

No.

In the Supreme Court of the United States

CENTRIPETAL NETWORKS, LLC, PETITIONER

v.

CISCO SYSTEMS, INC., RESPONDENT

*ON PETITION FOR A WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE FEDERAL CIRCUIT*

PETITION FOR A WRIT OF CERTIORARI

*MATTHEW J. DOWD
Counsel of Record
ROBERT J. SCHEFFEL
ELLIOT A. GEE
MORRIS D. YOUNG
DOWD SCHEFFEL PLLC
1717 Pennsylvania Ave. NW
Suite 1025
Washington, DC 20006
(202) 559-9175
mdowd@dowdscheffel.com*

QUESTION PRESENTED

Markman v. Westview Instruments, Inc., 517 U.S. 370 (1996), instructs that the court, not the jury, decides the scope of a patent claim, through the claim-construction process. This is paramount because the patent claim's scope defines the legal right to exclude and, consequentially, sets the boundary for the entire patent-infringement action, including claims, defenses, discovery, and admitted evidence.

Years of settled practice under *Markman* have led to the established practice that claims are construed early in the litigation so that plaintiffs and defendants alike will have a fair opportunity to develop evidence and present their respective cases. Because claim scope must be settled before parties develop their proofs, a late claim construction—announced after the evidentiary record has closed—demands notice and a fair chance to adjust. This case presents a stark deprivation of due process stemming from the Federal Circuit's increasing rudderless invocation of a standardless distinction between a “new” claim construction, on one hand, and a so-called “clarification” or “elaboration” after trial. In this case, the post-trial, post-verdict “elaboration” of two claim terms wiped out a \$2.6-billion judgment of willful infringement without affording the patent owner an opportunity to respond to the new construction.

The question presented is:

Whether a court, without providing notice, may adopt a new, dispositive, materially different claim construction after the evidentiary record is closed, and without permitting supplemental briefing or a meaningful opportunity to be heard.

PARTIES TO THE PROCEEDING BELOW

Petitioner Centripetal Networks, LLC was plaintiff in the district court and appellant in the court of appeals. Respondent Cisco Systems, Inc. was defendant in the district court and appellee in the court of appeals.

Centripetal Networks, LLC is not a publicly held corporation and therefore does not have a stock ticker symbol.

Cisco Systems, Inc.'s stock ticker symbol is CSCO.

CORPORATE DISCLOSURE STATEMENT

Pursuant to this Court's Rule 29.6, petitioner states that Centripetal Networks, LLC is not a publicly held corporation, is wholly owned by its parent CNI Holdings Inc. and no publicly held corporation owns 10% or more of the stock of Centripetal Networks, LLC.

RELATED PROCEEDINGS

This case arises from the following proceedings:

Centripetal Networks, LLC v. Cisco Systems, Inc.,
No. 2024-2097 (Fed. Cir. Apr. 29, 2026);

Centripetal Networks, Inc. v. Cisco Systems, Inc.,
No. 2021-1888 (Fed. Cir. June 23, 2022); and

Centripetal Networks, LLC v. Cisco Systems, Inc.,
No. 2:18-cv-00094 (EWH) (E.D. Va. Dec. 12, 2023)
(entering partial judgment pursuant to Rule 54(b)).

There are no other proceedings in state or federal trial or appellate courts, or in this Court, directly related to this case within the meaning of this Court's Rule 14.1(b)(iii).

TABLE OF CONTENTS

	Page
OPINIONS AND ORDERS BELOW	1
JURISDICTION	1
INTRODUCTION	2
STATEMENT OF THE CASE	4
I. Centripetal And Its Patented Innovation	4
II. Proceedings Below	4
A. District Court Trial in 2020	4
B. First Federal Circuit Appeal.....	7
C. Remand and Rule 63 Proceeding.....	8
D. Second Federal Circuit Appeal	12
REASONS FOR GRANTING THE PETITION	14
I. A Defined Claim Scope is a Necessary Predicate for the Fair Adjudication of Patent Rights.....	15
A. Claim Scope and the <i>Markman</i> Claim- Construction Process	15
B. Changing Claim Construction After the Close of Evidence Violates Settled Rules.....	20
II. The Federal Circuit’s Conflicting Approaches.....	21
III. The Decision is Wrong	24
A. The Federal Circuit Mischaracterized the Substantial Claim-Construction Shift	24
B. Centripetal Had No Notice or Opportunity to Respond to the New Claim Constructions.....	26
C. The Same Error Independently Controlled the ’806 Patent	28

IV. The Federal Circuit’s Error is a Recurring Issue of Exceptional Importance	31
V. The Case Is An Excellent Vehicle For Resolving The Question Presented	33
CONCLUSION	34

TABLE OF APPENDICES

APPENDIX A — OPINION OF THE UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT, FILED APRIL 29, 2026	1a
APPENDIX B — OPINION OF THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA, FILED JUNE 14, 2024.....	28a
APPENDIX C — OPINION OF THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA, FILED DECEMBER 11, 2023	57a
APPENDIX D — OPINION OF THE UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT, FILED JUNE 23, 2022	139a
APPENDIX E — OPINION OF THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA, FILED OCTOBER 5, 2020	170a
APPENDIX F — OPINION OF THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA, FILED OCTOBER 2, 2020	402a

TABLE OF AUTHORITIES

Cases	Page(s)
<i>Adnexus Inc. v. Meta Platforms, Inc.</i> , 160 F.4th 1216 (Fed. Cir. 2025).....	16
<i>Avid Technology, Inc. v. Harmonic, Inc.</i> , 812 F.3d 1040 (Fed. Cir. 2016)	19
<i>Aylus Networks, Inc. v. Apple Inc.</i> , 856 F.3d 1353 (Fed. Cir. 2017)	19, 25
<i>Barry v. DePuy Synthes Cos.</i> , 164 F.4th 896 (Fed. Cir. 2026)	17
<i>Bloomer v. McQuewan</i> , 55 U.S. (14 How.) 539 (1852)	15
<i>CCS Fitness, Inc. v. Brunswick Corp.</i> , 288 F.3d 1359 (Fed. Cir. 2002)	21
<i>Cordis Corp. v. Boston Scientific Corp.</i> , 658 F.3d 1347 (Fed. Cir. 2011)	23
<i>Cuozzo Speed Techs., LLC v. Lee</i> , 579 U.S. 261 (2016)	18
<i>Eon-Net LP v. Flagstar Bancorp.</i> , 249 F. App'x 189 (Fed. Cir. 2007)	20, 26
<i>Google LLC v. EcoFactor, Inc.</i> , 92 F.4th 1049 (Fed. Cir. 2024)	27
<i>Hamilton Beach Brands, Inc. v. f'real Foods, LLC</i> , 908 F.3d 1328 (Fed. Cir. 2018)	27
<i>Hewlett-Packard Co. v. Mustek Systems, Inc.</i> , 340 F.3d 1314 (Fed. Cir. 2003)	20
<i>In re Hiniker Co.</i> , 150 F.3d 1362 (Fed. Cir. 1998)	31
<i>Interactive Gift Express, Inc. v. Compuserve Inc.</i> , 256 F.3d 1323 (Fed. Cir. 2001)	21
<i>Magnolia Medical Technologies, Inc. v. Kurin, Inc.</i> , 169 F.4th 1094 (Fed. Cir. 2026).....	22

<i>Markman v. Westview Instruments, Inc.</i> , 52 F.3d 967 (Fed. Cir. 1995), <i>aff'd</i> 517 U.S. 370 (1996)	15, 19
<i>Markman v. Westview Instruments, Inc.</i> , 517 U.S. 370 (1996)	2, 7, 8, 9, 14, 15, 16, 17, 18, 24, 25, 26, 28, 33
<i>Mformation Technologies, Inc. v.</i> <i>Research in Motion Ltd.</i> , 7, 64 F.3d 1392 (Fed. Cir. 2014)	22
<i>Mullane v. Cent. Hanover Bank & Tr. Co.</i> , 339 U.S. 306 (1950)	26
<i>NeoMagic Corp. v. Trident Microsystems, Inc.</i> , 287 F.3d 1062 (Fed. Cir. 2002)	17
<i>O2 Micro Int'l, Ltd. v.</i> <i>Beyond Innovation Tech. Co., Ltd.</i> , 521 F.3d 1351 (Fed. Cir. 2008)	19
<i>Oakley, Inc. v. Sunglass Hut Int'l</i> , 316 F.3d 1331 (Fed. Cir. 2003)	16
<i>Parker v. Hulme</i> , 18 F. Cas. 1138 (C.C.E.D. Pa. 1849)	15
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005) (en banc)	15, 18
<i>Roemer v. Peddie</i> , 132 U.S. 313 (1889)	19
<i>Scriber-Schroth Co. v. Cleveland Trust Co.</i> , 311 U.S. 211 (1940)	19
<i>SRI Int'l v. Matsushita Elec. Corp. of America</i> , 775 F.2d 1107 (Fed. Cir. 1985)	17
<i>Teva Pharmaceuticals USA, Inc. v. Sandoz, Inc.</i> , 574 U.S. 318 (2015)	16
<i>Thorner v. Sony Comput. Entm't Am. LLC</i> , 669 F.3d 1362 (Fed. Cir. 2012)	19

<i>TNS Media Research, LLC v.</i> <i>TiVo Research & Analytics, Inc.</i> , 629 F. App'x 916 (Fed. Cir. 2015)	20
<i>Wi-LAN, Inc. v. Apple, Inc.</i> , 811 F.3d 455 (Fed. Cir. 2016)	20, 21
<i>Winans v. Denmead</i> , 56 U.S. (15 How.) 330 (1854)	15
<i>Wyeth LLC v. AstraZeneca Pharmaceuticals LP</i> , 180 F.4th 1371 (Fed. Cir. 2026)	23

Statutes and Other Authorities

28 U.S.C. §1254(1)	1
35 U.S.C. § 101	16
35 U.S.C. § 102	16
35 U.S.C. § 103	16
35 U.S.C. § 112	16
35 U.S.C. § 154(a)(1)	15
35 U.S.C. § 271	16
35 U.S.C. §§ 311-319	18
Clarify, <i>Merriam-Webster's Collegiate</i> <i>Dictionary</i> (11th ed. 2020)	22
Elaborate, <i>Merriam-Webster's Collegiate</i> <i>Dictionary</i> (11th ed. 2020)	22
Fed. R. Civ. P. 63	3, 8, 9, 13, 25, 26, 27, 28
Fed. R. Evid. 401	16
Fed. R. Evid. 402	16
Kristen Jakobsen Osenga, <i>Linguistics and</i> <i>Claim Construction</i> , 38 Rutgers L.J. 61 (2006)	19

Mark A. Lemley, <i>The Changing Meaning of Patent Claim Terms</i> , 104 Mich. L. Rev. 101 (2005).....	31
Peter S. Menell, et al., <i>Patent Case Management Judicial Guide</i> 5-5 (3d ed. 2016).....	17

Petitioner respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the Federal Circuit.

OPINIONS AND ORDERS BELOW

The opinion of the United States Court of Appeals for the Federal Circuit is not published in the Federal Reporter but can be found at 2026 WL 1162800 and reproduced at Pet.App. 1a-421a.

JURISDICTION

The judgment of the court of appeals was entered on April 29, 2026. On July 22, 2026, the Chief Justice extended the time within which to file a petition for a writ of certiorari to and including September 18, 2026. The jurisdiction of this Court is invoked under 28 U.S.C. §1254(1).

INTRODUCTION

The fair adjudication of property rights, particularly patent rights, requires a court to construe the scope of the legal right so that the parties—plaintiffs and defendants alike—have fair notice and an opportunity to present evidence in support of their claims and defenses. In patent litigation, the patent claim is “the portion of the patent document that defines the scope of the patentee’s rights.” *Markman v. Westview Instruments, Inc.*, 517 U.S. 370, 372 (1996). Defining the patent claim through claim construction informs the entire patent litigation, including the evidence presented by the parties, witnesses, and expert testimony. When a court changes the claim construction after all evidence is presented—especially after a full trial with a finding on infringement—fundamental principles of due process require that the parties are afforded notice and an opportunity to respond to the new claim construction, *e.g.*, with additional evidence or argument as may be relevant to the changed scope of the legal dispute.

In this case, the appeals court incorrectly condoned a district court’s new claim constructions that came after a full trial on the merits and after a remand proceeding to a new judge—all without notice and opportunity for Petitioner Centripetal Networks, LLC to present evidence and arguments responsive to the new claim constructions.

The appeals court’s decision reflects a continued wayward course that drifts far from *Markman* and other settled principles that require either (a) a defined legal scope of the patent within which the parties can litigate the case and present their respective claims and defenses to the jury or court for decision-making, or (b) fair notice and opportunity to present responsive evidence and argument to a changed claim interpretation that a court adopts late in the game. The Federal Circuit has

increasingly condoned eleventh-hour claim constructions under the guise of “clarifications” or “elaborations.” But those terms capture a distinction without a difference, and they hide the basic flaw with changing the legal scope of the patent dispute after the parties have tried their case.

The belated claim construction here is particularly egregious. Agreeing to the ordinary meaning of the two key terms, Centripetal and Respondent Cisco Systems Inc. presented their evidence over the course of a twenty-two-day bench trial. The court then found that Cisco willfully infringed Centripetal’s asserted patents. That verdict was cast aside, however, after the disqualification of the late Judge Henry Coke Morgan, Jr. based on the belated discovery of his wife’s ownership of less than \$5,000 in Cisco stock. The appellate court remanded the case but left intact the claim-construction framework that governed the trial.

A second judge presided over the subsequent Rule 63 hearing. Despite considering largely the same infringement evidence, the second judge found non-infringement, after materially changing the meaning of two key patent claims, and without affording Centripetal notice and an opportunity to introduce evidence and argument responsive to the new claim interpretations.

In short, Cisco’s liability of \$2.6 billion for willful infringement was lost on substantially a nearly identical factual record but due to a materially different understanding of two claim terms. The result has laid bare the problem with the Federal Circuit’s outcome-driven approach contravening the need for notice about new claim constructions. This Court’s intervention is needed to ensure that plaintiffs and defendants alike are not subject to patent rulings predicated on shifting property rights that change after the evidence is fully litigated.

STATEMENT OF THE CASE

I. Centripetal And Its Patented Innovation

Centripetal is an innovator in secure network design. It developed award-winning technology and was granted numerous patents for its innovations in network security. It developed its own product RuleGATE that embodies the inventions protected by the two patents litigated here.

U.S. Patent No. 9,686,193 (“the ’193 patent”), known as the “Exfiltration” patent, covers novel methods that prevent hackers from accessing secure computer networks, thus preventing exfiltration of confidential information. Pet.App. 3-5a. At a high level, the invention works by filtering packets (discrete “packages” of data) that are transmitted through computer networks. *Id.*

U.S. Patent No. 9,203,806 (“the ’806 patent”), known as the “Rule Swap” patent, enables seamless updates of a network device’s packet-filtering rules. Pet.App. 5-6a. The rules are used to scan data in the packets to screen and prevent entry of dangerous packets, *e.g.*, those containing malware. The invention updates a first rule set by sending a signal instructing the implementation of the “second rule set,” with the process involving five specific steps that accomplish the seamless rule swap without loss of packets, and thus without loss of data. *Id.*

II. Proceedings Below

A. District Court Trial in 2020

Centripetal sued Cisco in the U.S. District Court for the Eastern District of Virginia in February 2018. Pet.App. 171a. Centripetal sued Cisco for infringing several patents, including the ’193 and ’806 patents.

The ’193 patent, in Centripetal’s view, covered Cisco’s systems that filter packets based on quarantining packets that are tagged as problematic. For packets that contain those tags, *e.g.*, particular types of transfers, Cisco’s systems drop the packets. For the ’806 patent,

Centripetal contended that Cisco's switches, routers, and firewalls (in combination with certain management programs) allow for swapping of packet-filtering rules during a period when traffic is ceased, rather than dropping packets while the rules were swapped.

Cisco's alleged infringement occurred after Centripetal confidentially shared with Cisco confidential information about its products and patents under a non-disclosure agreement. Cisco had extensive meetings and discussions with Centripetal about its patented technology. But Cisco declined to license the patents and instead started marketing its own competing products that were later found to be copies of Centripetal's inventions. Pet.App. 368a-383a.

Early in the case, the parties identified several patent claim terms to be construed by the court. Pet.App. 60a-61a; Pet.App. 219a-220a. The parties agreed on the construction of five claim terms, disputed six terms, and agreed that six others would be construed using their plain and ordinary meanings. *Id.*

For the '193 patent, both parties agreed that, for the dispositive claim limitation—"particular type of data transfer"—the plain meaning would be the applicable construction. *Id.* For the '806 patent, the parties likewise agreed that the "responsive to being signaled" limitation would use a plain-and-ordinary-meaning construction. *Id.* The claim constructions were reflected in the court's *Markman* Order, issued on February 20, 2020.

In May and June 2020, the court conducted a twenty-two-day remote bench trial using the court's constructions, including the plain-and-ordinary meanings for terms in the '193 and '806 patents. *See* Pet.App. 9a. The bench trial produced an extensive body of evidence, with "an over 3,507-page record, 26 witnesses, and over 300 exhibits." Pet.App. 141a.

On October 5, 2020, the court found that Cisco willfully infringed, *inter alia*, the asserted '193 and '806 claims. Pet.App. 9a. Judge Morgan's detailed opinion analyzed the witness testimony and documentary evidence presented at trial, and he found that Cisco willfully copied Centripetal's patented inventions. Pet.App. 378a. He summarized how "Cisco was provided with demonstrations of [Centripetal's] product and confidential information regarding Centripetal's proprietary algorithms." *Id.* Less than a year after its meetings with Centripetal, "Cisco released the 'network of the future,'" which included products "embedded with new software functionality that was outlined and detailed to [Cisco] by [Centripetal's] disclosure of the patents and multiple technical discussions and demonstrations." *Id.*

For the '193 patent, Judge Morgan determined Cisco's products met the two-stage limitation based on quarantining packets having data tags such as a "Secure Group Tag" ("SGT"). Pet.App. 298a-299a. The SGTs are data tags that categorize the packets. He found that "the Cisco system operates in a two-stage process that meets the functionality required by the asserted claims." Pet.App. 293a. He made specific findings based on Cisco's expert testimony that Cisco's products transmit or drop packets based on the associated packet SGT. Pet.App. 287a-292a.

For the '806 patent, Cisco's accused products met the "responsive to being signaled" limitation. The accused products perform the five enumerated steps that occur after the rule-swap signal used to switch to the second rule set. Pet.App. 317a-318a. The process used in Cisco's devices, Judge Morgan found, "is the exact functionality as described by the cease and cache elements of the '806 Patent." Pet.App. 318a-319a.

Cisco's noninfringement defense was rejected as not credible because Cisco's own documents contradicted it.

Pet. App. 379a. “[T]he adverse testimony of Cisco engineers” also undermined its defense. *Id.* After considering the evidence, including the credibility of the live expert witnesses, Judge Morgan found that the infringement and validity issues “were clear and not a close call.” Pet.App. 381a.

Before issuing his decision, on August 11, 2020, Judge Morgan learned that his wife owned 100 shares of Cisco stock (then valued at \$4,687.99). Pet.App. 403a. He promptly disclosed this news to the parties and “explain[ed] that the ‘shares did not and could not have influenced [his] opinion on any of the issues in this case.’” Pet.App. 404a. The “full draft of [his] opinion had been prepared” before he learned about the shares, and he had already decided “[v]irtually every issue.” *Id.* (internal quotation omitted).

Less than two weeks later, Cisco asked Judge Morgan to recuse himself based on his wife’s stock ownership. Dkt.No.551. On October 2, 2020, he denied the motion. Pet.App. 421a. Three days later, he issued his infringement ruling (that was adverse to his wife’s stock ownership).

B. First Federal Circuit Appeal

Cisco appealed the willful-infringement judgment and the denial of its recusal motion. Pet.App. 145a. In an opinion authored by Judge Dyk, the Federal Circuit ruled for Cisco on the recusal issue and remanded for further proceedings, but it did not rule on the infringement finding. Pet.App. 168a.

The remand also did not alter the district court’s *Markman* Order, noting that “the only rulings subject to vacatur are those issued after Judge Morgan learned of his wife’s financial interest in Cisco, on August 11, 2020.” Pet.App. 167a. This left in place Judge Morgan’s construction of the disputed claim terms, including the

adoption of the plain-and-ordinary-meaning construction for the key terms of the '193 and '806 patents.

C. Rule 63 Proceeding in 2023

On remand, the case was reassigned to Judge Elizabeth Wilson Hanes for proceeding under Federal Rule of Civil Procedure 63.¹ Because the *Markman* Order was unaffected by the Federal Circuit's remand, both parties agreed during a hearing in October 2022 that no new witnesses needed to be called. C.A. App.18611-18620; C.A. App. 18834; C.A. App. 18849-18856.

On May 25, 2023, Cisco moved to supplement the record. Dkt.No.691. Cisco wanted to add several new documents to the record, including a declaration by one of its experts who testified in the 2020 trial but whom Cisco chose not to recall during the hearing. *Id.* Cisco also sought to add a 39-page document titled Centripetal's Patent Owner's Preliminary Response ("POPR Exhibit"). Three pages of the document had been introduced and referenced during the 2020 trial, but Cisco did not rely on or enter into evidence the entire POPR Exhibit. On remand before Judge Hanes—some three years after trial—Cisco now saw an opportunity to change the claim construction. The POPR Exhibit had no relevance to how Cisco's products operate, *i.e.*, the infringement analysis. It was relevant only to claim construction.

The POPR Exhibit, dated January 4, 2019, had been filed in an *inter partes* review proceeding ("IPR") that Cisco filed in an unsuccessful effort to cancel the '193 patent before the U.S. Patent and Trademark Office ("USPTO"). Cisco had petitioned to cancel all '193 claims, but the USPTO denied the IPR petition because it failed to demonstrate that Cisco was reasonably likely to prove the '193 claims unpatentable. Before Judge Hanes,

¹ Judge Morgan passed away on May 1, 2022, while the appeal was pending.

Centripetal objected to adding the entire POPR Exhibit (including different portions not relied on during the trial) because Cisco was attempting to re-open claim construction despite the *Markman* Order remaining in effect.

Cisco's introduction of the POPR Exhibit was an apparent attempt to invoke the doctrine of "prosecution disclaimer." Dkt.No.731 at 7-8. Courts can use the prosecution-disclaimer doctrine to restrict the scope of a claim based on statements made during the patent application process. By the time of the Rule 63 hearing, however, claim construction had long passed, and the *Markman* Order entered by Judge Morgan remained in effect. *Id.*

On June 6, 2023, Judge Hanes conducted a hearing at which the parties agreed that the Rule 63 proceeding would be based on the fixed evidentiary record from trial, with no additional fact or expert witnesses. Dkt.No.716. On June 21, 2023, Judge Hanes certified familiarity of the record. The Rule 63 hearing took place across three days (June 23-25). Two technical witnesses provided a technical tutorial for the judge, but not about claim-construction issues. At certain points, the court chastised Cisco's tutorial as "look[ing] a lot like claim construction." Dkt.No.750 at 141; *see id.* ("I think you get very close, if not over the line, on claim construction.").

At the hearing's outset, Judge Hanes granted in part Cisco's motion to supplement the record. She denied entry of Cisco's expert declaration because the parties chose not to recall witnesses and it would be "unfair to Centripetal to have the statement come in without any ability to have this witness explain discrepancies." Dkt.No.750 at 11. She nonetheless allowed two exhibits, including the new POPR Exhibit. *Id.* at 8-10. She did not rule on the exhibits' potential relevancy, "leaving that to another day." *Id.* at 11.

Centripetal objected, explaining that it “would like to recall some witnesses based upon the claim construction issue” if the court was going to adopt a new construction adverse to Centripetal. Dkt.No.754 at 432-37. “[A]t the very least,” Centripetal explained, the court should “have a [claim-construction] briefing schedule and allow the parties to present their positions and come in here and argue them.” *Id.* Judge Hanes did not rule on Centripetal’s request during that hearing.

On December 11, 2023, Judge Hanes issued her decision on liability (“Remand Order”). Pet.App. 57a. For both patents, Judge Hanes reversed Judge Morgan’s earlier ruling and found no infringement, despite the factual evidence of infringement being the same. The new narrow claim interpretations became dispositive.

On the ’193 patent, the court found that Cisco’s products did not meet the “particular type of data transfer” limitation. Pet.App. 88a. Notwithstanding the parties’ agreement to use the plain-and-ordinary-meaning construction, Judge Hanes adopted an express construction of the claim—for the first time in the case’s three-year history—that reinterpreted the claim to require “filtration of a subset of packets sent between [endpoint] computers in two different networks.” Pet.App. 89a. This new construction rested, in large part, on the belated POPR Exhibit. Pet.App. 91a. The court viewed the POPR Exhibit as being “consistent with” its new claim construction. *Id.* The Remand Order did not analyze whether the POPR Exhibit’s statements rose to a “clear and unmistakable” disclaimer of claim scope, which Federal Circuit precedent requires.

On the ’806 patent, the Remand Order incorporated another new claim construction for the limitation about the signal initiating the swap to the second rule set. The court reinterpreted the claim to require that the “swap” signal be the but-for, *i.e.*, sole, cause of *each* step in the

claimed sequence of updating to the second rule set. Pet.App. 105a-106a. In other words, each of the five enumerated steps in the rule swap—in particular, the “cease processing” and “cache” steps—could not have a separate basis for being performed in Cisco’s devices. The rule-swap signal had to be the only reason that each step, including the “cease processing” and “cache” steps, occurs as part of the rule swap in Cisco’s devices. *Id.*

Surprisingly, this new view of the claim adopted the same theory that Cisco pushed in the 2020 trial but which Judge Morgan rejected. Pet.App. 316a-319a. Cisco had argued that, because the “cease processing” and “cache” steps also occur during a device’s baseline idle period, those two steps were not “responsive to” the rule-swap signal. Pet.App. 105a-106a. And he found that Cisco’s products performed each of the five enumerated steps when conducting the claimed rule swap after the rule-swap signal. *Id.*

What changed was the claim interpretation. Under the court’s new interpretation, the claim required more than showing the five steps occurring as a result of the swap signal. *See* Pet.App. 108a (“[W]hile there is a temporal relationship between a rule swap and the ceasing processing of packets, ... there is no causal relationship.”). The claim now required a showing that none of the five enumerated steps occurred but for the rule-swap signal. Pet.App. 106a (recognizing that Cisco’s products do perform the “cease processing” and “cache” steps as part of its rule swap).

Centripetal moved for reconsideration of the Remand Order. Dkt.No.787. Judge Hanes denied Centripetal’s motion. Pet.App. 56a (“Reconsideration Order”). In doing so, Judge Hanes admitted that even “further clarification is necessary” for the ’193 patent’s “particular type of data transfer” limitation. Pet.App. 32a-33a. The “further clarification” rested on new extrinsic evidence—

dictionaries neither party entered into evidence. Pet.App. 34a-36a. By using the dictionary definitions of the terms “type” and “data transfer,” the court changed the construction’s focus from “computers in two different networks” to a second new construction that focused on “the specific technique, or method, associated with the data transmission.” Pet.App. 34a-35a. Based on this “further clarification,” the court stood by its non-infringement finding. Pet.App. 35a-36a.

For the ’806 patent, Judge Hanes maintained the new construction, as set forth in the Remand Order. Under that interpretation, the court imposed its “causality” requirement for each of the enumerated five steps, leading to the noninfringement finding, in contrast to Judge Morgan’s infringement finding that did not interpret the claim as requiring a distinct “causality” requirement for each enumerated step.

Centripetal’s motion also asked to reopen the record so Centripetal could address the new claim construction for the ’193 patent. Pet.App. 36a. This request was denied because, according to the court, the new interpretation of “‘particular type of data transfer’ does not diverge from the term’s plain and ordinary meaning,” “Centripetal never requested the Court construe the term,” and Centripetal “has not held a consistent position on the term’s meaning.” Pet.App. 37a-38a.

D. Second Federal Circuit Appeal

Centripetal appealed to the Federal Circuit. Pet.App. 1a-2a. The appeals court affirmed in full, with an opinion again written by Judge Dyk.

For the ’193 patent, the Federal Circuit concluded that Centripetal had adequate notice of the new claim construction based on Cisco’s post-trial and non-infringement positions. Pet.App. 16a-17a. In the court’s view, Cisco’s continuous pressing of its *non-infringement*

theories was enough notice, even though, through three years, the district court never deviated from the plain-and-ordinary-meaning construction and did not apply a new construction—until after the Rule 63 hearing when denying Centripetal’s motion for a new trial. Pet.App. 17a. The court also relied on arguments and evidence that post-dated the 2020 trial as proof of sufficient notice of the district court’s new claim constructions adopted in December 2023 and June 2024. C.A. App. 17865-17866; C.A. App. 19450-19454; C.A. App. 21283.

The appeals court also affirmed the new post-Remand Order construction as correct. Pet.App. 12-13a. The court notably did not rely on the district court’s new dictionary definitions cited in the Reconsideration Order. The appeals court instead turned to eight lines of the patent specification. Pet.App. 13-15a.

The appeals court also relied on one paragraph in the new POPR Exhibit. Pet.App. 14a. The court concluded that “Centripetal’s statements in the IPR proceeding define the scope of the asserted claims to require two-stage filtering, with source and destination filtering being part of the first stage.” Pet.App. 15a-16a. In Centripetal’s view, the isolated reading of the POPR Exhibit overlooked the doctrine of claim differentiation: Separate ’193 claims (claims 16 and 17) commanded a broader construction of the “particular type of data transfer” limitation.² The appeals court’s opinion did not address this claim-differentiation point. *See* Pet.App. 16a n.6.

For the ’806 patent, the court held that Centripetal forfeited its claim-construction argument, without addressing that Cisco’s same claim-construction arguments were presented in the 2020 trial and rejected

² Oral Arg. 7:16-8:18; 26:18-27:59, at https://www.cafc.uscourts.gov/oral-arguments/24-2097_04072026.mp3.

by Judge Morgan. Pet.App. 18a-19a; Pet.App. 316a-319a. The court also agreed with the district court's construction that "the signal must be the but-for cause of ceasing processing packets" because "[t]he asserted claims specify a list of actions the claimed processors must be configured to do responsive to being signaled to process packets in accordance with the second rule set." Pet.App. 19a. (quotation omitted).

REASONS FOR GRANTING THE PETITION

The decision below is incompatible with settled norms of the *Markman* claim construction process and of affording fair notice and an opportunity to respond when a court changes the claim construction. *Markman* recognizes the importance of claim construction, as it "defines the scope of the patentee's rights." 517 U.S. at 372. Claim construction that is a moving target until after a trial is the antithesis of due process and fundamental fairness.

The Federal Circuit's error in this case and others stems in large part from its cases attempting to distinguish a "new" claim construction from a mere "elaboration" or "clarification" of an earlier claim construction. The court's precedents offer no standard by which to distinguish "new" from "elaboration" or "clarification," yet an "elaboration" or "clarification" can be outcome-determinative. Here, the multiple "clarifications" turned a \$2.6-billion willful infringement judgment into a goose egg.

This Court should grant certiorari to instruct that material changes to claim construction—whether deemed "new" or simply an "elaboration" or "clarification"—require sufficient notice and an opportunity for the parties to respond, and that the Federal Circuit must articulate an administrable standard by which courts and litigants can ensure fair process when a court alters the

legal boundary of the dispute through a changed claim construction.

I. A Defined Claim Scope is a Necessary Predicate for the Fair Adjudication of Patent Rights

A. Claim Scope and the *Markman* Process

The scope of the property right in patent cases is defined by the claims. The scope of the claims sets the boundary of the entire patent dispute, including the evidence the parties present.

1. The claims define the scope of the right to exclude. A patent is a grant of the right to exclude. 35 U.S.C. § 154(a)(1); *Bloomer v. McQuewan*, 55 U.S. (14 How.) 539, 549 (1852). Thirty years ago, this Court held that claim construction is for the court, not the jury. *Markman*, 517 U.S. at 372, 388-91. That decision rested in part on a foundational premise captured by Justice Curtis (a former patent practitioner) in *Winans v. Denmead*, 15 How. 330, 338 (1854)—namely that the *first* issue in a patent case is claim construction. *Markman*, 517 U.S. at 384-85 (“The first [issue] is a question of law, to be determined by the court, construing the letters-patent, and the description of the invention and specification of claim annexed to them.”).

That first step is of profound importance. Indeed, “[p]atent construction in particular ‘is a special occupation.’” *Id.* at 388 (quoting *Parker v. Hulme*, 18 F. Cas. 1138, 1140 (C.C.E.D. Pa. 1849) (No. 10,740)). Defining the claim scope defines the metes and bounds of the patent right. See *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc). Claim construction is so critical that it will frequently be case dispositive. See *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 989 (Fed. Cir. 1995) (en banc) (Mayer, J., concurring) (“[T]o decide what the claims mean is nearly always to decide the case.”), *aff’d* 517 U.S. 370 (1996).

Determining claim scope is a legal issue for a court, not the jury, but claim construction frequently encompasses subsidiary factual questions. *Teva Pharms. USA, Inc. v. Sandoz, Inc.*, 574 U.S. 318, 325-27 (2015). Claim construction is, after all, a practice with “evidentiary underpinnings” that “falls somewhere between a pristine legal standard and a simple historical fact.” *Markman*, 517 U.S. at 378, 388, 390.

2. Claim construction establishes the framework of the patent dispute. The interpreted claims define almost all aspects of patent litigation, including discovery, experts, infringement/invalidity theories, and the evidence presented to the fact-finder.

Significantly, claim scope drives nearly every theory in the case, for both plaintiffs and defendants. Infringement is necessarily determined based on claim scope. 35 U.S.C. § 271. Invalidity defenses, including those under 35 U.S.C. §§ 101, 102, 103, and 112, must account for claim scope. For instance, whether certain prior art is anticipatory will depend on whether the prior-art document meets “each and every limitation” of the claimed invention, but that can only be assessed by knowing what “each and every limitation” means. *E.g., Oakley, Inc. v. Sunglass Hut Int’l*, 316 F.3d 1331, 1339 (Fed. Cir. 2003) (identifying claim construction as “[t]he first step” in a validity analysis).

From a procedural perspective, claim construction will impact potentially dispositive motions, such as motions to dismiss for failure to state a claim. *See Adnexus Inc. v. Meta Platforms, Inc.*, 160 F.4th 1216, 1222 (Fed. Cir. 2025) (in motion-to-dismiss context, authorizing courts to “engage in claim construction, provided they give the parties appropriate notice and an opportunity to be heard”).

Claim interpretation also dictates the scope of admissible evidence. Fed. R. Evid. 401, 402. It in effect

cabins the pretrial discovery process and allows for the development of factual evidence and necessary expert testimony. It similarly controls the scope of admissible expert testimony, particularly on technical issues of infringement and validity. *E.g.*, *Barry v. DePuy Synthes Cos.*, 164 F.4th 896, 903 (Fed. Cir. 2026) (excluding as unreliable and “not helpful to the jury” expert testimony that contradicts the claim construction).

Generally, claim construction occurs separately from any infringement determination and consideration of the accused devices because, to not do so “would make infringement a matter of judicial whim.” *SRI Int’l v. Matsushita Elec. Corp. of Am.*, 775 F.2d 1107, 1118 (Fed. Cir. 1985); *accord NeoMagic Corp. v. Trident Microsystems, Inc.*, 287 F.3d 1062, 1074 (Fed. Cir. 2002) (“It is well settled that claims may not be construed by reference to the accused device.”). The patent document memorializes the right to exclude, and its legal scope should not and does not change depending on the device or method identified as infringing the patent.

For all these reasons, numerous courts, scholars, and judicial guides have recognized the value of early claim construction in patent litigation. *See, e.g.*, Peter S. Menell, et al., *Patent Case Management Judicial Guide* 5-5 (3d ed. 2016) (“A majority of courts have found that the most opportune time to hold the *Markman* hearing is midway through, or before the close of, fact discovery, and prior to expert discovery.”). The benefit of early claim construction also has motivated the most patent-active district courts to adopt local rules requiring an early claim construction. *Id.* at 2-4. In short, applying a new claim construction post-trial without additional argument or evidence is the anomaly.

