 Friskney et al.
2008/0301765 A1 12/2008 Nicol et al.
2009/0138938 A1 5/2009 Harrison et al.
2009/0172800 A1 7/2009 Wool
2009/0222877 A1 9/2009 Diehl et al.
2009/0240698 A1 9/2009 Shukla et al.
2009/0328219 A1 12/2009 Narayanaswamy
2010/0011433 A1 1/2010 Harrison et al.
2010/0011434 A1 1/2010 Kay
2010/0082811 A1 4/2010 Van Der Merwe et al.
2010/0095367 A1 4/2010 Narayanaswamy
2010/0107240 A1 4/2010 Thaler et al.
2010/0132027 A1 5/2010 Ou
2010/0199346 A1 8/2010 Ling et al.
2010/0211678 A1 8/2010 McDysan et al.
2010/0232445 A1 9/2010 Bellovin
2010/0242098 A1 9/2010 Kenworthy
2010/0268799 A1 10/2010 Maestas
2010/0296441 A1 11/2010 Barkan
2010/0303240 A1 12/2010 Beachem et al.
2011/0055916 A1 3/2011 Ahn
2011/0055923 A1 3/2011 Thomas
2011/0088092 A1 4/2011 Nguyen et al.
2011/0141900 A1 6/2011 Jayawardena et al.
2011/0185055 A1 7/2011 Nappier et al.
2011/0270956 A1 11/2011 McDysan et al.
2012/0023576 A1* 1/2012 Sorensen G06F 21/577 726/22
2012/0106354 A1 5/2012 Pleshek et al.
2012/0113987 A1 5/2012 Riddoch et al.
2012/0240135 A1 9/2012 Risbood et al.
2012/0264443 A1 10/2012 Ng et al.
2012/0314617 A1 12/2012 Erichsen et al.
2012/0331543 A1 12/2012 Bostrom et al.
2013/0047020 A1 2/2013 Hershko et al.
2013/0059527 A1 3/2013 Hasesaka et al.
2013/0061294 A1 3/2013 Kenworthy
2013/0117852 A1 5/2013 Stute
2013/0254766 A1 9/2013 Zuo et al.
2013/0305311 A1 11/2013 Puttaswamy Naga et al.
2014/0075510 A1 3/2014 Sonoda et al.
2014/0115654 A1 4/2014 Rogers et al.
2014/0201123 A1 7/2014 Ahn et al.
2014/0215574 A1 7/2014 Erb et al.
2014/0281030 A1 9/2014 Cui et al.
2014/0283004 A1 9/2014 Moore
2014/0283030 A1 9/2014 Moore et al.
2014/0317397 A1 10/2014 Martini
2014/0366132 A1 12/2014 Stiansen et al.
2015/0207813 A1* 7/2015 Reybok G06F 21/552 726/22
2015/0237012 A1 8/2015 Moore
2015/0304354 A1 10/2015 Rogers et al.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2015/0334125	A1	11/2015	Bartos et al.
2015/0350229	A1	12/2015	Mitchell
2015/0373043	A1	12/2015	Wang et al.

FOREIGN PATENT DOCUMENTS

CA	2600236	A1	10/2006
EP	1006701	A2	6/2000
EP	1313290	A1	5/2003
EP	1484884	A2	12/2004
EP	1677484	A2	7/2006
EP	2385676	A1	11/2011
EP	2498442	A1	9/2012
EP	1864226	B1	5/2013
KR	20010079361	A	8/2001
WO	2005046145	A1	5/2005
WO	2006093557	A2	9/2006
WO	2006105093	A2	10/2006
WO	2007109541	A2	9/2007
WO	2011038420	A2	3/2011
WO	2012146265	A1	11/2012

OTHER PUBLICATIONS

ISR for PCT/US2013/057502, dated Nov. 7, 2013.
International Search Report off International Application No. PCT/US2014/023286, dated Jun. 24, 2014.
ISR off International Application No. PCT/US2013/072566, dated Mar. 24, 2014.
ISR off International Application No. PCT/US2014/027723, dated Jun. 26, 2014.
"Control Plane Policing Implementation Best Practices"; Cisco Systems; Mar. 13, 2013; <https://web.archive.org/web/20130313135143/http:www.cisco.com/web/about/security/intelligence/coppwp_gs.html>.
Reumann, John; "Adaptive Packet Filters"; IEEE, 2001, Department of Electrical Engineering and Computer Science, the University of Michigan, Ann Arbor, MI.
Greenwald, Michael; "Designing an Academic Firewall: Policy, Practice, and Experience with SURF"; IEEE, Proceedings of SNDSS, 1996.
Mizuno et al., A New Remote Configurable Firewall System for Home-use Gateways, Jan. 2005. Second IEEE Consumer Communications and Networking Conference, pp. 599-601.
"SBIR Case Study: Centripetal Networks Subtitle: How CNI Leveraged DHS S&T SBIR Funding to Launch a Successful Cyber Security Division 2012 Principal Investigators' Meeting"; Sean Moore, Oct. 10, 2014.
John Kindervag; "Build Security Into Your Network's DNA: The Zero Trust Network Architecture", Forrester Research Inc.; Nov. 5, 2010, pp. 1-26.
Palo Alto Networks; "Designing a Zero Trust Network With Next-Generation Firewalls"; pp. 1-10; last viewed on Oct. 21, 2012.
Jan. 11, 2016—(US) Non Final Rejection—U.S. Appl. No. 14/698,560.
Apr. 27, 2011—(WO) International Search Report and Written Opinion—App PCT/US2010/054520.
Mar. 4, 2011—(US) Notice of Allowance—U.S. Appl. No. 11/316,331.
Mar 3, 2011—(EP) Communication Pursuant to Rules 70(2) and 70a(2)—App 06758213.0.
Feb. 14, 2011—(EP) Search Report—App 06758213.0.
Fulp, Errin: "Errin Fulp," XP002618346, www.cs.wfu.edu/fulp/ewfPub.html, pp. 1-5 (Copyright 2010).
Sep. 30, 2010—(US) Office Action—U.S. Appl. No. 11/390,976.
Sep. 10, 2010—(AU) Office Action—App 2006230171.
Aug. 20, 2010—(AU) Office Action—App 2005328336.
Jun. 23, 2010—(US) Final Rejection—U.S. Appl. No. 11/316,331.
Apr. 29, 2010—(US) Interview Summary—U.S. Appl. No. 11/390,976.
Mar. 26, 2010—(US) Final Rejection—U.S. Appl. No. 11/390,976.
Sep. 14, 2009 (US) Office Action—U.S. Appl. No. 11/316,331.
Jun. 24, 2009—(US) Office Action—U.S. Appl. No. 11/390,976.
Jul. 3, 2008—(WO) Written Opinion of the International Searching Authority—App PCT/US06/11291.
Aug. 31, 2007—(EP) Communication Pursuant to Rules 109 and 110—App 05857614.1.
Acharya et al, "OPTWALL: A Hierarchical Traffic-Aware Firewall," Department of Computer Science, Telecommunications Program, University of Pittsburgh, pp. 1-11 (2007).
Sep. 11, 2006—(WO) Written Opinion of the International Searching Authority—App PCT/US05/47008.
Tarsa et al., "Balancing Trie-Based Policy representations for Network Firewalls." Department of Computer Science, Wake Forest University, pp. 1-6 (2006).
Fulp, "Trie-Based Policy Representations for Network Firewalls," Proceedings of the IEEE International Symposium on Computer Communications (2005).
E. Fulp, "Optimization of Network Firewall Policies Using Ordered Sets and Directed Acyclical Graphs", Technical Report, Computer Solent Department, Wake Forest University, Jan. 2004.
E. Fulp et al., "Network Firewall Policy Tries", Technical Report, Computer Science Department, Wake Forest University, 2004.
E. Al-Shaer et al., "Modeling and Management of Firewall Policies", IEEE Transactions on Network and Service Management, 1(1): 2004.
F.W. Fulp, "Firewall Architectures for High Speed Networks", U.S. Department of Energy Grant Application, Funded Sep. 2003.
E. Al-Shaer et al., "Firewall Policy Advisor for Anomaly Discovery and Rule Editing", Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management, 2003.
V.P. Ranganath, "A Set-Based Approach to Packet Classification", Proceedings of the IASTED International Conference on Parallel and Distributed Computing and Systems, 889-894, 2003.
M. Christiansen et al., "Using IDDsfor Packet Filtering", Technical Report, BRICS. Oct. 2002.
Lee et al., "Development Framework for Firewall Processors," IEEE, pp. 352-355 (2002).
L. Qui et al., "Fast Firewall Implementations for Software and Hardware-Based Routers", Proceedings of ACM Sigmetrics, Jun. 2001.
D. Eppstein et al., "Internet Packet Filter Management and Rectangle Geometry", Proceedings of the Symposium on Discrete Algorithms, 827-835, 2001.
E. Fulp, "Preventing Denial of Service Attacks on Quality of Service", Proceedings of the 2001 DARPA Information Survivability Conference and Exposition II, 2001.
S. Goddard et al., "An Unavailability Analysis of Firewall Sandwich Configurations", Proceedings of the 6th IEEE Symposium on High Assurance Systems Engineering, 2001.
G.V. Rooij, "Real Stateful TCP Packet Filtering in IP Filter", Proceedings of the 10th USENIX Security Symposium, 2001.
P. Warkhede et al., "Fast Packet Classification for Two-Dimensional Conflict-Free Filters", Proceedings of IEEE INFOCOM, 1434-1443, 2001.
D. Decasper et al., "Router Plugins: A Software Architecture for Next-Generation Routers", IEEE/ACM Transactions on Networking, 8(1): Feb. 2000.
A. Feldmann et al., "Tradeoffs for Packet Classification", Proceedings of the IEEE INFOCOM, 397-413, 2000.
X. Gan et al., "LSMAC vs. LSNAT: Scalable Cluster-based Web servers", Journal of Networks, Software Tools, and Applications, 3(3): 175-185, 2000.
A. Hari et al., "Detecting and Resolving Packet Filter Conflicts", Proceedings of IEEE INFOCOM, 1203-1212, 2000.
O. Paul et al., "A full Bandwidth ATM Firewall", Proceedings of the 6th European Symposium on Research in Computer Security ESORICS'2000, 2000.
J. Xu et al., "Design and Evaluation of a High-Performance ATM Firewall Switch and Its Applications", IEEE Journal on Selected Areas in Communications, 17(6): 1190-1200, Jun. 1999.

(56) **References Cited**

OTHER PUBLICATIONS

C. Benecke, "A Parallel Packet Screen for High Speed Networks", Proceedings of the 15th Annual Computer Security Applications Conference, 1999.
R. Funke et al., "Performance Evaluation of Firewalls in Gigabit-Networks", Proceedings of the Symposium on Performance Evaluation of Computer and Telecommunication Systems, 1999.
S. Suri et al., "Packet Filtering in High Speed Networks", Proceedings of the Symposium on Discrete Algorithms, 969-970, 1999.
J. Ellermann et al., "Firewalls for ATM Networks", Proceedings of INFOSEC'COM, 1998.
V. Srinivasan et al., "Fast and Scalable Layer Four Switching", Proceedings of ACM SIGCOMM, 191-202, 1998.
M. Degermark et al., "Small Forwarding Tables for Fast Routing Lookups", Proceedings of ACM SIGCOMM, 4-13, 1997.
S,M. Bellovin et al., "Network Firewalls", IEEE Communications Magazine, 50-57, 1994.
W.E. Leland et al., "On the Self-Similar Nature of Ethernet Traffic", IEEE Transactions on Networking, 2(1); 15, 1994.
G. Brightwell et aL, "Counting Linear Extensions is #P-Complete", Proceedings of the Twenty-Third Annual ACM Symposium on Theory of Computing, 1991.
M. Al-Suwaiyel et al., "Algorithms for Tile Compaction", ACM Transactions on Database Systems, 9(2): 243-263, Jun. 1984.
D. Corner, "Analysis of a Heuristic for Full Tile Minimization", ACM Transactions on Database Systems, 6(3): 513-537, Sep. 1981.
R.L. Graham et al., "Optimization and Approximation in Deterministic Sequencing and Scheduling: A Survey", Annals of Discrete Mathematics, 5: 287-326, 1979.
E.L. Lawler, "Sequencing Jobs to Minimize Total Weighted Completion oTime Subject to Precedence Constraints", Annals of Discrete Mathematics, 2: 75-90, 1978.
J.K. Lenstra et al., "Complexity of Scheduling Under Precedence Constraints", Operations Research, 26(1): 22-35,1978.
R. Rivest, "On Self-Organizing Sequential Search Heuristics", Communications of the ACM, 19(2): 1976.
W.E. Smith, "Various Optimizers for Single-Stage Productions", Naval Research Logistics Quarterly, 3: 59-66, 1956.
Bellion, "High Performance Packet Classification", http://www.hipac.org (Publication Date Unknown).
Oct. 18, 2011—(EP) Communication Pursuant to Article 94(3)—App 06 758 213.0.
Jun. 9, 2011—(US) Notice of Allowance—U.S. Appl. No. 11/390,976.
Jun. 26, 2012—(EP) Extended Search Report—App 05857614.1.
Jun. 9, 2012—(AU) Notice of Acceptance—App 2006230171.
Nov. 11, 2011—(AU) Second Office Action—App 2006230171.
Jan. 17, 2013—(CA) Office Action—App 2,600,236.
Jan. 16, 2013—(CA) Office Action—App 2,594,020.
Nov. 20, 2012—(EP) Communication under rule 71(3)—App 06 758 213.0.
Apr. 18, 2013—(EP) Decision to Grant a European Patent—App 06758212.0.
Aug. 25, 2011—(US) Non Final Rejection—U.S. Appl. No. 12/871,806.
Feb. 6, 2012—(US) Final Rejection—U.S. Appl. No. 12/871,806.
Aug. 7, 2012—(US) Non Final Rejection—U.S. Appl. No. 12/871,806.
Nov. 26, 2012—(US) Final Rejection—U.S. Appl. No. 12/871,806.
Apr. 4, 2013—(US) Notice of Allowance—U.S. Appl. No. 12/871,806.
Jan. 14, 2015—(EP) Extended Search Report—App 10819667.6.
May 26, 2014—(CA) Office Action—App 2010297968.
May 25, 2015—(AU) Notice of Acceptance—App 2010297968.
May 14, 2015—(US) Non Final Rejection—U.S. Appl. No. 13/940,240.
Nov. 27, 2015—(US) Final Rejection—U.S. Appl. No. 13/940,240.
Jul. 10, 2015—(WO) Communication Relating to the Results of the Partial International Search for International App—PCT/US2015/024691.
Jul. 23, 2015—(WO) International Preliminary Report on Patentability—App PCT/US2013/072566.
Jan. 28, 2016—(WO) International Search Report and Written Opinion—App PCT/US2015/062691.
International Search Report and Written Opinion for International App. No. PCT/US2015/024691, dated Sep. 16, 2015.
International Preliminary Report on Patentability for International App. No. PCT/US2013/057502, dated Apr. 28, 2015.
International Preliminary Report on Patentability for International App. No. PCT/US2014/023286, dated Sep. 15, 2015.
International Preliminary Report on Patentability for International App. No. PCT/US2014/027723, dated Sep. 15, 2015.
Dec. 22, 2015—(US) Final Office Action—U.S. Appl. No. 14/714,207.
Feb. 26, 2016—(US) Non Final Office Action—U.S. Appl. No. 14/253,992.
Nov. 2, 2015—(AU) Office Action—App 2013372879.
Apr. 26, 2016—(US) Office Action—U.S. Appl. No. 14/745,207.
May 6, 2016—(US) Office Action—U.S. Appl. No. 14/714,207.
May 13, 2016—(US) Office Action—U.S. Appl. No. 13/940,240.
Jun. 14, 2016—(US) Office Action—U.S. Appl. No. 14/625,486.
Feb. 25, 2016—(AU) Office Action—App 2014249055.
Feb. 24, 2016—(AU) Office Action—App 2014228257.
Jun. 9, 2016—(WO) International Search Report—PCT/US2016/026339.
Jun. 16, 2016—(CA) Office Action—App 2,888,935.
Jul. 11, 2016—(EP) Office Action—App 14720824.3.
Jul. 22, 2016—(US) Office Action—U.S. Appl. No. 14/921,718.
Jul. 20, 2016—(AU) Office Action—App 2013335255.
Oct. 5, 2016—(US) Notice of Allowance—U.S. Appl. No. 14/698,560.
Sep. 13, 2016—(CA) Office Action—App 2,902,206.
Sep. 14, 2016—(CA) Office Action—App 2,897,737.
Sep. 26, 2016—(CA) Office Action—App 2,902,158.
Oct. 26, 2016—(US) Office Action—U.S. Appl. No. 13/940,240.
Nov. 21, 2016—(US) Office Action—U.S. Appl. No. 14/745,207.
Dec. 5, 2016—(US) Notice of Allowance—U.S. Appl. No. 14/714,207.
Singh, Rajeev et al. "Detecting and Reducing the Denial of Service attacks in WLANs", Dec. 2011, World Congress on Information and Communication TEchnologies, pp. 968-973.
Feb. 10, 2017—(US) Notice of Allowance—U.S. Appl. No. 14/625,486.
Feb. 15, 2017—(US) Notice of Allowance—U.S. Appl. No. 14/921,718.
Mar. 6, 2017—(WO) International Search Report and Written Opinion—App PCT/US2016/068008.
Jun. 7, 2017—(US) Office Action—U.S. Appl. No. 14/745,207.
Sep. 4, 2015 (US) Notice of Allowance—U.S. Appl. No. 14/702,755.
Jun. 7, 2017—(WO) International Search Report and Written Opinion—App PCT/US2016/067111.