3. The claim-construction mechanics. Claim construction typically occurs early in the case in order to facilitate a fair presentation of the relevant issues and

evidence. The *Markman* process concerns the type of relevant evidence, viewed through the lens of an ordinarily skilled artisan, as well as the procedure of gathering and analyzing the evidence to reach a final claim construction defining the legal right being litigated.

The Federal Circuit’s en banc decision in *Phillips* describes the type of evidence informing claim construction. Intrinsic evidence (the words of the claims, the teaching of the patent specification, and the patent’s drawings) is the primary evidence to consider when assessing how a person of ordinary skill in the art would understand a claim term. 415 F.3d at 1332.

Additionally, the prosecution history—the back and forth between the patent applicant and the USPTO examiner—likewise provides an evidentiary aid in interpreting the claims. Relevant prosecution-history-type evidence can also include post-grant review proceedings occurring after the patent grant, such as an IPR proceeding. An IPR is a statutory post-grant challenge. See 35 U.S.C. §§ 311-319; *Cuozzo Speed Techs., LLC v. Lee*, 579 U.S. 261, 267 (2016). During IPR proceedings, parties may take positions about how a person of ordinary skill in the art would understand a patent claim at issue.

There is also extrinsic evidence, which includes dictionary definitions, inventor testimony, expert testimony, and other documentary evidence probative of how a person of skill in the art would understand the terms. *Phillips*, 415 F.3d at 1318. *Phillips* reaffirmed that extrinsic evidence is generally secondary to intrinsic evidence. *Id.*

Procedurally, the claim construction (or *Markman*) process typically starts with the parties identifying disputed claim limitations that are relevant. They exchange proposed constructions of the disputed terms and detailed briefing. Particularly in complex matters, a

court conducts a *Markman* hearing, where parties can present argument and evidence, including expert testimony so the court can evaluate witness credibility. *Markman*, 52 F.3d at 981.

Not every claim term requires an explicit construction. *O2 Micro Int'l, Ltd. v. Beyond Innovation Tech. Co., Ltd.*, 521 F.3d 1351, 1362 (Fed. Cir. 2008). For some claim limitations, the parties may not dispute that the accused infringing device meets a given limitation. For others, the parties will agree that the ordinary meaning applies as the accepted construction. *Thorner v. Sony Comput. Entm't Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012) (holding ordinary meaning should apply unless there is an explicit definition or disavowal).

After the court receives complete briefing and evidence, the court rules on the meaning of the disputed claim terms based on the intrinsic and extrinsic evidence. Additionally, like canons of statutory interpretation, canons of claim interpretation can guide a court to the correct interpretation. Kristen Jakobsen Osenga, *Linguistics and Claim Construction*, 38 Rutgers L.J. 61, 105-07 (2006) (discussing canons of claim construction, including claim differentiation).

One fundamental precept in claim interpretation is the doctrine of prosecution disclaimer, which limits claim scope to exclude subject matter surrendered during prosecution. *Schriber-Schroth Co. v. Cleveland Trust Co.*, 311 U.S. 211, 220-21 (1940); *Roemer v. Peddie*, 132 U.S. 313, 317 (1889); *Aylus Networks, Inc. v. Apple Inc.*, 856 F.3d 1353, 1359-62 (Fed. Cir. 2017). Establishing prosecution disclaimer is a “demanding standard.” *Avid Tech., Inc. v. Harmonic, Inc.*, 812 F.3d 1040, 1045 (Fed. Cir. 2016). For disclaimer to attach, the disavowal must be “both clear and unmistakable”; it does not apply when statements and amendments have alternative meanings or are merely consistent with a given construction. *Id.*

With the claim construction in hand, a court can then proceed with adjudicating the patent-infringement action and asserted defenses.

B. Changing Claim Construction After the Close of Evidence Violates Settled Rules

Unsurprisingly, instances will arise where a claim construction needs to be changed, adjusted, or clarified mid-course or even very late in the patent-litigation proceeding. The proper approach when that happens is to afford the parties the proper notice and an opportunity to address the changed construction.

Many Federal Circuit cases recognize that the parties must be involved in claim construction of disputed terms, and the parties must be provided notice and opportunity to present argument and evidence about the correct construction. *See, e.g., Wi-LAN, Inc. v. Apple, Inc.*, 811 F.3d 455, 465-66 (Fed. Cir. 2016) (holding that while a court may elaborate post-trial on a meaning inherent in an existing construction, a court may not use a post-verdict reconstruction that changes claim scope and undermines a party's tried case); *TNS Media Research, LLC v. TiVo Research & Analytics, Inc.*, 629 F. App'x 916, 939 (Fed. Cir. 2015); *Eon-Net LP v. Flagstar Bancorp.*, 249 F. App'x 189, 195 (Fed. Cir. 2007) ("[W]here a district court construes a patent without following the necessary steps, we should remand the matter for further proceedings so that the district court can follow the appropriate steps."); *Hewlett-Packard Co. v. Mustek Sys., Inc.*, 340 F.3d 1314, 1321 (Fed. Cir. 2003) ("[I]t is too late at the JMOL stage to ... adopt a new and more detailed interpretation of the claim language and test the jury verdict by that new and more detailed interpretation.").

Those cases recognize that accepted norms, established through years of this Court's *Markman* decisions as well as other principles, require fair notice to

litigants when the claim construction is changed mid-stream. *Wi-LAN*, 811 F.3d at 465-66. A new claim construction fundamentally changes the scope of the legal right being litigated, and a shifting legal right cannot be fairly adjudicated.

The significance of changing claim constructions is similarly embedded in the Federal Circuit’s waiver/forfeiture jurisprudence. *CCS Fitness, Inc. v. Brunswick Corp.*, 288 F.3d 1359, 1370-71 (Fed. Cir. 2002) (“Our precedent makes clear that in the context of claim construction, a waiver may occur if a party raises a new issue on appeal, as by, e.g., presenting a new question of claim scope.” (citing *Interactive Gift Express, Inc. v. CompuServe Inc.*, 256 F.3d 1323, 1347 (Fed. Cir. 2001))). Just as it is unfair to ask the appeals court to rule on a new claim construction presented for the first time on appeal, it is equally unfair to expect a plaintiff or defendant to be bound by a new claim construction entered post-trial, post-verdict, and with no opportunity to respond.

II. The Federal Circuit’s Conflicting Approaches

The Federal Circuit’s body of cases has yielded a rudderless approach hinging on a meaningless distinction between a “new” claim construction, on the one hand, and a mere “clarification” or “elaboration,” on the other. The standardless precedent obscures the fundamental premise that a settled claim scope, *i.e.*, a defined legal right, is necessary before parties close their evidence presentation and before the court or jury decides infringement, validity, and other dispositive issues.

As noted above, the Federal Circuit does, on occasion, correct errors when a trial court changes the construction too late in the game. *E.g.*, *Wi-LAN*, 811 F.3d at 464-65 (agreeing that “the district court’s post-verdict addition of a complex multiplier requirement was a new claim construction,” and improper at the JMOL stage). Even where the plain-and-ordinary-meaning construction

applies as “the construction agreed upon by the parties,” a court cannot materially change that construction after adjudication and apply a new construction in a dispositive manner. *Magnolia Med. Techs., Inc. v. Kurin, Inc.*, 169 F.4th 1094, 1102-03 (Fed. Cir. 2026).

A distinct line of Federal Circuit precedent has created a carveout, however, for so-called claim-construction “clarifications” and “elaborations” that purportedly do not rise to the level of a “new” construction. In those instances, the appeals court minimizes the impact of the changed claim construction by characterizing it as a mere “elaboration” or “clarification.” The appeals court has never explained whether “elaboration” and “clarification” are conceptually identical, although dictionary definitions suggest some daylight between the two words’ meanings. *See, e.g.*, Elaborate, *Merriam-Webster’s Collegiate Dictionary* (11th ed. 2020) (defining “elaborate” as “to expand something in detail” or “to add details to”); Clarify, *Merriam-Webster’s Collegiate Dictionary* (11th ed. 2020) (defining “clarify” as “to make understandable” or “to free from confusion”).

For instance, in *Magnolia*, 169 F.4th at 1102, the district court changed from the plain and ordinary meaning and later interpreted the claim as requiring a separate “vent” and a separate “seal.” The Federal Circuit saw this as a “permissible clarification” of “what was inherent in the [plain-and-ordinary-meaning] construction.” *Id.*

In *Mformation Technologies, Inc. v. Research in Motion Ltd.*, 764 F.3d 1392, 1395 (Fed. Cir. 2014), the district court clarified its previous claim construction of the “establishing a connection” limitation to mean that the sub-step must be completed before the “transmitting the contents of the mailbox” sub-step can commence. The Federal Circuit characterized the changed construction

as “at most clarify[ing] its previous construction that was already present in the jury instructions.”

Similarly, in *Cordis Corp. v. Boston Scientific Corp.*, 658 F.3d 1347, 1355-57 (Fed. Cir. 2011), the district court construed the term “undulating” to mean having “a crest and a trough.” Later the district court applied a “post-verdict elaboration” that required multiple waves that was not infringed by a “U shape,” *i.e.*, two crests and one trough. *Id.* This “post-verdict elaboration” was, according to the Federal Circuit, only a clarification of the construction’s “inherent” meaning.

More recently, in *Wyeth LLC v. AstraZeneca Pharmaceuticals LP*, 180 F.4th 1371, 1378-79 (Fed. Cir. 2026), the court allowed a post-verdict “elaboration” of the pharmaceutical term “unit dosage”—about a single dosage form—to also require that the “unit dosage” produces the desired therapeutic effect in the patient.

These and similar decisions provide no standard by which one can discern between (a) a mere “clarification” or “elaboration” that does not require notice and an opportunity to respond and (b) a “new” construction that does. This standardless approach is particularly problematic when a “clarification” or “elaboration” effects a change that the parties did not anticipate—especially in instances, as here, where the “clarification” or “elaboration” completely flips the infringement outcome, wiping out a billion-dollar judgment of liability on the same fact record with respect to the infringement analysis.

Under any label, post-trial modification of claim terms is not appropriate when the party cannot meaningfully respond to the new claim understanding. Due process requires notice and fair opportunity to present evidence with the benefit of the court’s claim construction.

III. The Affirmance of Noninfringement is Erroneous

The Federal Circuit’s affirmance of noninfringement is wrong. Centripetal had no fair notice and no opportunity to address dispositive departures from the previously agreed-upon plain-meaning constructions. The meaning of the claim terms was the settled legal premise of a completed twenty-two-day trial and a final judgment. The claim constructions remained applicable after the Federal Circuit’s vacatur. Pet.App. 168a. The new post-trial claim constructions were determined without notice, *Markman* briefing, or an opportunity to be heard.

A. The Federal Circuit Mischaracterized the Substantial Claim-Construction Shift

The Federal Circuit failed to see the significant material change effected by the new construction of the ’193’s “particular type of data transfer” limitation, as compared to the earlier plain-meaning construction. The court instead vaguely referenced “any shift in the original construction,” but that characterization is a manifestation of the Federal Circuit’s rudderless approach to post-adjudication changes in claim constructions.

Here, the district court’s “clarification” in its Remand Order and later “further clarification” in the Reconsideration Order underscore that material difference with the new construction. It departed significantly from the earlier plain-meaning construction, as used during the trial and in Judge Morgan’s infringement ruling. Pet.App. 218a-221a.

The district court’s first explicit construction of “particular type of data transfer” (in the Remand Order) required “filtration of a subset of packets sent between [endpoint] computers in two different networks.” Pet.App. 88a-90a. Then, in the Reconsideration Order, the court changed again with its “further clarification.”

Pet.App. 32a. There, the court stated that the limitation “refers to the specific technique, or method, associated with the data transmission.” Pet.App. 35a. The initial “clarification” and the subsequent “further clarification” worked to drastically move the legal boundary twice, so much so that the twice-changed claim construction was determinative in overruling the willful infringement finding.

The substantial claim-interpretation change is also reflected in the district court’s need to rely on the new POPR Exhibit, admitted over Centripetal’s objection. The POPR Exhibit was the keystone to the district court’s new construction (later accepted by the Federal Circuit), stemming from the new application of prosecution-disclaimer doctrine. But neither the Federal Circuit nor the district court applied the “clear and unmistakable surrender” standard required by *Aylus Networks*, 856 F.3d at 1359-62. *See* Pet.App. 15a-16a; Pet.App. 91a.

Ultimately, Judge Hanes viewed the Rule 63 hearing as “day one of the trial,” which it was not. Dk.No.750 at 11. She also believed that the court was “permitted to revisit claim construction,” which created tension with the intact *Markman* Order. *Id.* In the end, the district court did in fact “revisit claim construction,” but in a manner that does violence to *Markman*’s objective of claim-construction uniformity as well as settled procedures to ensuring fair process when adjudicating patent rights.

Here, the Federal Circuit’s decision, as in its other decisions, expresses little about the claim-construction departure, well captured by its “any shift in the original construction” remark. Pet.App. 17a. Overlooking the magnitude of the “shift in the original construction” is a manifestation of the appeals court’s quagmire of cases advancing a meaningless distinction between a “new” construction and so-called “clarifications” and “elaborations.”

B. Centripetal Had No Notice of or Opportunity to Respond to the New Claim Constructions

Centripetal did not receive notice of the new interpretation of “particular type of data transfer” for the ’193 patent, until after the Rule 63 hearing. Neither party asked for an explicit construction of the “particular type of data transfer” limitation. At most, the district court expressed interest in reconsidering the claim constructions, despite the *Markman* Order remaining in force after the remand. *See* Dkt.No.750 at 11. Despite its expressed interest to reassess claim scope, the district court did not ask for any *Markman* briefing, as is standard, accepted practice. *Mullane v. Cent. Hanover Bank & Tr. Co.*, 339 U.S. 306, 314-15 (1950) (“The fundamental requisite of due process of law is the opportunity to be heard.”).

The Federal Circuit dismissed the lack of notice in a single paragraph. Pet.App. 16a-17a. The terse ruling embodies legal error on what constitutes sufficient notice in view of such a radically changed claim construction. *Eon-Net LP*, 249 F. App’x at 193-95 (vacating where “Eon-Net did not have notice that the district court would sua sponte grant summary judgment on issues of claim construction”).

First, the Federal Circuit did not account for the parties’ acceptance of the plain-meaning construction throughout the litigation, as opposed to the later new construction adopted after the Rule 63 hearing. That the court and the parties agreed to use the plain-meaning construction for three years is the antithesis of being on notice about a possible subsequent change after the Rule 63 hearing. If anything, Centripetal reasonably expected that the same plain-meaning construction applied by Judge Morgan would likewise be applied by Judge Hanes.

Second, the Federal Circuit relied on evidence that cannot establish fair notice. Two of the cited documents were filed in 2023 during the Rule 63 proceeding, long after the 2020 trial. *See* Pet.App. 16a-17a. The court also relied on Cisco’s counsel’s closing argument in the June 2023 Rule 63 hearing. Of course, closing argument is far too late to advance a new claim construction.

The Federal Circuit also relied on *Hamilton Beach Brands, Inc. v. freal Foods, LLC*, 908 F.3d 1328 (Fed. Cir. 2018), and *Google LLC v. EcoFactor, Inc.*, 92 F.4th 1049 (Fed. Cir. 2024). Neither case is remotely similar. In *Hamilton Beach*, the party had a chance to respond in its reply brief to a new claim construction proposed by the patent owner in its opposition. 908 F.3d at 1338. In *Google*, both parties recognized that “the core issue related to the scope and boundaries” of the disputed limitation. 92 F.4th at 1057. Neither case authorizes a district court to adopt and apply a new claim construction after a case has been tried.

Further, Centripetal explicitly informed the court that it “would like to recall some witnesses based upon the claim construction issue” if the court were to adopt a new construction adverse to Centripetal. *See, e.g.*, Dkt.No. 754 at 432-37. Because the request was denied, *id.*, the expectation was that the Rule 63 proceeding would use the same plain-meaning claim constructions applied by Judge Morgan.

The Federal Circuit’s legal error was not harmless for several reasons. Centripetal could have shown that the POPR Exhibit did not constitute a clear and unmistakable surrender under Federal Circuit precedent. Additional evidence would show that the new claim construction was wrong based on, for example, a correct reading of the patent specification and a correct application of the claim-differentiation doctrine. Had the Federal Circuit applied the law correctly and not accepted

the post hoc claim-construction change, then infringement should have been found, consistent with Judge Morgan's ruling.

C. The Court Committed Similar Error for the '806 Patent

The Federal Circuit's decision repeated a similar lack-of-notice error when affirming noninfringement of the '806 patent. The appeals court affirmed the changed construction of the term "responsive to being signaled," Pet.App. 18a-19a, that, after the Rule 63 hearing, became determinative of the district court's non-infringement ruling, Pet.App. 105a-116a. All evidence relevant to infringement of the '806 patent during the Rule 63 proceeding was the same evidence in the 2020 trial. The controlling difference was Judge Hanes's late-breaking construction of "responsive to being signaled," effected without *Markman* briefing or a hearing.

In its Remand Order, the district court applied a new express construction for the first time, requiring that the rule-swap signal be the but-for, *i.e.*, sole, cause of *each* enumerated step in the claimed sequence for updating to the second rule set. *Id.* That narrowing construction eliminated Centripetal's entire infringement theory and thus foreclosed Centripetal's ability to prove that Cisco's products meet the "responsive to being signaled" limitation. The new claim construction was the only difference, the factual evidence being identical.

The '806 patent is the "Rule Swap" patent. The invention enables the network device to swap one rule set with a second rule set, "on the fly without bringing down the network." Dkt.No.750 at 42. Evolving threat conditions may warrant the implementation of new rules that are more effective at addressing network threats. *Id.*

The rule-swap claim provides the steps employed for seamlessly updating to the second rule set. The claim includes five enumerated steps, as set forth below.

- [1] cease processing of one or more packets;
- [2] cache the one or more packets;
- [3] reconfigure to process packets in accordance with the second rule set;
- [4] signal completion of reconfiguration to process packets in accordance with the second rule set;
- and
- [5] responsive to receiving signaling that each other processor ... has completed reconfiguration ..., process, in accordance with the second rule set, the one or more packets.

Pet.App. 7a-8a. The five steps accomplish the update to the second rule set, which occurs “responsive to being signaled to process packets in accordance with the second rule set.” *Id.*

Using Centripetal’s plain-and-ordinary-meaning construction, Judge Morgan found that Cisco’s products met this limitation because Cisco’s products are configured to perform the five steps once the signal indicates that a second rule set should be implemented. Pet.App. 316a-319a. Absent the signal to switch to the second rule set, the Cisco products do not perform the five-step process set forth in the ’806 claim.

Cisco argued that, in its products, the first two steps (“cease processing” and “cache”) occur all the time, even outside the context of being responsive to the rule-swap signal. But simply because the first two steps may occur in Cisco’s default configuration does not avoid the “responsive to being signaled” limitation—unless the claim is narrowed to require that the rule-swap signal is the only reason the device performs the first two steps.

Cisco’s “responsive to being signaled” argument (adopted by the court as the predicate to the noninfringement finding) necessarily reinterpreted the claim as requiring the causal connection between the rule-swap signal and all five enumerated steps. In other words, even though the rule-swap signal is the reason why the Cisco products perform the five enumerated steps, the district court imposed a new construction that excluded that activity from infringement (in contrast to Judge Morgan’s earlier ruling).

Beyond the apparent change in claim interpretation, the new interpretation is wrong. The text, grammar, and structure of the claim do not impose any requirement that the swap signal must be the causative predicate for each of the five enumerated steps. To wit, when the five steps occur together in sequence, as a whole, as a result of the rule-swap signal, the claimed rule-swap sequence is performed, even if one or two of the enumerated steps occur in another process.

During the Federal Circuit oral argument, Judge Taranto noted that reading the five enumerated steps “as a single thing ... is obviously responsive because the signal triggers ... the sequence as a whole,” and that the dispute “is just a claim construction problem.” Oral Arg. 28:41-29:34. He also queried whether the “sequence as a whole” reading is “confirmed by the way ... the last step specifically adds the word ‘responsive’ ... and that’s missing from ... the ceasing step.” Oral Arg. 14:42-15:20. That view reflects a paradigmatic plain and ordinary reading of the term, based on standard English textual interpretation.

Equally important, there could not be waiver of Centripetal’s arguments about the plain meaning of the “responsive to being signaled” limitation because the arguments responded to precisely the same Cisco arguments Judge Morgan rejected in 2020. Pet.App.

316a-319a. Judge Morgan applied the plain-and-ordinary meaning construction in a manner consistent with Centripetal’s infringement case in both the 2020 trial and the Rule 63 proceeding. The subsequent about-face—on the factual finding of infringement to no infringement—is attributable solely to Judge Hanes’s narrowing construction requiring but-for causation. It is unclear how Centripetal could have forfeited its plain-meaning construction that prevailed at the first trial and then was rejected three years later.

Had the Federal Circuit and the district court applied the accepted plain-and-ordinary-meaning construction of “responsive to being signaled” correctly to the infringement-related facts (which were the same set of infringement facts from the 2020 trial), then Judge Morgan’s infringement ruling should have withstood the Rule 63 proceeding.

IV. The Federal Circuit’s Error is a Recurring Issue of Exceptional Importance

Disputes about fair notice and the opportunity to respond to late claim constructions arise frequently, and the Federal Circuit’s continued standardless rulings exacerbate the judicial landscape equally for patent owners and accused infringers. The Federal Circuit’s missteps are not isolated but follow from its failure to adequately respect the importance of the settled *Markman* process and associated procedural norms noted above.

1. Fair notice about the scope of an asserted patent claim is a fundamentally important issue in all patent cases. After all, “the name of the game is the claim.” *In re Hiniker Co.*, 150 F.3d 1362, 1369 (Fed. Cir. 1998) (quoting Judge Giles S. Rich’s famous phrase); *see also* Mark A. Lemley, *The Changing Meaning of Patent Claim Terms*, 104 Mich. L. Rev. 101, 101 (2005) (“The

claims of a patent are central to virtually every aspect of patent law.”).

It is critically important to ensure that any legal dispute—especially a patent dispute—is not decided based on moving definitions of the legal right. No fair judicial process condones moving-target adjudication. And because claim construction is so fundamental to every patent dispute, a shifting claim construction is anathema to the fair resolution of patent disputes.

2. The need for uniformity for such a fundamental patent-law issue is particularly acute. Clear patent-law rules promote investment, facilitate technology transfer, encourage competition through innovation, and strengthen the United States’s leadership in critical industries. Because patent law shapes decisions affecting countless innovators and billions of dollars in economic activity, the question presented is one of exceptional national importance. Without reasonable certainty about patent rights, the innovation-backed investments become susceptible to being coopted by infringers, free riders, and others who disregard the significant time and monetary resources needed to keep advancing innovation.

3. The Federal Circuit’s inconsistent treatment of late-construed patent claims, including after trial and verdict, is a recurring and significant hurdle to the fair adjudication of patent rights. Importantly, the question presented affects patent owners and accused infringers alike. Litigants asserting or defending against patent-infringement claims need an administrable rule that establishes what process is due when a court changes the claim construction during the course of the case. The sought-after relief does not favor those who favor strong patent rights. Nor does it favor those who believe that innovation is better advanced through other incentives. The Federal Circuit’s lack of an administrable rule acts as an equal-opportunity hurdle, impacting the business

expectations of companies that need patents to protect their research and investments and also of companies that compete and advance through other means.

V. The Case Is A Good Vehicle For Resolving The Question Presented

This case presents a clean vehicle to address the Federal Circuit's standardless precedent concerning when a late breaking, materially different claim construction requires a full and fair opportunity to respond to the new construction.

The non-infringement ruling by the court of appeals is predicated on a legal issue that, if resolved in Centripetal's favor, would grant Centripetal its sought-after relief. The construction of each claim limitation of each patent is outcome-determinative of the infringement question for each patent, as decided by the appeals court.

The issue has sufficiently percolated at the Federal Circuit. There is no indication that the appeals court is positioned to resolve the lack of a reasonable standard for assessing new claim constructions. The court's reliance on the distinction between a "new" construction and a so-called "elaboration" or "clarification" has been percolating for years.

Finally, the legal question has been preserved throughout the course of the litigation. Centripetal objected when the claim-construction issue first emerged at the Rule 63 hearing. Centripetal requested an opportunity to brief the issue and submit new evidence before the district court, and on appeal, it challenged the district court's application of new claim constructions, adopted without notice or *Markman* briefing.

CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully submitted.

MATTHEW J. DOWD
Counsel of Record
ROBERT J. SCHEFFEL
ELLIOT A. GEE
MORRIS D. YOUNG
DOWD SCHEFFEL PLLC
*1717 Pennsylvania Ave.,
NW
Suite 1025
Washington, DC 20006
(202) 559-9175
mdowd@dowdscheffel.com*

SEPTEMBER 2026

APPENDIX

TABLE OF APPENDICES

	<i>Page</i>
APPENDIX A – OPINION OF THE UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT, FILED APRIL 29, 2026	1a
APPENDIX B – MEMORANDUM ORDER OF THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA, NORFOLK DIVISION, FILED JUNE 14, 2024	23a
APPENDIX C – MEMORANDUM OPINION AND ORDER OF THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA, NORFOLK DIVISION, FILED DECEMBER 11, 2023	57a
APPENDIX D – OPINION OF THE UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT, FILED JUNE 23, 2022 . .	139a
APPENDIX E – OPINION AND ORDER OF THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA, NORFOLK DIVISION, FILED OCTOBER 5, 2020	170a
APPENDIX F – OPINION AND ORDER OF THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA, NORFOLK DIVISION, FILED OCTOBER 2, 2020	402a

1a

**APPENDIX A — OPINION OF THE UNITED
STATES COURT OF APPEALS FOR THE
FEDERAL CIRCUIT, FILED APRIL 29, 2026**

UNITED STATES COURT OF APPEALS
FOR THE FEDERAL CIRCUIT

2024-2097

CENTRIPETAL NETWORKS, LLC,

Plaintiff-Appellant

v.

CISCO SYSTEMS, INC.,

Defendant-Appellee

Filed April 29, 2026

OPINION

Appeal from the United States District Court for the
Eastern District of Virginia in No. 2:18-cv-00094-EWH-
LRL, Judge Elizabeth W. Hanes.

Before LOURIE, DYK, and TARANTO, *Circuit Judges*.

DYK, *Circuit Judge*.

Centripetal Networks, LLC (“Centripetal”) appeals
the district court’s judgment of noninfringement in favor
of Cisco Systems, Inc. (“Cisco”) as to the asserted claims

Appendix A

of three of its patents—U.S. Patent Nos. 9,686,193 (“’193 patent”), 9,203,806 (“’806 patent”), and 9,560,176 (“’176 patent”). These patents relate to filtering packets of data for security threats when they are transferred between computer networks.

The district court held that Cisco’s products do not infringe the ’193 patent because they filter packets by source and destination, which only meets step one of two filtration steps that the asserted claims require. The district court also held that Cisco’s products do not infringe the ’806 patent because the claim term “responsive to” requires but-for causation of “ceas[ing] processing” packets in “respons[e] to” a signal, and Cisco’s products do not perform this step. Finally, the district court held that Cisco’s products do not infringe the ’176 patent because they do not correlate packet ingress and egress records or automatically generate and implement new rules without human intervention as required by the asserted claims. We affirm all three rulings and accordingly *affirm* the district court’s judgment of noninfringement.

BACKGROUND

This case comes to us for a second time. Following a bench trial, the district court originally entered judgment holding that Cisco willfully infringed the asserted claims of the ’193, ’806, and ’176 patents. *Centripetal Networks, Inc. v. Cisco Sys., Inc.*, 38 F.4th 1025, 1027 (Fed. Cir. 2022). While the case was pending, the district judge discovered his wife owned Cisco stock. *Id.* at 1028. Cisco moved for the judge’s recusal under 28 U.S.C. § 455. *Id.* at 1029. In

Appendix A

an attempt to comply with the statutory requirements, the judge placed his wife's stock in a blind trust and denied Cisco's motion. *Id.* On appeal, we held that placing stock in a blind trust did not satisfy the requirements of § 455(f) and accordingly vacated the district court's judgment; ordered that the case "be assigned to a new judge . . . pursuant to Rule 63;" and remanded "for further proceedings before [the] newly appointed judge, who shall decide the case without regard for the vacated opinions and orders." *Id.* at 1040. On remand, the new judge concluded Cisco did not infringe the three asserted patents.

Although the district court did not resolve questions of infringement with respect to another asserted patent, U.S. Patent No. 9,917,856, the district court issued a Rule 54(b) judgment as to the three patents found not to infringe. Centripetal appeals.

I. THE ASSERTED PATENTS AND CISCO'S ACCUSED PRODUCTS

The case involves three separate patents. The '193 patent relates to filtering network data transfers to prevent "[a] category of cyber attack known as exfiltrations," '193 patent, col. 1 ll. 24–27, which "involve[] a circumstance where an attacker gains access to a computer inside of a network and sends protected information outside of that network," J.A. 34 n.5.¹ Claim 18, which is representative of the asserted claims, recites, in relevant part:

A system comprising:

1. Citations to the J.A. refer to the Confidential Joint Appendix filed by the parties at Dkt. No. 23.

4a

Appendix A

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. . . .

'193 patent, claim 18 (emphases added).

Appendix A

The specification of the '193 patent explains that “[t]he filtering process described herein may be viewed as having two (2) stages” where “the first stage may determine if the network policy allows any communications between the resources identified in the 5-tuple rule,”² for example, between the source and destination networks of a packet, and “the second stage may determine if the policy allows the specific method or type of communication . . . between the resources.” *Id.* col. 8 ll. 39–52. Similarly, in opposing a petition for Inter Partes Review (“IPR”) before the United States Patent and Trademark Office (“PTO”), Centripetal cited this language from the specification and confirmed that “[t]hese rules involve implementing a two-stage process for filtering traffic[.]” J.A. 19013 (quoting '193 patent, col. 8 ll. 45–52).

The '806 patent relates to swapping rules that network protection devices use to filter data packets. '806 patent, abstract. “Such rules are often grouped into rule sets, which may form one or more network policies.” *Id.* col. 1 ll. 11–13. Claim 9, which is representative of the asserted claims, recites, in relevant part:

A system comprising:

a plurality of processors; and

2. The 5-tuple refers to certain source, destination, and network flow information in a data packet header: “the source IP, the source port, the destination IP, the destination port, and the protocol.” J.A. 1991; *see also* '193 patent, col. 8 ll. 39–42.

6a

Appendix A

a memory comprising instructions that when executed by at least one processor of the plurality of processors cause the system to: . . .

configure at least two processors of the plurality of processors to process packets in accordance with the first rule set . . .

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.

'806 patent, claim 9 (emphases added).

7a

Appendix A

The '176 patent relates to a system that correlates packets transmitted and received by a network device. '176 patent, abstract. Claim 11, which is representative of the asserted claims, recites:

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

Appendix A

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.

'176 patent, claim 11 (emphases added).

Cisco markets and sells networking technology, including network security products. Centripetal alleges that several combinations of Cisco's networking hardware and software infringe the asserted claims. Most critical to this appeal are Cisco's switches and routers that are used to connect computing devices. Switches connect multiple devices on a single network, and routers connect devices across multiple networks.

*Appendix A***II. PROCEDURAL HISTORY**

In 2018, Centripetal sued Cisco for infringement of the '193, '806, and '176 patents.³ Between May 6 and June 11, 2020, the court held a twenty-two-day bench trial over video-conference. On October 5, 2020, the district court entered judgment in favor of Centripetal, finding that Cisco willfully infringed the asserted claims of the '193, '806, and '176 patents.

After trial, Cisco moved for the district court judge's recusal based on his wife's stock ownership in Cisco. The district judge placed the stock in a blind trust and denied the recusal motion, and Cisco appealed. On appeal, we concluded that the district court judge was required to recuse, vacated the judgment, and remanded the case for further proceedings with a new judge pursuant to Federal Rule of Civil Procedure 63 without regard to the vacated opinion. *Centripetal*, 38 F.4th at 1039–40.

On August 23, 2022, the case was reassigned to a new judge. Pursuant to Rule 63, the parties were given an opportunity to recall any witness whose testimony was material and disputed, but chose not to do so. Centripetal and Cisco also each filed a trial brief, presenting their claims and defenses, and filed proposed findings of fact and conclusions of law. The new judge then certified her familiarity with the record and held a hearing where

3. Various other patents were involved at other stages of the case. For example, the asserted claims of U.S. Patent No. 9,137,205 were found not infringed. As noted, issues of infringement as to the '856 patent remain pending.

Appendix A

each side presented a technology tutorial and presented argument on the '193, '806, and '176 patents.

On December 11, 2023, the district court issued an opinion granting judgment of noninfringement with respect to the three patents.⁴ As to the '193 patent, the district court first found that the asserted claims describe “a two-stage filtering method” where “[t]he first stage may determine if the network policy allows any communications between the resources identified in the 5-tuple rule” and “the second stage may determine if the policy allows the specific method or type of communication.” J.A. 41 (quoting '193 patent, col. 8 ll. 45–52). The court then concluded that the second stage requires “filtration of a subset of packets sent between computers in two different networks,” *i.e.*, that the system “drop some, but not all, packets sent between two different network destinations” which was a “functionality . . . not present in the accused technology.” J.A. 46.

As to the '806 patent, the district court concluded that Cisco's products do not infringe the asserted claims because the “cease/cache functionality . . . occurred as a part of normal packet processing in Cisco's accused devices, not in response to a signal to swap to a new rule set.” J.A. 60–61.

As to the '176 patent, the district court concluded that Centripetal “failed to show that (1) the accused

4. The asserted claims of the '856 patent were stayed and the district court issued a Rule 54(b) judgment.

Appendix A

technology correlates the packets entering and exiting a network device and that (2) responsive to the correlating, the system generates rules configured to identify patents in a specific network.” J.A. 75–76.

On January 8, 2024, Centripetal filed a motion for post-judgment relief. In relevant part, Centripetal argued that the district court misconstrued the asserted claims of the ’193 patent to require filtration of a subset of packets between two computers when the claims only require “filtration of a subset of data transfers from one *network* made up of many computers to a *second network*.” J.A. 22129 (emphases in original). Under its proposed construction, Centripetal argued that Cisco’s switches and routers infringe the asserted claims because they “block a particular subset of data transfers [from computers with a quarantine tag] from the first network to the second network.” J.A. 22132.

On June 14, 2024, the district court denied Centripetal’s motion. The district court acknowledged that “it is possible that the portion of first network packets described in the claim language contains packets that originated from multiple endpoint computers in the first network” and thus that “blocking the SGT-tagged packets received by the first network computing device may not mean blocking *all* packets from that device.” J.A. 93. However, the district court rejected Centripetal’s argument that Cisco’s quarantine procedure, which filters packets based on their source and destination, filtered by a “particular type of data transfer” as required by the claim language. *Id.* Instead, the district court clarified that the plain and

Appendix A

ordinary meaning of “‘particular type of data transfer’ refers to the specific technique, or method, associated with the transmission,” J.A. 94, and concluded that Cisco’s products do not infringe the asserted claims because they only filter packets by source and destination (stage 1 filtering), not the specific technique or method of the transfer, as required by stage 2.

Centripetal timely appeals. Because the district court entered partial final judgment under Rule 54(b), we have jurisdiction under 28 U.S.C. § 1295(a)(1).

DISCUSSION

In the context of a bench trial, we review a district court’s conclusions of law de novo and its factual findings for clear error. *Galderma Lab’sys, L.P. v. Lupin Inc.*, 122 F.4th 902, 907 (Fed. Cir. 2024). Infringement is a question of fact we review for clear error. *Id.* Claim construction based on intrinsic evidence is an issue of law that we review de novo. *Teva Pharms. USA, Inc. v. Sandoz, Inc.*, 574 U.S. 318, 326 (2015). To the extent the claim construction depends on extrinsic evidence, we review the district court’s factual findings under a clearly erroneous standard. *Id.* at 331.

I

With respect to the ’193 patent, Centripetal argues that the district court erred by improperly construing the term “particular type of data transfer” to exclude source and destination filtering pursuant to Cisco’s

Appendix A

quarantine procedure. Cisco argues that the district court's construction is supported by the specification and the prosecution history. We agree with Cisco.

Some background on Cisco's accused products is useful. Cisco's switches and routers are configured to apply packet-filtering rules, called access control lists ("ACLs"), that drop or forward packets. Centripetal alleges that a particular ACL, called the Security Group ACL ("SGACL") or "quarantine rule," which involves SGTtagging, infringes the '193 patent. This rule operates by directing a switch or router to drop a packet from a device tagged with a quarantine tag, if it is headed to a restricted destination.