* cited by examiner

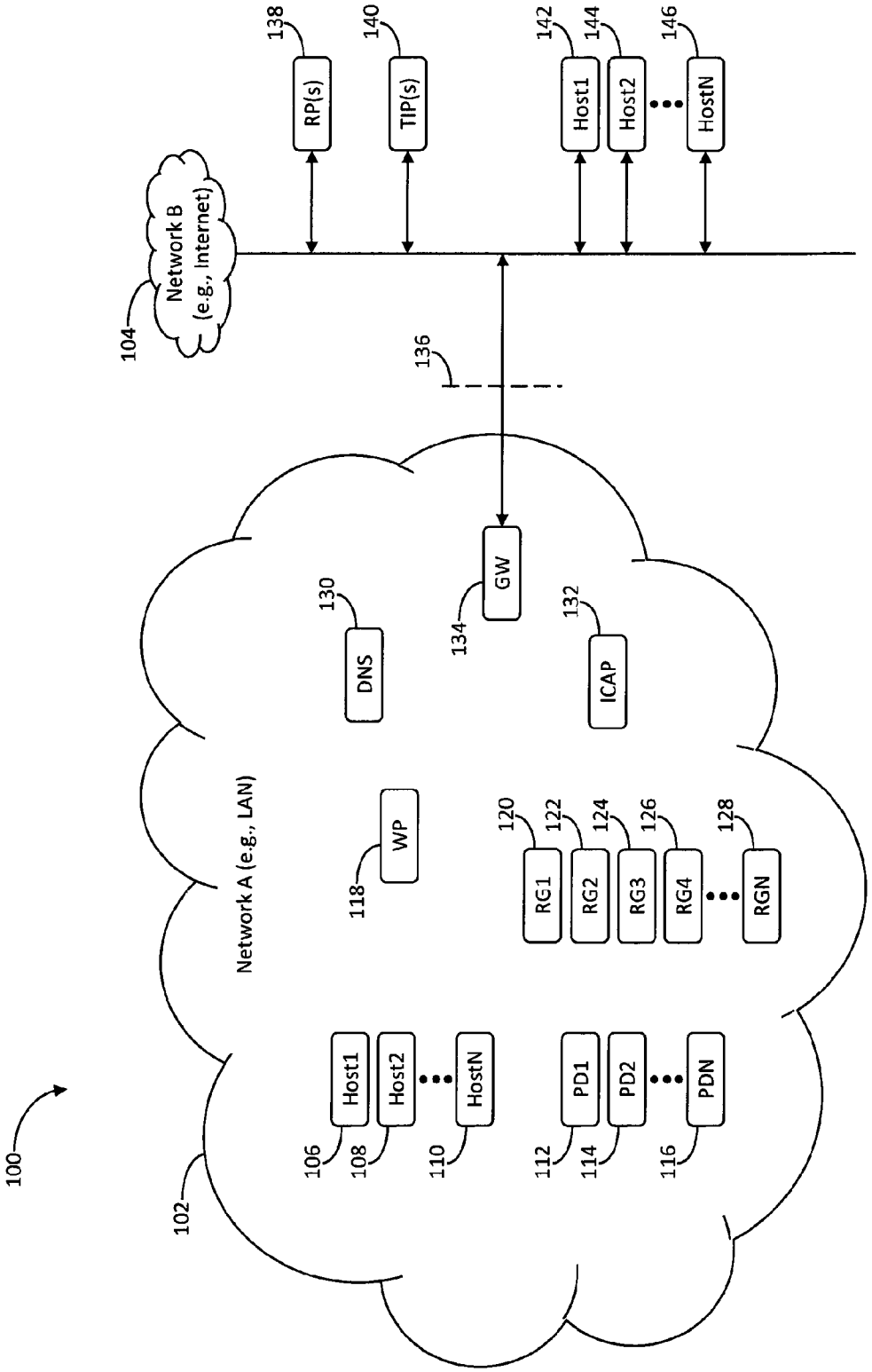

100
102
104
Network B (e.g., Internet)
Network A (e.g., LAN)
RP(s)
TIP(s)
Host1
Host2
HostN
GW
DNS
ICAP
WP
RG1
RG2
RG3
RG4
RGN
Host1
Host2
HostN
PD1
PD2
PDN
138
140
142
144
146
136
130
134
132
118
120
122
124
126
128
106
108
110
112
114
116

FIG. 1

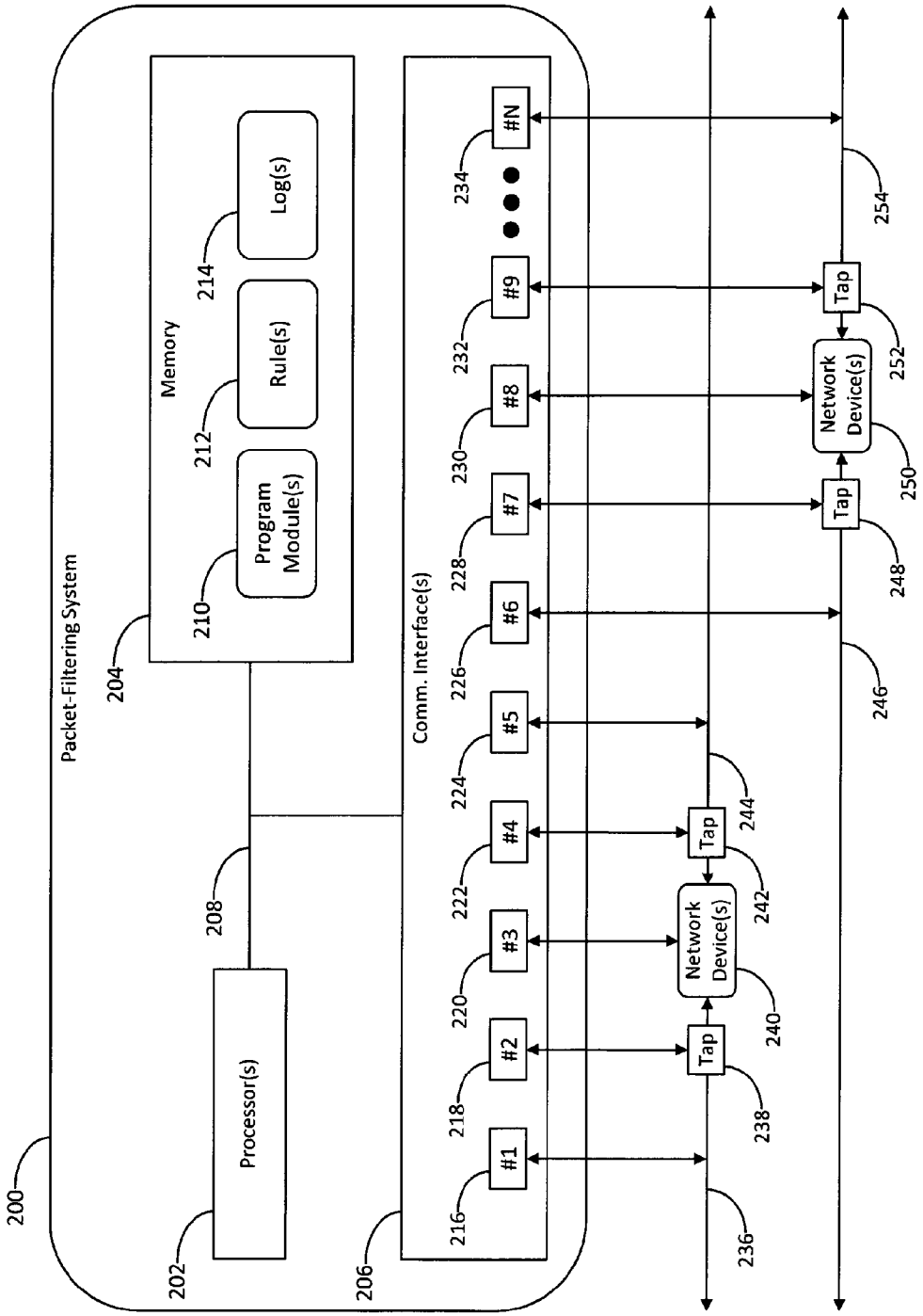


FIG. 2

Keysight, EX-1028
Page 416
CENTRIPETAL-SSCG 004709

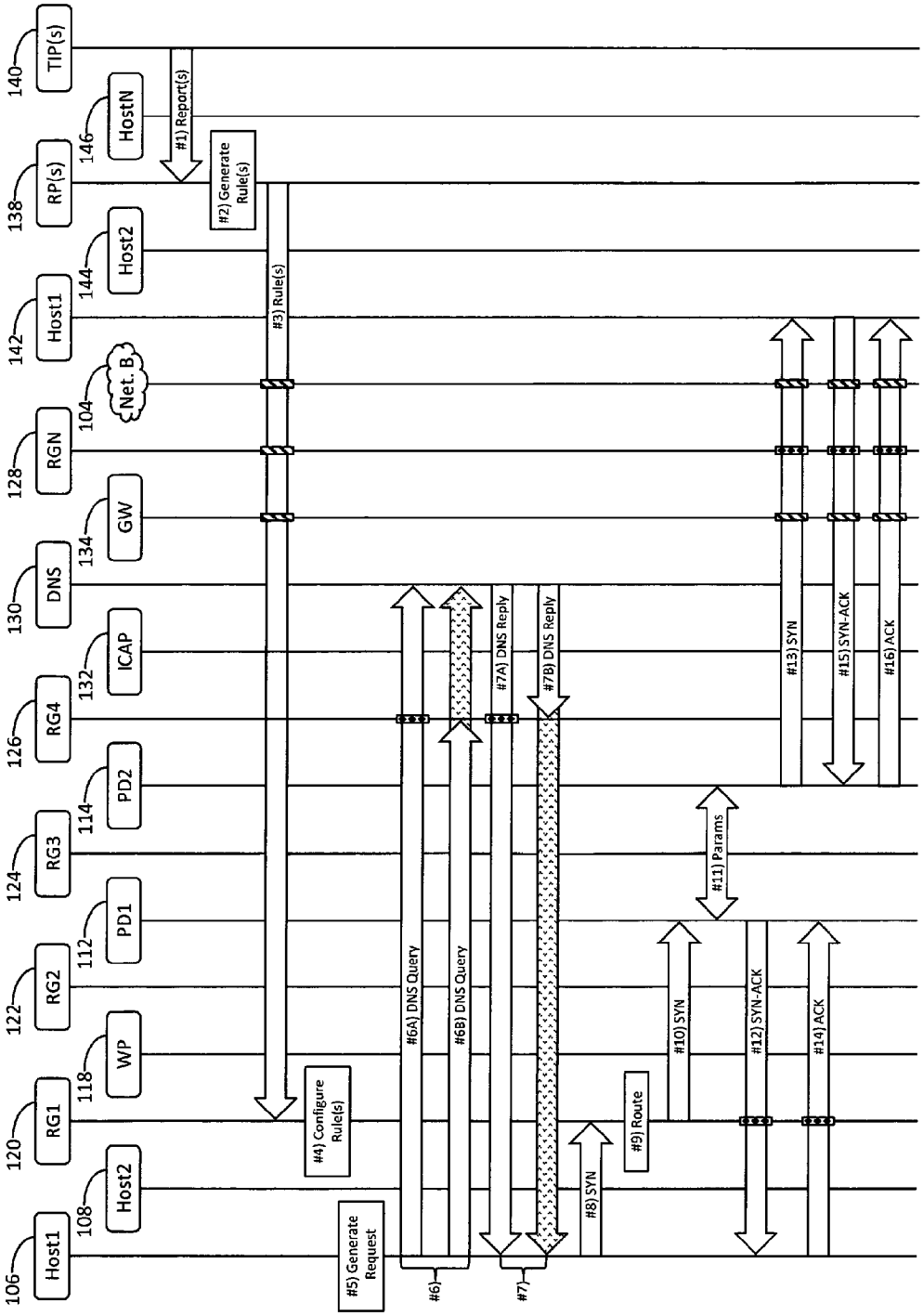

TIP(s)
HostN
RP(s)
Host2
Host1
Net. B
RGN
GW
DNS
ICAP
RG4
PD2
RG3
PD1
RG2
WP
RG1
Host2
Host1
140
146
138
144
142
104
128
134
130
132
126
114
124
112
122
118
120
108
106
#1) Report(s)
#2) Generate Rule(s)
#3) Rule(s)
#4) Configure Rule(s)
#5) Generate Request
#6A) DNS Query
#6B) DNS Query
#7A) DNS Reply
#7B) DNS Reply
#6)
#7)
#8) SYN
#9) Route
#10) SYN
#11) Params
#12) SYN-ACK
#13) SYN
#14) ACK
#15) SYN-ACK
#16) ACK

FIG. 3A

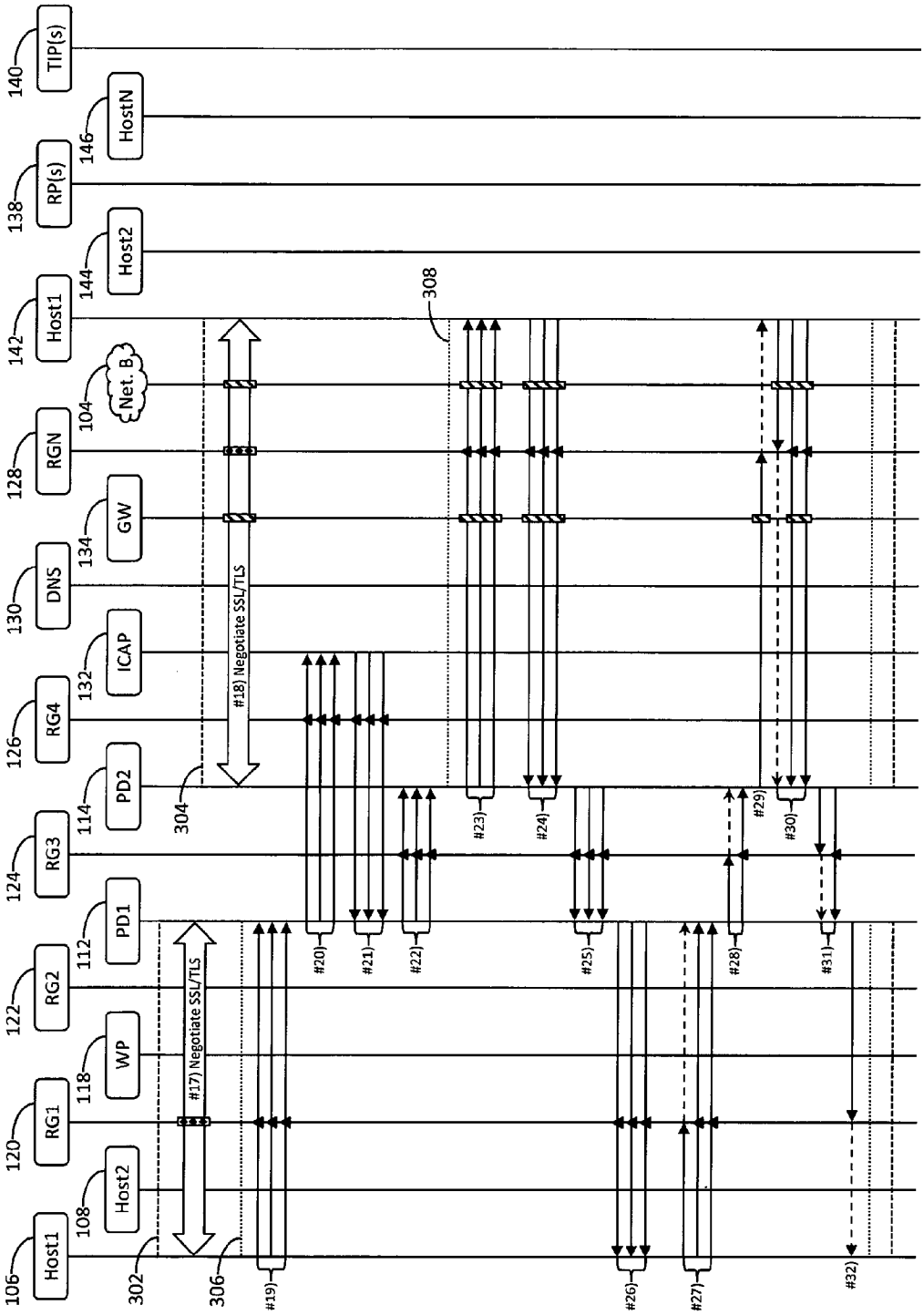

TIP(s)
140
HostN
146
RP(s)
138
Host2
144
Host1
142
Net. B
104
RGN
128
GW
134
DNS
130
ICAP
132
RG4
126
PD2
114
RG3
124
PD1
112
RG2
122
WP
118
RG1
120
Host2
108
Host1
106
308
304
302
306
#17) Negotiate SSL/TLS
#18) Negotiate SSL/TLS
#19)
#20)
#21)
#22)
#23)
#24)
#25)
#26)
#27)
#28)
#29)
#30)
#31)
#32)

FIG. 3B

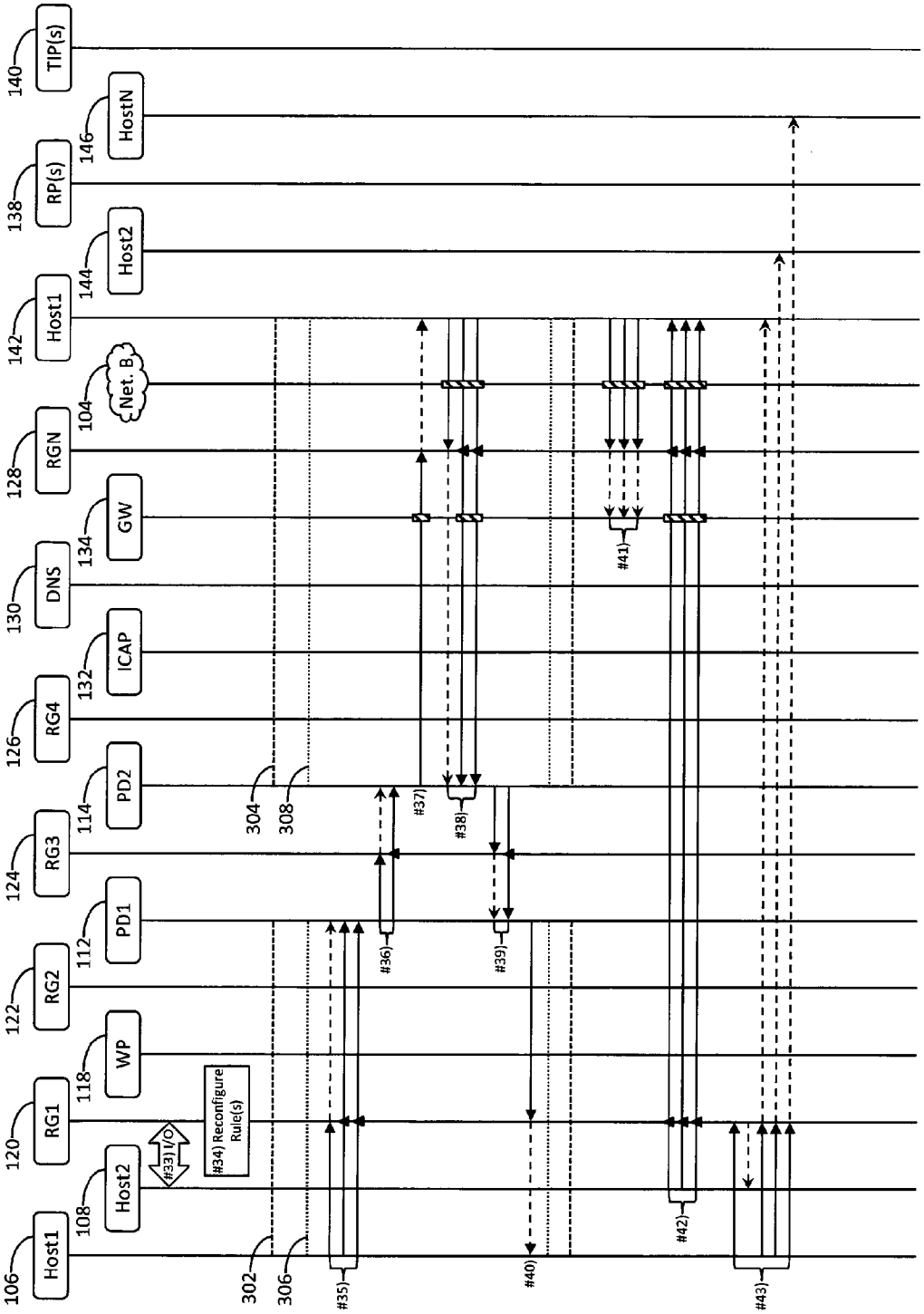

140 TIP(s)
146 HostN
138 RP(s)
144 Host2
142 Host1
104 Net. B.
128 RGN
134 GW
130 DNS
132 ICAP
126 RG4
114 PD2
124 RG3
112 PD1
122 RG2
118 WP
120 RG1
108 Host2
106 Host1
#33) I/O
#34) Reconfigure Rule(s)
304
308
302
306
#35)
#36)
#37)
#38)
#39)
#40)
#41)
#42)
#43)

FIG. 3C

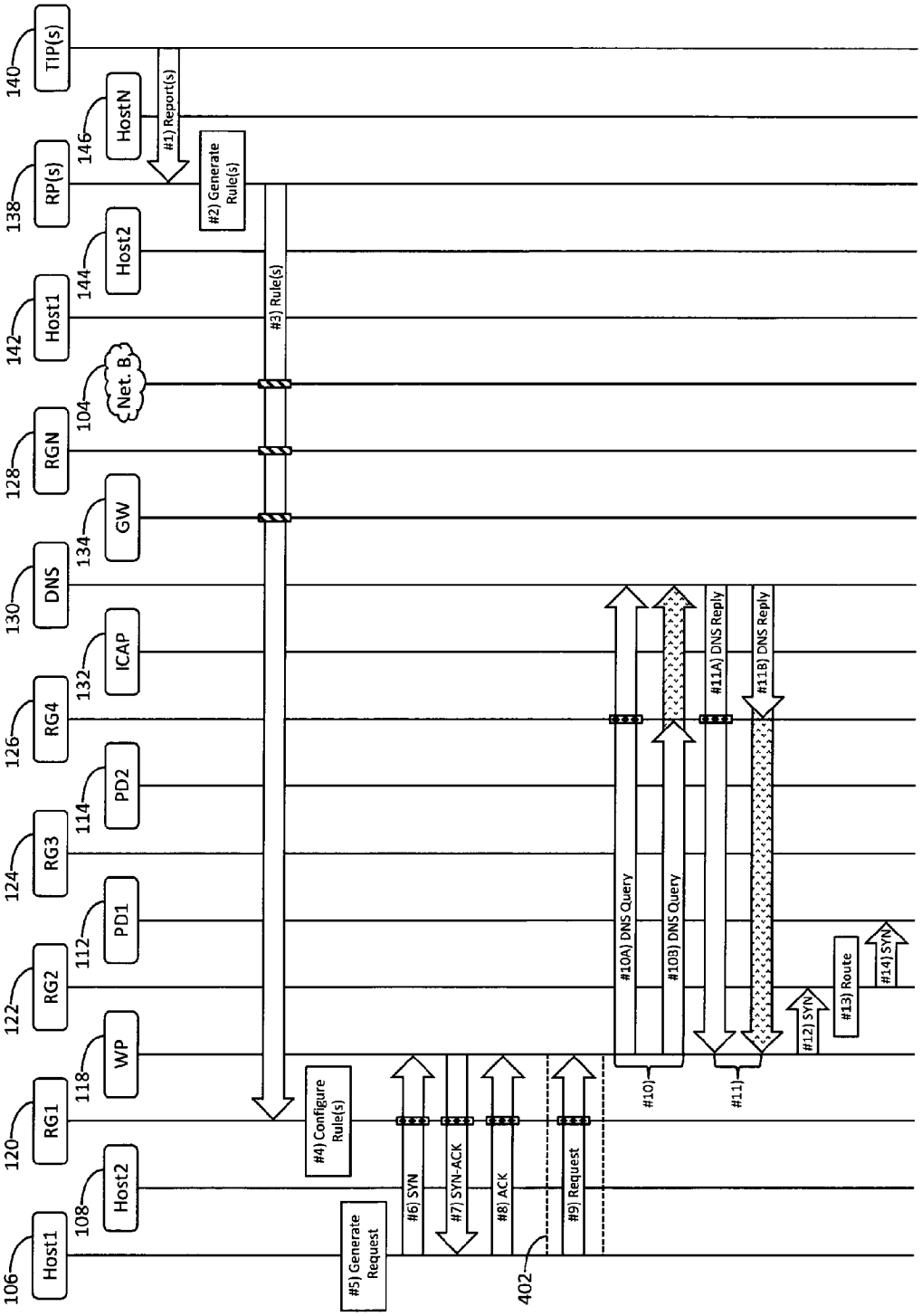


FIG. 4A

Keysight, EX-1028
CENTRIPETAL-USCO 004713

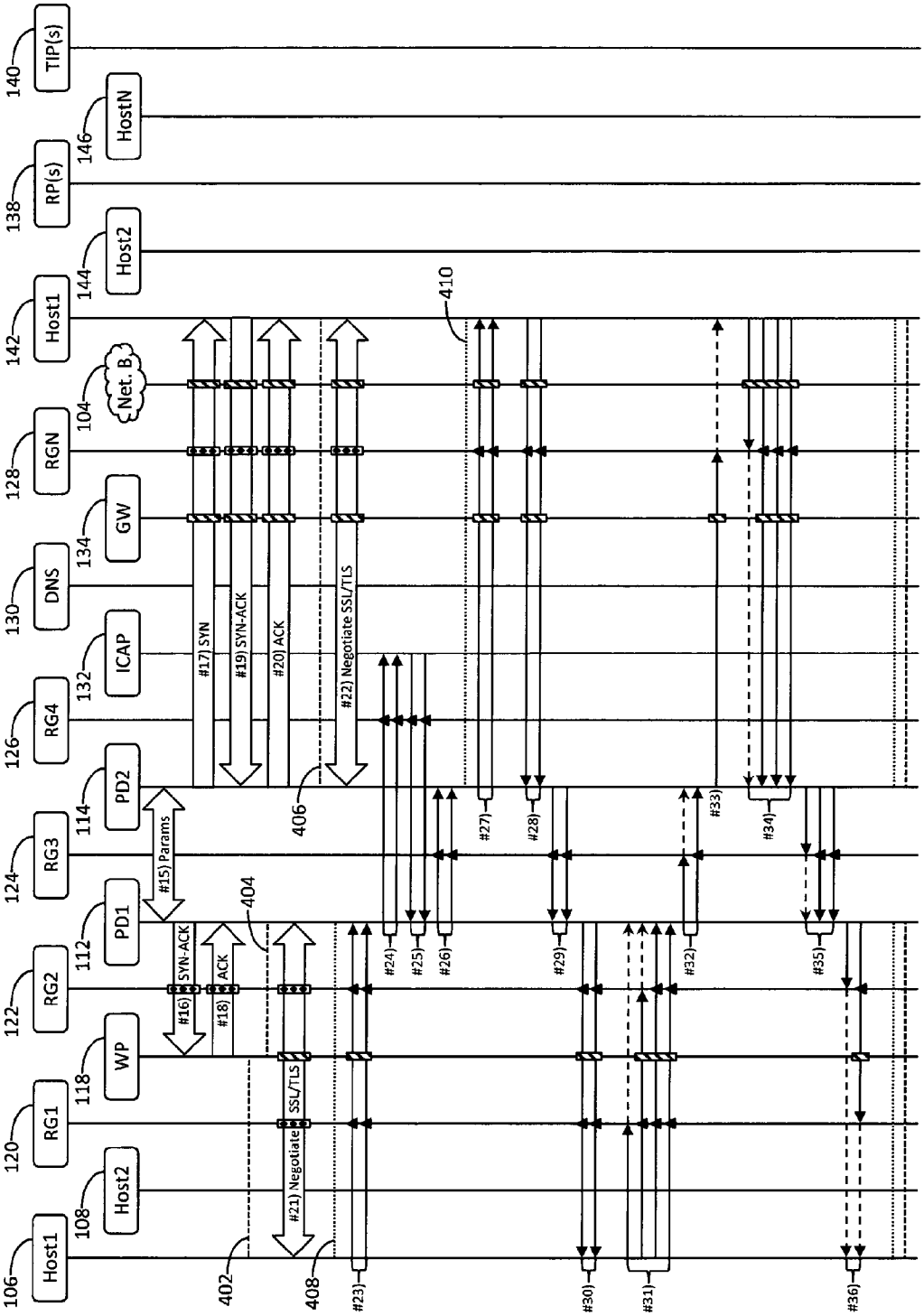

140 TIP(s)
146 HostN
138 RP(s)
144 Host2
142 Host1
104 Net. B
128 RGN
134 GW
130 DNS
132 ICAP
126 RG4
114 PD2
124 RG3
112 PD1
122 RG2
118 WP
120 RG1
108 Host2
106 Host1
#17) SYN
#19) SYN-ACK
#20) ACK
#22) Negotiate SSL/TLS
#15) Params
#16) SYN-ACK
#18) ACK
#21) Negotiate SSL/TLS
410
406
404
402
408
#23)
#24)
#25)
#26)
#27)
#28)
#29)
#30)
#31)
#32)
#33)
#34)
#35)
#36)

FIG. 4B

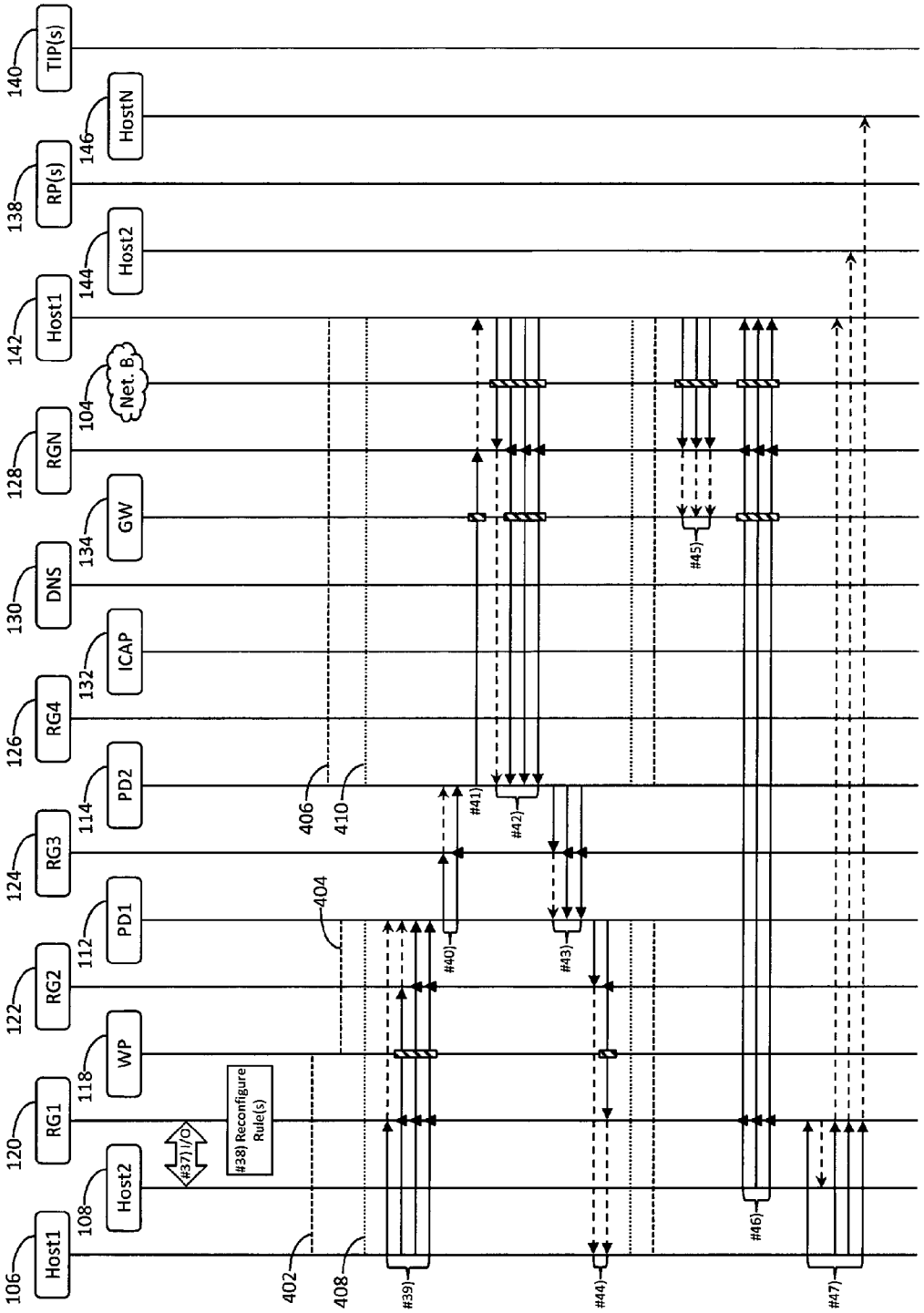

140 TIP(s)
146 HostN
138 RP(s)
144 Host2
142 Host1
104 Net. B
128 RGN
134 GW
130 DNS
132 ICAP
126 RG4
114 PD2
124 RG3
112 PD1
122 RG2
118 WP
120 RG1
108 Host2
106 Host1
#37) I/O
#38) Reconfigure Rule(s)
402
404
406
408
410
#39)
#40)
#41)
#42)
#43)
#44)
#45)
#46)
#47)