While the claim language itself is less than clear, both the specification and the prosecution history make clear that the claims require two-stage filtering; that the first stage involves determining if the rules permit communication between two resources using the 5-tuple rule, including source and destination filtering; and that the second stage involves filtering by method or type of communication, and does not include source and destination filtering.⁵

The specification is "the single best guide to the meaning of a disputed term." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1315 (Fed. Cir. 2005) (en banc) (quoting *Vitronics*

5. While the district court relied on a technical dictionary to construe the asserted claims of the '193 patent, resorting to dictionaries is unnecessary here given the clarity of the specification and prosecution history.

Appendix A

Corp. v. Conceptronic, Inc., 90 F.3d 1576, 1582 (Fed. Cir. 1996)). As described above, the specification of the '193 patent explains, “[t]he filtering process described herein may be viewed as having two (2) stages.” ’193 patent, col. 8 ll. 39–40. It goes on to clarify that “[c]onceptually, the first stage may determine if the network policy allows any communications between the resources [(network devices)] identified in the 5-tuple rule” and “the second stage may determine if the policy allows the specific method or type of communication . . . between the resources.” *Id.* col. 8 ll. 45–52.

Significantly, in its response to a petition for IPR, Centripetal told the PTO that

the independent claims of the '193 patent recite rules for preventing the transfer of a subset of packets out of the network. These rules involve implementing a two-stage process for filtering traffic:

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.

J.A. 19013 (emphasis in original) (quoting '193 patent, col. 8 ll. 45–52).

Appendix A

Centripetal continued, “[t]hus the ’193 patent discloses exemplary embodiments for preventing exfiltrations when packets match (1) a particular source and destination criteria (*e.g.* the addresses of the first and second network of each independent claim) . . . **and** (2) a particular type of data transfer[.]” J.A. 19014 (emphasis in original). Accordingly, “once it is determined that a received packet matches the source/destination criteria . . . , the second stage . . . occurs, wherein an operator is applied to drop packets associated with a ‘particular type of data transfer.’” *Id.* In distinguishing the prior art (Sourcefire), Centripetal argued that “Petitioner does not allege that Sourcefire discloses this claimed two-stage process.” J.A. 19024. These statements to the PTO make clear that the asserted claims of the ’193 patent disclose a two-stage filtering process and that the first stage involves filtering based on source and destination using the 5-tuple rule.

We recognized in *Aylus Networks, Inc. v. Apple Inc.*, 856 F.3d 1353 (Fed. Cir. 2017) that in “[a] patent owner’s preliminary response filed prior to an institution decision . . . the patent owner can define claim terms and otherwise make representations about claim scope to avoid prior art,” which the public is entitled to rely on. *Id.* at 1362 (citing *Biogen Idec, Inc. v. GlaxoSmithKline LLC*, 713 F.3d 1090, 1095 (Fed. Cir. 2013)). We accordingly held that “statements made by a patent owner during an IPR proceeding, whether before or after an institution decision, can be considered for claim construction.” *Id.*; *see also Shire Dev., LLC v. Watson Pharms., Inc.*, 787 F.3d 1359, 1366 (Fed. Cir. 2015). Here, Centripetal’s statements in the IPR proceeding define the scope of the asserted claims to

Appendix A

require two-stage filtering, with source and destination filtering being part of the first stage.

It is undisputed that the accused products here, Cisco's switches and routers implementing the quarantine rule, filter by source and destination at the first stage. *See* Oral Arg. at 5:00–5:25 (Centripetal agreeing that Cisco's quarantine rule is applied “based on the criteria in the 5-tuple”). Centripetal nonetheless argues that source and destination filtering also satisfies filtering at the second stage by “particular type of data transfer.” But on the face of the specification and prosecution history, the two stages are distinct and there is no indication that source and destination filtering would satisfy the second stage.⁶ Because Cisco's accused products only filter by source and destination, Cisco's products do not infringe the asserted claims of the '193 patent. *See* Oral Arg. at 7:00–7:15 (Centripetal agreeing it would lose based on this construction).

Centripetal also argues (somewhat inconsistently with the concession described above) that we should remand because the district court adopted a new claim construction in its post-judgment opinion, and Centripetal did not have the opportunity to present evidence of infringement under this construction. But Centripetal had adequate notice of Cisco's claim construction positions with respect to the

6. The unasserted claims of the '193 patent add limitations specifying certain types of data transfers. *See, e.g.*, '193 patent, claims 10–13, 15. Centripetal concedes in its Reply Brief that these are examples of “particular type[s] of data transfer[s].” Reply Br. 12.

Appendix A

'193 patent. In its post-trial proposed findings of fact and conclusions of law, Cisco argued that the asserted claims of the '193 patent require two-stage filtering and that its products, which allow or drop packets by source and destination, are only capable of filtering at the first stage. J.A. 17865–66. Cisco made the same argument in its trial brief and at the Rule 63 hearing. *See* J.A. 19450–54; 21283. Our cases make clear that, even in the PTAB context (with more stringent procedural requirements than in district court cases), any shift in the original construction does not create any unfairness where, as here, the challenger consistently put the patentee on notice of its interpretation of the asserted claims. *See Hamilton Beach Brands, Inc. v. f'real Foods, LLC*, 908 F.3d 1328, 1338–39 (Fed. Cir. 2018); *Google LLC v. EcoFactor, Inc.*, 92 F.4th 1049, 1057 (Fed. Cir. 2024).

Finally, Centripetal argues that Cisco's products infringe the asserted claims of the '193 patent even under the district court's construction. Centripetal's argument appears to be based on the theory that Cisco's switches and routers could be modified to filter by a "particular type of data transfer," but this hardly suggests that Cisco's switches and routers infringe in their current configurations. The testimony Centripetal cites to support the contention that Cisco's switches and routers already have this functionality only shows that the switches and routers can identify and flag suspicious types of data transfers which "would lead to the [implementation of] quarantine rules." J.A. 1512. Centripetal has not identified any evidence suggesting that *the quarantine rule* filters by "particular type of data transfer."

*Appendix A***II**

As to the '806 patent, the issue is whether the district court erred when it found Cisco's accused devices to be noninfringing because the claim-specified signal does not cause those devices to "cease processing" packets. '806 patent, claim 9. The accused products here are Cisco's switches, routers, and firewalls (in combination with certain management programs) which can implement rule swapping procedures to update packet-filtering rules. Once a rule swap procedure is activated, Cisco's products swap rules "during the devices' existing idle period between the processing of individual packets." J.A. 56; *see also* J.A. 58.

The district court found that the accused products do not infringe the asserted claims because they "cease [processing] . . . as a part of normal packet processing[,] . . . not in response to a signal to swap to a new rule set." J.A. 60–61. Centripetal argues that the district court must be reversed because "responsive to" only requires that "when the system receives a signal to perform a rule swap, it immediately proceeds to perform the entire rule-swapping sequence," Appellant's Br. 27, not that the signal be the but-for cause of each component part, such as "ceas[ing] processing." Nothing in the district court's opinion, J.A. 52–57, or anything Centripetal cites to us from its filings in the district court, indicates that Centripetal fairly presented the district court with this claim construction or argued that the plain and ordinary meaning leads to this interpretation of the claim (requiring causation of the sequence as a unit, but not of any individual

Appendix A

component). *See* Appellee’s Br. at 50 (asserting forfeiture of Centripetal’s causation position at Appellant’s Br. at 27, 44); Appellant’s Reply at 21–22 (not identifying where in the district court the position was presented). Under these circumstances, Centripetal forfeited this argument.

In any event, the most natural understanding of the claims is that the signal must be the but-for cause of ceasing processing packets. The asserted claims specify a list of actions the claimed processors must be configured to do “responsive to being signaled to process packets in accordance with the second rule set.” ’806 patent, claim 9. The first item on this list is “cease processing of one or more packets.” *Id.* The specification adds support to this interpretation as it describes this causal relationship set apart from any other elements of the rule swapping procedure: “Responsive to signaling the processors to process packets in accordance with the second rule set, the processors may cease processing packets.” *Id.*, col. 1 ll. 61–64.

As it is undisputed that Cisco’s accused products cease processing packets in the normal course of processing, and not in response to a signal, we conclude that the accused products do not infringe the asserted claims of the ’806 patent.

III

As to the ’176 patent, Centripetal alleges Cisco’s switches and routers, using a threat analysis program called Stealthwatch, infringe the asserted claims.

Appendix A

Stealthwatch analyzes logs of packet information (called NetFlow logs) and sends alerts to a management console based on suspected malicious activity. The district court concluded that the accused products do not infringe the asserted claims because Centripetal failed to show that Cisco's technology "correlates the packets entering and exiting a network device" and "responsive to the correlating, . . . generates rules configured to identify packets in a specific network." J.A. 76. Centripetal argues the district court's finding of noninfringement rests on erroneous factual findings. Again, we disagree.

The district court determined that Cisco's products do not infringe the '176 patent because they cannot correlate NetFlow records. Centripetal argues that the district court ignored evidence that the accused devices correlate logging records other than NetFlow records, namely Syslog and Webflow. But Centripetal conceded at the Rule 63 hearing that its infringement position was based on NetFlow records. J.A. 21464. ("I think the evidence shows that NetFlow data is what we're accusing of infringing."). And the district court cited ample evidence to support the conclusion that Cisco's products do not correlate ingress and egress NetFlow log entries. *See* J.A. 78–81. Even if we were to consider Centripetal's arguments based on Syslog and Webflow, these logging records are generated by proxy sources, not Cisco's switches and routers, *see* J.A. 75, 19969, 19979, and Centripetal's expert admitted that "we don't actually have a proxy in this case," J.A. 1978.⁷

7. At the Rule 63 hearing, Centripetal seemed to agree that its arguments based on proxy data required "a different claim construction." J.A. 21464.

Appendix A

The district court also did not err in concluding that Cisco's accused products do not satisfy the claim limitations because they require human intervention in determining whether to apply rules in particular situations. The asserted claims require that a "processor cause the system to: . . . generate . . . one or more rules" and "provision a device . . . with the one or more rules." '176 patent, claim 11. The specification further explains that the "packet correlator . . . may generate or update rule(s)" and "may provision [a] device . . . with rules." *Id.*, col. 13 ll. 14–19. The specification thus contemplates that the rules are automatically executed by the processor. Stealthwatch does not issue rules, as the term was construed to require "a condition or set of conditions that when satisfied cause a specific function to occur." J.A. 9. Rather, as the district court found, Stealthwatch only issues *alerts* which advise individuals of potentially problematic situations. A human administrator must examine these alerts and determine whether to respond by issuing a quarantine tag. The district court did not clearly err in finding Cisco's technology does not perform these limitations of the asserted claims.

CONCLUSION

We conclude that the asserted claims of the '193 patent require filtering data at two stages, and the district court did not err in concluding that Cisco's accused products only perform filtering at the first stage. As to the '806 patent, we conclude that "responsive to" requires that the claimed signal be the but-for cause of "ceas[ing] processing" packets and, under this construction, the district court

22a

Appendix A

did not err in concluding that Cisco's accused products do not infringe the asserted claims. We also conclude that the district court did not err in concluding that Cisco's products do not perform every limitation of the asserted claims of the '176 patent. Accordingly, we affirm.

AFFIRMED

COSTS

Costs to Cisco.

**APPENDIX B — MEMORANDUM ORDER
OF THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA,
NORFOLK DIVISION, FILED JUNE 14, 2024**

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
NORFOLK DIVISION

Civil Action No. 2:18-cv-00094 (EWH)

CENTRIPETAL NETWORKS, LLC,

Plaintiff,

v.

CISCO SYSTEMS, INC.,

Defendant.

Filed June 14, 2024

MEMORANDUM ORDER

This matter is before the Court on Plaintiff Centripetal Networks, LLC's Motion for Additional and Amended Findings and Amended Judgment under Rule 52(b), or, in the Alternative, For a New Trial Under Rule 59(a)(2) (the "Motion"). ECF No. 787. For the reasons below, the Motion is DENIED.

On December 11, 2023, this Court entered a Memorandum Opinion and Order ("Opinion") finding

Appendix B

that Centripetal had failed to meet its burden to establish infringement by Defendant Cisco Systems, Inc. of U.S. Patent Nos. 9,686,193 (“the ’193 Patent”); 9,203,806 (“the ’806 Patent”); and 9,560,176 (“the ’176 Patent”). ECF No. 780. The Court determined that because Centripetal had not met its burden in establishing infringement, it was not necessary to reach issues related to patent validity or damages. *Id.* at 1. The following day, the Clerk entered partial final judgment in favor of Cisco, and thereafter Centripetal timely filed this Motion for relief. ECF No. 781.

I. LEGAL STANDARD

Rule 52(b) of the Federal Rules of Civil Procedure provides that “[o]n a party’s motion filed no later than 28 days after the entry of judgment, the court may amend its findings—or make additional findings—and may amend the judgment accordingly.” Fed. R. Civ. P. 52(b). Likewise, under Rule 59(a)(2), “[a]fter a nonjury trial, the court may, on motion for a new trial, open the judgment if one has been entered, take additional testimony, amend findings of fact and conclusions of law or make new ones, and direct the entry of a new judgment.” Fed. R. Civ. P. 59(a)(2).

In patent cases, the standard applied when determining whether relief should be granted under Rule 52(b) or Rule 59(a)(2) is governed by the law of the regional circuit. *Bettcher Indus., Inc. v. Bunzl USA, Inc.*, 661 F.3d 629, 638 (Fed. Cir. 2011); 9C Charles Alan Wright & Arthur R. Miller, *Federal Practice and Procedure* § 2582 (3d ed. Supp. 2024). The United States Court of Appeals for the

Appendix B

Fourth Circuit has previously recognized three grounds for amending an earlier judgment: “(1) to accommodate an intervening change in controlling law; (2) to account for new evidence not available at trial; or (3) to correct a clear error of law or prevent manifest injustice.” *Pac. Ins. Co. v. Am. Nat. Fire Ins. Co.*, 148 F.3d 396, 403 (4th Cir. 1998). “It is not the intention or purpose of Rules 52(b) and 59(e) to permit parties to relitigate old matters, or give an unhappy litigant one additional chance to sway the judge.” *Floyd v. City of Spartanburg S.C.*, No. 7:20-CV-01305-JDA, 2024 WL 771047, at *2 (D.S.C. Feb. 26, 2024) (cleaned up); *see also Blick v. Shapiro & Brown, LLP*, 2018 WL 9619434, at *1 (W.D. Va. Aug. 10, 2018) (“A party who failed to prove his strongest case is not entitled to a second opportunity to litigate a point, to present evidence that was available but not previously offered, or to advance new theories by moving to amend a particular finding of fact or a conclusion of law.” (quotation marks and citations omitted)).

II. DISCUSSION

Centripetal asks the Court to either reverse the judgment and find that Cisco infringed each of the three patents or reopen the case to allow for the presentation of additional evidence. In support of this extraordinary remedy, Centripetal contends that the Court committed “clear errors of fact and law” in its prior decision. Mem. in Supp. at 1, ECF No. 788. Plaintiff attributes these purported errors, in large part, to the unique posture of this case, in which the undersigned applied Rule 63 of the

Appendix B

Federal Rules of Civil Procedure to adjudicate the dispute using the trial record developed by a different judge.

As a brief background, in 2020, the Honorable Henry Coke Morgan, Jr. conducted a six-week bench trial via videoconference. Op. at 1. Judge Morgan ruled in favor of Centripetal, finding that Cisco's accused technology infringed the '193, '806, '176, and '856 Patents.¹ *Id.* Cisco appealed. Without reaching the merits, the Federal Circuit vacated Judge Morgan's infringement ruling and denial of Cisco's motion for a new trial. *Centripetal Networks, Inc. v. Cisco Sys., Inc.*, 38 F.4th 1025, 1030–33, 1040 (Fed. Cir. 2022). The Court remanded the case for further proceedings before a new judge and directed that the proceedings be conducted pursuant to Federal Rule of Civil Procedure 63. *Id.* at 1040. Rule 63 provides that “[i]f a judge conducting a hearing or trial is unable to proceed, any other judge may proceed upon certifying familiarity with the record and determining that the case may be completed without prejudice to the parties.” Fed. R. Civ. P. 63. The Rule also states that “[i]n a hearing or a nonjury trial, the successor judge must, at a party's request, recall any witness whose testimony is material and disputed and who is available to testify again without undue burden.” *Id.*

1. Following remand, the Court stayed the proceedings with respect to U.S. Patent No. 9,917,856 (“the '856 Patent”) due to the PTAB's issuance of a final written decision declaring the '856 Patent claims asserted by Centripetal unpatentable. ECF No. 715; *see also* ECF No. 686.

Appendix B

Following remand, both parties submitted their respective positions on how the case should proceed. ECF Nos. 656, 657. Centripetal requested that the case be decided “based on the current record,” and noted that recalling witnesses would be “unnecessary and wasteful.” Pl.’s Notice at 1–2, ECF No. 656. In its post-trial motion, however, Centripetal now seeks to reopen the record and allow new testimony and evidence. Centripetal contends this approach is warranted because the Court “altered the settled understanding of the constructions reached by the initial presiding judge.” Mem. in Supp. at 1–2. Because the Court concludes that the claim language—as construed in the February 2020 claim construction order—was applied without modification, and that Centripetal fails to provide any other compelling reason for the Court to modify its judgment, it denies Centripetal’s Motion.

A. ’193 Patent

In its Opinion, the Court found that the Accused Switches and Routers² did not infringe claims 18 or 19 of the ’193 Patent. Op. at 24–30. Claim 18 of the ’193 Patent describes a system that first “receive[s] . . . a plurality of packets” from a “computing device” in a “first network.” ’193 Patent at 14:5–6. Then, if the packets are “destined for [a] second network,” and the system makes a “determination that the . . . portion of packets comprises data corresponding to [rule] criteria . . . configured to prevent a particular type of data transfer from the

2. Capitalized terms not defined herein are defined in the Court’s Memorandum Opinion. ECF No. 780.

Appendix B

first network to [the] second network,” an operator is applied that is “configured to drop packets associated with the particular type of data transfer.” *Id.* at 14:9–22. Alternatively, if the packets are “destined for a third network” and the system makes a “determination that the . . . packets comprise[] data that does not correspond to the [rule] criteria,” an operator is applied that is “configured to forward packets not associated with the particular type of data transfer to the third network.” *Id.* at 14:23–36. Claim 19 describes the same technique. *See id.* at 14:37–15:2; *see also* Op. ¶¶ 6–7.

The Court held that Centripetal failed to prove infringement because it could not show that the accused devices drop or forward packets based on the “particular type of data transfer.” Op. at 24. In its post-trial motion, Centripetal (1) argues that the Court’s analysis relied on a new, flawed construction of “particular type of data transfer from [a] first network to a second network,” and advocates that the Court find infringement under an alternate construction of the term; (2) requests that if the Court “adheres to its new construction,” the record be reopened and Centripetal be allowed the opportunity to present new evidence; and (3) argues that the Court’s decision included erroneous factual findings regarding the operation of Cisco’s Accused Switches and Routers.

1. Claim Construction

Centripetal’s first argument focuses on the Court’s analysis of claim language requiring packet filtering of a “particular type of data transfer.” As an initial matter,

Appendix B

Centripetal never requested that this Court construe the term “particular type of data transfer”—during the *Markman* process or any time prior to entry of the judgment. The Court was therefore entitled to apply the plain and ordinary meaning of the term and Centripetal has “waived its right to [now] request a construction.” *Eli Lilly & Co. v. Aradigm Corp.*, 376 F.3d 1352, 1360 (Fed. Cir. 2004); see *Conoco, Inc. v. Energy & Env’t Int’l, L.C.*, 460 F.3d 1349, 1359 (Fed. Cir. 2006) (“[L]itigants waive their right to present new claim construction disputes if they are raised for the first time after trial.”). Indeed, “[i]t is the parties’ obligation to raise a dispute regarding the proper scope of claims to the court.” *ATEN Int’l Co., Ltd. v. Uniclass Tech. Co., Ltd.*, 932 F.3d 1364, 1370 (Fed. Cir. 2019). Failure to do so is an implicit concession that the term is “clear and not in need of construction.” *Eli Lilly & Co.*, 376 F.3d at 1360. The Court was therefore entitled to presume that Centripetal chose not to propose a construction of the term “because one of ordinary skill in the art would understand [its] plain meaning[.]” *Unitherm Food Sys., Inc. v. Swift-Eckrich, Inc.*, 375 F.3d 1341, 1350 (Fed. Cir. 2004), *rev’d in part on other grounds*, 546 U.S. 394 (2006).

Applying the plain and ordinary meaning of “particular type of data transfer,” the Court found that Cisco’s Accused Switches and Routers did not infringe claims 18 and 19 of the ’193 Patent. The evidence showed that when Cisco’s Accused Switches and Routers receive packets containing scalable group tags (“SGT” tags), they apply certain rules to the packets—specifically, Security Group Access Control Lists (“SGACLs”). *Id.* ¶¶ 11–12.

Appendix B

SGT tags are appended to all of the packets transmitted by computers in a defined security group, and each SGT tag is associated with a different SGACL, which contains instructions as to how the packet should be treated. *Id.* ¶ 12. One such security group is the “quarantine” group. *Id.* ¶¶ 12, 15. All packets transmitted from quarantined computers are appended with a quarantine SGT tag, and when the packets pass through the Accused Switches and Routers, the devices apply the quarantine SGACL, causing the packets to be forwarded or dropped depending on their destination. *Id.* ¶ 15.

Moreover, “[a]lthough Centripetal alleged that the Accused Switches and Routers infringe the asserted claims of the ’93 Patent based on the use of SGACL rules and SGT tags generally, at trial it focused only on their use in effecting a quarantine.” *Id.* ¶ 14. Accordingly, the Court based its infringement analysis on the quarantine functionality. Two important factual findings regarding the operation of the quarantine rules drove the Court’s conclusion: (1) that *all* packets transmitted from a computer in the quarantine group are appended with the quarantine SGT tag, and (2) that the quarantine SGACL instructs an Accused Switch or Router to either drop or forward a packet containing a quarantine SGT tag based on the packet’s destination. *Id.* ¶¶ 15–18. “In other words, the quarantine rule can be set up to block a computer from accessing specific endpoints, such as part of a network containing sensitive company documents, while allowing access to other destinations, like the Internet.” *Id.* ¶ 16.

Appendix B

The Court found this functionality—forwarding or dropping *all* packets from a computing device depending on what network that device is attempting to access—did not meet the “particular type of data transfer” limitation described in claims 18 and 19 of the ’193 Patent. The claims require that “two conditions must be met: (1) the packets from a device in a first network must be ‘destined for [a] second network’ and (2) the packets must meet rule criteria ‘configured to prevent a particular type of data transfer from the first network to [the] second network.’” *Id.* at 25 (alterations in original) (quoting ’193 Patent at 14:9–16). The Court concluded that, at a minimum, the reference to “particular type of data transfer” in the claim must refer to a *subset* of the packets from the “computing device” in the “first network” that are “destined for [a] second network.” *Id.* at 24–29. The reason is simple—if *all* packets from the computing device satisfied the “particular type of data transfer” condition, the condition would be rendered superfluous. *Id.* at 25 (citing *W.L. Gore & Assocs., Inc. v. Medtronic, Inc.*, 834 F. Supp. 2d 465, 477 (E.D. Va. 2011)). Moreover, the notion that “particular type” does not mean “all types” is obvious and aligns with the plain and ordinary usage of the term. Therefore, because evidence showed that “the Accused Switches and Routers . . . drop *all* packets from a quarantined computer to a restricted network destination and allow *all* packets from a quarantined computer to a permitted network destination,” Centripetal failed to meet the “particular type of data transfer” condition required by the claims. *Id.* at 23, 25.

Appendix B

In its post-trial motion, Centripetal takes issue with this analysis, suggesting that the Court improperly focused on filtration of “a subset of packets sent between *computers* in two different networks,” while the claims merely disclose “filtering a subset of data *transfers* between two different *networks*.” Mem. in Supp. at 5 (emphasis in original). The Court takes Centripetal to be suggesting the possibility that the packets received from the “computing device” in the first network described in the claim language could originate from multiple source computers in that network. *Id.* at 5–8. In that scenario, Centripetal appears to be claiming that a “particular type of data transfer” could refer not to a subset of the packets sent from a single quarantined computer, but instead to the subset of packets that originated from quarantined computers as compared to non-quarantined computers. *Id.* at 8 (explaining that Cisco’s devices infringe because they are able to “block certain *computers* in the first network—namely those that have been assigned a ‘quarantine’ SGT tag—from transferring packets to a second network”) (emphasis added).

The Court finds that further clarification is necessary. In its ruling, the Court couched its analysis within a framework in which the first network packets *originated* from the computing device. The necessary implication was that the “computing device” was an endpoint computer in the first network—one that either was, or was not, subject to a quarantine.³ As explained

3. Contrary to Centripetal’s argument, the Court did not view the ’193 Patent claims as *requiring* filtration of packets from a single computer in a first network. Rather, this framing was used

Appendix B

above, Centripetal’s infringement theory focused on the quarantine functionality of the accused devices, in which quarantine SGT tags are used to restrict the network access of a quarantined computer. The Court rejected Centripetal’s argument that SGT-tagged packets constitute a “particular type of data transfer” from the first network computing device (*i.e.*, the quarantined computer) because that would mean blocking or allowing *all* of the data transfers between the device and the second network. Op. at 27.

As Centripetal’s post-trial arguments suggest, the Court did not address the possibility that the packets received from the “computing device” in the first network might not have originated from that device. That point is well taken, as common technical definitions of “computing device” lend themselves to a broader understanding that also encompasses, most notably, routers and switches. *See, e.g., Computing Device*, Computer Security Resource Center, Nat’l Inst. of Standards & Tech., <https://perma.cc/LE82-YSWP> (defining “computing device” as “[a] machine (real or virtual) for performing calculations automatically (including, but not limited to, computer, servers, routers,

because it aligned with the arguments the parties presented at trial. *See, e.g.*, Tr. 869:6–12; Op. at 22 (depicting PTX-563 at 415). The Court also did not “assume that each network described in the claims contains just a single computer.” Mem. in Supp. at 7. The Court recognized that networks are made up of many different network devices; its reference to a computing device in the network simply tracked the claim language. *See, e.g.*, Op. at 11; ’193 Patent at 14:5–6 (“receive, from a computing device located in a first network, a plurality of packets . . .”).

Appendix B

switches, etc.”)). Therefore, since a “computing device” in the first network could be understood by a person of ordinary skill in the art to be a device that forwards packets from multiple endpoint computers in the first network, it is possible that the portion of first network packets described in the claim language contains packets that originated from multiple endpoint computers in the first network.

In that circumstance, blocking the SGT-tagged packets received by the first network computing device may not mean blocking *all* packets from that device—some of the packets may not be tagged (because they may not have originated from computers subject to quarantine). Centripetal appears to insist this “subset” is a “particular type of data transfer” and therefore the Accused Switches and Routers infringe. The Court disagrees, however, and finds that this argument requires a further elaboration of the plain and ordinary meaning of “particular type of data transfer.”

In order to do so, the Court consults relevant technical dictionaries. *See CCS Fitness, Inc. v. Brunswick Corp.*, 288 F.3d 1359, 1366 (Fed. Cir. 2002) (“[D]ictionary definitions may establish a claim term’s ordinary meaning.”). The McGraw-Hill Dictionary of Scientific and Technical Terms defines a “data transfer” as “[t]he technique used by the hardware manufacturer to transmit data from computer to storage device or from storage device to computer; usually under specialized program control.” *McGraw-Hill Dictionary of Scientific and Technical Terms* 550 (6th ed. 2003). Further, Merriam-Webster’s relevant

Appendix B

definitions for “type” include “a particular kind, class, or group” and “something distinguishable as a variety.” *Merriam-Webster’s Collegiate Dictionary* 1354 (11th ed. 2020). Accordingly, since a key distinguishing feature of a data transfer is the technique it employs, the plain and ordinary meaning of “particular type of data transfer” refers to the specific technique, or method, associated with the data transmission.

Therefore, regardless of whether the packets originated from the computing device, or were instead forwarded by the device from multiple endpoint computers in the first network, the “particular type of data transfer” claim limitation is not met. The problem with Centripetal’s argument is that a quarantine SGT tag appended to a packet does not specify the technique or method of data transmission associated with that packet. Instead, the evidence shows that the quarantine SGT tag is applied to *all* packets transmitted from a quarantined computer, regardless of the type of transfer. *See* Op. ¶ 17. Centripetal’s alternative reading—that SGT-tagged packets are themselves a particular type of data transfer—improperly focuses on the origin of the transfer (*i.e.*, the quarantined computer or group of computers), rather than the specific technique or method of the transfer. And even if this were a possible way to interpret the dictionary definitions, the specification clearly refers to the usage the Court adopts. *Id.* at 25–26 (discussing the specification); ’193 Patent at 2:43–54 (explaining filtration method that would “allow users to surf (e.g., GET) to one or more websites attached to the Internet,” but prevent riskier types of data transfers associated with exfiltration, such as “users

Appendix B

. . . writing (e.g., PUT) data files or posting (e.g., POST) forms to one or more websites”). This confirms the Court’s interpretation of the plain and ordinary meaning of the term (based upon dictionary definitions) and indicates that such a reading is not contrary to the ’193 Patent disclosure. *See Renishaw PLC v. Marposs Societa’ per Azioni*, 158 F.3d 1243, 1250 (Fed. Cir. 1998) (noting that one should not use a “common meaning” or definition from a “relevant dictionary” to determine the ordinary meaning of a claim term if it would fly “in the face of the patent disclosure”).

For these additional reasons, Centripetal has failed to prove infringement of the ’193 Patent by a preponderance of the evidence.

2. Reopening the Record

In the alternative, Centripetal requests that if the Court declines to adopt its interpretation of the claim language, it should reopen the record to allow Centripetal to present additional infringement evidence. Mem. in Supp. at 9–11. Centripetal asserts that when it “determined that no further record supplementation was necessary, it did not have notice of the Court’s narrowed interpretation of the claims, which departed from the plain and ordinary meaning and thus prejudiced Centripetal.” *Id.* at 9.

As discussed above, the Court’s interpretation of “particular type of data transfer” does not diverge from the term’s plain and ordinary meaning. And Centripetal’s assertion that it structured its case based on a “settled understanding” that SGT-tagged packets constitute

Appendix B

a “particular type of data transfer” is contrary to the record. *Id.* at 2. Centripetal never requested the Court construe the term and, importantly, has not held a consistent position on the term’s meaning. In fact, as the Court recounted in its Opinion, certain of Centripetal’s arguments align with the Court’s understanding of the term. *See, e.g.*, Op. at 28 (quoting Centripetal PFF ¶ 160) (“[The Accused Switches and Routers] are designed to implement quarantine rules based on detecting abnormal behavior in a variety of data transfer types, including Hypertext Transfer Protocol (HTTP), HTTP GET, and HTTP POST.”). Likewise, Cisco has consistently taken the position, from the 2020 trial through the Rule 63 proceedings, that “particular type of data transfer” refers to the method of the transfer. *See, e.g.*, Tr. 2355:4–22, 2362:9–2363:3, 2370:12–2372:25, 2375:2–2377:1, 2387:2–13, 2404:23–2405:16; 2423:25–2424:15; 2425:17–2426:21; 3274:10–3280:20; Rule 63 Tr. 297:8–25, 301:1–304:21, 314:8–14.⁴ Centripetal has had ample opportunity to raise this issue; doing so for the first time in its post-trial motion is impermissible. *See Enovsys LLC v. Nextel Commc’ns, Inc.*, 614 F.3d 1333, 1344 (Fed. Cir. 2010) (finding claim construction argument raised for the first time post-judgment was waived when the party had “never requested the district court construe” the term or “offer[] a construction of the term”).

The authorities Centripetal relies on in support of its position are far different from this case. Centripetal

4. “Tr.” refers to the trial transcript. ECF Nos. 496–550. “Rule 63 Tr.” refers to the transcript from the Rule 63 hearing. ECF Nos. 750, 753–44.

Appendix B

principally cites to *Wi-Lan, Inc. v. Apple, Inc.*, 811 F.3d 455, 464 (Fed. Cir. 2016). There, the Federal Circuit found that a district court erred in its post-trial ruling on a motion for judgment as a matter of law when it vacated the jury’s verdict of invalidity by applying a construction of a claim term that differed from the Court’s previous construction of the term. *Id.* at 464–65. Here, of course, there was no construction for the Court to modify. Centripetal also cites instances where courts have granted a new trial when a litigant presented a new theory of liability at trial. *Twigg v. Norton Co.*, 894 F.2d 672, 675–76 (4th Cir. 1990); *Becton Dickinson & Co. v. Tyco Healthcare Grp. LP*, No. Civ.A. 02-1694 GMS, 2006 WL 890995, at *12 & n.7 (D. Del. Mar. 31, 2006). These cases are even farther off the mark, as it is Centripetal who now seeks to raise new theories of liability *post-trial*.

The Court adopted the plain and ordinary meaning of “particular type of data transfer”—a meaning that, at times, Centripetal embraced. Centripetal makes no compelling argument for the Court to reopen the record.

3. Factual Findings

Centripetal also alleges that the Court’s opinion “rests on erroneous factual findings about the functionality of Cisco’s Switches and Routers.” Mem. in Supp. at 11. Centripetal points to the Court’s factual finding that “if the accused devices receive a packet containing a quarantine SGT tag, the devices apply the quarantine SGACL rule and forward or drop the packet depending on whether it is destined for a restricted destination as specified by the

Appendix B

ACL rules.” Op. ¶ 15; Mem. in Supp. at 11–13. Centripetal maintains that this “description elides the complex series of operations that these devices perform,” noting that the devices check the destination of the packet before applying SGACLs. Mem. in Supp. at 12. Because of this, argues Centripetal, “the Court’s finding that SGACLs are only destination-based cannot be correct.” *Id.*

Centripetal’s “destination-based” argument misconstrues the Court’s factual finding and does not identify any clear error in need of correction. Centripetal claims that the Accused Switches and Routers engage in more than a “simple destination check” when effecting a quarantine because they make decisions “based on the particular type of data transfer.” Reply at 6, ECF No. 808. In support, Centripetal cites evidence showing that the Accused Routers and Switches use SGT tag information when making forward/drop decisions. *Id.* at 8. But the Court explicitly described this functionality (use of SGT tag information) in the factual finding that Centripetal disputes. *See* Op. ¶ 15. Thus, although couched as a factual error, Centripetal’s argument here is simply a repackaging of its earlier argument that SGT-tagged packets constitute a “particular type of data transfer.” As discussed above, the Court has rejected this legal argument and Centripetal fails to otherwise identify any clear error of fact. *See supra* Part II.A.1.

Centripetal’s Motion is denied as to the ’193 Patent.

*Appendix B***B. '806 Patent**

In its Opinion, the Court found that Centripetal failed to meet its burden to establish that Cisco's Accused Switches, Routers, and Firewalls infringed claims 9 and 17 of the '806 Patent. Op. at 37–44. Claim 9 provides that based on “instructions . . . executed by at least one processor,” the system “receive[s] a first rule set and a second rule set,” “preprocess[es]” both rule sets, and “configure[s] at least two processors . . . to process packets in accordance with the first rule set.” '806 Patent at 11:18–29. Then, the system “receive[s] . . . packets” and “process[es], in accordance with the first rule set, a portion of the . . . packets.” *Id.* at 11:29–35. Next, in order to effectuate the rule swap, the system “signal[s] each processor . . . to process packets in accordance with the second rule set,” and “responsive to being signaled,” “configure[s] each processor” to take a series of actions. *Id.* at 11:35–53. Specifically, the processors are configured to “cease processing of one or more packets” and “cache the one or more packets,” and the system then “reconfigure[s] [the processor] to process packets in accordance with the second rule set.” *Id.* Once reconfiguration is complete, the system “signal[s] completion of reconfiguration,” and “responsive to receiving signaling,” “process[es], in accordance with the second rule set, the one or more [cached] packets.” *Id.* at 11:45–53. Claim 17 describes the same technique. *Id.* at 12:32–64; *see also* Op. ¶ 23.