FIG. 4C

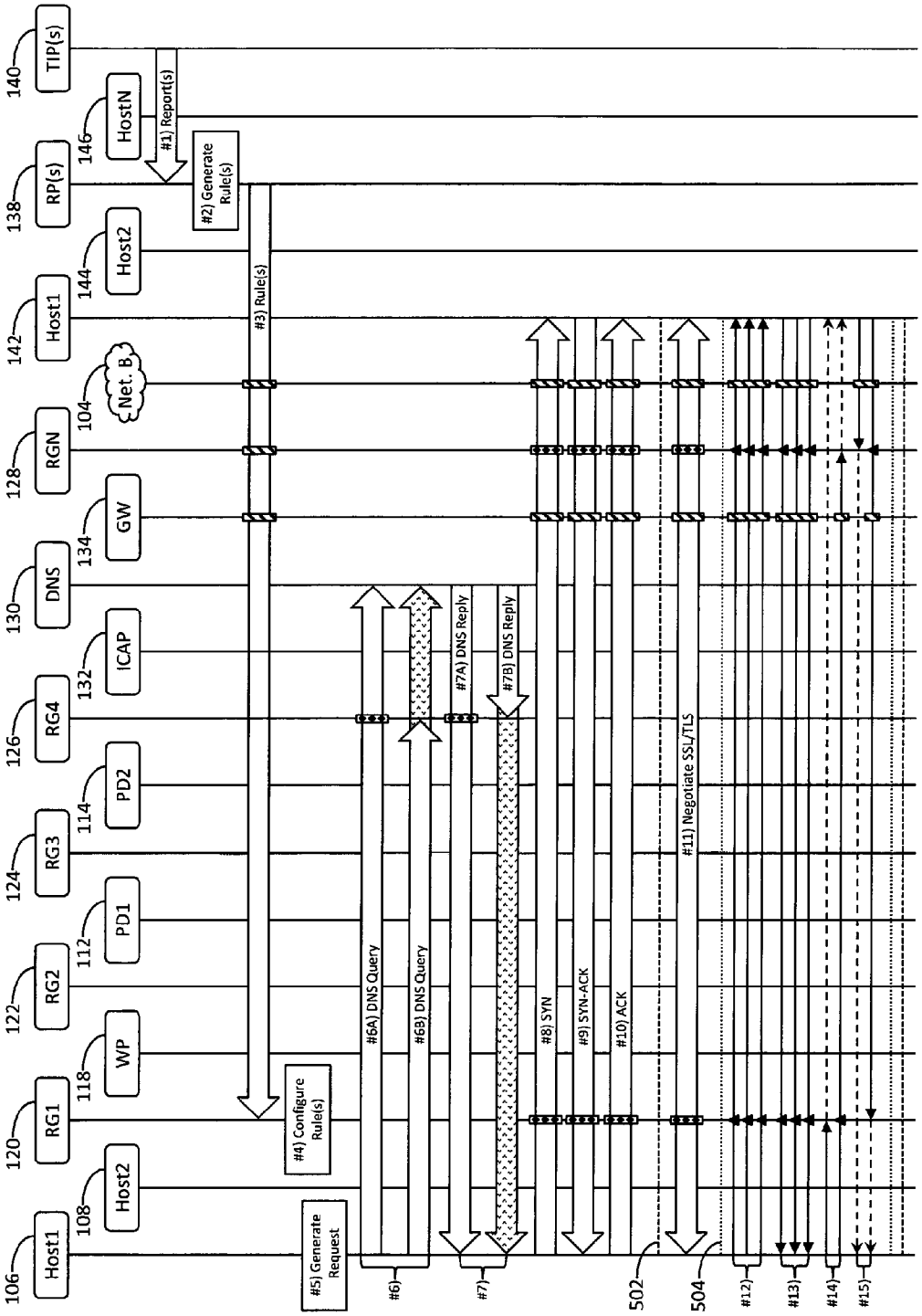


FIG. 5A

Keysight, EX-1028
CENTRIPETAL-USCA 004716

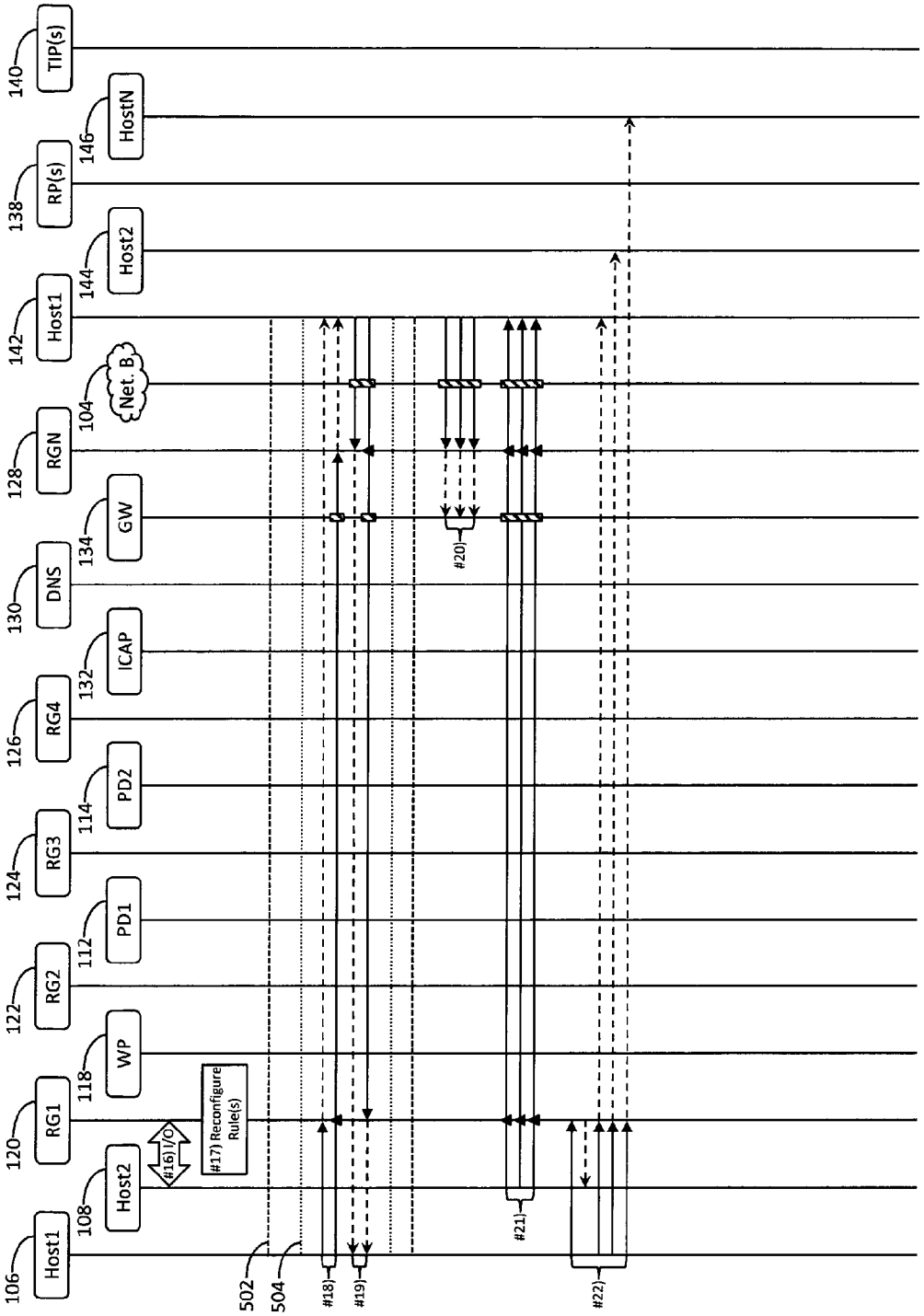


FIG. 5B

Keysight, EX-1028
CENTRIPETAL-USCO 004717

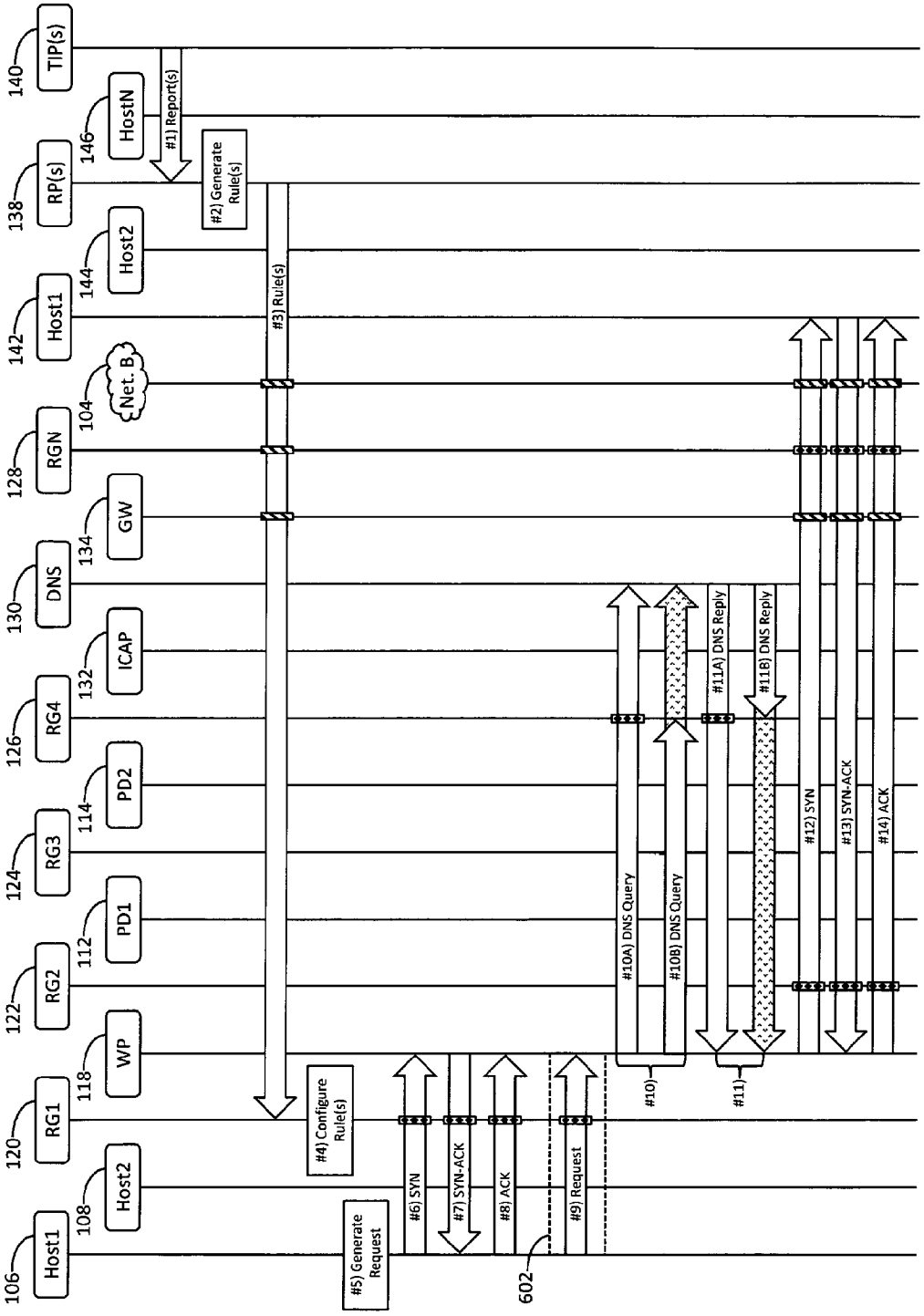


FIG. 6A

Keysight, EX-1028
CENTRIPETAL-SCS 004718

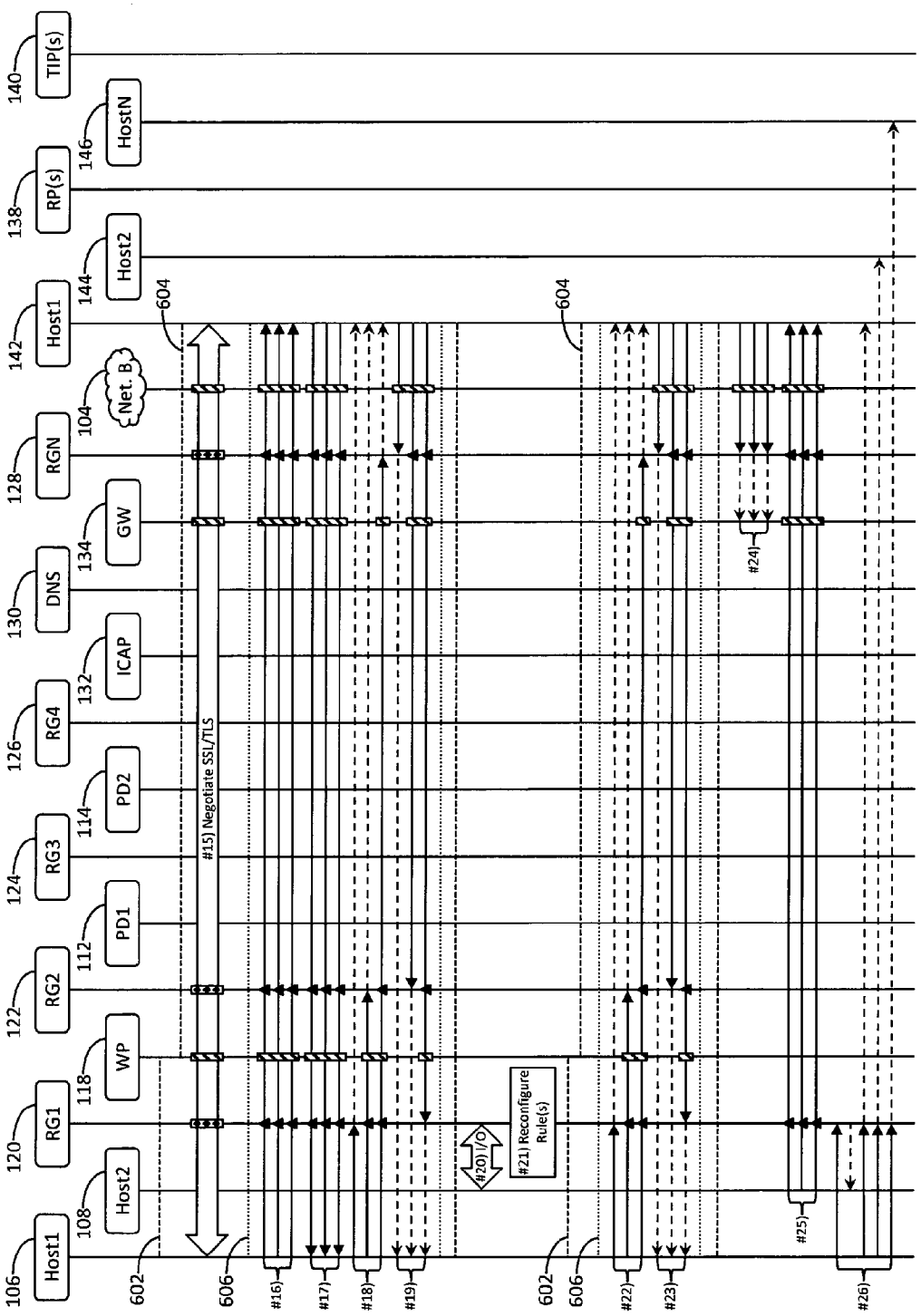


FIG. 6B

Keysight, EX-1028
CENTRIPETAL-SCO 004719

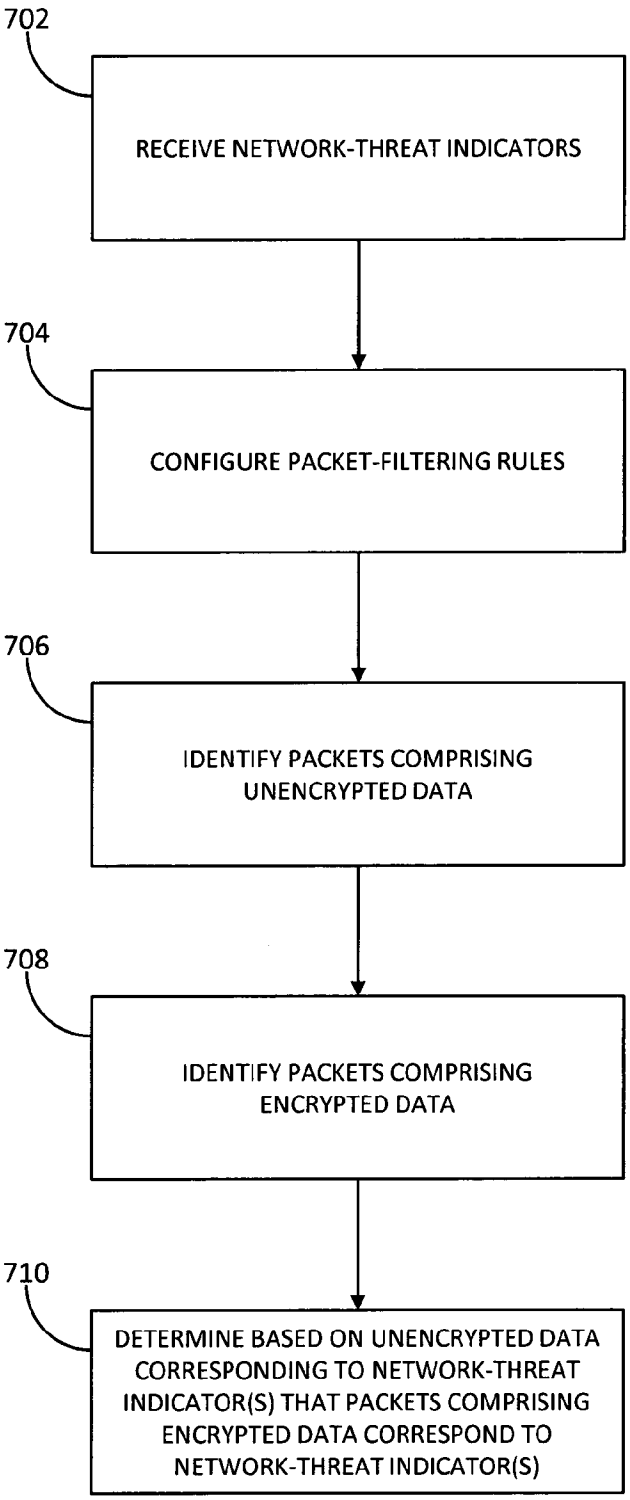


FIG. 7

Keysight, EX-1028
Page 427
CENTRIPETAL-SCO 004720

RULE-BASED NETWORK-THREAT DETECTION FOR ENCRYPTED COMMUNICATIONS

BACKGROUND

Network security is becoming increasingly important as the information age continues to unfold. Network threats may take a variety of forms (e.g., unauthorized requests or data transfers, viruses, malware, large volumes of traffic designed to overwhelm resources, and the like). Network-threat services provide information associated with network threats, for example, reports that include listings of network-threat indicators (e.g., network addresses, domain names, uniform resource identifiers (URIs), and the like). Such information may be utilized to identify network threats. Encrypted communications, however, may obfuscate data corresponding to network threats. Accordingly, there is a need for rule-based network-threat detection for encrypted communications.

SUMMARY

The following presents a simplified summary in order to provide a basic understanding of some aspects of the disclosure. It is intended neither to identify key or critical elements of the disclosure nor to delineate the scope of the disclosure. The following summary merely presents some concepts of the disclosure in a simplified form as a prelude to the description below.

Aspects of this disclosure relate to rule-based network-threat detection for encrypted communications. In accordance with embodiments of the disclosure, a packet-filtering system configured to filter packets in accordance with packet-filtering rules may receive data indicating network-threat indicators and may configure the packet-filtering rules to cause the packet-filtering system to identify packets comprising unencrypted data, and packets comprising encrypted data. A portion of the unencrypted data may correspond to one or more of the network-threat indicators, and the packet-filtering rules may be configured to cause the packet-filtering system to determine, based on the portion of the unencrypted data, that the packets comprising encrypted data correspond to the one or more network-threat indicators.

BRIEF DESCRIPTION OF THE DRAWINGS

The present disclosure is pointed out with particularity in the appended claims. Features of the disclosure will become more apparent upon a review of this disclosure in its entirety, including the drawing figures provided herewith.

Some features herein are illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings, in which like reference numerals refer to similar elements, and wherein:

FIG. **1** depicts an illustrative environment for rule-based network-threat detection for encrypted communications in accordance with one or more aspects of the disclosure;

FIG. **2** depicts an illustrative packet-filtering system for rule-based network-threat detection for encrypted communications in accordance with one or more aspects of the disclosure;

FIGS. **3**A-C, **4**A-C, **5**A-B, and **6**A-B depict illustrative event sequences for rule-based network-threat detection for encrypted communications in accordance with one or more aspects of the disclosure; and

FIG. **7** depicts an illustrative method for rule-based network-threat detection for encrypted communications in accordance with one or more aspects of the disclosure.

DETAILED DESCRIPTION

In the following description of various illustrative embodiments, reference is made to the accompanying drawings, which form a part hereof, and in which is shown, by way of illustration, various embodiments in which aspects of the disclosure may be practiced. It is to be understood that other embodiments may be utilized, and structural and functional modifications may be made, without departing from the scope of the disclosure.

Various connections between elements are discussed in the following description. These connections are general and, unless specified otherwise, may be direct or indirect, wired or wireless. In this respect, the specification is not intended to be limiting.

FIG. **1** depicts an illustrative environment for rule-based network-threat detection for encrypted communications in accordance with one or more aspects of the disclosure. Referring to FIG. **1**, environment **100** may include networks **102** and **104**. Network **102** may comprise one or more networks (e.g., Local Area Networks (LANs), Wide Area Networks (WANs), Virtual Private Networks (VPNs), or combinations thereof) associated with one or more individuals or entities (e.g., governments, corporations, service providers, or other organizations). Network **104** may comprise one or more networks (e.g., LANs, WANs, VPNs, or combinations thereof) that interface network **102** with one or more other networks (not illustrated). For example, network **104** may comprise the Internet, a similar network, or portions thereof.

Environment **100** may also include one or more hosts, such as computing or network devices (e.g., servers, desktop computers, laptop computers, tablet computers, mobile devices, smartphones, routers, gateways, firewalls, switches, access points, or the like). For example, network **102** may include hosts **106**, **108**, and **110**, proxy devices **112**, **114**, and **116**, web proxy **118**, rule gates **120**, **122**, **124**, **126**, and **128**, domain name system (DNS) **130**, Internet content adaptation protocol (ICAP) server **132**, and gateway **134**. As used herein, "host" (or "hosts") refers to any type of network device (or node) or computing device; while such devices may be assigned (or configured to be assigned) one or more network-layer addresses, the term "host" (or "hosts") does not imply such devices necessarily are assigned (or configured to be assigned) one or more network-layer addresses.

Gateway **134** may be located at border **136** between networks **102** and **104** and may interface network **102** or one or more hosts located therein with network **104** or one or more hosts located therein. For example, network **104** may include one or more rule providers **138**, one or more threat-intelligence providers **140**, and hosts **142**, **144**, and **146**, and gateway **134** may interface hosts **106**, **108**, and **110**, proxy devices **112**, **114**, and **116**, web proxy **118**, rule gates **120**, **122**, **124**, **126**, and **128**, DNS **130**, and ICAP server **132** with rule providers **138**, threat-intelligence providers **140**, and hosts **142**, **144**, and **146**.

FIG. **2** depicts an illustrative packet-filtering system for rule-based network-threat detection for encrypted communications in accordance with one or more aspects of the disclosure. Referring to FIG. **2**, packet-filtering system **200** may be associated with network **102** and may include one or more of rule gates **120**, **122**, **124**, **126**, and **128**. Packet-filtering system **200** may comprise one or more processors

Keysight, EX-1028
Page 428
CENTRIPETAL 004721

202, memory 204, one or more communication interfaces 206, and data bus 208. Data bus 208 may interface processors 202, memory 204, and communication interfaces 206. Memory 204 may comprise one or more program modules 210, rules 212, and logs 214. Program modules 210 may comprise instructions that when executed by processors 202 cause packet-filtering system 200 to perform one or more of the functions described herein. Rules 212 may comprise one or more packet-filtering rules in accordance with which packet-filtering system 200 is configured to filter packets received via communication interfaces 206. Logs 214 may include one or more entries generated by processors 202 in accordance with rules 212 for packets received by packet-filtering system 200 via communication interfaces 206.