The Court concluded that Cisco's accused devices did not use this rule swap technique. It recognized that the devices “all cease processing packets, albeit very briefly,

Appendix B

and use a form of a queue or buffer to store packets prior to processing.” Op. at 37. However, it found that the evidence did not show these actions were taken “responsive to being signaled to process packets in accordance with [a] second rule set.” *Id.* at 37–38. Instead, it determined that the evidence showed the cease processing and queue/buffer functionality “occurred as a part of normal packet processing in Cisco’s accused devices.” *Id.* at 38–39.

In its post-trial motion, Centripetal contends that the Court erred in (1) finding that the “responsive to” element was not met; (2) interpreting the “cease processing” element to require a ceasing of all packet processing; and (3) comparing the accused products to the specification, rather than the language of the claims. Mem. in Supp. at 15.

1. **“Responsive to”**

Centripetal first argues that the Court misunderstood how the accused Cisco products function and therefore misconstrued Centripetal’s infringement argument. Mem. in Supp. at 15–19; Reply at 8–12. Centripetal’s argument focuses on the “responsive to” element, asserting that the accused devices meet this requirement because they “receive a signal that causes them to switch from their normal packet processing mode to a rule-swapping state in which they cache packets (to avoid dropping them).” Reply at 11.

In finding that Centripetal failed to establish a causal relationship between the “signal . . . to process packets

Appendix B

in accordance with the second rule set” and the cease/cache functions, the Court credited the testimony of Cisco engineers, who explained that the accused devices cease processing packets and cache/buffer packets irrespective of whether a rule swap is occurring. *See* Op. at 38–39. In other words, the evidence showed that “the ceasing and caching of packets . . . occur[ed] *during* a rule swap, rather than because of it.” *Id.* at 38. Specifically, as to the Accused Switches and Routers, Cisco engineer Peter Jones noted that the devices swap from an old rule set to a new one during the existing “two or four internal clock periods” between packet processing. Tr. 2554:20–24. Mr. Jones also testified that while all packets are held in a packet buffer to await processing in the ordinary course, this buffer has no relationship to the accused Hitless ACL rule swap technique. Tr. 2563:10–19. He likewise explained that packet buffering in the Accused Switches operates the same way for all packets and regardless of whether the device is conducting a rule swap. Tr. 2563:7–19. Similar testimony was provided by Cisco engineer Hari Shankar with respect to the Accused Firewalls and the Transactional Commit Model update technique. Tr. 2521:6–12, 2525:2–17.

In contesting the Court’s finding, Centripetal introduces a new concept—the “mode” in which the accused devices are operating. Centripetal argues that unlike “normal packet processing,” the rule-swapping mode “causes a signal to cache packets that would otherwise be dropped by default.” Reply at 11. Centripetal argues that “the Court erred by assessing how Cisco’s products operate in their normal mode, during which there

Appendix B

is an extremely brief ‘idle period’ between the processing of each packet, instead of how they work in the special rule-swapping mode where there is no such idle period and the products cache packets (to avoid dropping them) while a new rule set is substituted for an older set.” Reply at 8–9; *see also* Mem. in Supp. at 18 (“By focusing on ‘idle’ time during normal processing rather than on what occurs during the rule swap process, the Court mistook Centripetal’s infringement case.”).

This “mode” concept is entirely new, was not previously raised or discussed, and finds no support in the record. It also suggests that Centripetal is now disputing, for the first time, the explanation provided by the Cisco engineers regarding how the accused devices operate. For example, the claim that there is no “idle period” when packets are being swapped directly conflicts with the testimony of Mr. Jones, who explained that this is precisely when the rule swap occurs. *See* Tr. 2554:22–24 (“So in our system it’s a fixed time pipeline, so there will be a packet every two or four internal clock periods. And the switch happens between those.”). It similarly conflicts with Mr. Shankar’s testimony regarding the operation of the firewalls. Op. ¶¶ 33–36. It also comes in stark contrast to Centripetal’s previous position that the Cisco engineer testimony supported its theory of infringement. For example, Centripetal directly quoted the following section of Mr. Jones’s cross-examination in its trial brief as support for the ’806 Patent cease and cache elements:

Q. And then during the two to four clock periods that you mentioned yesterday, when

Appendix B

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.

Pl. Centripetal Networks, LLC's Trial Br. at 12, ECF No. 703 (quoting Tr. 2572:7-20). To the extent Centripetal believed that the engineers were improperly discussing "normal mode," rather than "rule-swapping mode" in their testimony, it never raised such an issue and instead chose to rely on the testimony in support of its arguments.

Centripetal also cites to various statements made by its expert, Dr. Mitzenmacher. The Court considered the

Appendix B

testimony of Dr. Mitzenmacher and found that he “did not clearly offer an opinion as to th[e] causal relationship” between the “signal[] to process packets in accordance with the second rule set” and the ceasing processing and caching of the packets. *See* Op. at 38 (citing Tr. 601:23–25, 627:19–25, 707:11–12, 707:19–20). The Court likewise addressed Centripetal’s argument that one could infer causation because Cisco’s “new rule update techniques were designed to avoid dropping packets.” *Id.* at 39. Dr. Mitzenmacher opined that the no-dropped-packets functionality indicated to him that the accused devices would need to cease processing packets during a rule swap. *Id.* at 39 (citing Tr. 634:7–14, 706:3–5). Dr. Mitzenmacher also drew a connection between the lack of packet drops and the devices’ use of a packet buffer during a rule swap. *Id.* at 39–40 (citing Tr. 641:18–24, 712:17–23). However, the Court did not find this persuasive, noting that “[e]ven though a rule swap technique might be able to take advantage of . . . existing functionality to avoid dropped packets, this does not mean that the ceasing and caching operations are done ‘responsive to’ the rule swap.” *Id.* at 40. For these reasons, Centripetal fails to establish “a clear error of law” or “manifest injustice” warranting relief as to this issue. *P. Ins. Co.*, 148 F.3d at 403.

2. “Cease Processing”

Next, Centripetal argues that the Court misconstrued the term “cease processing of one or more packets.” Mem. in Supp. at 19. The Court understood the plain and ordinary meaning of this term to require the system to stop processing packets entirely. Op. at 42–44. Centripetal

Appendix B

maintains this was an error and that “cease processing” should be construed instead to mean “stop processing packets” in a specific way, namely “with the old rule set.” Mem. in Supp. at 19 (emphasis omitted). Centripetal cites to embodiments in the specification that it argues require such a limitation. *Id.* Further, Centripetal argues that the Court improperly treated an embodiment in the specification (Figure 4) as a limitation on the claims. *Id.*

It is Centripetal, not the Court, that seeks to impermissibly use the specification to modify the claim language. The Court did not treat an embodiment in the specification (Figure 4) as a limitation on the claims. It merely referenced Figure 4 as being consistent with its plain language analysis—that “cease processing of one or more packets” means that the system stops processing packets entirely. *See, e.g., Accent Packaging, Inc. v. Leggett & Platt, Inc.*, 707 F.3d 1318, 1326 (Fed. Cir. 2013); Op. at 42–43. Further, the Court rejects Centripetal’s suggestion that the specification can be used to modify abundantly clear claim language. *See Buckingham Mfg. Co. v. Bashlin Indus., Inc.*, No. 2:21-cv-1390, 2022 WL 17668809, at *14 (W.D. Pa. July 8, 2022) (rejecting construction that “adds words to the claims that are not present”); *Leviton Mfg. Co. v. Universal Sec. Instruments, Inc.*, 304 F. Supp. 2d 726, 739 (D. Md. 2004) (similar).

3. **Comparing Accused Products to Specification**

Lastly, Centripetal argues that the Court improperly relied on the patent specification. Centripetal points to

Appendix B

the Court’s observation that Cisco’s accused devices do not solve a problem described in the specification, namely, “processing packets in accordance with an outdated rule set.” Mem. in Supp. at 20. It argues this was “not the right comparison” because “[t]he only issue for infringement is whether the accused products meet the claims; whether they meet the specification is irrelevant.” *Id.* at 20–21 (emphasis omitted). The Court’s non-infringement conclusion does not rely on this analysis. Rather, the Court noted that this fact “further supported” its findings in order to provide additional context.⁵ Op. at 44.

Centripetal’s Motion is denied as to the ’806 Patent.

C. ’176 Patent

In its Opinion, the Court found that Centripetal failed to meet its burden to establish that Cisco’s Accused Switches and Routers infringed claims 11 and 21 of the ’176 Patent. Op. at 53– 61. Claim 11 provides that a system “identify a plurality of packets received by a network device from a host located in a first network”

5. Centripetal argues that the Court “misinterpreted” the testimony of Cisco engineer Mr. Shankar when it used his testimony to support its position that the specification further supports the Court’s non-infringement finding. Mem. in Supp. at 21. Centripetal argues that Mr. Shankar’s testimony is “not evidence of non-infringement” because he was discussing “what occurs during normal packet processing.” *Id.* This appears to be a species of Centripetal’s “mode” argument, addressed above. In any event, the Court’s non-infringement finding does not rely on this discussion of the specification.

Appendix B

and “generate a plurality of log entries corresponding to the plurality of packets *received by* the network device.” ’176 Patent at 17:10–13 (emphasis added). Likewise, the system is to “identify a plurality of packets transmitted by the network device to a host located in a second network” and “generate a plurality of log entries corresponding to the plurality of packets *transmitted by* the network device.” *Id.* at 17:14–18 (emphasis added). Then, “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 system “correlate[s] . . . the plurality of packets transmitted by the network device with the plurality of packets received by the network device.” *Id.* at 17:19–25. Finally, “responsive to correlating,” the system “generate[s], based on the correlating, one or more rules configured to identify packets received from the host located in the first network,” and “provision[s] a device located in the first network with the one or more rules.” *Id.* at 17:26–35. These steps are the same for claim 21. *Id.* at 18:63–19:23; *see also* Op. ¶ 45.

The Court found that the preponderance of the evidence did not establish that Cisco’s Accused Switches and Routers use this packet correlation technique. Op. at 53–54. Specifically, the Court found that Centripetal did not present evidence that Cisco’s accused devices “correlate . . . the plurality of packets transmitted by the network device with the plurality of packets received by the network device” based on the ingress and egress log entries corresponding to those sets of packets. Op. at 53–

Appendix B

59; *see* '176 Patent at 17:19–25. Instead, the Court found that the evidence showed the accused devices conducted a different kind of correlation—between internal NetFlow log records or proxy data and external threat behaviors. Op. at 57. The Court likewise found that Centripetal did not demonstrate that “responsive to correlating,” the devices “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” with those rules. Op. at 60; *see* '176 Patent at 17:26–35. The Court opined that “[w]hile the evidence shows that the system generates alerts, these alerts are not ‘rules,’” nor do they have the capability of identifying the packets received from the first network host. Op. at 60.

Centripetal argues that the Court’s findings regarding the correlation limitation and the generate and provision limitation were both in error.

1. “Correlate ” Limitation

Centripetal raises multiple issues with the Court’s finding that Centripetal did not establish that Cisco’s accused devices perform the correlation specified in the claims—specifically, a correlation between the “packets received by the network device” with the packets “transmitted by the network device” based on ingress and egress log entries reflecting the received/transmitted packets. Mem. in Supp. at 22–28; *see* Op. at 54; '176 Patent at 17:19–25.

Appendix B

First, Centripetal argues that the Court erred in concluding that Centripetal had failed to establish that Cisco’s Stealthwatch correlates ingress and egress NetFlow records. Mem. in Supp. at 23–25. Centripetal argues that the evidence was “undisputed” and that its expert, Dr. Cole, established the correlation limitation using Cisco documents. *Id.* at 23. These same arguments and evidence were previously presented to and considered by the Court. In its Opinion, the Court found that Centripetal had failed to prove the correlation limitation. Op. at 56–59. As the finder of fact, the Court gave the testimony of Dr. Cole “little weight,” noting the “paucity and indefiniteness of the evidence [he] relied on.” *Id.* at 58. The Court also reviewed and considered the documents relied on by Centripetal in concluding that Centripetal had not met its burden. *Id.* at 56–59. Centripetal fails to point to any clear error and the Court finds no reason to revisit its previous analysis.

Centripetal also claims that the countervailing evidence the Court cited to further support its conclusion does not establish that Stealthwatch is incapable of performing the claimed correlation. Mem. in Supp. at 23–24. But this argument misses the point. The Court found that Centripetal failed to meet its burden to show the accused devices perform each claim limitation. Cisco was not required to establish non-infringement (*i.e.*, that Stealthwatch does not perform the claimed correlation), and the observation that other documents bolstered the Court’s conclusion was appropriate.

Appendix B

Second, Centripetal argues that the Court failed to consider other ways in which the “correlate” element could be met—specifically, through deduplication of NetFlow data and the correlation of NetFlow with other data types, such as Syslogs and WebFlow. *Id.* at 25–27. However, these infringement theories were not presented at trial. As the Court noted in its Opinion, at trial, Centripetal only presented testimony from its expert, Dr. Cole, on Stealthwatch’s alleged correlation of ingress and egress NetFlow records. *Op.* at 55 (citing Tr. 993:19–999:15, 1102:16– 1103:4, 1106:5–8, 1108:1–5). Dr. Cole never discussed deduplication and noted that his infringement opinion did not involve a proxy, meaning that any correlation by Stealthwatch of Syslogs or WebFlow—which Centripetal has indicated are generated by proxy sources—does not support Dr. Cole’s infringement analysis. *Id.* (quoting Tr. 978:11–18). Further, Centripetal chose not to supplement the record or recall witnesses in the Rule 63 proceeding. Pl.’s Notice at 1–2. Instead, it asked the Court to rule based on the trial record that was developed before Judge Morgan. *Id.* As such, the Court finds that these new infringement theories, which are largely undeveloped in the record and lack supporting expert testimony, are unpersuasive based on the record before the Court, and further supplementation is improper at this stage.

Third, Centripetal claims that the Court improperly “compared the accused products to the discussion of packet obfuscation in the patent specification rather than applying the asserted claims.” *Mem. in Supp.* at 27. Contrary to Centripetal’s contentions, the Court

Appendix B

did not “require packet obfuscation as one of the [claim] limitations.” Mem. in Supp. at 28. The Court’s evaluation of Centripetal’s evidence related to the correlate element did not discuss packet obfuscation. The Court merely referenced the specification at the end of its analysis to provide context and to highlight that its conclusion was consistent with the fact that “the Accused Switches and Routers do not have the problem that the ’176 Patent was designed to solve.” Op. at 59.

2. Generate and Provision Limitation

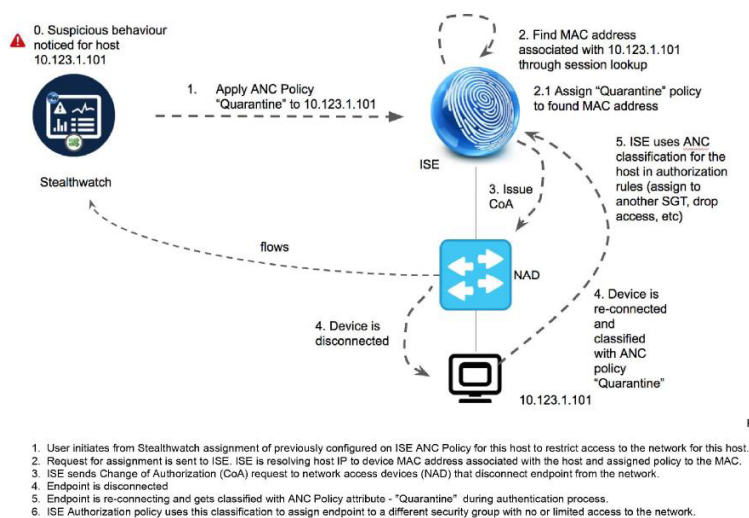
Next, Centripetal argues that the Court erred in concluding that Stealthwatch, based on the correlation, does not generate rules “configured to identify packets received from the host located in the first network” or “provision[] a device” with those rules. Mem. in Supp. at 28 (quoting ’176 Patent at 17:26–35). The parties agreed that “rule” means “a condition or set of conditions that when satisfied cause a specific function to occur.” Op. & Order (“*Markman* Order”) at 9, ECF No. 202.

Centripetal, similar to its previous arguments, asserts that Stealthwatch generates a “rule” “when it creates a policy update to initiate the quarantine.” Mem. in Supp. at 28; *see also* Centripetal PFF ¶ 372 (“Stealthwatch will respond to identified threats to generate rules that are sent to the Catalyst 9000 Switch and ISR/ASR Router to block specific packets that were identified to be threats.”). In its Opinion, the Court rejected this argument, finding that while Stealthwatch generates alerts, these do not, in and of themselves, “cause a specific function to occur.” Op.

Appendix B

at 60. Here, Centripetal contests this finding, claiming that the Court “misstated the operation of the Stealthwatch,” because “Stealthwatch . . . automatically generates the rule in response to the correlating of NetFlow and then propagates the responsive rule.” Mem. in Supp. at 29. In support, Centripetal principally relies on the following diagram from a Cisco technical document:

Tabular or graphic material set at this point is not displayable.



PTX-1089 at 1238.

At trial, Centripetal’s counsel asked its expert, Dr. Cole, about this diagram. Dr. Cole was asked, “[s]o what happens when they realize that there’s some suspicious

Appendix B

behavior noticed for the host?” Tr. 1002:11–12. Dr. Cole responded that “[i]t can go in and send a policy, which can also be thought of as rules, to take some action, in this case to quarantine a specific IP address.” Tr. 1002:13–15. But as the Court previously explained, the quarantine function does not occur absent human intervention. Op. at 60. Centripetal’s focus on step one of the diagram, “Apply ANC Policy ‘Quarantine,’” does not change that conclusion. As the explanation for step 1 below the diagram makes clear, the quarantine action is not automatically triggered from Stealthwatch alerting suspicious network behavior; instead, the quarantine is “initiat[ed]” by the “[u]ser.” PTX-1089 at 1238. Moreover, as detailed after the diagram, the “interaction between the user and the system” involves the user, “Adam the Analyst,” “notic[ing] the alert and open[ing] Host Report for the host to investigate host details,” “decid[ing] to limit access to the network for the host via ISE ANC,” “review[ing] if there are any ANC Policy already assigned to the host,” and “open[ing] ANC options available for the host and select[ing] ISE and ANC Policy appropriate for assignment,” all before “Stealthwatch sends assignement [sic] request to ISE and notif[ies] Adam if request is successfull [sic] and policy is assigned or any error occurred.” *Id.* at 1238–39. Therefore, even if the Court found that Stealthwatch practiced the claimed correlation (which it did not), the result of that correlation—the identification and alert of suspicious behavior—is not a “rule” because it does not “cause a specific function to occur” (*e.g.*, the quarantine of a particular IP address),

Appendix B

without significant human interaction. *See Markman* Order at 9; '176 Patent at 17:26–35.⁶

Finally, Centripetal takes issue with the Court's finding that, even setting aside the human inputs necessary to generate a rule, Centripetal "has not shown that the rules that would be created based on a Stealthwatch alert would have the ability to 'identify packets received from the host located in the first network.'" Op. at 60; Mem. in Supp. at 30. Centripetal argues, and Court agrees, that the Stealthwatch alert can identify a suspicious host in a network. Mem. in Supp. at 30; PTX-1089 at 1238. However, it is not clear why such alerts have any relationship to identifying packets received by the network device from a host in the first network, as distinguished from packets transmitted by the network device to a host in a second network. In any event, Centripetal's failure to prove multiple other claim limitations would prohibit relief.

6. In its *Markman* Order, the Court adopted the plain and ordinary meaning of "generate, based on the correlating, one or more rules." *Markman* Order at 19–20. In so doing, the Court rejected a narrower construction proposed by Cisco that automated rule generation be "based on the correlating, not based on user defined filters or rules." *Id.* Centripetal argues that this ruling supports its argument that the quarantine rules can satisfy that claim limitation. Mem. in Supp. at 30. However, Centripetal's argument conflates two distinct requirements: (1) that the "system . . . generate . . . one or more rules," and (2) that such rules be "based on the correlating." '176 Patent at 17:8–9, 29–31. Regardless of what the rules are "based on," the claims describe a *system* that "generate[s]" rules. *See id.* The quarantine rules, as made plain above, are not system generated.

56a

Appendix B

Centripetal's Motion is denied as to the '176 Patent.

III. CONCLUSION

For the reasons set forth above, Centripetal's post-trial motion is DENIED. ECF No. 787. The Clerk is DIRECTED to send a copy of this Order to all counsel of record.

It is so ORDERED.

/s/ Elizabeth W. Hanes
Elizabeth W. Hanes
United States District Judge

Date: June 14, 2024

**APPENDIX C — MEMORANDUM OPINION AND
ORDER OF THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA,
NORFOLK DIVISION, FILED DECEMBER 11, 2023**

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
NORFOLK DIVISION

CENTRIPETAL NETWORKS, LLC,

Plaintiff,

v.

CISCO SYSTEMS, INC.,

Defendant.

Civil Action No. 2:18-cv-00094 (EWH)

Signed December 11, 2023

MEMORANDUM OPINION AND ORDER

This is a patent infringement case with an unusual history. Commencing in May 2020, this Court held a six-week bench trial via the Zoom platform during the height of the COVID-19 pandemic. Before the Court issued its post-trial findings of fact and conclusions of law, Defendant Cisco Systems, Inc. (“Cisco”) moved for recusal of the presiding judge, the Honorable Henry Coke Morgan, Jr. ECF No. 551. The Court denied the motion and entered judgment in favor of Plaintiff Centripetal Networks, LLC (“Centripetal”). ECF Nos. 619, 621, 638. Cisco appealed. Before the appeal was decided, Judge

Appendix C

Morgan passed away. Thereafter, the United States Court of Appeals for the Federal Circuit reversed the denial of Cisco’s recusal motion. *Centripetal Networks, Inc. v. Cisco Sys., Inc.*, 38 F.4th 1025, 1030-33 (Fed. Cir.), *cert. denied*, ___ U.S. ___, 143 S. Ct. 487, 214 L.Ed.2d 278 (2022). As a result, the Federal Circuit vacated the infringement opinion and judgment in favor of Centripetal, as well as this Court’s denial of Cisco’s motion for a new trial. *Id.* at 1040. The Federal Circuit remanded the case for “further proceedings before a newly appointed judge, who shall decide the case without regard for the vacated opinions and orders” and directed that the remand be governed by Federal Rule of Civil Procedure 63. *Id.*

Based upon review of the record and the arguments of the parties, the Court FINDS that Centripetal has failed to meet its burden to establish infringement of the ’193, ’806, or ’176 Patents. Consistent with this determination, the Court enters the following findings of fact and conclusions of law. Fed. R. Civ. P. 52(a).¹ Having found that Centripetal has failed to establish infringement, the

1. While the Court has endeavored to separate factual findings from legal conclusions for each patent in the below analysis, the headings are not meant to be limiting. Findings of fact may include, apply, restate, or embody conclusions of law, and vice versa. Additionally, while the Court may cite testimony and/or documentary evidence to support a finding, this is not meant to imply that the cited evidence is the only evidentiary support for the finding. Some of the findings are based on the record or inferences from the record which are not cited. To the extent any of the proposed findings of fact or conclusions of law submitted by the parties are inconsistent with the Court’s findings and conclusions below, they are rejected.

Appendix C

Court need not reach issues related to patent validity or damages. Finding “no just reason for delay,” the Court DIRECTS the Clerk to enter partial final judgment in favor of Cisco pursuant to Rule 54(b) of the Federal Rules of Civil Procedure.

I. BACKGROUND

This case was brought by Centripetal Networks, Inc. against Cisco Systems, Inc. on February 13, 2018. ECF No. 1. On March 29, 2018, Centripetal filed an Amended Complaint, alleging infringement of U.S. Patent Nos. 9,560,077 (“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 9,560,176 (“the ’176 Patent”). ECF No. 29.

Between July 12, 2018, and September 18, 2018, Cisco filed petitions for *inter partes* review (“IPR”) challenging claims asserted in nine of the eleven asserted patents and requested that the Court stay the action to allow for the resolution of the petitions by the Patent Trial and Appeal Board (“PTAB”). ECF No. 45. On February 25, 2019, the Court granted the stay. ECF No. 58. Thereafter, Centripetal moved to lift the stay, and on September 18, 2019, the Court granted the request in part, lifting the stay as to patents and claims not then subject to IPR proceedings. ECF No. 68 at 7.

Appendix C

On February 6, 2020, the Court held a *Markman* hearing in which it construed certain disputed claim terms. ECF No. 202 (“*Markman* Order”). Specifically, the Court made the following determinations:

Term	Court’s Construction
Packets	Plain and ordinary meaning in the context of the claim in which the term appears
Preamble	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

Appendix C

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

Markman Order at 22.

Subsequently, Centripetal waived its right to a jury trial and consented to a bench trial. ECF No. 328 at 7:23-8:23. At the trial, Centripetal argued that Cisco infringed claims 18 and 19 of the '193 Patent, claims 9 and 17 of the '806 Patent, claims 11 and 21 of the '176 Patent, claims 24 and 25 of the '856 Patent, and claims 63 and 77 of the '205 Patent. ECF No. 411 at 2. The 22-day bench trial and subsequent damages hearing were held virtually using the Zoom video conference platform. *See* ECF Nos. 496-550 ("Tr.").

During the trial, Centripetal called numerous fact and expert witnesses. Centripetal's fact witnesses who provided live testimony included: Mr. Steven Rogers, Founder and CEO of Centripetal, Tr. 228:5-8; Dr. Sean Moore, the Chief Technology Officer and Vice President of Research at Centripetal and an inventor on all the asserted patents in this case, Tr. 301:21-25, 314:25-315:2; Mr. Jonathan Rogers, the Chief Operating Officer at Centripetal, Tr. 1194:10-11; and Mr. Christopher Gibbs, the Senior Vice President of Sales at Centripetal, Tr.

Appendix C

1296:24-1297:2. Centripetal also presented testimony from the following Cisco employees through video deposition: Mr. Saravanan Radhakrishnan, Mr. Rajagopal Venkatraman, Dr. David McGrew, Mr. Sunil Amin, and Mr. Sandeep Agrawal. Tr. 405:1-2, 407:13-14, 409:6-7, 410:15-16, 419:8-9.

Centripetal's expert witnesses who testified during its case-in-chief included: Dr. Nenad Medvidovic, an expert in computer science and computer architecture who presented a technology tutorial to the Court and also opined on the importance of the patented technology as it relates to the accused products, Tr. 18:4-16, 1144:22-1145:2; Dr. Michael Mitzenmacher, an expert in computer networking and computer security who presented an infringement opinion as to the '193, '806, and '205 Patents, Tr. 431:16-23; Dr. Eric Cole, an expert in cybersecurity and the cybersecurity industry who presented an infringement opinion as to the '856 and '176 Patents, Tr. 880:20-881:5, 886:9-11, 975:19-21; Dr. Aaron Striegel, an expert in computer networking and computer networks who opined on damages apportionment, Tr. 1337:6-14, 1337:19-23, 1340:1-6; Mr. Lance Gunderson, an expert in patent damages who opined on damages royalty rates, Tr. 1440:4-9, 1441:2-14; and Mr. James Malackowski, an expert in business and intellectual property valuation and patent licensing who opined on the valuation of the patents and future damages, Tr. 1573:14-19, 1577:4-11.

In Centripetal's rebuttal validity case, it additionally called the following expert witnesses: Dr. Alessandro Orso, an expert in computer networks and network

Appendix C

security who provided an opinion as to the validity of the '193 and '806 Patents, Tr. 2989:12-14, 22-25; Dr. Trent Jaeger, an expert in computer and network security who provided an opinion as to the validity of the '856 and '176 Patents, Tr. 3102:5-7, 18-23; and Dr. Aaron Striegel, a computer science expert who provided an opinion as to secondary considerations of non-obviousness for the asserted patents, Tr. 3196:16-18.

Cisco likewise called numerous fact and expert witnesses. Cisco's fact witnesses who provided live testimony included: Mr. Hari Shankar, a Principal Engineer and Software Architect at Cisco responsible for the design of certain features of the accused products, Tr. 2499:15, 2500:3-5; Mr. Daniel Llewallyn, a Software Engineer for Cisco who helped develop the Stealthwatch product line, Tr. 2141:19; Mr. Peter Jones, a Distinguished Engineer in the Enterprise Network Hardware Group at Cisco, Tr. 2543:12-17; Mr. Timothy Keanini, a Distinguished Engineer at Cisco involved with Stealthwatch, Tr. 2810:4-6; Mr. Karthik Subramanian, Partner at venture capital firm Evolution Equity Partners and previous leader of Cisco's Corporate Development Team for Cybersecurity, Tr. 2827:23-25, 2828:17-18; Mr. Michael Scheck, Senior Director of Incident Command at Cisco, Tr. 1658:23-24; Dr. David McGrew, a Cisco Fellow who was responsible for leading a research and development project at Cisco relevant to the '856 Patent, Tr. 1756:23, 1759:10-12; and Mr. Matt Watchinski, a Cisco employee responsible for Cisco's threat intelligence organization, Tr. 2682:11-13. Cisco also presented testimony from current and former Centripetal employees through video deposition, including: Mr.

Appendix C

Douglas DiSabello, Mr. Haig Colter, Dr. Sean Moore, Mr. Jess Parnell, Mr. Justin Rogers, Mr. Christopher Gibbs, and Mr. Gregory Akers. Tr. 1800:22-23, 2139:9-10, 2575:4-5, 2709:19-20, 2711:12-13, 2722:3-4, 2723:22-23.

Cisco's expert witnesses who testified at trial included: Dr. Kevin Almeroth, an expert in computer networks and network security who presented a technology tutorial to the Court and provided an opinion as to non-infringement, invalidity, and damages for the '176 Patent, Tr. 71:14-72:1, 2212:1-3, 12-18; Dr. Mark Crovella, an expert in computer networks and network security who provided an opinion as to non-infringement, invalidity, and damages for the '193 Patent, Tr. 2349:1-24; Dr. Narasimha Reddy, an expert in computer networks and network security who provided an opinion as to non-infringement, invalidity, and damages for the '806 Patent, Tr. 2579:20-22, 2580:6-10; Dr. Douglas Schmidt, an expert in computer networks and network security who provided an opinion as to non-infringement, invalidity, and damages for the '856 Patent, Tr. 1811:18-19, 1813:4; Dr. Kevin Jeffay, an expert in computer networks and network security who provided an opinion as to non-infringement and damages for the '205 Patent, Tr. 2727:2-19; and Dr. Stephen Becker, an expert in economic damages analysis who provided an opinion as to damages, Tr. 2863:3-19.

At the close of Centripetal's case in chief, Cisco made a motion for judgment on partial findings pursuant to Fed. R. Civ. P. 52(c). ECF No. 444. The Court denied the motion. Tr. 1635:14-1656:13. After the conclusion of the trial and prior to the Court's entry of its findings of fact

Appendix C

and conclusions of law, Cisco moved for Judge Morgan's recusal. ECF No. 557 at 3-11; *see also* 28 U.S.C. § 455(a), (b)(4). The Court denied the motion. *See* ECF No. 619. On October 5, 2020, Judge Morgan entered a decision on the merits finding that Cisco willfully infringed the asserted claims of the '806, '176, '193, and '856 Patents. ECF No. 621 at 29, 57, 72, 95, 107. The Court found the '205 Patent claims that were pursued at trial were not infringed. *Id.* at 123. Cisco subsequently moved for a new trial pursuant to Rule 59(a)(2) of the Federal Rules of Civil Procedure. ECF No. 625.

On November 18, 2020, the Court dismissed without prejudice Centripetal's claims related to the patents that had previously been stayed due to pending IPR proceedings. ECF No. 633. This included all asserted claims related to the '213 Patent, the '552 Patent, the '713 Patent, the '148 Patent, the '077 Patent, and the '722 Patent, as well as the '205 Patent claims that were not pursued at trial. *Id.*

On March 17, 2021, Judge Morgan denied Cisco's motion for a new trial and entered final judgment in favor of Centripetal. ECF No. 638. Cisco timely appealed to the Federal Circuit. On June 23, 2022, the Federal Circuit reversed the denial of Cisco's recusal motion and, as a result, vacated the infringement opinion and judgment in favor of Centripetal, as well as the Court's denial of Cisco's motion for a new trial. *Centripetal Networks, Inc.*, 38 F.4th at 1030-33, 1040. Following Judge Morgan's passing on May 1, 2022, the Court of Appeals instructed that the case "be assigned to a new judge in the normal course, pursuant

Appendix C

to Rule 63, which allows a replacement judge ‘if a judge conducting a hearing or trial is unable to proceed.’” *Id.* at 1039 (quoting Fed. R. Civ. P. 63). On August 23, 2022, this case was reassigned to the undersigned.

Rule 63 of the Federal Rules of Civil Procedure provides:

If a judge conducting a hearing or trial is unable to proceed, any other judge may proceed upon certifying familiarity with the record and determining that the case may be completed without prejudice to the parties. In a hearing or a nonjury trial, the successor judge must, at a party’s request, recall any witness whose testimony is material and disputed and who is available to testify again without undue burden. The successor judge may also recall any other witness.

In an analogous context, the United States Court of Appeals for the Fourth Circuit recognized that “parties may consent to having the entire case decided upon the record or they may agree as to which witnesses need to testify again.” *Henry A. Knott Co. v. Chesapeake & Potomac Tel. Co. of W. Va.*, 772 F.2d 78, 87 (4th Cir. 1985). Here, the parties were given the opportunity to recall any witness whose testimony was material and disputed. Neither party chose to recall any witnesses.

Cisco made two motions in connection with the Rule 63 hearing. First, Cisco moved to renew its motion to

Appendix C

partially stay the case as to the '856 Patent, and second, it moved to supplement the trial record. ECF Nos. 687, 691. The Court granted Cisco's renewed stay motion due to the PTAB's issuance of a final written decision declaring that the '856 Patent claims asserted by Centripetal were unpatentable.² ECF No. 715; *see also* ECF No. 686. The Court also granted in part Cisco's motion to supplement the record. ECF Nos. 750, 753, 754 ("R. 63 Tr.") at 10:4-5. Specifically, the Court granted Cisco's request to admit DTX-1 and DTX-369, which were both made available to Judge Morgan in their entirety during the trial but had only been partially admitted into the record. R. 63 Tr. 10:7-22. The Court also granted the request to admit two documents that post-dated the trial—Centripetal's preliminary response regarding the '176 Patent in IPR proceedings before the PTAB, attached as Exhibit 3 to Cisco's memorandum in support of its motion, and Exhibit 4, the Patent Office's decision denying institution of *inter partes* review of the '176 Patent. R. 63 Tr. 10:23-11:5; ECF Nos. 692-4, 692-5. The Court denied Cisco's request to admit the testimony of Dr. Sean Moore, finding that it was inappropriate given that Cisco had the opportunity to call Dr. Moore to appear at the Rule 63 hearing and chose not to do so. R. 63 Tr. 11:13-22; ECF No. 692-2.

On June 21, 2023, the undersigned certified her familiarity with the record, ECF No. 742, and on June 22, 23, and 26, 2023, the Court held a hearing pursuant to Rule

2. The Court had initially denied Cisco's request for a partial stay of the case as to the '856 Patent prior to the PTAB's issuance of its final written decision. *See* ECF No. 675 at 10:6-7; ECF No. 677.

Appendix C

63. The parties each presented a technology tutorial—through Dr. Nenad Medvidovic for Centripetal and Dr. Kevin Almeroth for Cisco. *See* R. 63 Tr. 13:17-208:17. Counsel for both sides also presented argument on each of the '193, '806, and '176 Patents. *See id.* at 217:25-702:2. Prior to the Rule 63 hearing, Centripetal and Cisco filed Proposed Findings of Fact and Conclusions of Law. ECF Nos. 725 (“Centripetal PFF” & “Centripetal PCL”),³ 737-1 (“Cisco PFFCL”). Following the hearing, the parties submitted supplemental proposed findings regarding the post-trial prosecution history of the '176 Patent. ECF Nos. 766, 768-1.

II. LEGAL STANDARD

The infringement analysis is a two-step process: “[f]irst, the Court determines the scope and meaning of the patent claims asserted, and then the properly construed claims are compared to the allegedly infringing device.” *Cordis Corp. v. Bos. Sci. Corp.*, 658 F.3d 1347, 1354 (Fed. Cir. 2011) (quoting *Cybor Corp. v. FAS Techs., Inc.*, 138 F.3d 1448, 1454 (Fed. Cir. 1998) (en banc)). In order to show infringement, “the plaintiff must establish by a preponderance of the evidence that the accused device infringes one or more claims of the patent either literally or under the doctrine of equivalents.” *Bayer AG v. Elan Pharm. Rsch. Corp.*, 212 F.3d 1241, 1247 (Fed. Cir. 2000).