Communication interfaces 206 may interface packet-filtering system 200 with one or more communication links of environment 100 (e.g., of networks 102 and 104). In some embodiments, one or more of communication interfaces 206 may interface directly with a communication link of environment 100. For example, interfaces 216 and 224 may interface directly with links 236 and 244, respectively. In some embodiments, one or more of communication interfaces 206 may interface indirectly with a communication link of environment 100. For example, interface 220 may interface with links 236 and 244 via one or more network devices 240. Network devices 240 may provide interface 220 with access to (or copies of) packets traversing one or more of links 236 and 244, for example, via a switched port analyzer (SPAN) port of network devices 240. Additionally or alternatively, interfaces 218 and 222 may interface with links 236 and 244 via tap devices 238 and 242. For example, packet-filtering system 200 may provision tap device 238 with one or more of rules 212 configured to cause tap device 238 to identify packets traversing link 236 that correspond to specified criteria and route (or forward) the packets (or copies thereof) to interface 218, and packet-filtering system 200 may provision tap device 242 with one or more of rules 212 configured to cause tap device 242 to identify packets traversing link 244 that correspond to specified criteria and route (or forward) the packets (or copies thereof) to interface 222. Similarly, interfaces 226 and 234 may interface directly with links 246 and 254, respectively; network devices 250 may provide interface 230 with access to (or copies of) packets traversing one or more of links 246 and 254; packet-filtering system 200 may provision tap device 248 with one or more of rules 212 configured to cause tap device 248 to identify packets traversing link 246 that correspond to specified criteria and route (or forward) the packets (or copies thereof) to interface 228; and packet-filtering system 200 may provision tap device 252 with one or more of rules 212 configured to cause tap device 252 to identify packets traversing link 254 that correspond to specified criteria and route (or forward) the packets (or copies thereof) to interface 232. In some embodiments, packet-filtering system 200 may comprise one or more of tap devices 238, 242, 248, and 252 or network devices 240 and 250.

FIGS. 3A-C, 4A-C, 5A-B, and 6A-B depict illustrative event sequences for rule-based network-threat detection for encrypted communications in accordance with one or more aspects of the disclosure. The depicted steps are merely illustrative and may be omitted, combined, or performed in an order other than that depicted; the numbering of the steps is merely for ease of reference and does not imply any particular ordering is necessary or preferred.

Referring to FIG. 3A, at step #1, threat-intelligence providers 140 may communicate one or more threat-intelligence reports to rule providers 138. The threat-intelligence reports may include one or more network-threat indicators, for example, domain names (e.g., fully qualified domain names (FQDNs)), URIs, network addresses, or the like. At step #2, rule providers 138 may utilize the threat-intelligence reports to generate one or more packet-filtering rules configured to identify packets comprising data corresponding to the network-threat indicators. At step #3, rule providers 138 may communicate the packet-filtering rules to rule gate 120. As indicated by the crosshatched boxes over the lines extending downward from network 104, rule gate 128, and gateway 134, the packet-filtering rules may traverse network 104, rule gate 128, and gateway 134. For example, network 104 and gateway 134 may interface rule providers 138 and rule gate 120, and rule gate 128 may interface a communication link interfacing network 104 and gateway 134. Rule gate 120 may receive the packet-filtering rules generated by rule providers 138 and, at step #4, may utilize the received packet-filtering rules to configure rules 212 to cause packet-filtering system 200 to identify packets comprising data corresponding to at least one of the plurality of network-threat indicators.

At step #5, host 106 may generate a request. For example, host 106 may execute a web browser, and the web browser may generate a request in response to user input (e.g., navigation of the web browser to a URI). The request may comprise a domain name, and host 106 may generate a DNS query comprising the domain name and, at step #6, may communicate the DNS query toward DNS 130. Rule gate 126 may interface a communication link interfacing host 106 and DNS 130, the domain name included in the request may correspond to one or more of the network-threat indicators, and rules 212 may be configured to cause rule gate 126 to one or more of identify one or more packets comprising the DNS query, determine that the packets comprise the domain name corresponding to the network-threat indicators, and responsive to one or more of identifying the packets or determining that the packets comprise the domain name corresponding to the network-threat indicators, one or more of log (as indicated by the diamond-patterned box over the line extending downward from rule gate 126) or drop the packets. Rule gate 126 may generate log data (e.g., one or more entries in logs 214) for the packets. For example, the packets may comprise a network address of host 106 (e.g., as a source address in their network-layer headers), and rule gate 126 may generate log data indicating the network address of host 106. As depicted by step #6A, the packets may be communicated to DNS 130. In some embodiments, rules 212 may be configured to cause rule gate 126 to, responsive to one or more of identifying the packets or determining that the packets comprise the domain name corresponding to the network-threat indicators, drop the packets, preventing them from reaching DNS 130, as depicted by step #6B.

DNS 130 may generate a reply to the DNS query and, at step #7, may communicate the reply toward host 106. The reply may comprise the domain name corresponding to the network-threat indicators, and rules 212 may be configured to cause rule gate 126 to one or more of identify one or more packets comprising the reply, determine that the packets comprise the domain name corresponding to the network-threat indicators, and responsive to one or more of identifying the packets or determining that the packets comprise the domain name corresponding to the network-threat indicators, one or more of log or drop the packets. Rule gate 126 may generate log data (e.g., one or more entries in logs 214) for the packets. For example, the packets may comprise the network address of host 106 (e.g., as a destination address in

their network-layer headers), and rule gate **126** may generate log data indicating the network address of host **106**. Similarly, the domain name may correspond to host **142**, the packets may comprise a network address of host **142** (e.g., DNS **130** may have resolved the domain name included in the query to the network address of host **142**), and rule gate **126** may generate log data indicating the network address of host **142**. As depicted by step #7A, the packets may be communicated to host **106**. In some embodiments, rules **212** may be configured to cause rule gate **126** to, responsive to determining that the packets comprise the domain name corresponding to the network-threat indicators, drop the packets, preventing them from reaching host **106**, as depicted by step #7B.

Packet-filtering system **200** may be configured to correlate packets identified by packet-filtering system **200** (e.g., the packets comprising the reply to the DNS query) with packets previously identified by packet-filtering system **200** (e.g., the packets comprising the DNS query). For example, packet-filtering system **200** may be configured to determine that packets identified by packet-filtering system **200** (e.g., the packets comprising the reply to the DNS query) are one or more of associated with, related to, or the product of packets previously identified by packet-filtering system **200** (e.g., the packets comprising the DNS query). Packet-filtering system **200** may be configured to correlate packets identified by packet-filtering system **200** with packets previously identified by packet-filtering system **200** based on data stored in logs **214** (e.g., the log data generated by rule gate **126** in steps #**6** and #**7**).