3. The Court refers to Centripetal’s Proposed Findings of Fact and Conclusions of Law as “Centripetal PFF” when discussing the Proposed Findings of Fact numbered paragraphs (pp. 1-163), and “Centripetal PCL” when discussing the Proposed Conclusions of Law numbered paragraphs (pp. 163-232).

Appendix C

“To prove literal infringement, the patentee must show that the accused device contains *each and every limitation* of the asserted claims.” *Ericsson, Inc. v. D-Link Sys., Inc.*, 773 F.3d 1201, 1215 (Fed. Cir. 2014) (emphasis in original). “[I]f even one limitation is not met, there is no literal infringement.” *E.I. du Pont De Nemours & Co. v. Unifrax I LLC*, 921 F.3d 1060, 1073 (Fed. Cir. 2019). Additionally, “[i]f an asserted claim does not literally read on an accused product, infringement may still occur under the doctrine of equivalents if there is not a substantial difference between the limitations of the claim and the accused product.” *Bayer AG*, 212 F.3d at 1250 (citing *Warner-Jenkinson Co. v. Hilton Davis Chem. Co.*, 520 U.S. 17, 29, 39-41, 117 S.Ct. 1040, 137 L.Ed.2d 146 (1997)). This can be demonstrated “by showing on a limitation by limitation basis that the accused product performs substantially the same function in substantially the same way with substantially the same result as each claim limitation of the patented product.” *Crown Packaging Tech., Inc. v. Rexam Beverage Can Co.*, 559 F.3d 1308, 1312 (Fed. Cir. 2009) (citing *Warner-Jenkinson Co.*, 520 U.S. at 17, 39-40, 117 S.Ct. 1040).

Infringement of a patent claim can be proven either directly or indirectly. To prove direct infringement, the plaintiff must show that the defendant itself “makes, uses, offers to sell, or sells any patented invention, within the United States.” 35 U.S.C. § 271(a). Indirect infringement allows a plaintiff to bring in the actions of other parties, such as the defendant’s customers, but requires the plaintiff to satisfy certain knowledge and intent requirements for the defendant. *Id.* § 271(b)-(c).

Appendix C

Centripetal has asserted that Cisco is liable as both a direct and indirect infringer. *See* Centripetal PCL ¶¶ 4-84.

III. TECHNOLOGY OVERVIEW**A. Networking and Security**

The three patents at issue in this case involve methods designed to enhance the security of computer networks. In particular, the patents involve ways in which data packets are processed as they proceed through different parts of networks.

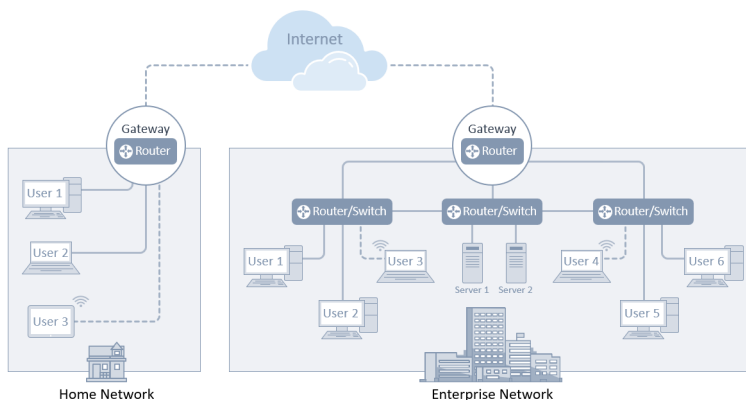
A network is comprised of computers that are connected through routers and switches. Switches generally connect computers within an organization, and routers generally connect computers to other computers outside of an organization. Tr. 624:12-19. The Internet is an interconnected network of networks. R. 63 Tr. 84:2-9.

Data flows through networks in the form of packets. Packets generally have two basic components—a header and a payload. R. 63 Tr. 19:23-20:9. The header contains the information that switches and routers need to deliver packets to their destination. R. 63 Tr. 86:7-10. The payload contains the underlying information that the packet is transmitting to its destination. R. 63 Tr. 20:1-4.

The diagram below depicts the general structure of two computer networks—a “Home Network” and an “Enterprise Network.” Fig. 1. The “Home Network” consists of three computers connected to a gateway router

Appendix C

(Users 1, 2, and 3). The “Enterprise Network” consists of three sets of computers (Users 1, 2, and 3, Servers 1 and 2, and Users 4, 5, and 6) connected to three separate routers or switches, which are all connected to a single gateway router.



Cisco Demonstrative, Rule 63 Hearing.

For User 1 in the Home Network to send an email to User 6 in the Enterprise Network, a series of packets containing that email (also referred to as the packet “flow”) are forwarded from User 1 to the gateway router in the Home Network, pass through any number of other networks (depicted in the above diagram as the “Internet”), then through the gateway router of the Enterprise Network, to a final router or switch, then to User 6’s computer.

As packets are transmitted between different networks, security is a key consideration. To enhance

Appendix C

network security, protections are implemented in firewalls⁴ and similar appliances, as well as in routers and switches themselves. R. 63 Tr. 116:8-14, 11-16. These network devices can use certain kinds of rules (access control lists, or “ACLs”) to determine which packets are allowed to access various network resources. Tr. 537:18-21, 2550:1-4.

The patents at issue here each involve specific ways these kinds of devices process packets to enhance network security. The ’193 Patent involves a method for blocking data exfiltrations,⁵ the ’806 Patent involves a technique for changing packet-filtering rules, and the ’176 Patent involves a process for tracing the source of packets that pass through a network device.

B. Centripetal’s RuleGATE Product

Centripetal has asserted that each of the patents is practiced by Centripetal’s RuleGATE product, a packet-filtering device that was first sold in the United States in December 2014. Tr. 285:24-286:1, 1381:13-1385:19; PTX-1215 (patent-by-patent analysis). The RuleGATE product ingests data from multiple threat intelligence feeds and was marketed by Centripetal as being able to

4. Firewalls are specialized devices installed in the network that filter incoming and outgoing traffic to block malicious activity. R. 63 Tr. 117:11-16.

5. Exfiltration involves a circumstance where an attacker gains access to a computer inside of a network and sends protected information outside of that network. R. 63 Tr. 107:5-16.

Appendix C

run up to 5 million different security rules on packets. PTX-550; PTX-547 at 389. The product can be deployed either “inline” or “out-of-band.” Tr. 1382:12-22. Packets are processed directly through a device in an “inline” configuration, while an “out-of-band” setup indirectly monitors packets. *Id.*

C. Overview of Cisco’s Technology

Centripetal’s infringement case focused on a set of updates Cisco made in 2017 to certain of its switches, routers, firewalls, and related technology. Centripetal argued that these updates implemented network security functionality into Cisco’s devices that infringes on Centripetal’s patents. Centripetal’s allegations of infringement are against combinations of Cisco hardware and software. A brief description of each of these products is provided below.

Catalyst 9000 Switches

Centripetal accused Cisco’s switches that are part of the Catalyst 9000 series, including the Catalyst 9300, 9400, and 9500 series running IOS-XE 16.5 and subsequent releases, as well as the Catalyst 9800 series wireless controller running IOS-XE 16.10 and subsequent releases, of infringement (the “Accused Switches”). ECF No. 408 at 17 n.3; *see also* Tr. 434:14-17. In addition to the operating system running on the switches (i.e., the software code), customers are also able to add a “software subscription referred to as Cisco [Digital Network Architecture (“DNA”) Center],” which is discussed further

Appendix C

below. PTX-560 at 772. Cisco advertised the Accused Switches as being “built for security” and “a critical part of an end-to-end integrated security solution, one that detects and stops threats.” PTX-1260 at 849. The Accused Switches are able to enforce a variety of security rules to either forward or drop packets. Tr. 39:15-40:4, 440:8-442:25, 450:23-452:11. Centripetal argued the Accused Switches infringe the asserted claims in the ’193 Patent, the ’806 Patent (when used in combination with the DNA Center), and the ’176 Patent (when used in combination with Stealthwatch and Cognitive Threat Analytics). Tr. 433:12-434:1 (’193 Patent); Tr. 571:17-572:3 (’806 Patent); Tr. 975:17-21, 995:19-21 (’176 Patent).

ISR/ASR Routers

Centripetal accused Cisco’s Integrated Services Routers (“ISR”) and Aggregation Services Routers (“ASR”), including the 1000 and 4000 series ISR and the 1000 series ASR routers running the IOS-XE 16.5 operating system and subsequent versions, of infringement (the “Accused Routers”). ECF No. 408 at 17 n.4; Tr. 433:24-434:1. Cisco advertised the Accused Routers as “includ[ing] integrated security, advanced analytics, automated provisioning, and application optimization, to deliver a complete solution.” PTX-1226 at 638; Tr. 443:17-444:10. Similar to the Accused Switches, Centripetal alleged that the Accused Routers infringe the asserted claims of the ’193 Patent, the ’806 Patent (when used in combination with the DNA Center), and the ’176 Patent (when used in combination with Stealthwatch and Cognitive Threat Analytics). Tr. 433:12-434:1 (’193

Appendix C

Patent); Tr. 571:17-572:3 ('806 Patent); Tr. 975:17-21, 995:19-21 ('176 Patent).

Digital Network Architecture Center

Cisco's Digital Network Architecture ("DNA") Center is a subscription service that can be used to configure and manage the Accused Switches and Routers. Tr. 55:13-21, 575:15-577:8, 579:10-580:24; PTX-560 at 772; PTX-1294 at 3. Specifically, the DNA Center manages and sends rules to the Accused Switches and Routers. Tr. 575:15-577:8; PTX-1263 at 179. As noted, Centripetal accused the DNA Center, when used in combination with the Accused Switches or Routers, of infringing the asserted claims in the '806 Patent. Tr. 571:17-572:3.

Stealthwatch with Cognitive Threat Analytics

Stealthwatch is a part of the DNA Center subscription that can be used with the Accused Switches and Routers. Tr. 450:23-452:11, 453:16-454:20; *see also* PTX-577 at 007; PTX-992 at 1-2. It was updated in 2017 to include Cognitive Threat Analytics. Tr. at 2148:8-11. Cisco advertised Stealthwatch with Cognitive Threat Analytics as having the ability to analyze traffic flowing from the Accused Switches and Routers to "detect and respond to threats in real-time." PTX-482 at 664. The key components of Stealthwatch include two pieces of hardware—the Stealthwatch Flow Collector and the Stealthwatch Management Console. Tr. 2143:2-12. Cisco indicated that Cognitive Threat Analytics is a cloud-based service that is based overseas in Dublin and London. Tr.

Appendix C

2183:9-15; 2189:19-2190:1. As noted, Centripetal accused Stealthwatch with Cognitive Threat Analytics, when used with the Accused Switches and Routers, of infringing the asserted claims of the '176 Patent. Tr. 975:17-21, 995:19-21.

Identity Services Engine

Cisco's Identity Services Engine is software that can be used with the Accused Switches and Routers to provide "[c]entral network device management" and "granular control of who can access which network device." PTX-411 at 891. The Identity Services Engine is responsible for "tracking [the] identity of users and user computers on a network and for setting the limits of user and computer access to other devices on the network." Tr. 149:20-23. The parties dispute whether the Identity Services Engine is accused of infringement. *See infra* note 8. In any case, the device plays a role in the quarantine rule that Centripetal has accused of infringing the asserted '193 Patent claims.

Adaptive Security Appliance and Firepower Firewalls

Centripetal also accused certain of Cisco's firewalls, including the Adaptive Security Appliance 5500 with Firepower services (version 9.4 and later) and Cisco's Firepower Appliance 1000, 2100, 4100, and 9300 series running Firepower Threat Defense 6.0 and later (the "Accused Firewalls"), of infringement. ECF No. 408 at 17 n.5; *see also* Centripetal PFF ¶ 78. Centripetal argued that the Accused Firewalls, used in combination with the Firepower Management Center, infringe the asserted claims of the '806 Patent. Tr. 435:4-16, 571:17-572:3, 642:4-12.

*Appendix C***Firepower Management Center**

The Firepower Management Center is Cisco software that is used to manage the Accused Firewalls. Tr. 63:24-64:10, 558:1-14. It can configure and operate multiple firewall devices in the network. Tr. 558:1-14, 643:6-10. In 2017, the Threat Intelligence Director was added to the Firepower Management Center. PTX-1291 at 1, 7; Tr. 651:18-653:6. The Threat Intelligence Director receives rules from various sources and preprocesses them into rule sets that can be used by Firepower Management Center. Tr. 651:18-653:6. As noted, Centripetal accused the Firepower Management Center with the Threat Intelligence Director, in combination with the Accused Firewalls, of infringing the asserted claims of the '806 Patent. Tr. 435:4-16, 571:17-572:3. 642:4-12.

IV. '193 PATENT**A. Findings of Fact****Asserted Claims in the '193 Patent**

1. The '193 Patent was issued on June 20, 2017, and has the title "Filtering Network Data Transfers." ECF No. 701 ("Stip.") ¶¶ 8-9. The patent was filed on February 18, 2015, as a continuation of application No.13/795,882. Stip. ¶ 9. The patent has a priority date of March 12, 2013. Stip. ¶ 10; JTX-4 ("193 Patent") at 1:6-9.

2. The asserted claims are claims 18 and 19. Stip. ¶ 11. They are, respectively, a packet-filtering system

Appendix C

claim and a computer readable media claim. *Id.* 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

Appendix C

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.

'193 Patent at 14:1-36.

3. Claim 19 is identical to claim 18 except that it is a computer readable media⁶ claim. Stip. ¶ 13. Claim 19

6. Computer readable media is software comprising source code that is loaded into computer hardware through a device such as a CD-ROM, memory card, or flash drive. Tr. 473:3-23. This media comprises readable instructions for the intended computer to operate. *Id.*

Appendix C

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.” ’193 Patent at 14:1-15:2. For all relevant purposes, the parties treat claims 18 and 19 the same. Stip. ¶ 13.

4. The ’193 Patent describes a method of filtering packets to prevent data exfiltrations. The specification explains that “[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.” ’193 Patent at 1:24-27. It notes that one reason for this is that “many exfiltrations are facilitated by using popular network data transfer protocols . . . that often appear to an observer (e.g., a conventional cyber defense system) as normal network behavior.” ’193 Patent at 1:27-32. One of the inventors of the ’193 Patent, Dr. Sean Moore, characterized the technology as involving the prevention of exfiltration of confidential data by cyber criminals. Tr. 343:12-16. Likewise, Centripetal’s expert witness on the ’193 Patent, Dr. Mitzenmacher, noted that the ’193 Patent claims relate to the forwarding or dropping of packets for the purpose of preventing exfiltrations. Tr. 465:16-21.

5. At a basic level, claims 18 and 19 describe a system that drops or forwards packets based on two criteria: (1) the destination of the packets and (2) the type of data

Appendix C

transfer associated with the packets. '193 Patent at 14:1-15:2.

6. As set forth in claim 18, the system first “receive[s] . . . a plurality of packets” from a computer in a “first network.” *Id.* at 14:5-6. Then, if the packets are “destined for [a] second network,” and the system makes a “determination that the . . . portion of packets comprises data corresponding to [rule] criteria . . . configured to prevent a particular type of data transfer from the first network to [the] second network,” an operator is applied that is “configured to drop packets associated with the particular type of data transfer.” *Id.* at 14:9-22.

7. Alternatively, if the packets are “destined for a third network” and the system makes a “determination that the . . . packets comprise[] data that does not correspond to the [rule] criteria,” the claim states that an operator is applied that is “configured to forward packets not associated with the particular type of data transfer to the third network.” *Id.* at 14:23-36. Claim 19 describes the same technique. *See id.* at 14:41-56.

8. The patent’s specification describes this as a two-stage filtering method:

[T]he 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,

Appendix C

encrypted communication, etc.) between the resources.

'193 Patent at 8:45-52. The specification further explains that this filtration method would “allow users to surf (e.g., GET) to one or more websites attached to the Internet,” but prevent riskier types of data transfers associated with exfiltration, such as “users . . . writing (e.g., PUT) data files or posting (e.g., POST) forms to one or more websites.” *Id.* at 2:43-54; *see also id.* at 7:10-20, 7:32-37. The specification distinguishes this solution from quarantining a network computer entirely, noting that “[w]hile enterprise X could simply block all communications to networks . . . it does not fully trust, this would likely result in enterprise X blocking access to most of the Internet.” *Id.* at 7:26-29.

The Accused Switches and Routers

9. Centripetal alleged that Cisco’s Accused Switches and Routers⁷ infringe claims 18 and 19 of the '193 Patent when the devices use specific packet-filtering rules to determine if a packet should be permitted or dropped. Centripetal PFF ¶¶ 153-60; Centripetal PCL ¶¶ 19-30; Tr. 791:14-792:24; *see also* Tr. 2377:13-2379:1. At trial, Centripetal relied on the infringement opinion of expert witness Dr. Michael Mitzenmacher and Cisco relied

7. The parties dispute whether Centripetal’s infringement theory also requires the involvement of the Identity Services Engine management device. *See* Cisco PFFCL ¶ 67; Centripetal PFF ¶ 129. The Court need not reach this question because it finds that the Accused Switches and Routers do not filter packets by the “particular type of data transfer” required by the claims.

Appendix C

on the non-infringement opinion of expert witness Dr. Mark Crovella. Both parties also called a variety of fact witnesses.

10. To begin, Cisco's Accused Switches and Routers apply packet-filtering rules to drop or forward packets that are transmitted through the devices. Tr. 488:1-489:3; PTX-1276 at 216. To do this, the devices use processors, specifically a programmable Application Specific Integrated Circuit containing a Unified Access Data Plane. Tr. 477:23-478:8; PTX-1303 at 056. The devices also contain memory that stores software instructions, which are embodied in the operating system running on the devices. Tr. 477:16-23; PTX-1303 at 056.

11. The sets of rules that the accused devices apply to packets are called access control lists, or "ACLs," which can cause the devices to forward or drop packets based on certain criteria. Tr. 494:3-9, 496:20-498:2, 2549:15-2550:11. There are numerous types of ACL rule sets; however, Centripetal's infringement theory focuses on a specific type, the Security Group ACL or "SGACL." Centripetal PCL ¶ 26; Tr. 2389:1-8; *see also* PTX-1276 at 216.⁸

8. The Accused Switches and Routers apply various sets of ACL rules when a packet enters the device and when it exits the device (i.e., on ingress and egress). Cisco's non-infringement expert, Dr. Crovella, explained that group access control lists ("GACLs") are applied on both ingress and egress. Tr. 2388:21-2389:19; *see also* PTX-1276 at 216. Security Group ACLs are one type of GACL. Tr. 2389:1-3.

Appendix C

12. The accused devices apply SGACL rules to packets by using scalable group tags or “SGT” tags. Tr. 494:12-24, 496:19-498:2; *see also* PTX-1276 at 216. When a packet enters an Accused Switch or Router, the device checks for the existence of an SGT tag, and if it detects one, applies the corresponding SGACL rule associated with the tag. Tr. 2383:11-19; 2423:19-2424:15. These SGT tags are attached to packets transmitted from network computers to reference the security group that the computer is assigned. *See* PTX-563 at 414-15 (listing groups such as “Supplier,” “Employee,” and “Quarantine”). Each security group is assigned a different SGT tag, and all packets transmitted from a computer in a particular security group are appended with the same SGT tag. *See* Tr. 525:7-23; Tr. 2379:2-15; PTX-1276 at 211.

13. Network administrators can modify the security group of a computer through the Identity Services Engine, a separate Cisco management device. Tr. 149:16-151:4, 527:2-17, 1698:10-14; PTX-1326; PTX-1089 at 1238 (“[Identity Services Engine] Adaptive Network Control . . . is used to change the authorization state without having to modify the overall authorization policy. . .”).

14. Although Centripetal alleged that the Accused Switches and Routers infringe the asserted claims of the ’193 Patent based on the use of SGACL rules and SGT tags generally, at trial it focused only on their use in effecting a quarantine. Centripetal PFF ¶¶ 129, 143-44, 161-66. Centripetal’s expert Dr. Mitzenmacher explained

Appendix C

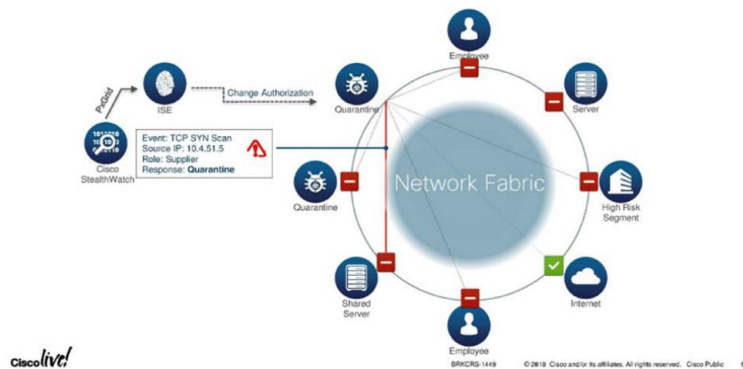
that this was because the quarantine rule was a “primary exemplar” of the accused devices’ functionality. *See* Tr. 791:17-792:24; *see also* Centripetal PFF ¶¶ 144, 154-160.

15. The quarantine rule operates as follows: if the accused devices receive a packet containing a quarantine SGT tag, the devices apply the quarantine SGACL rule and forward or drop the packet depending on whether it is destined for a restricted destination as specified by the ACL rules. Tr. 2388:18-2389:19, 2423:19-2424:7; PTX-1276 at 216; *see also* PTX-1280 at 021; PTX-1356 at 001-005. The purpose of the quarantine rule is to limit a computer’s access to certain network destinations. *See, e.g.*, PTX-1280 at 021.

16. In other words, the quarantine rule can be set up to block a computer from accessing specific endpoints, such as part of a network containing sensitive company documents, while allowing access to other destinations, like the Internet. This is shown in the following diagram from a Cisco presentation discussed at trial:

Appendix C

Rapid Threat Containment with TrustSec, ISE and Stealthwatch



PTX-563 at 415; *see also* Tr. 869:6-12.

17. Importantly, a quarantine SGT tag is attached to *all* packets transmitted from a quarantined computer. Tr. 870:15-17, 2379:2-2380:2. Additionally, the Accused Switches and Routers only need to know the destination of a packet containing a quarantine SGT tag in order to process the packet with the quarantine SGACL rule. Tr. 869:1-12, 2377:2-10, 2385:23-2386:15, 2423:22-2424:15. Using this destination information, the Accused Switches and Routers will therefore drop *all* packets from a quarantined computer to a restricted network destination and allow *all* packets from a quarantined computer to a permitted network destination. Tr. 525:7-23, 2379:2-15, 2388:18-2389:19, 2423:19-2424:7; PTX-1276 at 216; *see also* PTX-1280 at 021; PTX-1356 at 001-005. The evidence does not show that a subset or portion of the packets—either from a quarantined computer to a

Appendix C

restricted destination or from a quarantined computer to a permitted destination—can be dropped while other packets to that same destination are allowed.

18. This understanding was confirmed by Centripetal’s expert, Dr. Mitzenmacher, in response to a question from the Court:

THE COURT: Well, this this means that if your end user was, for example, a corporation and was a separate network, that you could allow some information to go to the corporation and other information not to go to them that was generated from the same source?

WITNESS: So the way typically the policies are instrumented is you restrict according to source and destination. So you would say, well, I’m not going to let you reach out to this other location, to this other network, right, and it will block sort of that—it will block the communication between you and that other network.

Tr. 527:23-528:8; *see also* Tr. 869:8-12 (Dr. Mitzenmacher: “[T]he primary goal of the quarantine is to block that host from accessing certain other networks. . . . It looks at the person trying to reach out from inside and it blocks to where they can go to.”); Tr. 545:22-546:12 (Dr. Mitzenmacher: “[I]f it’s trying to go to one of these bad places, it’s going to get dropped, and if it’s going to a good place or a place that’s not one of the bad places, it will

Appendix C

be okay.”); Tr. 2387:2-3 (Cisco expert Dr. Crovella: “The quarantine rule doesn’t do any check to see what kind of data transfer is contained in the packet.”); PTX-1280 at 021.

B. Conclusions of Law

Centripetal has not met its burden to establish infringement of the ’193 Patent because it has failed to show by a preponderance of the evidence that Cisco’s technology performs each of the limitations in the patent claims. In particular, Centripetal has failed to establish that Cisco’s routers and switches drop or forward packets based on the “particular type of data transfer.” ’193 Patent at 14:9-22, 14:27-36, 14:44-56, 14:60-15:2.

In relevant part, the claims indicate that if packets received by the system are “destined for [a] second network” and those packets meet rule criteria “configured to prevent a particular type of data transfer from the first network to [the] second network,” an operator is applied that is “configured to drop [those] packets associated with the particular type of data transfer.” ’193 Patent at 14:9-22. The claims likewise specify that if packets are “destined for [a] third network” and “comprise[] data that does not correspond to the [type of data transfer] criteria,” an operator is applied that is “configured to forward [those] packets not associated with the particular type of data transfer toward the third network.” *Id.* at 14:22-36.

The disagreement between the parties comes down to whether the “particular type of data transfer” claim

Appendix C

limitation requires a system to drop some, but not all, packets sent between two different network destinations. The evidence is overwhelming that this functionality is not present in the accused technology. *See supra* ¶¶ 15-18. Because the Court finds that the asserted claims of the '193 Patent require this functionality—filtration of a subset of packets sent between computers in two different networks—Centripetal fails to prove infringement of the '193 Patent claims. The language of the claim limitation, the patent specification, and Centripetal's statements to the PTAB all support the Court's understanding of this claim requirement. *See N. Am. Container, Inc. v. Plastipak Packaging, Inc.*, 415 F.3d 1335, 1344 (Fed. Cir. 2005) (explaining that the infringement analysis begins by determining “the scope and meaning of the patent claims asserted” (quoting *Cybor Corp.*, 138 F.3d at 1454)).

The claim language is instructive. In order for the system to drop packets, two conditions must be met: (1) the packets from a device in a first network must be “destined for [a] second network” and (2) the packets must meet rule criteria “configured to prevent a particular type of data transfer from the first network to [the] second network.” '193 Patent at 14:9-16. To give effect to both of these conditions, it is necessarily the case that only a portion of the packets destined for the second network meet the type of data transfer rule criteria specified by the second condition. Otherwise, the second condition would be rendered superfluous. *See W.L. Gore & Assocs., Inc. v. Medtronic, Inc.*, 834 F. Supp. 2d 465, 477 (E.D. Va. 2011) (“Claim differentiation creates a presumption that the difference between claim language is significant and

Appendix C

that the Court should not construe terms in such a way as to render the language of a claim superfluous.”), *aff’d*, 530 F. App’x 939 (Fed. Cir. 2013).

The patent’s specification confirms the Court’s reading. See *Phillips v. AWH Corp.*, 415 F.3d 1303, 1315 (Fed. Cir. 2005) (“[T]he descriptive part of the specification aids in ascertaining the scope and meaning of the claims inasmuch as the words of the claims must be based on the description. The specification is, thus, the primary basis for construing the claims.” (quoting *Standard Oil Co. v. Am. Cyanamid Co.*, 774 F.2d 448, 452 (Fed. Cir. 1985))). The specification discusses functionality that would prevent users communicating with a computer in a network from conducting certain types of data transfers (e.g., risky transfers associated with exfiltration) without blocking a user’s access to that destination entirely. The specification provides the example of “allow[ing] users to surf (e.g., GET) to one or more websites attached to the Internet, . . . [while] prevent[ing] such user(s) from . . . writing (e.g., PUT) data files or posting (e.g., POST) forms.” ’193 Patent at 2:46-49. The specification notes that administrators could use this functionality “to prevent . . . exfiltrations (e.g., file transfers containing sensitive information, posting of login credentials[,]. . . etc.) to network nodes (e.g., web sites) that they may not trust.” *Id.* at 2:50-54. In other words, the patent is not designed to block all transfers between a computer and certain network destinations (like Cisco’s accused technology does), but instead allows an administrator to permit low-risk types of communication between computers in different networks, while blocking high-risk types of communication.

Appendix C

Finally, Centripetal’s statements to the PTAB are consistent with the Court’s interpretation. When Centripetal defended the validity of its patent before the PTAB, it distinguished the claims from prior art by emphasizing the second condition, i.e., filtration by “particular type of data transfer.” Centripetal stated that “[t]his two-stage process is reflected in each independent claim,” which includes “claims . . . 18[] and 19.” DTX-369 at 011, 018. Regarding the “second stage,” Centripetal quoted the portion of the ’193 Patent’s specification that explained “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.” *Id.* at 017 (quoting ’193 Patent at 8:48-51); *see also Aylus Networks, Inc. v. Apple Inc.*, 856 F.3d 1353, 1362 (Fed. Cir. 2017) (stating that a patent holder’s statements before the PTAB can be considered for claim construction).

Centripetal’s contrary interpretation of the claim limitation at the Rule 63 hearing—namely, that a “particular type of data transfer” refers to the *network* associated with the data transfer—is unavailing. Centripetal argued that Cisco’s Accused Switches and Routers “prevent[] particular types of data transfers to or from potentially compromised computers—*e.g.*, transfers involving networks with sensitive information—but allow transfers involving other networks, such as the Internet.” ECF No. 703 at 10. More specifically, Centripetal has asserted that the “particular type of data transfer that is being prevented is packets that contain SGT tags that specify what network that packet can go to.” R. 63 Tr. 238:5-7.

Appendix C

This construction is impermissible because it reads out relevant claim language. Recall that in order to drop a packet, the claims require two conditions to be met: (1) the packets from the first network must be “destined for [a] second network” and (2) the packets must meet rule criteria “configured to prevent a particular type of data transfer from the first network to [the] second network.” Patent ’193 at 14:9-16. The claim language refers to the “particular type of data transfer” as a kind of data transfer between the first network and a second network. However, in Centripetal’s construction, the “particular type of data transfer” would encompass *all* data transfers between the first network and the second network. *See, e.g.*, R. 63 Tr. 260:5-9 (“[T]he type of data transfer from that network to another network is going to be one type. If I have a data transfer from a network to a third network, I think that is a different type of data transfer. . . .”). This construction would render the check for a particular type of data transfer unnecessary, as the claims already require the system to check that the packets are destined for the second network in the first step. *See Andersen Corp. v. Fiber Composites, LLC*, 474 F.3d 1361, 1369-70 (Fed. Cir. 2007) (discussing the doctrine of claim differentiation). As a result, the Court rejects Centripetal’s construction.

At times, Centripetal has also appeared to put forward a different construction, namely that a “particular type of data transfer” refers to the kind of communications contained in the transfer, but that the claim language does not require the system to drop *only* those particular data transfers. *See, e.g.*, Tr. 3281:13-3282:2. Centripetal

Appendix C

elicited testimony at trial that suggested the claim requirements could be satisfied by a system that first detects a “particular type of data transfer” to a specific network (such as an HTTP POST command indicative of exfiltration) and then uses that information to block all future traffic to that destination. *See, e.g.*, 787:8-13 (Dr. Mitzenmacher: “The particular type of data transfer you’re trying to stop is the exfiltration . . . And the way that was detected, right—one of the ways that can be detected is that you notice certain types of HTTP POST or HTTP GET commands.”); *see also* Tr. 512:20-513:2, 517:25-518:7, 786:5-24; Centripetal PFF ¶ 160 (“[The Accused Switches and Routers] are designed to implement quarantine rules based on detecting abnormal behavior in a variety of data transfer types, including Hypertext Transfer Protocol (HTTP), HTTP GET, and HTTP POST.”).

This second construction similarly reads out the second claim limitation that the packets meet rule criteria “configured to prevent a particular type of data transfer from the first network to [the] second network.” *See* Patent ’193 at 14:9-14. Just as in the analysis above, if the quarantine rule blocks *all* packets traveling to the second network, this necessarily means that no further determination is necessary beyond checking where the packets are headed. The fact that a rule blocking all packets to the second network may have been based on an earlier detection of abnormal traffic to that network is immaterial.⁹ As such, the Court rejects this construction.

9. The Court recognizes that it is possible to describe a quarantine rule that blocks all transfers between two networks as one “configured to prevent a particular type of data transfer,”

Appendix C

For the reasons stated above, the claim language, the patent’s specification, and Centripetal’s statements to the PTAB all support the Court’s conclusion that “particular type of data transfer” refers to a subset of transfers between computers in two different networks. Because the Court finds that Cisco’s quarantine rule does not have this functionality, the Accused Switches and Routers do not “determin[e] that . . . packets comprise[] data corresponding to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer” or “drop packets associated with the particular type of data transfer.” ’193 Patent at 14:9-12, 18-20.¹⁰

in the same way that revoking an individual’s driving privileges obviously prevents that person from driving on a particular road. In other words, under this construction, “particular type” means “all types.” However, this is an unnatural reading that is undercut by the language of the patent specification discussing filtration of only a subset of data transfers between network destinations. *See* ’193 Patent at 2:46-50 (describing functionality “allow[ing] users to surf (e.g., GET) to one or more websites attached to the Internet, . . . [while] prevent[ing] such user(s) from . . . writing (e.g., PUT) data files or posting (e.g., POST) forms”).

10. To the extent Centripetal has accused the operation of SGT tags and corresponding SGACL rules that do not involve a quarantine, the Court notes that Centripetal only presented evidence as it relates to a quarantine. While it is, of course, possible that non-quarantine SGT tags operate in a different manner than quarantine SGT tags, Centripetal has not presented any evidence of this. It would also appear that Centripetal does not believe there are material differences given its choice to present testimony of the quarantine rule as the “exemplar” for its infringement theory. *See* Tr. 791:17-792:24.

Appendix C

Accordingly, the Court FINDS that Cisco's Accused Switches and Routers do not literally infringe claims 18 or 19 of the '193 Patent.

C. Doctrine of Equivalents

Centripetal argued under the doctrine of equivalents that the Accused Switches and Routers “perform substantially the same function in substantially the same way” to achieve the same result outlined in the claims “because the collection of packets is dropped based on the corresponding rule and operator.” Centripetal PFF ¶ 176. In its literal infringement analysis, the Court found that Cisco's technology does not meet the “particular type of data transfer” limitation because the evidence does not show that the quarantine rule is able to block a subset of the packets transferred between computers in two different networks, as the claims require. This analysis is no different when viewed under the doctrine of equivalents. The patented filtration technique is not literally present in Cisco's technology, and Centripetal likewise does not show that a substantially similar function is performed by the accused devices. For this reason, the Accused Switches and Routers do not perform the substantially the same function or achieve the same result. Therefore, the Court FINDS that Centripetal has not met its burden of proof to show infringement of claims 18 or 19 under the doctrine of equivalents. *See VirnetX, Inc. v. Cisco Sys., Inc.*, 767 F.3d 1308, 1322-23 (Fed. Cir. 2014) (discussing the requirements for finding infringement under the doctrine of equivalents).

*Appendix C***V. '806 PATENT****A. Findings of Fact****Asserted Claims in the '806 Patent**

19. The '806 Patent was issued on December 1, 2015, and has the title “Rule Swapping in a Packet Network.” Stip. ¶¶ 14-15. The patent was filed on January 11, 2013, which is the patent’s priority date. *Id.* ¶¶ 15-16.

20. The asserted claims are claims 9 and 17. *Id.* ¶ 17. They are, respectively, a packet-filtering system claim and a computer readable media claim. *Id.* 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;

Appendix C

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.

Appendix C

21. Claim 9 is identical to claim 17 in every respect except that claim 17 is a computer readable media claim. Stip. ¶ 19. 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.” ’806 Patent at 11:16-21, 12:32-34. For all relevant purposes, the parties treat claims 9 and 17 the same. Stip. ¶ 19.

22. The ’806 Patent describes a method for network protection devices to swap different sets of rules applied to packets passing through the devices. The specification notes that “[n]etwork protection devices may require time to switch between different rule sets[,] [and] [a]s rule sets increase in complexity, the time required for switching between them presents obstacles for effective implementation.” ’806 Patent at 1:20-22. It identifies two specific problems: (1) “a network protection device may be unable to process network traffic while switching between rule sets,” and (2) “while implementing a new rule set, a network protection device may continue processing packets in accordance with an outdated rule set.” *Id.* at 1:22-28. The specification explains that “[i]n certain circumstances (e.g., in the event of a network attack), such processing [with an outdated rule set] may exacerbate rather than mitigate the impetus for the rule set switch (e.g., the effect of the network attack).” *Id.* at 1:28-31.