For example, for one or more packets logged by packet-filtering system **200** (e.g., the packets comprising the DNS query or the packets comprising the reply to the DNS query), logs **214** may comprise one or more entries indicating one or more of network-layer information (e.g., information derived from one or more network-layer header fields of the packets, such as a protocol type, a destination network address, a source network address, a signature or authentication information (e.g., information from an Internet protocol security (IPsec) encapsulating security payload (ESP)), or the like), transport-layer information (e.g., a destination port, a source port, a checksum or similar data (e.g., error detection or correction values, such as those utilized by the transmission control protocol (TCP) or the user datagram protocol (UDP)), or the like), application-layer information (e.g., information derived from one or more application-layer header fields of the packets, such as a domain name, a uniform resource locator (URL), a uniform resource identifier (URI), an extension, a method, state information, media-type information, a signature, a key, a timestamp, an application identifier, a session identifier, a flow identifier, sequence information, authentication information, or the like), other data in the packets (e.g., payload data), or one or more environmental variables (e.g., information associated with but not solely derived from the packets themselves, such as one or more arrival (or receipt) or departure (or transmission) times of the packets (e.g., at or from one or more of rule gates **120**, **122**, **124**, **126**, or **128**, tap devices **238**, **242**, **248**, or **252**, or network devices **240** or **250**), one or more ingress or egress identifiers (e.g., associated with one or more physical or logical network interfaces, ports, or communication-media types of one or more of rule gates **120**, **122**, **124**, **126**, or **128**, tap devices **238**, **242**, **248**, or **252**, or network devices **240** or **250** via which the packets were one or more of received or transmitted), one or more device identifiers (e.g., associated with one or more of rule gates **120**, **122**, **124**, **126**, or **128**, tap devices **238**, **242**, **248**, or **252**, or network devices **240** or **250** via which the packets were one or more of received or transmitted), or the like), and packet-filtering system **200** may utilize such entries to correlate one or more packets identified by packet-filtering system **200** with one or more packets previously identified by packet-filtering system **200**.

In some embodiments, packet-filtering system **200** may implement one or more aspects of the technology described in U.S. patent application Ser. No. 14/618,967, filed Feb. 10, 2015, and entitled "CORRELATING PACKETS IN COMMUNICATIONS NETWORKS," the disclosure of which is incorporated by reference herein in its entirety and made part hereof, or similar technology (e.g., to correlate one or more packets identified by packet-filtering system **200** with one or more packets previously identified by packet-filtering system **200**).

Host **106** may generate one or more packets destined for host **142** comprising data (e.g., a TCP:SYN handshake message) configured to establish a connection (e.g., a TCP connection or tunnel) between hosts **106** and **142** and, at step #**8**, may communicate the packets toward host **142**. Rule gate **120** may interface a communication link interfacing hosts **106** and **142**, and rules **212** may be configured to cause rule gate **120** to one or more of identify the packets or determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more of the packets comprising the DNS query or the reply to the DNS query based on data stored in logs **214** (e.g., the log data generated by rule gate **126** in one or more of steps #**6** or #**7**).

At step #**9**, rule gate **120** may route the packets comprising the data configured to establish the connection between hosts **106** and **142** to proxy device **112** and, at step #**10**, may communicate the packets to proxy device **112**. For example, rules **212** may be configured to cause rule gate **120** to route the packets to proxy device **112** based on data in the packets, for example, one or more ports (e.g., port **443**) indicated by transport-layer headers in the packets, indicating the connection between hosts **106** and **142** will be utilized to establish an encrypted communication session or tunnel (e.g., a session established in accordance with the transport layer security (TLS) protocol, secure sockets layer (SSL) protocol, secure shell (SSH) protocol, or the like). In some embodiments, rules **212** may be configured to cause rule gate **120** to route the packets to proxy device **112** based on a determination that one or more of hosts **106** or **142** is associated with a network address for which rules **212** indicate encrypted communications should be established via one or more of proxy devices **112**, **114**, or **116**. For example, proxy devices **112**, **114**, and **116** may be part of a proxy system (e.g., a SSL/TLS proxy system) that enables packet-filtering system **200** to filter packets comprising encrypted data based on information within the encrypted data, and rules **212** may be configured to cause rule gate **120** to route the packets to proxy device **112** based on a determination that host **142** is associated with a network address of a domain corresponding to the network-threat indicators.

Additionally or alternatively, network **102** may include one or more hosts for which rules **212** indicate connections utilized to establish encrypted communication sessions (e.g., connections with hosts corresponding to network-threat indicators) should be established via one or more of proxy devices **112**, **114**, or **116**, as well as one or more hosts for which rules **212** indicate connections utilized to establish encrypted communication sessions should not be established

via one or more of proxy devices **112**, **114**, and **116**, for example, hosts that generate sensitive data (e.g., personally identifiable information (PII)), inspection of which may present privacy or regulatory concerns (e.g., data subject to the health insurance portability and accountability act (HIPAA), or the like), and rules **212** may be configured to cause rule gate **120** to route the packets to proxy device **112** based on a determination that host **106** is associated with a network address for which rules **212** indicate encrypted communications should be established via one or more of proxy devices **112**, **114**, or **116**.

For example, link **236** may interface host **106** with rule gate **120**, link **244** may interface rule gate **120** with host **142**, link **246** may interface rule gate **120** with proxy device **112**, link **254** may interface proxy devices **112** and **114** and may comprise a communication link internal to a proxy system comprising proxy devices **112** and **114**, and rules **212** may be configured to cause rule gate **120** to route (or redirect) packets received from host **106** via one or more of interfaces **216**, **218**, or **220** and destined for host **142** (or a portion thereof (e.g., packets comprising data configured to establish a connection between hosts **106** and **142** and indicating the connection will be utilized to establish an encrypted communication session)) to host **142** via interface **226**. Additionally or alternatively, rules **212** may be configured to cause rule gate **120** to forward copies of (or mirror) packets received from host **106** via one or more of interfaces **216**, **218**, **220**, or **222** and destined for host **142** (or a portion thereof (e.g., packets comprising data configured to establish a connection between hosts **106** and **142** and indicating the connection will be utilized to establish an encrypted communication session)) to proxy device **112** via interface **226**.

At step #**11**, proxy devices **112** and **114** may exchange one or more parameters determined from the packets comprising the data configured to establish the connection between hosts **106** and **142**, for example, one or more network addresses in network-layer headers of the packets (e.g., network addresses of hosts **106** and **142**) or ports indicated by transport-layer headers in the packets (e.g., indicating the type of encrypted communication session the connection will be utilized to establish). Proxy device **112** may utilize the parameters to generate packets comprising data configured to establish a connection between proxy device **112** and host **106** (e.g., a TCP:SYN-ACK handshake message) and, at step #**12**, may communicate the packets to host **106**. Rules **212** may be configured to cause rule gate **120** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more of the packets comprising the DNS query or the reply to the DNS query based on data stored in logs **214** (e.g., the log data generated by rule gate **126** in one or more of steps #**6** or #**7**), and one or more of log or drop the packets.

Similarly, proxy device **114** may utilize the parameters to generate packets comprising data configured to establish a connection between proxy device **114** and host **142** (e.g., a TCP:SYN handshake message) and, at step #**13**, may communicate the packets to host **142**. Rule gate **128** may interface a communication link interfacing proxy device **114** and host **142**, and rules **212** may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of steps #**6**, #**7**, or #**12**), and one or more of log or drop the packets.

Responsive to receiving the packets from proxy device **112**, host **106** may generate packets comprising data configured to establish the connection between proxy device **112** and host **106** (e.g., a TCP:ACK handshake message) and, at step #**14**, may communicate the packets to proxy device **112**. Rules **212** may be configured to cause rule gate **120** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of steps #**6**, #**7**, #**12**, or #**13**), and one or more of log or drop the packets.

Responsive to receiving the packets from proxy device **114**, host **142** may generate packets comprising data configured to establish the connection between proxy device **114** and host **142** (e.g., a TCP:SYN-ACK handshake message) and, at step #**15**, may communicate the packets to proxy device **114**. Rules **212** may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**, **7**, or **12-14**), and one or more of log or drop the packets.

Responsive to receiving the packets from host **142**, proxy device **114** may generate packets comprising data configured to establish the connection between proxy device **114** and host **142** (e.g., a TCP:ACK handshake message) and, at step #**16**, may communicate the packets to host **142**. Rules **212** may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**, **7**, or **12-15**), and one or more of log or drop the packets.

Referring to FIG. **3**B, proxy device **112** may receive the packets comprising data configured to establish the connection between proxy device **112** and host **106** communicated by host **106** in step #**14**, and connection **302** (e.g., a TCP connection) between proxy device **112** and host **106** may be established. Similarly, host **142** may receive the packets comprising data configured to establish the connection between proxy device **114** and host **142** communicated by proxy device **114** in step #**16**, and connection **304** (e.g., a TCP connection) between proxy device **114** and host **142** may be established.

At step #**17**, proxy device **112** and host **106** may communicate packets comprising data configured to establish encrypted communication session **306** (e.g., a SSL/TLS

session) between proxy device **112** and host **106** via connection **302**. Rules **212** may be configured to cause rule gate **120** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**, **7**, or **12-16**), and one or more of log or drop the packets. Additionally or alternatively, rules **212** may be configured to cause rule gate **120** to one or more of identify the packets or determine that the packets comprise data corresponding to the network-threat indicators based on data included in the packets. For example, in some embodiments, host **106** may comprise a client (e.g., web browser), host **142** may comprise a server (e.g., web server), the packets may comprise one or more handshake messages configured to establish session **306** that comprise unencrypted data including a domain name corresponding to the network-threat indicators, for example, a hello message generated by the client (e.g., including the domain name in the server name indication extension, or the like) or a certificate message generated by the server (e.g., including the domain name in one or more of the subject common name field or the extension subjectAltName (of type dNSName), or the like), and rules **212** may be configured to cause rule gate **120** to one or more of identify the packets or determine that the packets comprise data corresponding to the network-threat indicators based on data included in the one or more handshake messages configured to establish session **306**. In such embodiments, rules **212** may be configured to cause packet-filtering system **200** to one or more of identify the packets or determine that the packets comprise data corresponding to the network-threat indicators based on the certificate message comprising other data (e.g., in addition to or in lieu of the domain name) corresponding to one or more of the network-threat indicators, for example, data indicating at least one of a serial number (or type thereof) indicated by rules **212**, an issuer (or type thereof) indicated by rules **212**, a validity time-range (or type thereof) indicated by rules **212**, a key (or type thereof) indicated by rules **212**, a digital signature (e.g., fingerprint) (or type thereof) indicated by rules **212**, or a signing authority (or type thereof) indicated by rules **212**.

Similarly, at step #**18**, proxy device **114** and host **142** may communicate packets comprising data configured to establish encrypted communication session **308** (e.g., a SSL/TLS session) between proxy device **114** and host **142** via connection **304**, and rules **212** may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**, **7**, or **12-17**) or the packets comprising one or more handshake messages configured to establish session **308** that comprise unencrypted data (e.g., including the domain name) corresponding to the network-threat indicators, and one or more of log or drop the packets.

Host **106** may generate packets comprising data encrypted in accordance with one or more parameters of session **306** and, at step #**19**, may communicate the packets to proxy device **112** via session **306**. Rules **212** may be configured to cause rule gate **120** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**, **7**, or **12-18**), and one or more of log (as indicated by the triangles over the line extending downward from rule gate **120**) or drop the packets.

Proxy device **112** may receive the packets and decrypt the data in accordance with the parameters of session **306**. The packets may comprise a request (e.g., a hypertext transfer protocol (HTTP) request), and proxy device **112** may comprise an ICAP client, which, at step #**20**, may communicate the packets to ICAP server **132**. Rule gate **126** may interface a communication link interfacing proxy device **112** and ICAP server **132**, and rules **212** may be configured to cause rule gate **126** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**, **7**, or **12-19**), and one or more of log or drop the packets.

ICAP server **132** may generate packets comprising data responsive to the request (e.g., a response, modified request, or the like) and, at step #**21**, may communicate the packets to proxy device **112**. Rules **212** may be configured to cause rule gate **126** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**, **7**, or **12-20**), and one or more of log or drop the packets. Additionally or alternatively, rules **212** may be configured to cause rule gate **126** to one or more of identify the packets or determine that the packets comprise data corresponding to the network-threat indicators based on data included in the packets, for example, the data responsive to the request (e.g., a modified request) may comprise data (e.g., a domain name, URI, or the like) corresponding to the network-threat indicators.

Proxy device **112** may generate packets (e.g., based on the data generated by ICAP server **132**) and, at step #**22**, may communicate the packets to proxy device **114**. Rule gate **124** may interface a communication link internal to the proxy system comprising proxy devices **112** and **114**, and thus packets traversing the communication link may comprise unencrypted data (e.g., rule gate **124** may be "the man in the middle" of proxy devices **112** and **114**), and rules **212** may be configured to cause rule gate **124** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-

threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**, **7**, or **12-21**), and one or more of log or drop the packets.

Additionally or alternatively, rules **212** may be configured to cause rule gate **124** to one or more of identify the packets or determine that the packets comprise data corresponding to the network-threat indicators based on data included in the packets, for example, unencrypted data in the packets corresponding to one or more of the network-threat indicators. For example, in some embodiments, packet-filtering system **200** may implement one or more aspects of the technology described in U.S. patent application Ser. No. 13/795,822, filed Mar. 12, 2013, and entitled "FILTERING NETWORK DATA TRANSFERS," the disclosure of which is incorporated by reference herein in its entirety and made part hereof, or similar technology, and rules **212** may be configured to cause rule gate **124** to one or more of identify the packets or determine that the packets comprise data corresponding to the network-threat indicators based on the packets comprising one or more of a URI specified by rules **212**, data indicating a protocol version specified by rules **212**, data indicating a method specified by rules **212**, data indicating a request specified by rules **212**, or data indicating a command specified by rules **212**. Additionally or alternatively, rules **212** may be configured to cause rule gate **124** to one or more of identify the packets or determine that the packets comprise data corresponding to the one or more network-threat indicators based on unencrypted data in the packets comprising a URI meeting or exceeding a threshold size specified by rules **212** (e.g., a URI likely being utilized to exfiltrate data).

Proxy device **114** may receive the packets and generate one or more corresponding packets comprising data encrypted in accordance with one or more parameters of session **308** and, at step #**23**, may communicate the packets to host **142**. Rules **212** may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**, **7**, or **12-22**), and one or more of log or drop the packets.

Host **142** may generate one or more packets comprising data encrypted in accordance with one or more parameters of session **308** and, at step #**24**, may communicate the packets to proxy device **114**. Rules **212** may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**, **7**, or **12-23**), and one or more of log or drop the packets.

Proxy device **114** may receive the packets and generate one or more corresponding packets comprising unencrypted data and, at step #**25**, may communicate the packets to proxy device **112**. Rules **212** may be configured to cause rule gate **124** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**, **7**, or **12-24**), and one or more of log or drop the packets.

Proxy device **112** may receive the packets and generate one or more corresponding packets comprising data encrypted in accordance with one or more parameters of session **306** and, at step #**26**, may communicate the packets to host **106**. Rules **212** may be configured to cause rule gate **120** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**, **7**, or **12-25**), and one or more of log or drop the packets.

Host **106** may generate one or more packets comprising data encrypted in accordance with one or more parameters of session **306** and, at step #**27**, may communicate the packets toward proxy device **112**. Rules **212** may be configured to cause rule gate **120** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**, **7**, or **12-26**), and one or more of log or drop the packets.

Proxy device **112** may receive one or more of the packets and generate one or more corresponding packets comprising unencrypted data and, at step #**28**, may communicate the packets toward proxy device **114**. Rules **212** may be configured to cause rule gate **124** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**, **7**, or **12-27**), and one or more of log or drop the packets.

Proxy device **114** may receive one or more of the packets and generate one or more corresponding packets comprising data encrypted in accordance with one or more parameters of session **308** and, at step #**29**, may communicate the packets toward host **142**. Rules **212** may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or

more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**, **7**, or **12-28**), and one or more of log or drop the packets.

Host **142** may generate one or more packets comprising data encrypted in accordance with one or more parameters of session **308** and, at step #**30**, may communicate the packets toward proxy device **114**. Rules **212** may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**, **7**, or **12-29**), and one or more of log or drop the packets.

Proxy device **114** may receive one or more of the packets and generate one or more corresponding packets comprising unencrypted data and, at step #**31**, may communicate the packets toward proxy device **112**. Rules **212** may be configured to cause rule gate **124** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**, **7**, or **12-30**), and one or more of log or drop the packets.

Proxy device **112** may receive one or more of the packets and generate one or more corresponding packets comprising data encrypted in accordance with one or more parameters of session **306** and, at step #**32**, may communicate the packets toward host **106**. Rules **212** may be configured to cause rule gate **120** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**, **7**, or **12-31**), and one or more of log or drop the packets.

Referring to FIG. **3**C, at step #**33**, rule gate **120** may one or more of update a console (or interface) associated with packet-filtering system **200** running on host **108** or receive one or more updates to rules **212** via the console. For example, the console may provide data regarding one or more threats to network **102** corresponding to the network-threat indicators, and rule gate **120** may update the console based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**, **7**, or **12-32**). In some embodiments, the console may provide data identifying network threats associated with one or more of hosts **106**, **108**, **110**, **142**, **144**, or **146**, and rule gate **120** may update data associated with one or more of hosts **106** or **142** based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**, **7**, or **12-32**).

At step #**34**, rule gate **120** may reconfigure rules **212** based on one or more of updates received via the console or data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**, **7**, or **12-32**). For example, packet-filtering system **200** may implement one or more aspects of the technology described in U.S. patent application Ser. No. 14/690,302, filed Apr. 17, 2015, and entitled "RULE-BASED NETWORK-THREAT DETECTION," the disclosure of which is incorporated by reference herein in its entirety and made part hereof, or similar technology, and rule gate **120** may reconfigure rules **212** based on one or more risk scores updated to reflect data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**, **7**, or **12-32**).

Host **106** may generate one or more packets comprising data encrypted in accordance with one or more parameters of session **306** and, at step #**35**, may communicate the packets toward proxy device **112**. Rules **212** (e.g., one or more of rules **212** reconfigured in step #**34**) may be configured to cause rule gate **120** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**, **7**, or **12-32**), and one or more of log or drop the packets.

Proxy device **112** may receive one or more of the packets and generate one or more corresponding packets comprising unencrypted data and, at step #**36**, may communicate the packets toward proxy device **114**. Rules **212** (e.g., one or more of rules **212** reconfigured in step #**34**) may be configured to cause rule gate **124** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**, **7**, **12-32**, or **35**), and one or more of log or drop the packets.

Proxy device **114** may receive one or more of the packets and generate one or more corresponding packets comprising data encrypted in accordance with one or more parameters of session **308** and, at step #**37**, may communicate the packets toward host **142**. Rules **212** (e.g., one or more of rules **212** reconfigured in step #**34**) may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**, **7**, **12-32**, **35**, or **36**), and one or more of log or drop the packets.

Host **142** may generate one or more packets comprising data encrypted in accordance with one or more parameters of session **308** and, at step #**38**, may communicate the packets toward proxy device **114**. Rules **212** (e.g., one or more of rules **212** reconfigured in step #**34**) may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**, **7**, **12-32**, or **35-37**), and one or more of log or drop the packets.

Proxy device **114** may receive one or more of the packets and generate one or more corresponding packets comprising unencrypted data and, at step #**39**, may communicate the packets toward proxy device **112**. Rules **212** (e.g., one or more of rules **212** reconfigured in step #**34**) may be configured to cause rule gate **124** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**, **7**, **12-32**, or **35-38**), and one or more of log or drop the packets.

Proxy device **112** may receive one or more of the packets and generate one or more corresponding packets comprising data encrypted in accordance with one or more parameters of session **306** and, at step #**40**, may communicate the packets toward host **106**. Rules **212** (e.g., one or more of rules **212** reconfigured in step #**34**) may be configured to cause rule gate **120** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**, **7**, **12-32**, or **35-39**), and one or more of log or drop the packets.

Host **142** may generate one or more packets destined for one or more of hosts **106**, **108**, or **110** and, at step #**41**, may communicate the packets toward gateway **134**. Rules **212** (e.g., one or more of rules **212** reconfigured in step #**34**) may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**, **7**, **12-32**, or **35-40**), and one or more of log or drop the packets.

Host **108** may generate one or more packets and, at step #**42**, may communicate the packets to host **142**. Rules **212** (e.g., one or more of rules **212** reconfigured in step #**34**) may be configured to cause rule gates **120** and **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**, **7**, **12-32**, or **35-41**), and one or more of log or drop the packets.

Host **106** may generate one or more packets destined for hosts **108**, **142**, **144**, and **146** and, at step #**43**, may communicate the packets toward hosts **108**, **142**, **144**, and **146**. Rules **212** (e.g., one or more of rules **212** reconfigured in step #**34**) may be configured to cause rule gate **120** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**, **7**, **12-32**, or **35-42**), and one or more of log or drop the packets.

Referring to FIG. **4**A, step #s **1-5** substantially correspond to step #s **1-5** of FIG. **3**A.

Host **106** (e.g., the web browser) may be configured to utilize web proxy **118** and responsive to the request, may generate packets comprising data configured to establish a connection between host **106** and web proxy **118** (e.g., a TCP:SYN handshake message) and, at step #**6**, may communicate the packets to web proxy **118**. Rule gate **120** may interface a communication link interfacing host **106** and web proxy **118**, and rules **212** may be configured to cause rule gate **120** to one or more of identify the packets, for example, based on one or more network addresses included in their network-layer headers (e.g., a network address of web proxy **118**) or one or more ports (e.g., port **80**) indicated by transport-layer headers in the packets, and one or more of log or drop the packets.

Responsive to receiving the packets from host **106**, web proxy **118** may generate packets comprising data configured to establish the connection between host **106** and web proxy **118** (e.g., a TCP:SYN-ACK handshake message) and, at step #**7**, may communicate the packets to host **106**. Rules **212** may be configured to cause rule gate **120** to one or more of identify the packets, for example, based on one or more network addresses included in their network-layer headers (e.g., a network address of web proxy **118**) or one or more ports (e.g., port **80**) indicated by transport-layer headers in the packets, and one or more of log or drop the packets.

Responsive to receiving the packets from web proxy **118**, host **106** may generate packets comprising data configured to establish the connection between host **106** and web proxy **118** (e.g., a TCP:ACK handshake message) and, at step #**8**, may communicate the packets to web proxy **118**. Rules **212** may be configured to cause rule gate **120** to one or more of identify the packets, for example, based on one or more network addresses included in their network-layer headers (e.g., a network address of web proxy **118**) or one or more ports (e.g., port **80**) indicated by transport-layer headers in the packets, and one or more of log or drop the packets.

Web proxy **118** may receive the packets from host **106**, and connection **402** (e.g., a TCP connection) between host **106** and web proxy **118** may be established. Host **106** may

generate packets comprising a request (e.g., an HTTP CONNECT request), and, at step #**9**, may communicate the packets to web proxy **118** via connection **402**. Rules **212** may be configured to cause rule gate **120** to one or more of identify the packets, for example, based on one or more network addresses included in their network-layer headers (e.g., a network address of web proxy **118**) or one or more ports (e.g., port **80**) indicated by transport-layer headers in the packets, determine the packets comprise data corresponding to the network-threat indicators, for example, a domain name (e.g., FQDN) in the request, and one or more of log or drop the packets.

Web proxy **118** may generate a DNS query comprising the domain name and, at step #**10**, may communicate the DNS query toward DNS **130**. The domain name included in the request may correspond to one or more of the network-threat indicators, and rules **212** may be configured to cause rule gate **126** to one or more of identify one or more packets comprising the DNS query, determine that the packets comprise the domain name corresponding to the network-threat indicators, and one or more of log or drop the packets. For example, the packets may comprise a network address of web proxy **118** (e.g., as a source address in their network-layer headers), and rule gate **126** may generate log data indicating the network address of web proxy **118**. As depicted by step #**10**A, the packets may be communicated to DNS **130**. In some embodiments, rules **212** may be configured to cause rule gate **126** to, responsive to determining that the packets comprise the domain name corresponding to the network-threat indicators, drop the packets, preventing them from reaching DNS **130**, as depicted by step #**10**B.

DNS **130** may generate a reply to the DNS query and, at step #**11**, may communicate the reply toward web proxy **118**. The reply may comprise the domain name corresponding to the network-threat indicators, and rules **212** may be configured to cause rule gate **126** to one or more of identify one or more packets comprising the reply, determine that the packets comprise the domain name corresponding to the network-threat indicators, and one or more of log or drop the packets. For example, the packets may comprise the network address of web proxy **118** (e.g., as a destination address in their network-layer headers), and rule gate **126** may generate log data indicating the network address of web proxy **118**. Similarly, the domain name may correspond to host **142**, the packets may comprise a network address of host **142** (e.g., DNS **130** may have resolved the domain name included in the query to the network address of host **142**), and rule gate **126** may generate log data indicating the network address of host **142**. As depicted by step #**11**A, the packets may be communicated to web proxy **118**. In some embodiments, rules **212** may be configured to cause rule gate **126** to, responsive to determining that the packets comprise the domain name corresponding to the network-threat indicators, drop the packets, preventing them from reaching web proxy **118**, as depicted by step #**11**B.

Web proxy **118** may generate one or more packets destined for host **142** comprising data (e.g., a TCP:SYN handshake message) configured to establish a connection (e.g., a TCP connection or tunnel) between web proxy **118** and host **142** and, at step #**12**, may communicate the packets toward host **142**. Rule gate **122** may interface a communication link interfacing web proxy **118** and host **142**, and rules **212** may be configured to cause rule gate **122** to one or more of identify the packets or determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more of the packets comprising the request, the DNS query, or the reply to the DNS query based on data stored in logs **214** (e.g., the log data generated by rule gates **120** and **126** in one or more of step #s **6-11**).

At step #**13**, rule gate **122** may route the packets comprising the data configured to establish the connection between web proxy **118** and host **142** to proxy device **112** and, at step #**14**, may communicate the packets to proxy device **112**. For example, rules **212** may be configured to cause rule gate **122** to route the packets to proxy device **112** based on data in the packets, for example, one or more ports (e.g., port **443**) indicated by transport-layer headers in the packets, indicating the connection between web proxy **118** and host **142** will be utilized to establish an encrypted communication session or tunnel (e.g., a session established in accordance with the transport layer security (TLS) protocol, secure sockets layer (SSL) protocol, secure shell (SSH) protocol, or the like).

Referring to FIG. **4**B, at step #**15**, proxy devices **112** and **114** may exchange one or more parameters determined from the packets comprising the data configured to establish the connection between web proxy **118** and host **142**, for example, one or more network addresses in network-layer headers of the packets (e.g., network addresses of web proxy **118** and host **142**) or ports indicated by transport-layer headers in the packets (e.g., indicating the type of encrypted communication session the connection will be utilized to establish). Proxy device **112** may utilize the parameters to generate packets comprising data configured to establish a connection between proxy device **112** and web proxy **118** (e.g., a TCP:SYN-ACK handshake message) and, at step #**16**, may communicate the packets to web proxy **118**. Rules **212** may be configured to cause rule gate **122** to one or more of identify the packets or determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more of the packets comprising the request, the DNS query, or the reply to the DNS query based on data stored in logs **214** (e.g., the log data generated by rule gates **120** and **126** in one or more of step #s **6-11**).

Similarly, proxy device **114** may utilize the parameters to generate packets comprising data configured to establish a connection between proxy device **114** and host **142** (e.g., a TCP:SYN handshake message) and, at step #**17**, may communicate the packets to host **142**. Rules **212** may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6-11** or **16**), and one or more of log or drop the packets.

Responsive to receiving the packets from proxy device **112**, web proxy **118** may generate packets comprising data configured to establish the connection between proxy device **112** and web proxy **118** (e.g., a TCP:ACK handshake message) and, at step #**18**, may communicate the packets to proxy device **112**. Rules **212** may be configured to cause rule gate **122** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example,

by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6-11**, **16**, or **17**), and one or more of log or drop the packets.

Responsive to receiving the packets from proxy device **114**, host **142** may generate packets comprising data configured to establish the connection between proxy device **114** and host **142** (e.g., a TCP:SYN-ACK handshake message) and, at step #**19**, may communicate the packets to proxy device **114**. Rules **212** may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6-11** or **16-18**), and one or more of log or drop the packets.

Responsive to receiving the packets from host **142**, proxy device **114** may generate packets comprising data configured to establish the connection between proxy device **114** and host **142** (e.g., a TCP:ACK handshake message) and, at step #**20**, may communicate the packets to host **142**. Rules **212** may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6-11** or **16-19**), and one or more of log or drop the packets.

Proxy device **112** may receive the packets comprising data configured to establish the connection between proxy device **112** and web proxy **118** communicated by web proxy **118** in step #**18**, and connection **404** (e.g., a TCP connection) between proxy device **112** and web proxy **118** may be established. Similarly, host **142** may receive the packets comprising data configured to establish the connection between proxy device **114** and host **142** communicated by proxy device **114** in step #**20**, and connection **406** (e.g., a TCP connection) between proxy device **114** and host **142** may be established.

At step #**21**, proxy device **112** and host **106** may communicate packets comprising data configured to establish encrypted communication session **408** (e.g., a SSL/TLS session) between proxy device **112** and host **106** via connections **402** and **404**. Rules **212** may be configured to cause one or more of rule gates **120** or **122** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6-11** or **16-20**) or the packets comprising one or more handshake messages configured to establish session **408** that comprise unencrypted data (e.g., including the domain name) corresponding to the network-threat indicators. and one or more of log or drop the packets.

Similarly, at step #**22**, proxy device **114** and host **142** may communicate packets comprising data configured to establish encrypted communication session **410** (e.g., a SSL/TLS session) between proxy device **114** and host **142** via connection **406**, and rules **212** may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6-11** or **16-21**) or the packets comprising one or more handshake messages configured to establish session **410** that comprise unencrypted data (e.g., including the domain name) corresponding to the network-threat indicators, and one or more of log or drop the packets.

Referring to FIGS. **4**B-C, step #s **23-47** substantially correspond to step #s **19-43** of FIGS. **3**B-C; however, rules **212** may be configured to cause one or more of rule gates **120** or **122** to one or more of identify, drop, or log the packets communicated in one or more of step #s **23**, **30**, **31**, **36**, **39**, or **44** of FIGS. **4**B-C.

Referring to FIG. **5**A, step #s **1-7** substantially correspond to step #s **1-7** of FIG. **3**A.

Host **106** may generate one or more packets destined for host **142** comprising data (e.g., a TCP:SYN handshake message) configured to establish a connection (e.g., a TCP connection or tunnel) between hosts **106** and **142** and, at step #**8**, may communicate the packets to host **142**. Rules **212** may be configured to cause one or more of rule gates **120** or **128** to one or more of identify the packets or determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more of the packets comprising the DNS query or the reply to the DNS query based on data stored in logs **214** (e.g., the log data generated by rule gate **126** in one or more of steps #**6** or #**7**).

Responsive to receiving the packets from host **106**, host **142** may generate packets comprising data configured to establish the connection between hosts **106** and **142** (e.g., a TCP:SYN-ACK handshake message) and, at step #**9**, may communicate the packets to host **106**. Rules **212** may be configured to cause one or more of rule gates **120** or **128** to one or more of identify the packets or determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more of the packets comprising the DNS query or the reply to the DNS query based on data stored in logs **214** (e.g., the log data generated by rule gate **126** in one or more of steps #**6** or #**7**).

Responsive to receiving the packets from host **142**, host **106** may generate packets comprising data configured to establish the connection between hosts **106** and **142** (e.g., a TCP:ACK handshake message) and, at step #**10**, may communicate the packets to host **142**. Rules **212** may be configured to cause one or more of rule gates **120** or **128** to one or more of identify the packets or determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating

the packets with one or more of the packets comprising the DNS query or the reply to the DNS query based on data stored in logs **214** (e.g., the log data generated by rule gate **126** in one or more of steps #**6** or #**7**).

Host **142** may receive the packets comprising data configured to establish the connection between hosts **106** and **142** communicated by host **106** in step #**10**, and connection **502** (e.g., a TCP connection) between hosts **106** and **142** may be established.

At step #**11**, hosts **106** and **142** may communicate packets comprising data configured to establish encrypted communication session **504** (e.g., a SSL/TLS session) between hosts **106** and **142** via connection **502**. Rules **212** may be configured to cause one or more of rule gates **120** or **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6-10**) or the packets comprising one or more handshake messages configured to establish session **504** that comprise unencrypted data (e.g., including the domain name) corresponding to the network-threat indicators, and one or more of log or drop the packets.

Host **106** may generate packets comprising data encrypted in accordance with one or more parameters of session **504** and, at step #**12**, may communicate the packets to host **142**. Rules **212** may be configured to cause one or more of rule gates **120** or **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6-11**), and one or more of log or drop the packets.

Host **142** may generate packets comprising data encrypted in accordance with one or more parameters of session **504** and, at step #**13**, may communicate the packets to host **106**. Rules **212** may be configured to cause one or more of rule gates **120** or **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6-12**), and one or more of log or drop the packets.

Host **106** may generate packets comprising data encrypted in accordance with one or more parameters of session **504** and, at step #**14**, may communicate the packets toward host **142**. Rules **212** may be configured to cause one or more of rule gates **120** or **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6-13**), and one or more of log or drop the packets.

Host **142** may generate packets comprising data encrypted in accordance with one or more parameters of session **504** and, at step #**15**, may communicate the packets toward host **106**. Rules **212** may be configured to cause one or more of rule gates **120** or **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6-14**), and one or more of log or drop the packets.