Appendix C

23. Claims 9 and 17 describe a rule swapping technique responsive to these concerns. Claim 9 provides that based on “instructions . . . executed by at least one processor,” the system “receive[s] a first rule set and a second rule set,” “preprocess[es]” both rule sets, and “configure[s] at least two processors . . . to process packets in accordance with the first rule set.” ’806 Patent at 11:18-29. Then, the system “receive[s] . . . packets” and “process[es], in accordance with the first rule set, a portion of the . . . packets.” *Id.* at 11:29-35. Next, in order to effectuate the rule swap, the system “signal[s] each processor . . . to process packets in accordance with the second rule set,” and “responsive to being signaled,” “configure[s] each processor” to take a series of actions. *Id.* at 11:35-53. Specifically, the processors are configured to “cease processing of one or more packets,” “cache the one or more packets,” and the system “reconfigure[s] [the processor] to process packets in accordance with the second rule set.” *Id.* Once reconfiguration is complete, the system “signal[s] completion of reconfiguration,” and “responsive to receiving signaling,” “process[es], in accordance with the second rule set, the one or more [cached] packets.” *Id.* at 11:45-53. Claim 17 describes the same technique. *Id.* at 12:32-64.

The Accused Switches, Routers, and DNA Center

24. Centripetal accused two combinations of Cisco products of infringing claims 9 and 17 of the ’806 Patent. At trial, Centripetal relied on the infringement opinion of expert witness Dr. Michael Mitzenmacher and Cisco

Appendix C

relied on the non-infringement opinion of expert witness Dr. Narasimha Reddy. Both parties also called a variety of fact witnesses.

25. The first accused combination is the Accused Switches and Routers combined with Cisco's DNA Center. Tr. 571:19-25; Centripetal PFF ¶ 227. Specifically, Centripetal accused these technologies of infringing the asserted claims when the switches and routers use a particular method of updating packet-filtering rules called the "FED 2.0 Hitless ACL Update." Centripetal PFF ¶ 247; *see also* Tr. 2550:18-25.

26. The Accused Switches and Routers apply sets of rules (ACLs) to packets received by the devices that cause the packets to be dropped or forwarded. Tr. 2550:1-7. The devices can receive these rule sets from a variety of sources, including the DNA Center. Tr. 2571:12-17.

27. When the switches and routers receive a new set of rules, the devices may swap out the old rules using the Hitless ACL update technique. Tr. 2550:18-2551:12. This rule update technique is also referred to as the "Hitless TCAM update." Tr. 2552:13-17; PTX 1303 at 073. According to Cisco engineer Peter Jones, this technique "refers to the ability to have a new or updated set of ACL[s] applied to a given string of packets without disabling packet processing while that change is made." Tr. 2550:23-25. He explained that, "[u]sing the Hitless update, while preparing the updated rule set for the system [the devices]

Appendix C

continue[] to process packets with the old rule set.” Tr. 2552:20-23; *see also* Tr. 2571:22-2572:1.¹¹

28. Then, once the new rules are successfully programmed, the rules are swapped, and the Accused Switches and Routers start processing packets from that point forward with the new rule set. Tr. 2552:23-25, 2572:2-20. This swap happens during the devices’ existing idle period between the processing of individual packets. Tr. 2554:20-24 (Cisco engineer Peter Jones explaining that the swap occurs during the “two or four internal clock periods” between packet processing); Tr. 2619:21-25 (Cisco expert Dr. Reddy explaining that these clock periods are typically “less than a billionth of a second”). This fixed time pipeline is not affected by the rule swap; the packets continue to be processed normally regardless of whether a rule swap is occurring. Tr. 2550:12-2551:12, 2554:22-24.

29. During packet processing, packets pass through buffers in the Accused Switches and Routers. Tr. 623:18-22, 626:25-627:4, 2563:14-19; DTX-562 at 043. A packet buffer is “a piece of memory to store the contents of a packet.” Tr. 2523:10-11; *see also* Tr. 628:7-13 (Dr. Mitzenmacher explaining that “a buffer generally refers to something that you . . . leave data waiting [in] for a short period of time, until you’re ready for it”). Storing packets in a packet

11. The Hitless ACL update replaced a prior rule swap technique used by Cisco’s switches and routers that involved processing packets using a new rule set before it was fully programmed into the accused devices’ software. Tr. 2552:18-23; PTX-1195 at 003, 005. This resulted in packets being discarded during the swap process. Tr. 2552:20-23; PTX-1195 at 003.

Appendix C

buffer is “a function of any . . . network interface.” PTX-1917 (Cisco engineer Martin Hughes); *see also* DTX-1688 at 166:21-168:10. In the Accused Switches, packets waiting to be processed are stored in a part of the device called the “Packet Buffers Complex.” Tr. 2563:22-2564:12; DTX-562 at 043. The Accused Routers have a similar buffer called the “Dispatcher Packet Buffer.” Tr. 623:18-22. Packets are stored in these buffers in the normal course of packet processing as well as during a rule swap. Tr. 623:18-22, 2563:7-19, 2565:11-18; PTX-1313 at 062.

**The Accused Firewalls and the
Firepower Management Center**

30. Centripetal also accused a second combination of Cisco products of infringing claims 9 and 17 of the '806 Patent: the Accused Firewalls combined with the Firepower Management Center. Tr. 435:4-16, 571:15-572:3, 642:4-12. Centripetal accused these technologies of infringing the asserted claims when the firewalls use a specific method of updating packet-filtering rules called the “Transactional Commit Model.” Tr. 680:8-681:6; *see also* Centripetal PFF ¶¶ 291, 293.

31. The Accused Firewalls can apply sets of rules (ACLs) to packets received by the devices that cause the packets to be dropped or forwarded. Tr. 647:17-21. The firewalls can receive these rules from the Threat Intelligence Director, which is integrated into the Firepower Management Center. Tr. 648:24-649:5; *see also* Tr. 651:20-11.

Appendix C

32. Centripetal alleged that when the Accused Firewalls receive a new set of rules from the Threat Intelligence Director, the devices may swap out the old rules using the Transactional Commit Model.¹² *See* Centripetal PFF ¶ 291.

33. Using this technique, Cisco engineer Hari Shankar explained that when an Accused Firewall receives a new rule set, the rules must first be programmed into

12. Cisco has disputed that the Accused Firewalls operate in this manner. As to the first Accused Firewall, the Firepower Appliance running Firepower Threat Defense software, Cisco engineer Hari Shankar testified that the Firepower Threat Defense software does not include the accused Transactional Commit Model feature. Tr. 2515:5-12; *see also* Tr. 2612:21-23, 2642:20-23 (Cisco expert Dr. Reddy stating that the Transactional Commit Model is not used in the Firepower appliance). Therefore, Cisco argued Centripetal's infringement theory is untenable as to this Accused Firewall. *See* Cisco PFFCL ¶ 210. The second Accused Firewall is the Adaptive Security Appliance with Firepower Services. Tr. 571:25-572:3, 2583:16-2584:11. This firewall, Mr. Shankar noted, is actually two separately managed software firewalls "bolted together" on the same hardware, and only one of those two firewalls (the Adaptive Security Appliance software), has the accused Transactional Commit Model feature. Tr. 2504:17-25, 2514:10-21, 2612:24-2613:1; *see also* PFFCL ¶ 211. Cisco argued that this is fatal to Centripetal's infringement theory because the Adaptive Security Appliance software receives rule updates from a non-accused management device, the Adaptive Security Device Manager. Cisco PFFCL ¶ 211-12; Tr. 2511:21-2513:3, 2612:21-2613:1. However, because the Court finds that Centripetal failed to prove infringement even if the Accused Firewalls process rule updates from the Firepower Management Center using the Transactional Commit Model, it need not resolve this dispute.

Appendix C

the firewall's software. Tr. 2516:5-15. During this time, the firewall continues to process packets using the old rule set. Tr. 2516:11-21.¹³

34. Then, once programming is complete, Mr. Shankar testified that the firewalls "switch[] a mode so that any subsequent lookups will actually start using the new rule set instead of the old one." Tr. 2517:11-13. This switch occurs during the time between the firewall's processing of individual packets. Tr. 2521:6-12 (Mr. Shankar explaining that the "[t]he last packet that came before the programming is complete" is processed under "the old rule set," and "[t]he next packet" is processed under "the new rule set"). Packet processing time is not changed as a result of the rule change execution. Tr. 2522:8-15.

35. Mr. Shankar explained that it was acceptable for a firewall to use an old rule set while it was programming the new rule set because it typically takes a human hours to actually create the firewall rules. Tr. 2518:22-2519:7.

13. Similar to the Hitless ACL update, the Transactional Commit Model replaced an earlier rule swap technique in which a new rule set was applied before compilation was completed. Tr. 689:4-690:7. As noted in Cisco documentation, "[w]ith the legacy model, rule updates take effect immediately but rule matching slows down during the rule compilation period." PTX-1241 at 253. In contrast, when the Transactional Commit Model feature is enabled, "a rule update is applied after the rule compilation is completed; without affecting the rule matching performance . . . [and] [t]his feature is useful to prevent potential packet drops during [a] large compilation of rules under high traffic conditions." *Id.* at 253-54.

Appendix C

Therefore, he did not view the “extra few minutes for the firewall to fully program” the new rules to be an issue. *Id.*; see also PTX-1196 at 007 (“[I]t is acceptable to have [a] reasonable amount of delay for the new rules to take effect.”).

36. Like the Accused Switches and Routers, the Accused Firewalls use buffers when processing packets. Centripetal’s expert Dr. Mitzenmacher explained that packets are stored in a “packet buffer cache” while “waiting for the system to be ready to process them.” Tr. 707:17-20, 712:17-20. Specifically, he indicated that the firewall buffer was referred to as a “receive ring” in Cisco’s documentation. Tr. 708:11-18; PTX-1277 at 012. Cisco engineer Mr. Shankar explained that this buffer is used during normal packet processing as well as during rule swaps. Tr. 2524:17-2525:11. Likewise, Mr. Shankar testified that the packet buffer in the Accused Firewalls operates “independent of whether rules are getting updated.” Tr. 2525:7-8, 13-17. He specifically noted that packets are not placed in a buffer in response to an update to a rule set. Tr. 2525:18-20.

B. Conclusions of Law

Centripetal has not met its burden to establish infringement of the ’806 Patent because it has failed to show by a preponderance of the evidence that Cisco’s technology performs each of the limitations in the claims. In relevant part, the claims indicate that, in order to effectuate a rule swap, the system “signal[s] each processor . . . to process packets in accordance with

Appendix C

the second rule set,” and “responsive to being signaled,” “configure[s] each processor” to, among other things, “cease processing of one or more packets” and “cache the one or more packets.” ’806 Patent at 11:35-53. As to these claim elements, Centripetal fails to establish that, *responsive to* a signal to process packets in accordance with a second rule set, Cisco’s Accused Switches, Routers, or Firewalls *cease processing* packets or *cache* those packets.

As an initial matter, the evidence shows that the Accused Switches, Routers, and Firewalls all cease processing packets, albeit very briefly,¹⁴ and use a form of a queue or buffer to store packets prior to processing. *See supra* ¶¶ 27-29, 33-36. Assuming the use of a packet buffer satisfies the claim requirement to “cache” packets,¹⁵

14. Cisco takes some issue with this characterization, noting that “describing the interval that occurs during a normal cadence as a ‘ceasing’ of processing makes no more sense than saying someone’s heart ‘ceases’ beating when it is between two normal beats, or that the beat of a song ‘ceases’ between the regular hits on the drum.” Cisco PFFCL ¶ 169.

15. There is some dispute as to whether a packet buffer is the same as the “cache” described in the claim language. Dr. Mitzenmacher treated the terms the same when offering his infringement opinion. *See* Tr. 628:7-13 (“So both ‘cache’ and ‘buffer’ are ways that are used by computer scientists to talk about—they’re terms that really just mean memory.”). However, Dr. Sean Moore, one of the ’806 Patent’s inventors, distinguished between the two terms when discussing functionality covered by the patent. DTX-1688 at 167:21-168:1 (“[C]aching would be used in this sense, in this context, for, oh, those packets that you are currently processing through the old policy, you don’t want to like

Appendix C

Centripetal still fails to show that the ceasing or purported caching are taken “responsive to being signaled to process packets in accordance with the second rule set.” ’806 Patent at 11:39-42.

Centripetal’s expert at trial, Dr. Mitzenmacher, did not clearly offer an opinion as to this causal relationship. At various points, he described the ceasing and caching of packets as occurring *during* a rule swap, rather than because of it. *See, e.g.*, Tr. 627:19-25 (in reference to the Accused Routers, using Cisco engineer Martin Hughes’ testimony: “[T]he point is you need to have the packets saved while this processing switch occurs, while you’re switching the rules, and this testimony [of Mr. Hughes] verifies that the router product ha[s] a buffer and will store the packets in the buffer while they’re awaiting for processing.”); Tr. 601:23-25 (in reference to the Accused Switches, describing a “cache that hold[s] the actual packets while they’re waiting”); Tr. 707:11-12, 19-20 (in reference to the Accused Firewalls, identifying memory in the products and testifying, “[t]hat’s what stores packets before while they’re waiting for service,” and noting that “RAM is holding the packets while it’s waiting for the system to be ready to process them”).

The fact that two actions may occur at the same time or in succession, of course, does not show that one

put those back on the buffer from whence you extracted them in the first place.”). Since the Court finds that Centripetal has failed to establish infringement on the basis that the accused devices cease processing or cache packets responsive to a rule change signal, it need not reach this argument.

Appendix C

is taken “responsive to” the other. Cisco’s engineers explained that the cease/cache functionality described by Dr. Mitzenmacher occurred as a part of normal packet processing in Cisco’s accused devices, not in response to a signal to swap to a new rule set. As to the Accused Switches and Routers, Cisco engineer Peter Jones noted that the devices swap between an old and a new rule set during the existing “two or four internal clock periods” between packet processing. Tr. 2554:20-24. Mr. Jones also testified that while all packets are held in a packet buffer to await processing in the ordinary course, this buffer has no relationship to the accused Hitless ACL rule swap technique. Tr. 2563:10-19. He explained that packet buffering in the Accused Switches operates the same way for all packets and regardless of whether the device is conducting a rule swap. Tr. 2563:7-19. Similar testimony was provided by Cisco engineer Hari Shankar with respect to the Accused Firewalls and the Transactional Commit Model update technique. Tr. 2521:6-12, 2525:2-8, 13-17. Therefore, while there is temporal relationship between a rule swap and the ceasing processing of packets, this evidence shows that there is not a causal relationship.

Centripetal responded to Cisco’s argument by emphasizing that the new rule update techniques were designed to avoid dropping packets. Centripetal PCL ¶ 39 (“Cisco has implemented this new rule swap functionality in conjunction with the normal processing functionality to greatly improve the security functionality of its products without dropping packets.”). Dr. Mitzenmacher explained that the inclusion of this feature indicated to him that the accused devices would need to cease processing packets

Appendix C

during a rule swap. Tr. 634:7-14 (“[A]t the end, you update these rules, and because you’re not dropping packets or somehow avoiding—having packets avoid the rules during this transition, that also tells me that there’s a signaling process that says, hey, we stop with the first rule set; we’re starting to put in the second rule set.”); Tr. 706:3-5 (“[W]hat you’re doing is saying that I’m not going to have a period where I’m going to drop the packets.”). Dr. Mitzenmacher also drew a connection between the lack of packet drops and the devices’ use of a packet buffer during a rule swap. Tr. 641:18-24 (“The switches and routers use a first rule set until an update arrives, and when the update arrives, then they use this update operation to perform the swap, as mentioned, without dropping any packets using the cache—and, again, it’s a packet buffer or cache—and after the rule set is swapped, then you begin processing with the second rule set, as according to the claim.”); *see also* Tr. 712:17-23 (“[T]he reason that [the Accused Firewalls] don’t drop any packets during the time period they’re doing the swap is because they’re using this packet buffer cache.”); PTX-1196 at 007.

The flaw in Centripetal’s no-dropped-packets argument, however, is that it does not refute Cisco’s explanation and show *causation* between a signal in the accused devices to swap to a new rule set and the ceasing and caching operations. As discussed, Cisco’s engineers testified that, as to the accused devices: (1) there is an existing idle period between the processing of each packet and (2) packets are stored in a buffer before processing. *See supra* ¶¶ 27-29, 33-36. Even though a rule swap technique might be able to take advantage of this

Appendix C

existing functionality to avoid dropped packets, this does not mean that the ceasing and caching operations are done “responsive to” the rule swap.

Dr. Mitzenmacher’s discussion of the accused devices’ capability to cache packets does not change this analysis. In his direct testimony on the “cease” and “cache” elements, Dr. Mitzenmacher relied on diagrams showing the *normal* packet-processing architecture inside each of the accused devices. *See* PTX-1390 at 029 (Accused Switches); PTX-1313 at 062 (Accused Routers); PTX-1277 at 007 (Accused Firewalls). With respect to each diagram, he indicated that there is a portion of the processor where packets are stored, i.e., the packet buffer. *See, e.g.*, Tr. 621:21-22 (“It’s a holding place for information.”); *see also* PTX-1917. While this may show that the devices “hold the data while you’re doing the swap-over,” Tr. 621:23-24, it does not establish causation; because the buffers are part of normal packet processing, they “hold the data” regardless of whether a swap is occurring.

Further, Centripetal’s attempt to characterize the testimony of Cisco engineer Mr. Jones as supporting its infringement position is unavailing. Centripetal argued that “[d]uring cross-examination, Mr. Jones admitted that the Catalyst 9000 Switch infringed every element . . . of the ’93 Patent[’s]” asserted claims. Centripetal PFF ¶ 236. The relevant portion of the cross examination is copied below:

Appendix C

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.

Appendix C

Q: And you do that swap in between—in that two to four clock cycles that you mentioned yesterday; correct?

A: Right.

Tr: 2572:2-20.

At the Rule 63 hearing, Centripetal argued that Mr. Jones's agreement that "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" indicates that the Accused Switches cease processing responsive to a signal to swap to a new rule set. *See* R. 63 Tr. 345:16-347:1. However, Mr. Jones's statement can only be interpreted to mean that the signal is sent "to stop processing packets with the old rule set," not to stop the processing of those packets entirely, as the claims require. The distinction is important, as an instruction to stop processing packets in one way (with the old set) and to start processing the packets in another way (with the new set) does not require that the device cease processing the packets entirely in response to the instruction. Instead, as Mr. Jones explained, the swap occurs during the existing idle period between individual packet processing, i.e., the "two to four clock cycles" referenced above. *See* Tr. 2554:20-24. As such, Mr. Jones did not admit that the Catalyst 9000 Switch infringed the cease processing element of the asserted '193 Patent claims.

Appendix C

To the extent Centripetal’s position is that the cease processing limitation can be met by a signal to stop processing packets in a certain way (i.e., to “stop processing packets with the old rule set”), the Court rejects this interpretation of the claim requirements. *See, e.g.*, R. 63 Tr. 353:21-22 (Centripetal’s counsel explaining that their argument is that “[c]ease processing of the packets means you stop processing the packets with the first rule set”). As Cisco pointed out, Centripetal’s argument improperly adds language to the claim, converting the claim requirement that the system “cease processing of one or more packets” in response to a signal to switch to a new rule set, to a requirement that it merely “cease processing of one or more packets *with the old rule set*” in response to the rule swap signal. Cisco PFFCL ¶ 172. Figure 4 in the patent specification makes clear that the claim requirement refers to ceasing processing of the packets altogether, not just with the old rule set:

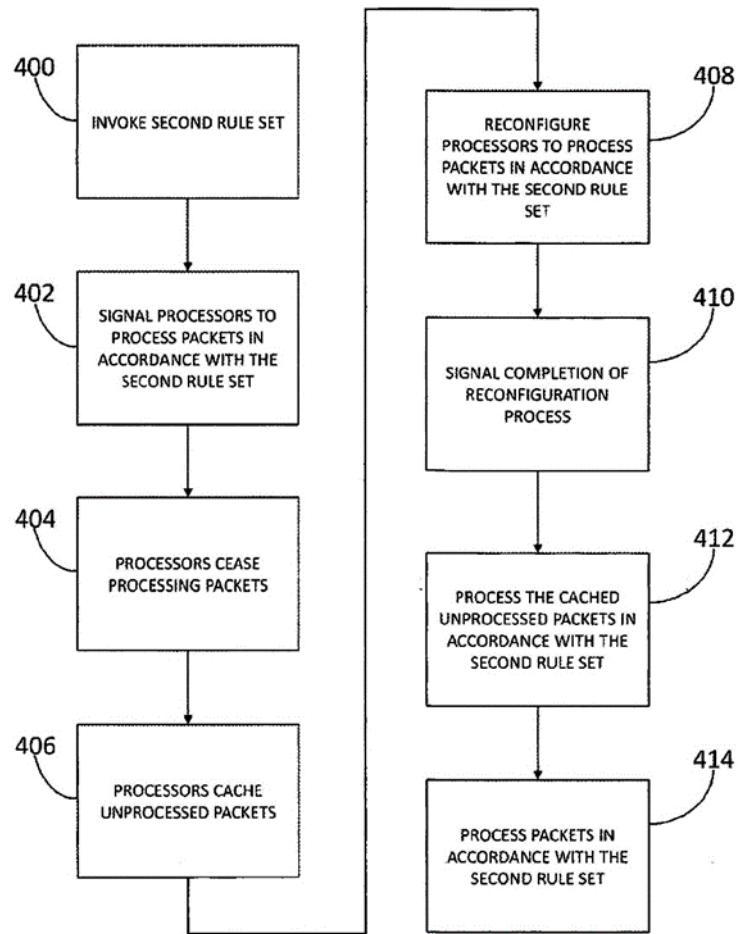


FIG. 4

'806 Patent, Fig. 4. As shown, step 402 reflects the "signal . . . to process packets in accordance with the second rule set." Then, in steps 404 and 406, the "processors cease

Appendix C

processing packets” and “cache [the] *unprocessed packets*” (emphasis added). After reconfiguration, step 412 provides that the system is to “process the cached unprocessed packets in accordance with the second rule set.” It is plain that what is being described is a process in which the system stops processing the packets altogether, rather than only with the first rule set. This is also consistent with how Centripetal’s expert, Dr. Mitzenmacher, described the claim requirements. Tr. 620:1-4 (“So once you’re starting to do the swap for the second rule set, you want to stop processing any packets. Because as you’re doing the update, as the rules are changing, you’re in a state of flux.”). Centripetal’s apparent argument that the cease processing element is satisfied when the accused devices stop processing packets with the old rule set is inconsistent with the claim requirements.

Finally, the Court’s finding of non-infringement is further supported by considering the problem that the ’806 Patent was designed to address—specifically, that “while implementing a new rule set, a network protection device may continue processing packets in accordance with an outdated rule set.” ’806 Patent at 1:25-28. The specification explains that using an outdated rule set “may exacerbate rather than mitigate the impetus for the rule set switch (e.g., the effect of the network attack).” *Id.* at 1:28-31. The cease processing and cache limitations respond to this issue. Specifically, during configuration of a new rule set, the claims indicate that the system stops processing any packets and stores them in a cache to be processed by the new rule set once configuration is complete. ’806 Patent at 11:39-53. This solution avoids the

Appendix C

problem of processing packets with an outdated rule set while the system is configuring the new rule set.

Critically, Cisco’s engineers explained that the problem that the patent was designed to solve—processing packets with an outdated rule set—*still occurs in the accused devices*. See, e.g., Tr. 2518:22-2519:7. Cisco engineer Mr. Shankar explained that he did not view the processing of packets using the old rule set during the “extra few minutes for the firewall to fully program” the new rules to be an issue, as he compared that brief delay to the hours that it takes a human administrator to actually create the new firewall rules (during which time the device would also be processing packets using the old rule set). Tr. 2518:22-2519:7; *see also* PTX-1196 at 007.

For these reasons, the Court FINDS that Cisco’s Accused Switches and Routers combined with the DNA Center and Cisco’s Accused Firewalls combined with the Firepower Management Center do not literally infringe claims 9 or 17 of the ’806 Patent.

C. Doctrine of Equivalents

Having considered literal infringement, the Court must also determine if the Accused Switches, Routers, and Firewalls still infringe under the doctrine of equivalents. The element the Court ultimately found lacking in the literal infringement analysis above was that the ceasing and caching of the packets did not occur “responsive to” a signal to swap rule sets. Centripetal did not assert that an equivalent of this limitation existed,

Appendix C

contending instead that the accused devices satisfied the “preprocessing” element under this doctrine. Centripetal PFF ¶ 301 (arguing that the Accused Switches, Routers, and Firewalls “perform substantially the same function in substantially the same way, to achieve substantially the same result as the ‘preprocessing’ element set forth in the asserted claims”). Centripetal argued that “[s]ubstantially the same function as the ‘preprocessing’ element is performed by receiving information regarding threats, including actions such as blocking and monitoring, which has the same goal of turning information into rules and reprocess them in a format appropriate.” *Id.* (citing Tr. 713:21-714:3). However, Centripetal did not provide any argument under the doctrine of equivalents to establish the causal relationship between the rule switch and the “cease” and “cache” limitations. Moreover, the argument made related to the “preprocessing” element does not relate at all to the “responsive to” element. Accordingly, the Court FINDS that Centripetal has not met its burden to establish infringement under this theory.

VI. '176 PATENT**A. Findings of Fact****Asserted Claims in the '176 Patent**

37. The '176 Patent was issued on January 31, 2017, and has the title “Correlating Packets in Communication Networks.” JTX-3 (“'176 Patent”). The patent was filed on May 15, 2015, and has a priority date of February 10, 2015. Stip. ¶ 21-22.

Appendix C

38. The asserted claims of the '176 Patent are claims 11 and 21. They are, respectively, a system claim and a computer readable media claim. Stip. ¶ 23. 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

Appendix C

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.

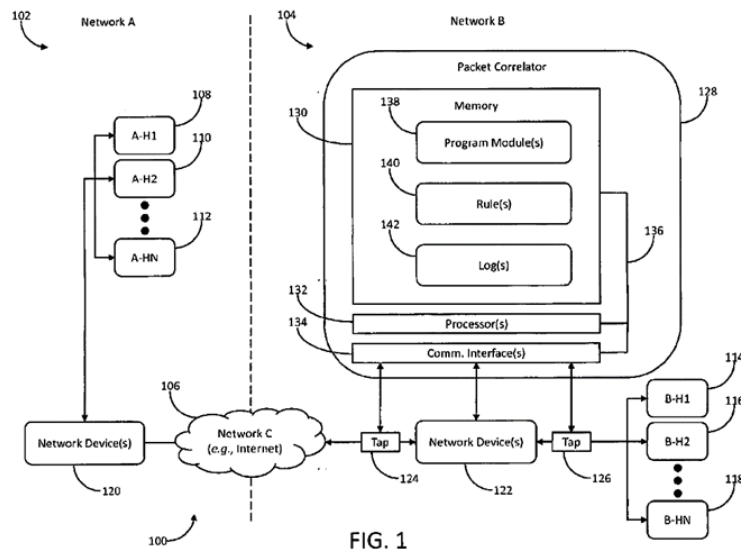
'176 Patent at 17:6-35.

39. Claim 11 is identical to claim 21 in every respect except that claim 21 is a computer readable media claim. 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.” *Id.* at 17:6-9, 18:63-65. For all relevant purposes, the parties treat the two claims the same. Stip. ¶ 25.

Appendix C

40. The '176 Patent addresses the issue of a packet's flow becoming obscured when it passes through a network device. '176 Patent at Title, 1:16-25. A flow refers to a group of packets that contain information distinguishing them from other packets (e.g., each of the packets that comprise an email). *Id.* at 1:18-21. The specification explains that "[n]etwork 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." *Id.* at 1:21-25.

41. Figure 1 of the specification is helpful to understand the problem and the patent's solution:



Id. at Fig. 1.

Appendix C

42. The diagram above contains two networks (Network A and Network B) that are connected by a third network (Network C, e.g., the Internet). The endpoints are the host computers in Network A (A-H1, H2, etc.) and the host computers in Network B (B-H1, B-H2, etc.). Packets sent between these two endpoints travel through various network devices, including the network devices labeled 120 and 122.

43. As explained in the specification, when packets enter a network device, the device may “alter one or more aspects of the packets . . . in a way that obfuscates the association” between the packets entering the device from the packets leaving the device, “at least from the perspective of devices other than the network device[.]” *Id.* at 5:14-20. That is to say, packets comprising an email message from host computer B-H1, for example, could pass through network device 122 and become camouflaged, such that other devices in the network would no longer be able to detect that the packets originated from host B-H1.

44. The solution depicted in Figure 1 shows two “taps” (124 and 126) installed on both sides of network device 122 and a corresponding packet correlator (128). The specification explains that in some embodiments, these taps receive packets coming in and out of a network device and generate log records that are sent to the packet correlator. *See, e.g., id.* at 3:60-4:3, 6:13-28. The specification explains that the packet correlator may use the logs to correlate the packets transmitted by the device with the packets received by the network device. *Id.* at 8:46-48. Then, “[r]esponsive to correlating,” the packet

Appendix C

correlator may “generate or update” rules used by the tap devices to identify packets coming from a specific source. *Id.* at 12:55, 13:14-18.

45. These general descriptions align with the language of the claims asserted by Centripetal. Specifically, the method outlined in claim 11 provides that the system “identify a plurality of packets *received by a network device* from a host located in a first network” and “generate a plurality of log entries corresponding to the plurality of packets received by the network device.” *Id.* at 17:10-13 (emphasis added). Similarly, the claims provide that the system “identify a plurality of packets *transmitted by the network device* to a host located in a second network” and “generate a plurality of log entries corresponding to the plurality of packets transmitted by the network device.” *Id.* at 17:14-18 (emphasis added).¹⁶ Then, “based on the plurality of log entries corresponding to the plurality of packets received by the network device and the plurality of packets transmitted by the network device,” the system is to “correlate . . . the plurality of packets transmitted by the network device with the plurality of packets received by the network device.” *Id.* at 17:19-25. Finally, “responsive to correlating,” the

16. Since the language refers to packets “received by a network device” and thereafter refers to actions taken by “*the* network device,” the claims are referring to actions taken by the same network device. See *Convolve, Inc. v. Compaq Comput. Corp.*, 812 F.3d 1313, 1321 (Fed. Cir. 2016) (construing a claim reciting “a processor” and then subsequently referencing functionality for “the processor” to require at least one processor to “perform all of the recited steps” referencing “the” processor).

Appendix C

system is to “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.” *Id.* at 17:26-35. These steps are the same for claim 21. *Id.* at 18:63-19:23.

46. In other words, the claims describe a system responsive to the obfuscation problem identified in the specification. If the network device alters the packets it receives from the computer in the first network before sending the packets to the second network “in a way that obfuscates the association” between the packets, this correlation technique can help identify the packets originating from the first network computer. *See* ’176 Patent at 5:13-20.

**The Accused Switches, Routers, and Stealthwatch
with Cognitive Threat Analytics**

47. Centripetal alleged that Cisco’s Accused Switches and Routers using Stealthwatch with Cognitive Threat Analytics infringe claims 11 and 21 of the ’176 Patent. Tr. 975:17-21, 976:16-19, 995:19-21, 1107:23-1108:10. At trial, Centripetal relied on the infringement opinion of expert witness Dr. Eric Cole and Cisco relied on the non-infringement opinion of expert witness Dr. Kevin Almeroth. Both parties also called a variety of fact witnesses.

48. The Accused Switches and Routers receive and transmit packets using processors and memory storing

Appendix C

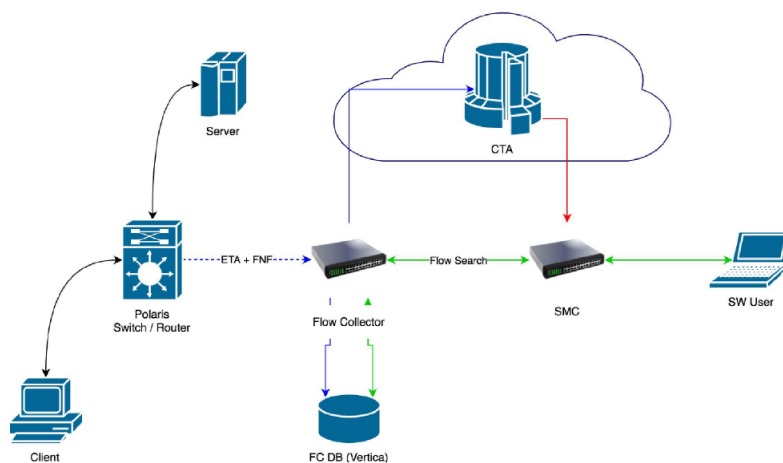
software instructions. Tr. 477:12-478:14, 484:13-485:3; PTX-1303 at 056; PTX-1313 at 018.

49. As packets transit through the Accused Switches and Routers, the devices can generate NetFlow logs. Tr. 977:18-25, 984:5-13; PTX-1060 at 008. NetFlow is a type of log that contains summaries of information about the packets flowing through the devices. Tr. 984:7-13. NetFlow records can be reported by a switch or router to track “every conversation, or flow, that passes through it. It collects a range of information about these exchanges in a flow record.” PTX-1417 at 107; *see also* PTX-1060 at 008 (“When processed, NetFlow data can tell you the important details in network transactions’ endpoints of data communication, information about when the conversation occurred, how long it lasted, and what protocols were used.”).

50. The Accused Switches and Routers are capable of exporting NetFlow when the packet enters the device (the “ingress” NetFlow record) and when the packet exits the device (the “egress” NetFlow record). Tr. 986:12-987:1; PTX-1060 at 023; Tr. 2171:23-2172:9, 2180:23-2181:3.

51. The Accused Switches and Routers can be configured to send these NetFlow logs to Stealthwatch, which analyzes traffic flow and monitors for threats. Tr. 998:3-17; PTX-1009 at 009.

52. Centripetal’s witness, Dr. Cole, used the following diagram from Cisco’s technical documentation to depict the accused system:

Appendix C

PTX-1089 at 0979.

53. The diagram shows a “Client” and a “Server” that are communicating with each other through a Cisco switch or router (shown above as the “Polaris Switch/Router”). Tr. 2189:7-18. As packets pass through the switch or router, the device exports NetFlow records to a Stealthwatch Flow Collector. Tr. 2189:19-23.

54. The Stealthwatch Flow Collector analyzes the NetFlow and sends alarms to the Stealthwatch Management Console (labeled as “SMC” above). Tr. 2147:23-2148:7, 2191:8-10. The Stealthwatch Flow Collector can also send information to Cognitive Threat Analytics (labeled as “CTA” above), which analyzes the flow information for malicious activity and can send additional alarms to the Stealthwatch Management Console. Tr. 2189:19-2190:1, 2147:7-22.

Appendix C

55. Cisco indicated that it tells its customers not to export both ingress and egress NetFlow records to Stealthwatch. *See* Tr. 2177:7-12, 2180:15-2181:3; PTX-569 at 282. Cisco engineer Daniel Llewallyn explained that Stealthwatch was built to assume the NetFlow records it ingests are ingress records. Tr. 2171:9-13, 2177:8-10, 2178:22-2179:7 (discussing PTX-569 at 282). If an Accused Switch or Router were to transmit both ingress and egress NetFlow log records to the Stealthwatch Flow Collector, the clear weight of the evidence shows that Stealthwatch does not compare these records to each other. According to Mr. Llewallyn, “[a]ny concept of ingress/egress is gone by the time [the data] gets inside the Stealthwatch flow. . . . [I]t’s just keeping up with how many bytes and packets went in [a] direction.” Tr. 2181:22-2182:4. Cisco’s technical documentation indicates that if a user enables the export of both ingress and egress NetFlow records to Stealthwatch, this “may cause the [Stealthwatch] Flow Collector to double report traffic stats.” PTX-569 at 282; *see also* Tr. 2177:8-2181:3. Additionally, the Stealthwatch Flow Collector contains code directing it to ignore duplicative egress NetFlow records. Tr. 2173:4-8, 2174:3-2175:21, 2177:15-18; DTX-1616 at 443-44, 466; Tr. 2254:11-15 (Dr. Almeroth: “[T]here’s a variable called ignore egress that attempts to ignore egress records from the same device for which there is already ingress information. And if it is unsuccessful, then it will double count those records erroneously.”).¹⁷

17. Centripetal points out that Cisco relied on an older, non-accused version of Stealthwatch source code containing the “ignore egress” code. *See* Centripetal PCL ¶ 47. However, the Court does not find this to be a persuasive basis to discredit the evidence. Mr.