Referring to FIG. **5**B, steps #**16** and #**17** substantially correspond to steps #**33** and #**34** of FIG. **3**C.

Host **106** may generate packets comprising data encrypted in accordance with one or more parameters of session **504** and, at step #**18**, may communicate the packets toward host **142**. Rules **212** (e.g., one or more of rules **212** reconfigured in step #**17**) may be configured to cause one or more of rule gates **120** or **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6-15**), and one or more of log or drop the packets.

Host **142** may generate packets comprising data encrypted in accordance with on or more parameters of session **504** and, at step #**19**, may communicate the packets toward host **106**. Rules **212** (e.g., one or more of rules **212** reconfigured in step #**17**) may be configured to cause one or more of rule gates **120** or **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6-15** and **18**), and one or more of log or drop the packets.

Step #s **20-22** substantially correspond to step #s **41-43** of FIG. **3**C.

Referring to FIG. **6**A, step #s **1-11** substantially correspond to step #s **1-11** of FIG. **4**A.

Web proxy **118** may generate one or more packets destined for host **142** comprising data (e.g., a TCP:SYN handshake message) configured to establish a connection (e.g., a TCP connection or tunnel) between web proxy **118** and host **142** and, at step #**12**, may communicate the packets to host **142**. Rules **212** may be configured to cause one or more of rule gates **122** or **128** to one or more of identify the packets or determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more of the packets comprising the DNS query or the reply

to the DNS query based on data stored in logs **214** (e.g., the log data generated by rule gate **126** in one or more of steps #**10** or #**11**).

Responsive to receiving the packets from web proxy **118**, host **142** may generate packets comprising data configured to establish the connection between web proxy **118** and host **142** (e.g., a TCP:SYN-ACK handshake message) and, at step #**13**, may communicate the packets to web proxy **118**. Rules **212** may be configured to cause one or more of rule gates **122** or **128** to one or more of identify the packets or determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more of the packets comprising the DNS query or the reply to the DNS query based on data stored in logs **214** (e.g., the log data generated by rule gate **126** in one or more of steps #**10** or #**11**).

Responsive to receiving the packets from host **142**, web proxy **118** may generate packets comprising data configured to establish the connection between web proxy **118** and host **142** (e.g., a TCP:ACK handshake message) and, at step #**14**, may communicate the packets to host **142**. Rules **212** may be configured to cause one or more of rule gates **122** or **128** to one or more of identify the packets or determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more of the packets comprising the DNS query or the reply to the DNS query based on data stored in logs **214** (e.g., the log data generated by rule gate **126** in one or more of steps #**10** or #**11**).

Referring to FIG. **6**B, host **142** may receive the packets comprising data configured to establish the connection between web proxy **118** and host **142** communicated by web proxy **118** in step #**14**, and connection **604** (e.g., a TCP connection) between web proxy **118** and host **142** may be established.

At step #**15**, hosts **106** and **142** may communicate packets comprising data configured to establish encrypted communication session **606** (e.g., a SSL/TLS session) between hosts **106** and **142** via connections **602** and **604**. Rules **212** may be configured to cause one or more of rule gates **120**, **122**, or **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of step #s **6**-**15**) or the packets comprising one or more handshake messages configured to establish session **606** that comprise unencrypted data (e.g., including the domain name) corresponding to the network-threat indicators, and one or more of log or drop the packets.

Step #s **16**-**26** substantially correspond to step #s **12**-**22** of FIGS. **5**A-B; however, rules **212** may be configured to cause one or more of rule gates **120**, **122**, or **128** to one or more of identify, drop, or log the packets communicated in one or more of step #s **16**-**19**, **22**, or **23** of FIG. **6**B.

FIG. **7** depicts an illustrative method for rule-based network-threat detection for encrypted communications in accordance with one or more aspects of the disclosure. Referring to FIG. **7**, in step **702**, a packet-filtering system may receive data indicating network-threat indicators. For example, packet-filtering system **200** may receive packet-filtering rules generated by rule provides **138** based on network-threat indicators provided by threat-intelligence providers **140**. In step **704**, the packet-filtering system may configure packet-filtering rules in accordance with which it is configured to filter packets. For example, packet-filtering system **200** may configure rules **212**.

In step **706**, the packet-filtering system may identify packets comprising unencrypted data. For example, packet-filtering system **200** may identify packets comprising a DNS query, a reply to a DNS query, or a handshake message configured to establish an encrypted communication session. In step **708**, the packet-filtering system may identify packets comprising encrypted data. For example, packet-filtering system **200** may identify packets encrypted in accordance with one or more parameters of sessions **306**, **308**, **408**, **410**, **504**, or **606**.

In step **710**, the packet-filtering system may determine based on a portion of the unencrypted data corresponding to the network-threat indicators that the packets comprising encrypted data correspond to the network-threat indicators. For example, packet-filtering system **200** may determine that a domain name included in the DNS query, the reply to the DNS query, or the handshake message corresponds to the network-threat indicators, and packet-filtering system **200** may determine that one or more of the packets encrypted in accordance with the parameters of sessions **306**, **308**, **408**, **410**, **504**, or **606** correlate to one or more packets comprising the DNS query, the reply to the DNS query, or the one or more handshake messages.

The functions and steps described herein may be embodied in computer-usable data or computer-executable instructions, such as in one or more program modules, executed by one or more computers or other devices to perform one or more functions described herein. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types when executed by one or more processors in a computer or other data-processing device. The computer-executable instructions may be stored on a computer-readable medium such as a hard disk, optical disk, removable storage media, solid-state memory, RAM, etc. As will be appreciated, the functionality of the program modules may be combined or distributed as desired. In addition, the functionality may be embodied in whole or in part in firmware or hardware equivalents, such as integrated circuits, application-specific integrated circuits (ASICs), field-programmable gate arrays (FPGA), and the like. Particular data structures may be used to more effectively implement one or more aspects of the disclosure, and such data structures are contemplated to be within the scope of computer-executable instructions and computer-usable data described herein.

Although not required, one of ordinary skill in the art will appreciate that various aspects described herein may be embodied as a method, system, apparatus, or one or more computer-readable media storing computer-executable instructions. Accordingly, aspects may take the form of an entirely hardware embodiment, an entirely software embodiment, an entirely firmware embodiment, or an embodiment combining software, hardware, and firmware aspects in any combination.

As described herein, the various methods and acts may be operative across one or more computing devices and networks. The functionality may be distributed in any manner or may be located in a single computing device (e.g., a server, client computer, or the like).

Aspects of the disclosure have been described in terms of illustrative embodiments thereof. Numerous other embodiments, modifications, and variations within the scope and spirit of the appended claims will occur to persons of ordinary skill in the art from a review of this disclosure. For example, one of ordinary skill in the art will appreciate that the steps illustrated in the illustrative figures may be performed in other than the recited order and that one or more illustrated steps may be optional. Any and all features in the following claims may be combined or rearranged in any way possible.

What is claimed is:

1. A method comprising:

receiving, by a packet-filtering system comprising a hardware processor and a memory and configured to filter packets in accordance with a plurality of packet-filtering rules, data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprises a domain name identified as a network threat;

identifying packets comprising unencrypted data;

identifying packets comprising encrypted data;

determining, by the packet-filtering system and based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;

filtering, by the packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by the plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules:

packets comprising the portion of the unencrypted data that corresponds to one or more network-threat indicators of the plurality of network-threat indicators; and

the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and

routing, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.

2. The method of claim **1**, wherein:

the packets comprising unencrypted data comprise one or more packets comprising at least one of a domain name system (DNS) query or a reply to the DNS query, the method further comprising:

determining that the at least one of the DNS query or the reply to the DNS query comprises the domain name identified as the network threat.

3. The method of claim **2**, wherein the portion of the unencrypted data comprises one or more network addresses included in the at least one of the DNS query or the reply to the DNS query, the method further comprising:

determining that the packets comprising encrypted data comprise one or more packet headers comprising at least one of the one or more network addresses.

4. The method of claim **2**, wherein the portion of the unencrypted data comprises one or more network addresses included in one or more headers of the one or more packets comprising the at least one of the DNS query or the reply to the DNS query, the method further comprising:

determining that the packets comprising encrypted data comprise one or more packet headers comprising at least one of the one or more network addresses.

5. The method of claim **4**, wherein the one or more network addresses comprise a network address of a web proxy that generated the DNS query in response to a request received from a host, the method further comprising:

identifying one or more packets comprising the request.

6. The method of claim **1**, wherein one or more packets, of the packets comprising unencrypted data, comprise data configured to establish an encrypted communication session between a first host and a second host, the method further comprising:

routing the one or more packets comprising data configured to establish the encrypted communication session between the first host and the second host to the proxy system.

7. The method of claim **6**, the method further comprising:

routing the one or more packets to the proxy system based on a determination that at least one of the first host or the second host corresponds to the domain name identified as the network threat.

8. The method of claim **6**, wherein:

the plurality of packet-filtering rules indicate:

one or more network addresses for which encrypted communications are to be established via the proxy system, and

one or more network addresses for which encrypted communications are to not be established via the proxy system, the method further comprising:

routing the one or more packets to the proxy system based on a determination that at least one of the first host or the second host corresponds to the one or more network addresses for which encrypted communications are to be established via the proxy system.

9. The method of claim **6**, wherein:

the packet-filtering system comprises:

one or more interfaces interfacing the packet-filtering system with one or more communication links interfacing the first host and the second host, and

one or more interfaces interfacing the packet-filtering system with the proxy system, the method further comprising:

redirecting packets received via the one or more interfaces interfacing the packet-filtering system with the one or more communication links interfacing the first host and the second host to the one or more interfaces interfacing the packet-filtering system with the proxy system.

10. The method of claim **6**, wherein:

the packet-filtering system comprises:

one or more interfaces interfacing the packet-filtering system with one or more communication links interfacing the first host and the second host, and

one or more interfaces interfacing the packet-filtering system with the proxy system, the method further comprising:

forwarding copies of packets received via the one or more interfaces interfacing the packet-filtering system with the one or more communication links interfacing the first host and the second host to the one or more interfaces interfacing the packet-filtering system with the proxy system.

11. The method of claim 6, the method further comprising:

identifying, via a communication link interfacing the first host and the proxy system, the packets comprising encrypted data; and

identifying, via an internal communication link of the proxy system, packets corresponding to the packets comprising encrypted data.

12. The method of claim 11, the method further comprising: identifying, via a communication link interfacing the proxy system and the second host, packets generated by the proxy system based on the packets corresponding to the packets comprising encrypted data.

13. The method of claim 6, the method further comprising:

generating, by the proxy system, one or more packets based on the filtered packets, comprising encrypted data, routed to the proxy system by the packet-filtering system;

responsive to determining that one or more packets generated by the proxy system correspond to one or more criteria specified by the plurality of packet-filtering rules, at least one of:

dropping the one or more packets generated by the proxy system;

logging the one or more packets generated by the proxy system;

dropping one or more other packets generated by the proxy system;

logging one or more other packets generated by the proxy system;

dropping one or more other packets comprising encrypted data; or

logging one or more other packets comprising encrypted data.

14. The method of claim 13, wherein the determining that one or more packets generated by the proxy system based on one or more of the packets comprising encrypted data correspond to one or more criteria specified by the plurality of packet-filtering rules comprises determining that the one or more packets generated by the proxy system comprise at least one of a uniform resource identifier (URI) specified by the plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules.

15. The method of claim 13, wherein the determining comprises determining that the one or more packets generated by the proxy system comprise a uniform resource identifier (URI) meeting a threshold size specified by the plurality of packet-filtering rules.

16. The method of claim 6, the method further comprising: identifying, via a communication link interfacing the proxy system and an Internet content adaptation protocol (ICAP) server, one or more packets comprising at least one of an ICAP request, a response generated by the ICAP server, or a modified request generated by the ICAP server.

17. The method of claim 1, wherein the packets comprising encrypted data comprise packets received from a first host and destined for a second host, the method further comprising at least one of dropping or logging packets other than the packets comprising encrypted data based on a determination that the packets other than the packets comprising encrypted data were at least one of received from the second host or destined for the first host.

18. The method of claim 1, wherein:

the packets comprising unencrypted data comprise one or more packets comprising one or more handshake messages configured to establish an encrypted communication session between a client and a server, the method further comprising:

determining that the one or more handshake messages comprise the domain name identified as the network threat.

19. The method of claim 18, the method further comprising: responsive to determining that the one or more handshake messages comprise the domain name identified as the network threat, at least one of dropping or logging the packets comprising encrypted data.

20. The method of claim 18, wherein:

the one or more handshake messages comprise at least one of a hello message generated by the client or a certificate message generated by the server; and

the determining that the one or more handshake messages comprise the domain name identified as the network threat comprises determining the at least one of the hello message generated by the client or the certificate message generated by the server comprises the domain name identified as the network threat.

21. The method of claim 18, wherein the portion of the unencrypted data comprises one or more network addresses included in one or more headers of the one or more packets comprising the one or more handshake messages, the method further comprising

determining that the packets comprising encrypted data comprise one or more packet headers comprising at least one of the one or more network addresses.

22. The method of claim 21, wherein the one or more network addresses comprise a network address of the server and a network address of a web proxy, the method further comprising:

identifying one or more packets comprising one or more packet headers comprising the network address of the web proxy and a network address of the client; and

determining that the packets comprising encrypted data comprise one or more packet headers comprising the network address of the server and the network address of the client.

23. The method of claim 1, wherein the packets comprising unencrypted data comprise a certificate message for an encrypted communication session, the method further comprising:

at least one of dropping or logging one or more of the packets comprising encrypted data based on a determination that the certificate message comprises data indicating at least one of a serial number indicated by the plurality of packet-filtering rules, an issuer indicated by the plurality of packet-filtering rules, a validity time-range indicated by the plurality of packet-filtering rules, a key indicated by the plurality of packet-filtering rules, or a signing authority indicated by the plurality of packet-filtering rules.

24. A packet-filtering system comprising:

at least one hardware processor; and

memory storing instructions that when executed by the at least one hardware processor cause the packet-filtering system to:

receive data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprise a domain name identified as a network threat;

identify packets comprising unencrypted data;

identify packets comprising encrypted data;

determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;

filter, based on at least one of a uniform resource identifier (URI) specified by a plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules:

packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators; and

the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and

route, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.

25. One or more non-transitory computer-readable media comprising instructions that when executed by at least one hardware processor of a packet-filtering system cause the packet-filtering system to:

receive data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprise a domain name identified as a network threat;

identify packets comprising unencrypted data;

identify packets comprising encrypted data;

determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;

filter, by the packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by a plurality of packet-filtering rules indicating one or more of the plurality of network-threat indicators, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules:

packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators; and

the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and

route, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.

* * * * *

CERTIFICATE OF SERVICE

I hereby certify that, on this 27th day of August, 2021, I filed the foregoing Non-Confidential Brief for Defendant-Appellant Cisco Systems, Inc. with the Clerk of the United States Court of Appeals for the Federal Circuit via the CM/ECF system, which will send notice of such filing to all registered CM/ECF users.

/s/ William F. Lee
WILLIAM F. LEE
WILMER CUTLER PICKERING
HALE AND DORR LLP
60 State Street
Boston, MA 02109
(617) 526-6000

CERTIFICATE OF CONFIDENTIAL MATERIAL

The foregoing document contains 15 unique words (including numbers) marked confidential.

[X] This number does not exceed the maximum of 15 words permitted by Fed. Cir. R. 25.1(d)(1)(A).

[ ] This number does not exceed the maximum of 50 words permitted by Fed. Cir. R. 25.1(d)(1)(B) for cases under 19 U.S.C. § 1516a or 28 U.S.C. § 1491(b).

[ ] This number exceeds the maximum permitted by Federal Circuit Rule 25.1(d)(1), and the filing is accompanied by a motion to waive the confidentiality requirements.

/s/ William F. Lee
WILLIAM F. LEE
WILMER CUTLER PICKERING
HALE AND DORR LLP
60 State Street
Boston, MA 02109
(617) 526-6000

August 27, 2021

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATIONS

The foregoing filing complies with the relevant type-volume limitation of the Federal Rules of Appellate Procedure and Federal Circuit Rules because:

1. The filing has been prepared using a proportionally-spaced typeface and includes 13,993 words.

2. The brief has been prepared using Microsoft Word for Office 365 in 14-point Times New Roman font. As permitted by Fed. R. App. P. 32(g), the undersigned has relied upon the word count feature of this word processing system in preparing this certificate.

/s/ William F. Lee
WILLIAM F. LEE
WILMER CUTLER PICKERING
HALE AND DORR LLP
60 State Street
Boston, MA 02109
(617) 526-6000

August 27, 2021