Appendix C

56. Instead, the record demonstrates that the data analysis conducted by Stealthwatch involves the review of network traffic in order to detect malicious activity, by comparing NetFlow and other types of logging records (such as Syslog or WebFlow) with outside sources of data, such as threat intelligence feeds. *See, e.g.*, PTX-1065 at 005 (“Stealthwatch . . . correlates threat behaviors seen in the enterprise with those seen globally.”). According to Centripetal, “Syslog” is a “type of logging” that proxy sources can send to Stealthwatch, and “WebFlow” is “produced by Syslogs.” Centripetal PFF ¶¶ 351, 382. The Accused Switches and Routers are not proxy sources. *See* Tr. 978:11-18.

57. A human administrator can use the information (i.e., alarms) produced by this Stealthwatch analysis (by interacting with the laptop above labeled “SW User”) to generate new packet-filtering rules to better protect the network. Tr. 2190:2-4; PTX-1089 at 1239. These rules can then issued by the human administrator. Tr. 2190:5-22.

B. Conclusions of Law

Centripetal has not met its burden to establish infringement of the '176 Patent because it has failed to show by a preponderance of the evidence that Cisco's technology performs each of the limitations in the claims. Specifically, Centripetal has failed to show that (1) the

Llewallyn testified that the ignore egress source code continued to exist in the accused version of Stealthwatch and Centripetal did not present evidence suggesting otherwise. Tr. 2177:15-18; *see also* Tr. 2287:5-2288:19.

Appendix C

accused technology correlates the packets entering and exiting a network device and that (2) responsive to the correlating, the system generates rules configured to identify packets in a specific network.

Turning first to the correlation limitation, the claims require the system to correlate the “packets received by the network device” with the packets “transmitted by the network device” based on ingress and egress log entries reflecting the received/transmitted packets. ’176 Patent at 17:19-25. Centripetal argued that this claim limitation is satisfied when the Accused Switches and Routers send ingress and egress NetFlow and/or Syslog logs to Stealthwatch, which purportedly correlates the logs “to provide a detailed overview of all traffic that is occurring on the network.” Centripetal PFF ¶ 352. Centripetal also noted that “[Cognitive Threat Analytics], working within Stealthwatch, can leverage the correlations of NetFlow telemetry to detect malicious threats to the security of the network.” Centripetal PFF ¶ 352.¹⁸ Cisco disputed that Stealthwatch is capable of conducting the correlation disclosed by the claims and argued that Centripetal’s expert, Dr. Cole, “provided only conclusory statements without support in any documentary evidence, source code, or Cisco engineer testimony” in support of his correlation opinion. Cisco PFFCL ¶ 262.

The Court agrees with Cisco and finds that Centripetal has not established that the accused technology conducts

18. Centripetal’s expert, Dr. Cole, explained that NetFlow telemetry “is just another word for NetFlow log information.” Tr. 997:7-8.

Appendix C

the kind of correlation specified in the claim language. As an initial matter, it is helpful to first clarify which Cisco logs Centripetal has argued are being correlated by Stealthwatch with Cognitive Threat Analytics. In its Proposed Findings of Fact and Conclusions of Law, Centripetal suggested that the logs can either be NetFlow or other logging records such as Syslog or Webflow. *See* Centripetal PFF ¶ 352 (citing PTX-1065 at 005) (“Stealthwatch correlates NetFlow and/or Syslog information. . . .”); *id.* ¶ 365 (stating that the accused devices “will send the Netflow logs . . . to Stealthwatch, which will correlate the packet data from packets received and transmitted”); *id.* ¶ 371 (“[Cognitive Threat Analytics] uses the Netflow records that include bidirectional flow and ingress and egress data and correlates this packet data with Webflow. . . .”). Centripetal’s infringement expert, Dr. Cole, similarly noted that Syslog records could “fit the logging criteria of the patent language.” Tr. 985:5-8.

Despite these arguments, the record demonstrates that Centripetal’s infringement theory can only be understood to relate to the correlation of ingress and egress *NetFlow* records. Importantly, Dr. Cole’s infringement opinion only relied on Stealthwatch’s alleged correlation of ingress and egress NetFlow. *See, e.g.*, Tr. 993:19-999:15 (Dr. Cole’s direct examination explaining how NetFlow meets the “correlate” claim element); Tr. 1102:16-1103:4, 1106:5-8, 1108:1-5 (Dr. Cole: “[T]he important thing for me are the ingress and egress Netflow data. There’s nothing in the claim that’s exclusive to just those two, so there can be other data in there as long as those two NetFlow records are being correlated.”); Tr. 1116:23-

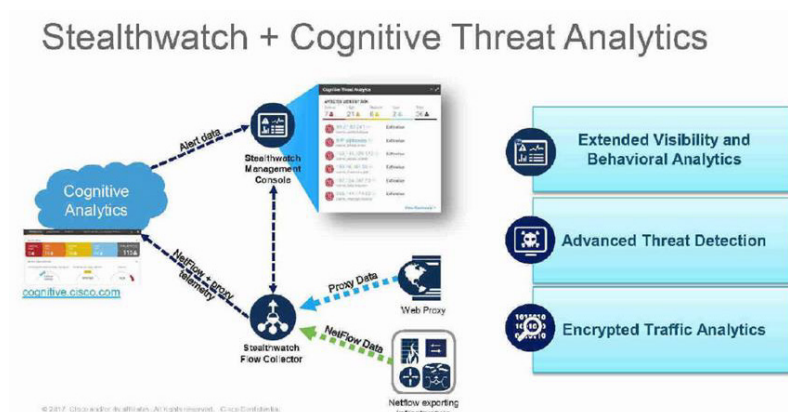
Appendix C

1117:1 (Dr. Cole: “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 NetFlows.”). Dr. Cole also noted that his infringement theory did not involve a proxy, meaning that any correlation by Stealthwatch of Syslogs or WebFlow, which Centripetal indicated are generated by proxy sources, does not support Dr. Cole’s infringement analysis. *See* Tr. 978:11-18 (“[W]ith the ’176 patent, there’s actually not a proxy in the claim language. So we don’t actually have a proxy in this case.”). And finally, Centripetal’s counsel largely conceded at the Rule 63 hearing that its infringement theory involved only the correlation of ingress and egress NetFlow records. *See* R. 63 Tr. 482:5-25 (“[T]he evidence shows that the NetFlow data—that’s what we focused on—that was infringing. . . . So if we had a different claim construction, we might look at the proxy data. We may have alternative theories. We may have [S]yslog, and we have other stuff. . . . I think the evidence shows that the NetFlow data is what we’re accusing of infringing.”). For these reasons, the Court will consider only whether the evidence shows that ingress and egress *Netflow* records are correlated by Stealthwatch with Cognitive Threat Analytics.

Dr. Cole testified that he relied on testing, a review of Cisco source code, and Cisco documents in reaching his opinion that ingress and egress NetFlow records are correlated by Stealthwatch with Cognitive Threat Analytics. Tr. 999:7-15. Despite this assertion, at trial Dr. Cole did not discuss the correlation testing or point

Appendix C

to specific pieces of source code showing correlation.¹⁹ See Tr. 993:19-999:15 (Dr. Cole’s direct testimony on the “correlate” claim element). Because of this, the Court focuses on the three Cisco documents that were discussed by Dr. Cole. First, Dr. Cole relied on a diagram that depicts NetFlow data and Proxy data being sent to the Stealthwatch Flow Collector:



PTX-1065 at 005. Below the diagram, the document also includes explanatory language noting that “Stealthwatch . . . correlates threat behaviors seen in the enterprise with those seen globally” and that the “[c]ustomer may use either NetFlow or proxy data, or both.” *Id.*

19. To be clear, Dr. Cole discussed his testing and relied on other Cisco documents in support of his opinions as to other elements of the claims, for example that the Accused Switches and Routers can be set to report both ingress and egress NetFlow records. See, e.g., 981:7-993:18 (Dr. Cole’s direct testimony on the “identify” and “generate” claim elements).

Appendix C

While this document indicates that Stealthwatch engages in correlation, it does not show the kind of correlation required by the claim language. The claim requires a correlation of “packets transmitted by the network device” with “packets received by the network device” based on the ingress and egress log entries corresponding to those sets of packets. ’176 Patent at 17:19-25. Instead, the diagram above depicts a combination of “NetFlow Data” and “Proxy Data,” and the explanatory text describes correlation of internal and external threat behaviors.

Dr. Cole opined that the document showed that Stealthwatch engages in the claimed correlation because the document states that a “[c]ustomer may use either NetFlow or proxy data or both.” Tr. 1116:6-1117:1; PTX-1065 at 005. Dr. Cole said that this indicated “customers can just use NetFlow by itself to do that correlation. It does not need to use the proxy data.” Tr. 1116:12-13. Dr. Cole’s opinion is contradicted by the evidence. As explained above, the text accompanying the diagram explains that Stealthwatch “correlates threat behaviors seen in the enterprise with those seen globally.” PTX-1065 at 005. This capability is markedly different than correlating packets entering and exiting a network device using ingress and egress NetFlow records. The document’s statement that a “[c]ustomer may use either NetFlow or proxy data or both,” considered in context, is better understood to mean that the customer may correlate external threat behaviors with NetFlow, proxy data, or both Netflow and proxy data.

Appendix C

Additionally, Dr. Cole relied on language in two different versions of Stealthwatch release notes that referenced correlation:

[Cognitive Threat Analytics] 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. According to measurements by Cisco, the number of both confirmed and detected threats should increase by approximately 10%[.]

PTX-591 at 522; *see also* PTX-1009 at 009. Dr. Cole opined that “[r]eading this entire document and all the other pieces of evidence, this is one piece, in my opinion, [that] supports that [Cognitive Threat Analytics] not only correlates the WebFlow and the NetFlow, but also the NetFlow data is also correlated among itself.” Tr. 1109:11-14; *see also* R. 63 Tr. 484:3-11. Dr. Cole did not provide any support for this opinion beyond claiming that “somebody who has read the entire document would understand that it would mean WebFlow, NetFlow and NetFlow among itself.” Tr. 1109:17-19.

Given the paucity and indefiniteness of the evidence Dr. Cole relied on, the Court gives little weight to his opinion that Stealthwatch is capable of correlating ingress and egress NetFlow records. Moreover, the Court’s conclusion is bolstered by the evidence presented by Cisco showing that the opposite is true. First, Cisco’s technical

Appendix C

documentation indicates that if a user enables the export of both ingress and egress records to Stealthwatch, this “may cause the [Stealthwatch] Flow Collector to double report traffic stats.” PTX-569 at 282. Second, if a customer were to export both, the Stealthwatch Flow Collector contains code directing it to ignore duplicative egress NetFlow records. Tr. 2173:4-8. Third, consistent with this understanding, Cisco engineer Daniel Llewallyn explained that Stealthwatch was built to assume all the NetFlow records it ingests are ingress records. Tr. 2171:9-13. And finally, Mr. Llewallyn explained that even if both ingress and egress records were collected by Stealthwatch, that distinction is lost before any correlation could occur. Tr. 2181:14-2182:15 (“Any concept of ingress/egress is gone by the time it gets inside the Stealthwatch flow. . . . [I]t’s just keeping up with how many bytes and packets went in this direction.”). For these reasons, the Court finds that Centripetal has not shown that the accused system practices the correlation limitation.²⁰

This conclusion is further supported by considering the problem that the ’176 Patent was designed to solve—

20. After Centripetal rested its infringement case, it called an invalidity expert, Dr. Trent Jaeger, who put forward a different interpretation of the ’176 Patent claim elements—specifically, that the claim language does not require ingress and egress NetFlow records to refer to the same network device because of the reference in the claim language to “one or more network devices.” Tr. 3157:16-23. This is not persuasive. Given that the claim language first refers to “a network device,” and then recites requirements of “the network device,” all of the claim requirements of “the network device” must be satisfied by a single network device to infringe. *See supra* note 16.

Appendix C

packet obfuscation by a network device. *See* '176 Patent at 5:14-20 (stating that a network device may “alter one or more aspects of the packets . . . in a way that obfuscates the association” between the packets entering the device from the packets leaving the device, “at least from the perspective of devices other than the network device[]”). Importantly, it is the *network device* doing the obfuscation, thwarting other network devices from identifying packets associated with a particular source. But in the accused Cisco system, the network device is a *Cisco device*. Cisco’s expert, Dr. Almeroth, explained that because Cisco controls the network device (i.e., the Accused Switches and Routers), Cisco is capable of seeing any changes to the packets made by it. Tr. 2297:12-2298:15. For that reason, Cisco need not rely on correlation to determine what is happening inside of the device. *See* Tr. 2297:21-24 (comparing the network device to a tunnel into which a fleeing car may travel in order to change its appearance during a period of no visibility, and explaining that in this “analogy, Cisco is the tunnel” and “[t]hey actually have someone in the tunnel watching the cars, and they can actually see when somebody jumps out of a car and gets into another”). Given this functionality, the Accused Switches and Routers do not have the problem that the '176 Patent was designed to solve.

The Court also finds that Centripetal has failed to provide sufficient evidence that the accused technology “generate[s], based on the correlating, one or more rules configured to identify packets received from the host located in the first network” or “provision[s] a device” with those rules. *See* '176 Patent at 17:29-31. Centripetal argued

Appendix C

that this claim limitation is met because Stealthwatch with Cognitive Threat Analytics generates alerts that are sent to the Stealthwatch Management Console. Tr. 1113:17-1114:6, 1001:1-7, 1002:4-1003:21, 1005:4-19, 1112:18-1113:8. This functionality, however, does not meet the claim limitation.

Specifically, Centripetal has failed to show that the accused system generates and provisions *rules* responsive to the correlating to identify packets in a specific network. While the evidence shows that the system generates alerts, these alerts are not “rules,” as the term is defined by the Court’s claim construction order. *See Markman* Order at 9 (adopting the parties’ agreed construction that a rule is “a condition or set of conditions that when satisfied cause a specific function to occur”). Centripetal’s expert, Dr. Cole, referred to the quarantine command issued by Cisco’s Identity Services Engine (discussed above in relation to the ’193 Patent) as a “rule” that could be generated by Stealthwatch. Tr. 1002:4-1003:1. However, an Identity Services Engine quarantine must be manually initiated by a human administrator. Tr. 2267:13-2268:4, 2300:21-2301:13, 2185:22-2188:5. In contrast, the claims refer to the system itself generating rules based on the correlating, not a human. ’176 Patent at 17:29-31. Further, Centripetal has not shown that the rules that would be created based on a Stealthwatch alert would have the ability to “identify packets received from the host located in the first network,” as required by the claim language. *Id.* at 17:29-31; *see also* Tr. 2265:2-22.

Appendix C

For these reasons, the Court finds that Centripetal has failed to establish both the correlation limitation and the limitation requiring generation of rules responsive to the correlating. Accordingly, the Court FINDS that Cisco's Accused Switches and Routers, using Stealthwatch with Cognitive Threat Analytics, do not literally infringe claims 11 or 21 of the '176 Patent.

C. Doctrine of Equivalents

Centripetal acknowledged that it did not present any evidence to establish infringement of the '176 Patent claims under the doctrine of equivalents. Tr. 1088:2-7 ("We did not put in evidence of doctrine of equivalents with Dr. Cole. We believe there is literal infringement on this, and doctrine of equivalents is not necessary for these patents."). The patentee bears the burden of proving equivalence. *Carroll Touch Inc. v. Electro Mech. Sys., Inc.*, 15 F.3d 1573, 1578-79 (Fed. Cir. 1993). As such, and given Centripetal's concession, the Court FINDS that Centripetal has not met its burden to establish infringement under the doctrine of equivalents.

VII. CONCLUSION

For the reasons set forth above, the Court FINDS that Centripetal has failed to prove infringement of the '193, '806, or '176 Patents by a preponderance of the evidence.²¹

21. Having found that Centripetal has failed to establish the limitations discussed above, the Court does not find it necessary to address Cisco's other arguments regarding Centripetal's alleged failure to meet the additional elements of direct and indirect infringement.

138a

Appendix C

Therefore, the Court need not reach issues related to patent validity or damages. Finding “no just reason for delay,” the Court DIRECTS the Clerk to enter partial final judgment in favor of Cisco pursuant to Rule 54(b) of the Federal Rules of Civil Procedure.

It is so ORDERED.

/s/ Elizabeth W. Hanes
Elizabeth W. Hanes
United States District Judge

Date: December 11, 2023

**APPENDIX D — OPINION OF THE UNITED STATES
COURT OF APPEALS FOR THE FEDERAL CIRCUIT,
FILED JUNE 23, 2022**

UNITED STATES COURT OF APPEALS
FOR THE FEDERAL CIRCUIT

2021-1888

CENTRIPETAL NETWORKS, INC.,

Plaintiff-Appellee,

v.

CISCO SYSTEMS, INC.,

Defendant-Appellant.

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

Decided: June 23, 2022

Before DYK, TARANTO, and CUNNINGHAM, *Circuit Judges.*

DYK, *Circuit Judge.*

Appellant Cisco Systems, Inc. (“Cisco”) appeals from the judgment of the U.S. District Court for the Eastern District of Virginia holding that Cisco willfully infringed claims 9 and 17 of U.S. Patent No. 9,203,806 (“the ’806 patent”); claims 11 and 21 of U.S. Patent No. 9,560,176

Appendix D

(“the ’176 patent”); claims 18 and 19 of U.S. Patent No. 9,686,193 (“the ’193 patent”); and claims 24 and 25 of U.S. Patent No. 9,917,856 (“the ’856 patent”). The court awarded enhanced damages and royalties exceeding \$2.75 billion to patentee-appellee Centripetal Networks, Inc. (“Centripetal”). *See Centripetal Networks, Inc. v. Cisco Sys., Inc.*, 492 F. Supp. 3d 495, 608 (E.D. Va. 2020) (“*Merits Op.*”).

Because we hold that the district court judge was disqualified from hearing the case once he became aware of his wife’s ownership of Cisco stock on August 11, 2020, *see* 28 U.S.C. § 455(b)(4), we reverse the district court’s denial of Cisco’s motion for recusal, *Centripetal Networks, Inc. v. Cisco Sys., Inc.*, 492 F. Supp. 3d 615 (E.D. Va. 2020) (“*Recusal Op.*”), vacate all orders and opinions of the court entered on or after August 11, 2020, including the final judgment, and remand for further proceedings before a different district court judge.

BACKGROUND

This case began on February 13, 2018, when Centripetal sued Cisco for infringement of ten of Centripetal’s U.S. patents in the Eastern District of Virginia.¹ The patents relate to systems that perform computer networking security functions. Cisco petitioned for *inter partes* review

1. On March 29, 2018, Centripetal filed an Amended Complaint adding infringement of claims 1-25 of the ’856 patent to its causes of action, bringing the total number of asserted patents to eleven. *See* Am. Compl. at 157 (¶ 356), ECF No. 29, Case No. 18-cv-94-HCM-LRL (E.D. Va. Mar. 29, 2018).

Appendix D

(“IPR”) of many of the asserted claims, and Centripetal subsequently narrowed the claims in the district court proceeding to those not undergoing IPR.²

The case was originally assigned to Judge Mark S. Davis. On November 6, 2018, Centripetal requested that the case be reassigned to Judge Henry C. Morgan, Jr., who had recently presided over a jury trial involving related technology and five of the same patents. That motion was granted on November 27, 2018, over Cisco’s opposition. Beginning on May 6, 2020, Judge Morgan presided over a 22-day bench trial, which included an over 3,507-page record, 26 witnesses, and over 300 exhibits. Judge Morgan heard final arguments on June 25, 2020.

While the case was still pending before him, Judge Morgan learned that his wife owned Cisco stock. He sent an email to the parties on August 12, 2020, notifying them that while preparing his 2019 financial disclosure report to the judiciary the previous day, his judicial assistant had discovered that his wife owned 100 shares of Cisco stock valued at \$4,687.99. The judge informed the parties that his wife had purchased the stock in October 2019 on the advice of her stockbroker and had “no independent recollection of approving the transaction.” *Recusal Op.*, 492 F. Supp. 3d at 617. He further explained that at the time he was informed of the existence of the stock, a “full draft of [his] opinion [on the bench trial] had been prepared” and “[v]irtually every issue was decided prior

2. The Patent Trial and Appeal Board later found the claims of six related patents, which are not the subject of these proceedings, to be unpatentable.

Appendix D

thereto.” *Id.* (citation omitted). Finally, he stated that the “shares did not and could not have influenced [his] opinion on any of the issues in th[e] case.” *Id.* (internal quotation marks and citation omitted).

The statute governing recusal of federal judges in such circumstances is 28 U.S.C. § 455. It provides, in relevant part:

- (a) Any justice, judge, or magistrate of the United States shall disqualify himself in any proceeding in which his impartiality might reasonably be questioned.
- (b) He shall also disqualify himself in the following circumstances: . . .
 - (4) 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. . .
- (c) A judge should inform himself about his personal and fiduciary financial interests, and make a reasonable effort to inform himself about the personal financial interests of his spouse and minor children residing in his household. . . .

Appendix D

- (f) Notwithstanding the [above], if any . . . judge . . . 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 . . . *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 . . . judge [or his spouse], as the case may be, *divests himself or herself of the interest that provides the grounds for the disqualification*.

28 U.S.C. § 455 (emphasis added).

Following Judge Morgan’s disclosure, Centripetal notified the court that it had no objection to the judge’s continuing to preside over the case. *Recusal Op.*, 492 F. Supp. 3d at 617-18. Cisco, on the other hand, filed a motion for miscellaneous relief nine days later (hereinafter “Motion for Recusal”), requesting Judge Morgan’s recusal under both § 455(a) and (b)(4). *Id.* at 618. Judge Morgan ordered Centripetal to file a response. Centripetal opposed the Motion for Recusal on the grounds that § 455(b)(4) was inapplicable and, even if it were applicable, the § 455(b)(4) violation could be cured by divestiture pursuant to § 455(f).

On September 9, 2020, Judge Morgan heard oral argument on the motion. At the hearing, Judge Morgan stated that at the time he learned of his wife’s ownership of the Cisco stock, he had already completed a 130-

Appendix D

page draft of his opinion, though he had not “decided 100 percent of it.” J.A. 18580. He told the parties that although he recognized “the simplest thing would be to sell the stock,” he had “already strongly indicated that [he] might be considering awarding damages in the case” by “ask[ing] for additional evidence on damages” at trial, “and that might mean that [the final] judgment would have an adverse effect upon Cisco’s stock.” J.A. 18577. Selling the stock in light of that possibility, he said, “would defeat the very purpose of the Rules,” implying concern about insider trading. *Id.*

Accordingly, Judge Morgan explained, instead of selling his wife’s stock, he had it placed in a blind trust set up solely for the Cisco stock. Under the terms of the trust, Judge Morgan was to be notified when the trust assets had been completely disposed of or when their value became less than \$1,000. *See* Appellant’s Suppl. Br. 4. There is no suggestion in the briefs or record that Judge Morgan received any such notification while the case was pending before him.

On October 2, 2020, Judge Morgan issued an opinion and order denying Cisco’s Motion for Recusal. Therein, he concluded that because “a reasonable person would not conclude that [he had known] of th[e] interest [in Cisco] and yet heard the case[,] . . . [§] 455(a) d[id] not warrant recusal.” *Recusal Op.*, 492 F. Supp. 3d at 622. As for § 455(b)(4), Judge Morgan found it did not apply in this case because he had not discovered his wife’s interest in Cisco until he had decided “virtually” every issue and “mostly drafted [the] opinion.” *Id.* at 623. Even if § 455(b)(4) did apply, Judge Morgan concluded that placing the

Appendix D

Cisco shares in a blind trust “cured” any conflict because it constituted “divestiture” under a safe harbor provided by § 455(f). *Id.* at 624.

On October 5, 2020, Judge Morgan issued a 167-page Opinion and Order containing his findings of fact and conclusions of law that Cisco willfully infringed the asserted claims of the ’856, ’176, ’193, and ’806 patents. He awarded Centripetal damages of \$755,808,545 (enhanced 2.5 times to \$1,889,521,362.50), pre-judgment interest of \$13,717,925, and “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.” *Merits Op.*, 492 F. Supp. 3d at 608.

Cisco moved for amended findings and judgment under Rule 52(b) with respect to direct infringement and damages and for a new trial under Rule 59(a)(2). *See Centripetal Networks, Inc. v. Cisco Sys., Inc.*, 526 F. Supp. 3d 137, 139-40 (E.D. Va. 2021). The court denied those motions on March 17, 2021. *Id.* at 140. Cisco timely appealed to this court, raising issues pertaining to the district court’s infringement and damages findings and also raising the question “[w]hether the district judge should have recused himself under 28 U.S.C. § 455(b).” Appellant’s Br. at 5. On March 18, 2022, we issued an order limiting the issues to be addressed at oral argument solely to the recusal issue. Following the April 4, 2022 oral argument, we granted Centripetal’s motion for leave to file supplemental briefs on the recusal issue. That briefing concluded on April 29, 2022.

Appendix D

We have jurisdiction over this matter under 28 U.S.C. § 1295(a)(1).

DISCUSSION

Cisco has waived any argument that Judge Morgan was disqualified from hearing the case under § 455(a).³ Rather, Cisco argues that Judge Morgan was required to recuse under § 455(b)(4) absent divestiture under § 455(f). We agree. Indeed, Centripetal itself does not dispute that recusal was required absent divestiture. *See* Appellee’s Resp. Br. at 60; Appellee’s Suppl. Br. at 2. There are thus two primary questions before us. The first is whether Judge Morgan was relieved of his duty to disqualify under § 455(b)(4) because his wife had “divest[ed] . . . herself of the [financial] interest [in Cisco]” pursuant to § 455(f). If we conclude that the requirements of § 455(f) were not satisfied, the second question is the proper remedy, which turns in large part on whether Judge Morgan’s failure to disqualify himself was harmless error. *See Liljeberg v. Health Servs. Acquisition Corp.*, 486 U.S. 847, 862, 108 S. Ct. 2194, 100 L. Ed. 2d 855 (1988).

We review a district court’s denial of a motion for recusal for abuse of discretion. *See United States v. Mitchell*, 886 F.2d 667, 671 (4th Cir. 1989); *see also Shell Oil Co. v. United States*, 672 F.3d 1283, 1288 (Fed. Cir. 2012) (“Consistent with the vast majority of courts to

3. Recusal under § 455(a) may be waived, but recusal under § 455(b) cannot be waived. *See* § 455(e).

Appendix D

consider this issue, we review a judge’s failure to recuse for an abuse of discretion.”⁴

I

We first address whether placement of the Cisco stock in a blind trust satisfied the statutory requirements of § 455(f). Section 455(f) stands as the only exception to the bright-line rule that a federal judge is disqualified “based on a known financial interest in a party.” *Chase Manhattan Bank v. Affiliated FM Ins. Co.*, 343 F.3d 120, 127 (2d Cir. 2003). As noted above, it provides:

Notwithstanding [§ 455(a) and (b)(4)], if any . . . judge . . . 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 . . . 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 [] judge [or his spouse], as the case may be, *divests*

4. We have indicated that recusal motions are governed by the law of the regional circuit. See *Hewlett-Packard Co. v. Bausch & Lomb Inc.*, 882 F.2d 1556, 1567 n.8 (Fed. Cir. 1989). Here, whether we apply the law of this Circuit or the Fourth Circuit, the outcome is the same. Whether applying the regional circuit law is the correct approach in light of the substantial interest in having a uniform standard on issues of recusal, with respect to the various trial-level tribunals that we review, must await another case.

Appendix D

himself or herself of the interest that provides the grounds for the disqualification.

§ 455(f) (emphasis added).

Here, there is no dispute that the Cisco stock constitutes a “financial interest” and that “substantial judicial time [had] been devoted to the matter,” such that Judge Morgan’s wife could have divested herself of that interest under § 455(f) to avoid the judge’s disqualification.⁵ What is disputed between the parties is whether her placement of the stock in a blind trust qualified as divestment.

A “blind trust” is “an arrangement whereby a person, such as a public official, in an effort to avoid conflicts of interest, places certain personal assets under the control of an independent trustee with the provision that the person is to have no knowledge of how those assets are managed.” *Blind Trust*, *Webster’s New World Dictionary* 149 (3d ed. 1988). According to Centripetal, placing the stock in the blind trust qualified as divestment.

5. Cisco does not suggest that divestiture under § 455(f) was unavailable because Judge Morgan’s wife’s interests would be “substantially affected” by the outcome.

We have no occasion to decide if divestment under § 455(f) would alleviate the need to recuse in all cases. Some courts suggest that it does not apply in all cases. *See, e.g., Union Carbide Corp. v. U.S. Cutting Serv., Inc.*, 782 F.2d 710, 715 (7th Cir. 1986) (“We do not mean to endorse sale as a cure for disqualification in all cases[;] Section 455(b) is only one node in the network of statutory and non-statutory ethical principles that control the conduct of federal judges.”).

Appendix D

Although it is well established that selling a financial interest in a company qualifies as divestment,⁶ Centripetal admits that there are no cases holding that placement of stock in a blind trust constitutes divestment. The only authority Centripetal cites for its argument that placing stock in a blind trust is a valid divestment mechanism under § 455(f) is an unsupported assertion in a law review article. *See* Appellee’s Resp. Br. at 60 (citing Marianne M. Jennings & Nim Razook, *Duck When a Conflict of Interest Blinds You: Judicial Conflicts of Interest in the Matters of Scalia and Ginsburg*, 39 U.S.F. L. Rev. 873, 904 (2005)).

In a case turning on statutory interpretation, “our first job is to try to determine congressional intent, using traditional tools of statutory construction.” *Dole v. United Steelworkers of Am.*, 494 U.S. 26, 35, 110 S. Ct. 929, 108 L. Ed. 2d 23 (1990) (quoting *NLRB v. Food & Com. Workers*, 484 U.S. 112, 123, 108 S. Ct. 413, 98 L. Ed. 2d 429 (1987)). “Our ‘starting point is the language of the statute,’” *id.* (quoting *Schreiber v. Burlington N., Inc.*, 472 U.S. 1, 5, 105 S. Ct. 2458, 86 L. Ed. 2d 1 (1985)), but we also “look to the provisions of the whole law, and its object and policy,” *id.* (quoting *Massachusetts v. Morash*, 490 U.S. 107, 115, 109 S. Ct. 1668, 104 L. Ed. 2d 98 (1989)); *see also K Mart Corp. v. Cartier, Inc.*, 486 U.S. 281, 291, 108 S. Ct. 1811, 100 L. Ed. 2d 313 (1988) (same).

6. *See, e.g., In re Certain Underwriter*, 294 F.3d 297, 300-04 (2d Cir. 2002) (finding that district court judge’s sale of stock in parties constituted divestment); *see also In re Initial Pub. Offering Sec. Litig.*, 174 F. Supp. 2d 70, 81-90 (S.D.N.Y. 2001) (tracing legislative history to support holding that a judge may continue to preside over a matter if she sells stock in a party).

Appendix D

Because § 455 does not define “divest,” we look first to the word’s “ordinary meaning . . . at the time Congress enacted the statute.” *Wis. Cent. Ltd. v. United States*, 138 S. Ct. 2067, 2070, 201 L. Ed. 2d 490 (2018) (quoting *Perrin v. United States*, 444 U.S. 37, 42, 100 S. Ct. 311, 62 L. Ed. 2d 199 (1979)); see *Mohamad v. Palestinian Auth.*, 566 U.S. 449, 454, 132 S. Ct. 1702, 182 L. Ed. 2d 720 (2012) (citing *FCC v. AT&T Inc.*, 562 U.S. 397, 403, 131 S. Ct. 1177, 179 L. Ed. 2d 132 (2011)). When Congress enacted § 455(f) in 1988, Judicial Improvements and Access to Justice Act, Pub. L. No. 100-702, 102 Stat. 4642, 4667 (1988), “divest” was ordinarily understood to mean to “dispossess or deprive,” *Divest*, 1 *Webster’s Third New International Dictionary* 663 (1986); see also *Divest*, *Webster’s New World Dictionary* 400 (3d ed. 1988) (same); *Divest*, 4 *Oxford English Dictionary* 889 (2d ed. 1988) (same). What must be “divested” under § 455(f) is “the financial interest” giving rise to the disqualification. The statute defines “financial interest” as “ownership of a legal or equitable interest, however small.” § 455(d)(4) (emphasis added). Thus, it logically follows that to “divest” oneself of “ownership” of a legal or equitable interest is possible only if one is “deprived or dispossesse[d]” of ownership—something that is possible only if the interest is sold or given away.

Also telling is Congress’s use of the present tense in § 455(b)(4), providing that a judge should not sit when he or she “has a financial interest” in a party. That verb usage suggests that selling or donating the stock is the only cure envisioned under § 455(f). But at the time of Judge Morgan’s actions, his wife still “ha[d] a financial

Appendix D

interest” in Cisco. While placing the stock in a blind trust removed her control over the stock, it did not eliminate her beneficial interest in Cisco.

There is authority suggesting that placement of stock in a blind trust does not constitute divestiture. The Judicial Conference’s Committee on Codes of Conduct has ruled, well before the events of this case, that “[a] judge’s use of a blind trust does not obviate the judge’s recusal obligations.” Advisory Op. 110, Comm. on Codes of Conduct, Jud. Conf. of the U.S. (Aug. 2013); *see also* M. Margaret McKeown, *To Judge or Not to Judge: Transparency and Recusal in the Federal System*, 30 Rev. Litig. 653, 669 n.57 (2011) (“[A] judge cannot avoid recusal by placing assets in a blind trust . . .”). We are entitled to give some weight to the committee’s views because Congress enacted § 455(b) to match Canon 3C of the Code of Judicial Conduct, which provides in relevant part that a judge “shall disqualify himself in a proceeding” where he “knows that he . . . or his spouse . . . has a financial interest . . . in a party to the proceeding,”⁷ and to ensure that statutory and ethical duties were consistent with each other, *see* H.R. Rep. No. 93-1453 (1974), *reprinted in* 1974 U.S.C.C.A.N. 6351, 6351, 6353 (amendments to § 455 were meant to “conform generally with the recently adopted canon of the Code of Judicial Conduct which relates to disqualification of judges for bias, prejudice or conflict of interest” in order to make “both the statutory and the ethical standard virtually identical”); *Liljeberg*, 486 U.S.

7. *See* Code of Judicial Conduct for United States Judges, Canon 3(C)(1)(c), *reprinted in* 69 F.R.D. 273, 277 (1975).

Appendix D

at 858 n.7 (explaining that the 1974 amendment to § 455 was “to conform with the recently adopted ABA Code of Judicial Conduct, Canon 3C”); *see also Union Carbide Corp. v. U.S. Cutting Serv., Inc.*, 782 F.2d 710, 715 (7th Cir. 1986) (“In matters of judicial ethics[,] we are bound to give some weight to the view of the committee of judges that the Judicial Conference of the United States has established to advise federal judges on ethical questions.”).

There are, moreover, two central purposes of the statute that would be undermined by defining divestment to include placement of stock in a blind trust. First, unless the trustee immediately sold the stock interest upon creation of the blind trust (which did not occur here), the blind trust would allow a judge to continue to sit on a case for which he knows he or his spouse has a beneficial interest in the outcome, in direct contravention of the statute’s purpose. *See Chase*, 343 F.3d at 128 (“Congress has . . . provided that a known financial interest in a party, no matter how small, is a disqualifying conflict of interest and one that cannot even be waived by the parties.”). The significance of this factor is apparent in how the Executive Branch handles corresponding rules governing recusal of executive branch officials who have a “financial interest” in a particular government action. *See* 18 U.S.C. § 208(a). A regulation interpreting § 208 “and other Federal conflict of interest statutes and regulations” provides that recusal rules continue to “apply to the assets that an interested party transfers to [a blind] trust until such time as he or she is notified by the independent trustee that such asset has been disposed of or has a value of less than \$1,000.”

Appendix D

5 C.F.R. § 2634.403(a)(2).⁸ The reason for this requirement, the regulation provides, is that until the interest is disposed of, “the interested party knows what assets he or she placed in the trust” and therefore, “the possibility still exists that the interested party could be influenced in the performance of official duties by those interests.” *Id.*

Second, even if the trustee had sold the stock at the time the blind trust was created, the exception provided under § 455(f) is nevertheless a narrow one, and construing “divest” to include placement of stock in a blind trust would be in direct conflict with another provision of the statute. Section 455(c) provides that “[a] judge should inform himself about his personal and fiduciary financial interests, and make a reasonable effort to inform himself about the personal financial interests of his spouse and minor children residing in his household.” This was exactly the Judicial Conference Committee’s concern in Advisory Opinion 110. It explained that “[t]he Committee has consistently advised that the use of a blind trust would be incompatible with a judge’s duty to ‘keep informed’ about financial interests under Canon 3C(2),” after which § 455(c) is modeled. Advisory Op. 110. That logic makes sense here, since there would have been no way for Judge Morgan to keep informed of his personal financial interests (and thus comply with his obligations

8. The \$1,000 limit for the executive branch is not applicable to judges. Any interest, “however small,” is disqualifying. *In re Va. Elec. & Power Co.*, 539 F.2d 357, 368 (4th Cir. 1976) (“If a judge has an ownership interest in a party or in the subject matter in controversy, it matters not at all whether the interest is a large or infinitesimally small amount.”).

Appendix D

under § 455(c)), if his or his wife's stock were kept in a blind trust, which is, by definition, designed to shield him from such knowledge.⁹

* * *

In light of the foregoing, we hold that placing assets in a blind trust is not divestment under § 455(f), and Judge Morgan was disqualified from further proceedings in the case under § 455(b)(4).

II

We next consider the appropriate remedy. “Although § 455 defines the circumstances that mandate disqualification of federal judges, it neither prescribes nor prohibits any particular remedy for a violation of that duty.” *Liljeberg*, 486 U.S. at 862. Here, the question is whether the rulings Judge Morgan made after August 11, 2020, when he became aware of his wife's financial interest in Cisco, should be vacated as a remedy for his failure to recuse.

9. Although Judge Morgan suggested there would be an appearance of insider trading if he sold the stock, no such possibility exists. Selling the stock to comply with ethical obligations is not insider trading, as was made clear in the Stop Trading on Congressional Knowledge Act of 2012 (“STOCK Act”), Pub. L. 112-105, 126 Stat. 291, 298 (2012). Although the STOCK Act provides that the insider trading restrictions of securities law apply to judicial employees (as well as to members of Congress and other federal officials), it states that nothing in the Act shall be construed to “be in derogation of existing . . . ethical obligations governing . . . judicial officers.” *Id.* at 297-98 Here, the sale of the stock would have been done to comply with ethical obligations.

Appendix D

As we explained in *Shell*, to determine whether vacatur is the appropriate remedy for a violation of § 455(b), we apply the harmless error analysis set forth by the Supreme Court in *Liljeberg*. Under that test, “mandatory recusal does not require mandatory vacatur.” *Shell*, 672 F.3d at 1293; *see also Williamson v. Ind. Univ.*, 345 F.3d 459, 464-65 (7th Cir. 2003) (finding vacatur “is not automatically justified” for a violation of § 455 “if [the] error was harmless”). Although *Liljeberg* involved a violation of § 455(a), it is now well-recognized that the harmless error analysis applies equally to violations of § 455(b). *See Shell*, 672 F.3d at 1292; *Polaroid Corp. v. Eastman Kodak Co.*, 867 F.2d 1415, 1421 (Fed. Cir. 1989); *see also Patterson v. Mobil Oil Corp.*, 335 F.3d 476, 485 (5th Cir. 2003) (“[W]e are confident that § 455(b) violations are also subject to the doctrine of harmless error.”).¹⁰

Under *Liljeberg*, there are three factors courts should consider when deciding whether to vacate a judgment: (1) “the risk of injustice to the parties in the particular case”; (2) “the risk that the denial of relief will produce injustice in other cases”; and (3) “the risk of undermining the public’s confidence in the judicial process.” 486 U.S.

10. Another distinction is that *Liljeberg* involved a Rule 60(b) motion, whereas this case involves a motion for recusal. This court and others have held that the same analysis generally applies to motions for recusal and Rule 60(b) motions. *See Polaroid Corp. v. Eastman Kodak Co.*, 867 F.2d 1415, 1421 (Fed. Cir. 1989); *In re Sch. Asbestos Litig. v. Kelly*, 977 F.2d 764, 785 (3d Cir. 1992). However, in the Rule 60(b) context, the interests of finality must be given due weight. *See Buck v. Davis*, 580 U.S. 100, 137 S. Ct. 759, 779, 197 L. Ed. 2d 1 (2017) (citing *Gonzalez v. Crosby*, 545 U.S. 524, 529, 125 S. Ct. 2641, 162 L. Ed. 2d 480 (2005)).

Appendix D

at 864. Each of these factors weighs against a finding of harmless error in this case.

A

1

There are several circumstances in which courts have found the first *Liljeberg* factor—“the risk of injustice to the parties in the particular case”—weighs in favor of finding harmless error for violations of § 455. None is present in this case.

The first is where the ruling involves a pure question of law that is subject to plenary review on appeal, a posture that some courts in some circumstances have found relevant.¹¹ That is not what we have here. The rulings at

11. See *United States v. Cerceda*, 172 F.3d 806, 813 n.10 (11th Cir. 1999) (en banc) (“In cases where the Court of Appeals reviews a district judge’s challenged actions and affirms them on the merits either before or at the same time it considers whether the judge violated section 455(a), the possibility of a significant risk of injustice is substantially reduced—particularly if the review of the merits was plenary.”); see also *Williamson*, 345 F.3d at 464-65 (“On appeal, this court reviews the grant of summary judgment *de novo* . . . and therefore Williamson has received a full review by an impartial panel.”); *Patterson*, 335 F.3d at 485 (“Because we review a summary judgment ruling *de novo*, using the same standards as the district court, the parties are guaranteed a fair, impartial review of the merits of the ruling.”); *In re Sch. Asbestos Litig.*, 977 F.2d at 787 (finding no “serious injustice to the parties in th[e] case” pre-trial where summary judgment rulings were subject to plenary review upon final judgment); *Parker v. Connors Steel Co.*, 855 F.2d

Appendix D

issue in this case resulted from a bench trial in which Judge Morgan exercised broad discretion in making findings of fact and credibility determinations. Indeed, Centripetal relies heavily on Judge Morgan’s “broad discretion” in arguing for affirmance of the judgment. Appellee’s Resp. Br. at 51 (quoting *Conoco, Inc. v. Energy & Env’t Int’l, L.C.*, 460 F.3d 1349, 1362-63 (Fed. Cir. 2006)); *see also, e.g., id.* at 50 (“After weighing the evidence, the court found Dr. Striegel credible and accepted his analysis.”); *id.* at 51 (citing *Endo Pharms. Inc. v. Actavis LLC*, 922 F.3d 1365, 1374 n.10 (Fed. Cir. 2019) (explaining credibility findings are not disturbed on appeal)); *id.* at 59 (stressing that “the court ‘made detailed factual findings’ as to why the close call factor supported enhancement, including the impact of its credibility determinations”).

The second circumstance is where the opposing party has delayed raising a known ground for recusal.

1510, 1526 (11th Cir. 1999) (concluding that judge’s potential bias presented no risk of injustice to party seeking vacatur because court exercised plenary review over merits in same appeal and concluded that district judge’s grant of summary judgment was proper); *In re Continental Airlines Corp.*, 901 F.2d 1259, 1263 (5th Cir. 1990) (“The risk of injustice to the parties in allowing a summary judgment ruling to stand is usually slight,” as “[s]uch rulings are subject to de novo review.”). *But see Shell*, 672 F.3d at 1294 (“[A] judge’s failure to recuse does not automatically constitute harmless error whenever there is *de novo* review on appeal.”); *see also Ward v. Village of Monroeville*, 409 U.S. 57, 61, 93 S. Ct. 80, 34 L. Ed. 2d 267 (1972) (rejecting the notion, in the context of state law proceeding where judge had a financial interest in the outcome, that “any unfairness at the trial level [could] be corrected on appeal and trial de novo in the County Court of Common Pleas”).

Appendix D

See, e.g., In re United Shoe Mach. Corp., 276 F.2d 77, 79 (1st Cir. 1960) (“[K]nowing of a ground for requesting disqualification, [a party] can not be permitted to wait and decide whether he likes subsequent treatment that he receives.”); *Ogala Sioux Tribe v. Homestake Mining Co.*, 722 F.2d 1407, 1414 (8th Cir. 1983) (denying relief in part because alleged grounds for disqualification were known at the time the case was decided by the trial judge but not raised until the case was on appeal); *In re IBM Corp.*, 618 F.2d 923, 932 (2d Cir. 1980) (adopting timeliness requirement for § 455); *see also Liljeberg*, 486 U.S. at 868 (“It is [] appropriate to vacate the judgment unless it can be said that respondent did not make a timely request for relief . . .”).

In *Polaroid*, we affirmed the district court’s denial of a motion for disqualification and vacatur made six-and-a-half years after the judge’s decision and disclosure that her mother-in-law held stock in one of the parties. 867 F.2d at 1416-17. In denying vacatur, we noted that “[t]he passage of time” is a factor in the “equity/fairness equation,” *id.* at 1418-20, and we considered all that the judge who denied the motion had to say about “Kodak’s acquiescence, aging of witnesses, fading of memories, and the unfairness of vacating . . . [the] orders and requiring Polaroid to start all over,” *id.* at 1420.

Here, there has been no such delay. Cisco moved for Judge Morgan’s recusal just nine days after he disclosed his wife’s ownership of Cisco stock.

The third circumstance where courts have declined vacatur is where substantial time has passed since the

Appendix D

rulings in question (even though there has been no delay in making the motion when the facts became known). In this respect, Centripetal relies on the Eleventh Circuit’s en banc decision in *United States v. Cerceda*, 172 F.3d 806 (11th Cir. 1999) (en banc). But in that case, which dealt with the possible re-trial of multiple criminal defendants, it had been six years since one of the trials, and one of the key witnesses—who had been 84 years old and in poor health at the time of the first trial—would have been over 90 years old at the time of a new trial. *Id.* at 815. Centripetal has made no comparable showing in this case. Beyond a conclusory assertion in its supplemental brief that “evidence ha[s] gone stale,” Appellee’s Suppl. Br. at 6, Centripetal has not made any actual showing of staleness of evidence or fading of witness’ memories in the time since the trial was held two years ago.¹²

Even if it had, any prejudice caused by the passage of time may be tempered by the fact that, as discussed in further detail below, this case would proceed under Federal Rule of Civil Procedure 63 on remand. Under that rule, a newly assigned judge has the ability to resolve the case based on the transcript from the previous trial. 11 Charles Alan Wright & Arthur R. Miller, *Federal Practice & Procedure* § 2922 n.19 (3d ed. 2022) (collecting cases).¹³

12. Moreover, we question whether the relevant date for staleness is the date the judge declined to recuse or the date of the decision on appeal. If the former is the relevant date, the lack of prejudice is even clearer here.

13. The replacement judge may recall any witness, and must do so at the request of a party if the testimony is “material and disputed” and the witness is available to testify again without undue

Appendix D

The fourth circumstance where courts have refused vacatur for a violation of § 455(b) is where one party has “made a showing of special hardship by reason of their reliance on the original judgment.” *Liljeberg*, 486 U.S. at 869. There has been no such showing in this case.

2

Unable to bring this case under existing authorities, Centripetal nonetheless makes several arguments as to why the first *Liljeberg* factor weighs against vacatur. It argues that there is no risk of injustice to Cisco because Judge Morgan had “decided the case” prior to learning of his wife’s ownership of Cisco stock, and therefore the judgment should stand since it was decided at a time when there was no § 455(b)(4) violation. Appellee’s Resp. Br. at 63 (citing J.A. 30). But that is not a fair characterization of the facts. At the September 9, 2020 hearing on Cisco’s motion for recusal, Judge Morgan stated that at the time he learned of his wife’s financial interest in Cisco, he had drafted “130-some pages” of the opinion. J.A. 18580. But the opinion issued on October 5, 2020 was 167 pages, showing that the judge went on to draft an additional 37 pages after learning of the stock ownership. And although

burden. Fed. R. Civ. P. 63. “If, on the other hand, there are issues of credibility that cannot properly be resolved on the basis of the record or for any other reason the replacement judge concludes that it is not possible to proceed in fairness to the parties, the judge has discretion to grant a new trial.” 11 Wright & Miller, *Federal Practice & Procedure* § 2922 (providing cases). “If a new trial is granted, the record of the previous trial may be used as a substitute for testimony of unavailable witnesses.” *Id.*

Appendix D

at that same hearing he stated that his views as to the appropriate resolution of the case were fixed, he admitted that he had not “decided 100 percent of it.” *Id.* In any event, until an opinion is issued, it is well within a judge’s prerogative to change his mind or to otherwise revise the decision. Here, the opinion was subject to revision until the time it issued.

Moreover, after learning of his wife’s stock ownership, Judge Morgan continued to sit on post-trial motions that needed to be decided but had not even been briefed by the parties. Cisco’s post-trial motions were rejected in a 49-page opinion and order issued on March 17, 2021, while Judge Morgan knew his wife continued to hold stock in Cisco.¹⁴

Centripetal next argues that there is no risk of injustice to Cisco because there is no evidence of actual bias, relying on a case applying § 455(a) (requiring recusal where there is an appearance of impropriety) in which the court declined to vacate orders, at least in part, because there was no evidence of actual bias.¹⁵ *See* Appellee’s Suppl. Br. at 8 (citing *In re Sch. Asbestos Litig. v. Kelly*, 977 F.2d 764, 785-87 (3d Cir. 1992) (declining to vacate

14. *See United States v. O’Keefe*, 128 F.3d 885, 891 (5th Cir. 1997) (“Once a judge recuses himself from a case, the judge may take no action other than the ministerial acts necessary to transfer the case to another judge.”); *see also Shell*, 672 F.3d at 1291 (citing *O’Keefe*, 128 F.3d at 891).

15. On this point, Centripetal oddly relies on Cisco’s waiver of any violation of § 455(a) as somehow an admission that Judge Morgan held no actual bias. There was no such admission.

Appendix D

orders en masse where there was, among other things, no “likelihood of actual bias”). Section 455(b)(4) is different. Unlike § 455(a), it is not triggered by an appearance of impropriety, but by a known financial interest, which creates not only an appearance of impropriety but impropriety itself. We have previously ordered vacatur under § 455(b)(4) notwithstanding “that there [wa]s neither an allegation nor suggestion that the judge was unduly influenced by his wife’s financial interest.” *Shell*, 672 F.3d at 1291.

The objective of the statute—public confidence in the judiciary—would be severely undermined by requiring a showing of actual bias in order to vacate orders infected with a § 455(b)(4) violation. Making such a bias determination would require the sort of line drawing that the statute was designed to avoid.¹⁶ We note that in the closely related context of orders rendered by judges with a “direct, personal, substantial [and] pecuniary” interest in reaching a certain outcome in a case, the Supreme Court has rejected the notion that a showing of actual bias is required for a due process violation. *Ward v. Village of Monroeville*, 409 U.S. 57, 60, 93 S. Ct. 80, 34 L. Ed. 2d

16. The reason § 455(b)(4) establishes a bright-line rule and does not require a showing of prejudice is because of the great difficulty in establishing actual prejudice in any particular case. *See Chase*, 343 F.3d at 128 (“[A] bright-line test . . . avoids many difficult line-drawing decisions and is in that sense actually helpful to judges.”); *see also* H.R. Rep. No. 93-1453, *reprinted in* 1974 U.S.C.C.A.N. 6351, 6358 (1974) (observing that without a bright-line rule, a judge would be left to “decide the disqualification issue at his peril, with the possibility that if he decided to sit he may be subject to criticism or that public confidence in the federal judicial system may be weakened”).

Appendix D

267 (1972); *see also id.* at 61 (finding that if a state statute governing the disqualification of interested, biased, or prejudiced judges required “that an accused [person] must show [actual prejudice] in his particular case, the statute requires too much and protects too little”); *Aetna Life Ins. Co. v. Lavoie*, 475 U.S. 813, 825, 106 S. Ct. 1580, 89 L. Ed. 2d 823 (1986) (“The Due Process Clause ‘may sometimes bar trial by judges who have no actual bias and who would do their very best to weigh the scales of justice equally between contending parties. But to perform its high function in the best way, justice must satisfy the appearance of justice.’” (quoting *In re Murchison*, 349 U.S. 133, 136, 75 S. Ct. 623, 99 L. Ed. 942 (1955))).

Centripetal also relies on the time and cost of the litigation thus far, the complexity of the case, and the delay in obtaining judgment, as weighing against vacatur. But Centripetal cites no case where these considerations alone led to a finding of harmless error, and we do not think that those factors here significantly weigh against vacatur. These considerations would exist in every case where a ground for recusal arises after significant trial proceedings.

Finally, to the extent that Centripetal argues that there is no need to vacate Judge Morgan’s rulings because his wife owned stock in the losing party (and his interests would be adversely affected, not benefited, by his decision), *see Appellee’s Resp. Br.* at 63, that fact does not remove the risk of prejudice. Where a judge becomes aware of a possible appearance of impropriety, there is a substantial risk that he or she might bend over backwards to rule

Appendix D

against that party to try to prove that there is no bias. See *In re Sch. Asbestos Litig.*, 977 F.2d at 782 (“[B]ias c[an] manifest itself in a number of ways.”). Congress did not make recusal obligations contingent on which party’s stock was owned, and we are aware of no case suggesting that this is a relevant factor.

Accordingly, considering all relevant factors, we find that the risk of injustice to the parties weighs against a finding of harmless error and in favor of vacatur.

B

The second *Liljeberg* factor also weighs against finding harmless error and in favor of vacatur. In *Liljeberg*, the Supreme Court indicated that a relevant consideration is whether granting or denying vacatur “w[ould] [] produce injustice in other cases.” 486 U.S. at 868. The Court indicated that this factor weighs in favor of vacatur when it “may prevent a substantive injustice in some future case by encouraging a judge or litigant to more carefully examine possible grounds for disqualification and to promptly disclose them when discovered.” *Id.*

Centripetal argues that the refusal to vacate here would have no effect in other cases because the facts of this case are unusual, see Appellee’s Suppl. Br. at 9 (“Rarely will a judge discover a financial interest in a party months after an extensive bench trial, after the judge already invested years of resources and time, and after the judge decided to rule against that party and nearly completed his trial opinion in the case, but before finalizing and

Appendix D

publishing that opinion.” (emphasis omitted)), and because the denial of Cisco’s Motion for Recusal “rest[ed] on the specific facts of this case,” Appellee’s Resp. Br. at 63 (quoting *Polaroid*, 867 F.2d at 1420). We disagree. Refusal to vacate here would have a significant adverse effect in other cases. While the specific facts of this case may be unique, they are symptomatic of an increasingly common problem, as discussed in the next section. A vacatur here would signal to judges in other cases the importance of complying strictly with the procedures spelled out in § 455(f). A failure to vacate would suggest that sitting on a case in which the judge’s family has a financial interest is not a serious issue.

We find the second factor weighs in favor of vacatur.

C

Finally, and perhaps most significantly, the denial of vacatur here risks “undermining the public’s confidence in the judicial process.” *Liljeberg*, 486 U.S. at 864. Centripetal argues that “[v]acating under the unusual facts of this case” would cause the public to “lose confidence in the finality of judgments.” Appellee’s Suppl. Br. at 10-11. Quite the contrary. The failure to vacate here would strike at the heart of what the statute was designed to protect. The Supreme Court in *Liljeberg* explained that the purpose of § 455 is to “promote public confidence in the integrity of the judicial process.” 486 U.S. at 860; *see also Davis v. Xerox*, 811 F.2d 1293, 1296 (9th Cir. 1987) (noting that “Congress was willing to accept disruptions” that may be caused by remedying violations of § 455 “in return for

Appendix D

the perceived benefits of promoting public confidence in the judiciary”). It is seriously inimical to the credibility of the judiciary for a judge to preside over a case in which he has a known financial interest in one of the parties and for courts to allow those rulings to stand.

This assessment is confirmed by responses to the recent reports of many federal judges presiding over cases in which they or relevant family members owned stock in a party. *See* James V. Grimaldi et al., *131 Federal Judges Broke the Law by Hearing Cases Where They Had a Financial Interest*, Wall St. J. (Sept. 28, 2021). Congress responded by recently enacting the Courthouse Ethics and Transparency Act, Pub. L. No. 117-125, 136 Stat 1205 (2022), which requires judges to make more timely and accessible disclosures of their financial holdings and potential conflicts of interest. *See also* 168 Cong. Rec. H4522 (daily ed. Apr. 27, 2022) (statement of Rep. Hakeem Jeffries) (“Failure to recuse can cause real harm to parties seeking fair and impartial justice and leave a cloud of doubt over any decision that is made once the conflicts are subsequently uncovered.”). Chief Justice Roberts similarly responded by devoting a substantial portion of his 2021 Year-End Report on the Federal Judiciary to discussing the importance of judges complying with their ethical obligations. Chief Justice John G. Roberts, Jr., 2021 Year-End Report on the Federal Judiciary, 3.

It simply cannot plausibly be argued that public confidence in the judiciary will be degraded by a decision that vacates a judge’s rulings rendered while he had a known financial interest in one of the parties. Rather, in

Appendix D

the circumstances here, vacatur is essential to preserve public confidence.

* * *

We therefore conclude that the *Liljeberg* factors weigh against finding harmless error in this case. We note that in cases involving recusal under § 455(b)(4), few circuit decisions have declined to vacate a prior ruling made while the judge was aware of the disqualifying interest and failed to divest. Still rarer are decisions declining to vacate substantive rulings in such circumstances. We think it should be a very unusual case where vacatur is denied when a judge discovers a clear disqualifying interest under § 455(b)(4), recusal is required, there is a failure to divest, and the judge proceeds to rule on the case despite that clear obligation.

III

Because we find Judge Morgan's violation of § 455(b)(4) was not harmless error, vacatur is the appropriate remedy. *See Shell*, 672 F.3d at 1293. Because § 455(b)(4) requires "actual knowledge" of disqualifying circumstances, *Chase*, 343 F.3d at 127, the only rulings subject to vacatur are those issued after Judge Morgan learned of his wife's financial interest in Cisco, on August 11, 2020. Those rulings are the Opinion & Order denying Cisco's Motion for Miscellaneous Relief (i.e., Motion for Recusal), ECF No. 619 (Oct. 2, 2020); the Opinion & Order re Infringement and Damages, ECF No. 621 (Oct. 5, 2020); and the Opinion & Order Denying Post-Judgment Motions & Declaring the Case Final, ECF No. 638 (Mar. 17, 2021).

Appendix D

Centripetal argues that reassignment to a new judge is not necessary if we vacate and remand. Allowing the same judge to reaffirm his own rulings would severely undermine § 455, which is why cases are routinely reassigned upon vacatur of judgment under § 455. *See, e.g., Shell*, 672 F.3d at 1294. In any event, that argument is moot in light of the unfortunate death of Judge Morgan on May 1, 2022, of which we take judicial notice.¹⁷ Accordingly, upon remand the case will be assigned to a new judge in the normal course, pursuant to Rule 63, which allows a replacement judge “if a judge conducting a hearing or trial is unable to proceed.” Fed. R. Civ. P. 63.

CONCLUSION

For the foregoing reasons, we reverse the Opinion & Order denying Cisco’s Motion for Miscellaneous Relief (ECF No. 619), *see Recusal Op.*, 492 F. Supp. 3d 615, we vacate the Opinion & Order re Infringement and Damages (ECF No. 621), *see Merits Op.*, 492 F. Supp. 3d 495, and the Opinion & Order Denying Post-Judgment Motions & Declaring the Case Final (ECF No. 638), and remand for further proceedings before a newly appointed judge, who shall decide the case without regard for the vacated opinions and orders.

17. *See* Obituary, *Judge Henry Coke Morgan Jr.*, *Virginian-Pilot* (May 8, 2022), available at <https://www.legacy.com/us/obituaries/pilotonline/name/henry-morgan-obituary?id=34660901>.

169a

Appendix D

**REVERSED IN PART, VACATED IN PART, AND
REMANDED**

COSTS

Costs to Appellant.

170a

**APPENDIX E — OPINION AND ORDER OF THE
UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA, NORFOLK
DIVISION, FILED OCTOBER 5, 2020**

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
NORFOLK DIVISION

Civil Action No. 2:18cv94

CENTRIPETAL NETWORKS, INC.,

Plaintiff,

v.

CISCO SYSTEMS, INC.,

Defendant.

Filed 10/05/2020

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.

*Appendix E***I. PROCEDURAL POSTURE¹**

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.

3. On March 29, 2018, Centripetal filed an Amended Complaint, asserting infringement of U.S. Patent Nos. 9,560,077 (“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.

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

Appendix E

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.

*Appendix E***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:

Appendix E

- 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

Appendix E

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;

Appendix E

- 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;

Appendix E

- 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.

Appendix E

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;

Appendix E

- 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

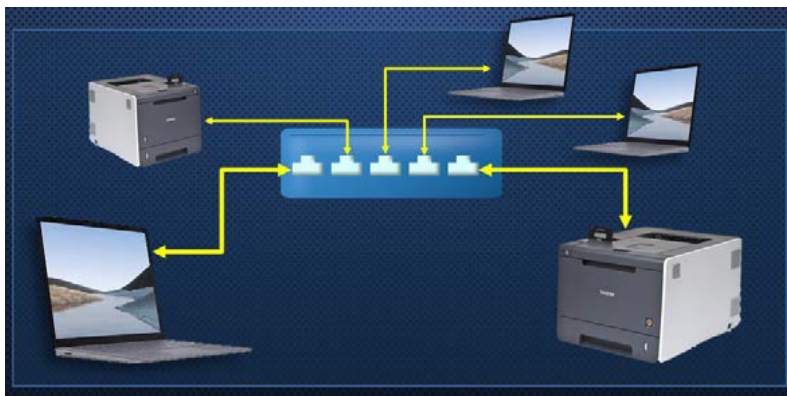
The asserted patents in this case deal with systems that engage in complex computer networking security functions. Accordingly, the Court heard detailed technological testimony regarding the structure and function of computer networks in general, as well as the specific processes employed to secure these 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.

Appendix E

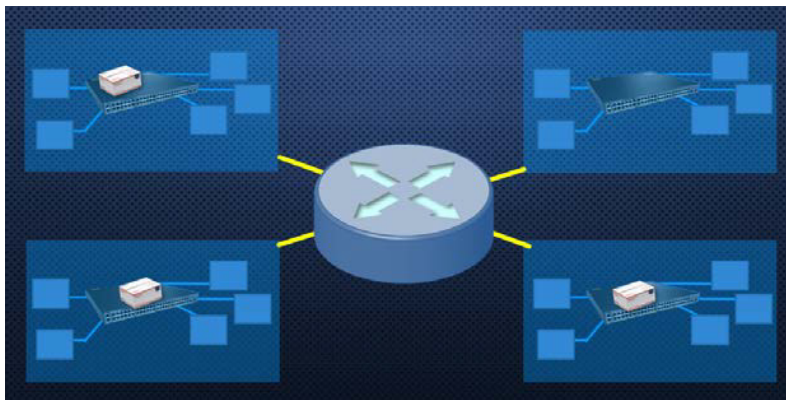
Medvidovic used analogies to explain these complex network devices. He compared the operation of a switch to that of a telephone switchboard operator. Tr. 20:13-22. Therefore, similar to an operator connecting people, switches in a network operate to automatically connect different devices together such as a computer with another computer or a computer to a printer. Tr. 20:24-21:2; *see* Fig. 1.

FIG. 1

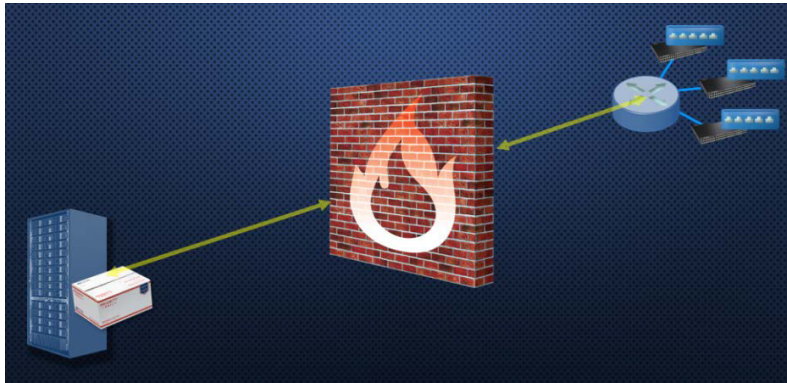
Comparatively, routers function similarly to a 911 dispatcher who sends and controls the distribution of emergency vehicles to the intended location. Tr. 22:9-19. Routers decide the most optimal way to automatically send computing data to a desired location. Tr. 22:24-23:2. They are constantly evaluating 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

Appendix E

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.

Appendix E

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.

*Appendix E***FIG. 4**

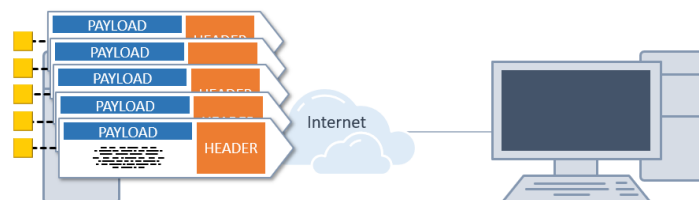
The international nature of the internet requires that the sending of data between all of these providers be based on uniformly developed standards that are globally applicable. Tr. 77:5-17. One such organization, the Internet Engineering Task Force (“IETF”) is responsible for developing universal internet 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.

Appendix E

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.

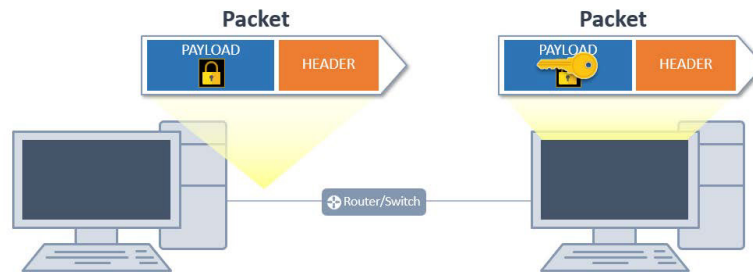
Packets consist of two different parts: the header and the payload; *see* Fig. 5.

FIG. 5

Appendix E

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

Appendix E

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

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.

Appendix E

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 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

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

Appendix E

(“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 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

Appendix E

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.

*Appendix E***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.

Appendix E

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

*Appendix E**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.

Appendix E

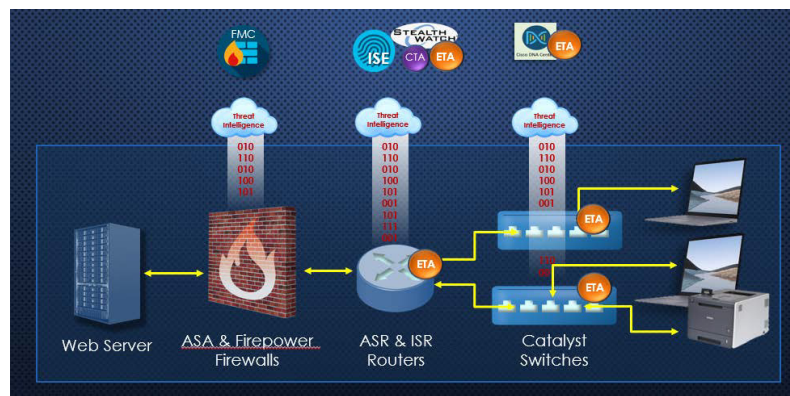
ix. Firepower Management Center

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)



*Appendix E***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.

Appendix E

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,

Appendix E

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.

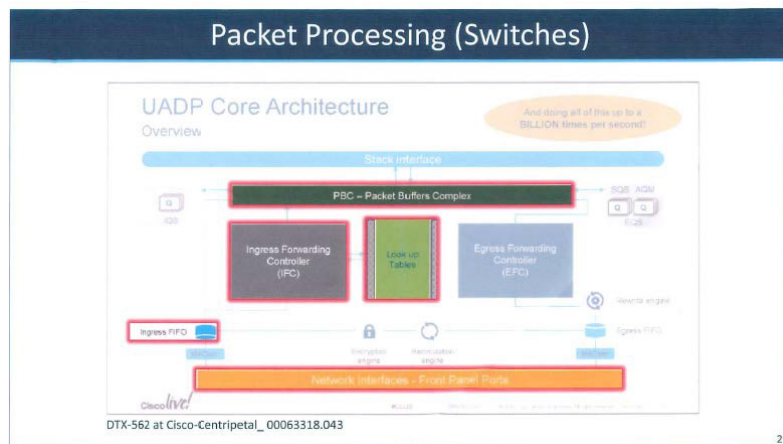
199a

Appendix E

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



Appendix E

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.

Appendix E

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.

Appendix E

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

Appendix E

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?

Appendix E

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 through 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.

Appendix E

Q. Okay. And what happens when the new rule set, rule set 2, has been configured and it's ready for use?

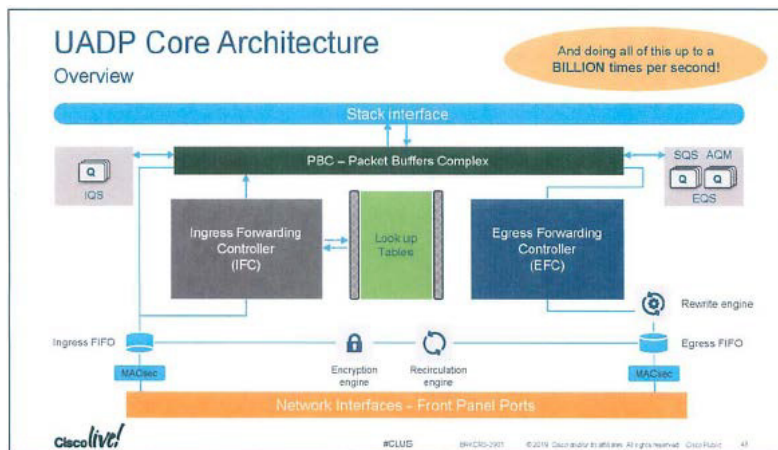
A. At that point, we continue processing the packets as in the normal course of action, and the only difference is that when the packet is now being processed against the rule set, the pointer that was pointing to the old rule set now points to the new rule set, and the packet will be processed for the 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 is 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:

206a

Appendix E

DTX-562

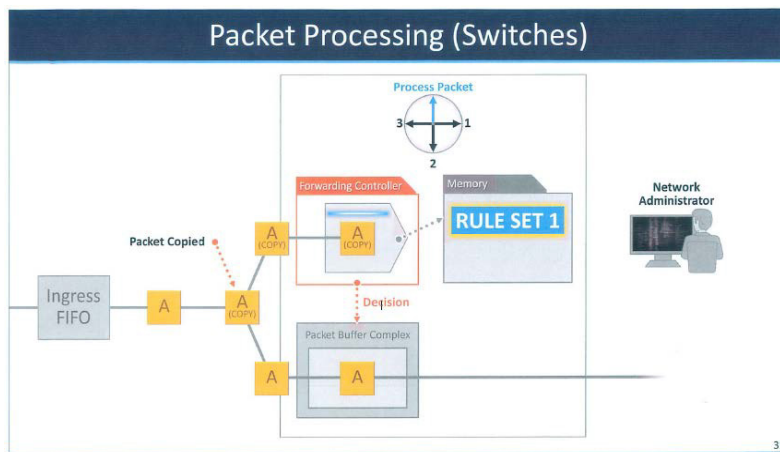


In this diagram, there is a full picture of a packet's process through a switch or router without any highlighting limitation only on ingress. Therefore, Mr. Jones provided a complete picture of how rules are applied within the accused products on both ingress and egress. To support his opinions, Mr. 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:

207a

Appendix E

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

Appendix E

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.

Appendix E

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,

Appendix E

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 media⁴ 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-

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.

Appendix E

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.

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

Appendix E

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:

Appendix E

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

Appendix E

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

Appendix E

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,

Appendix E

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.

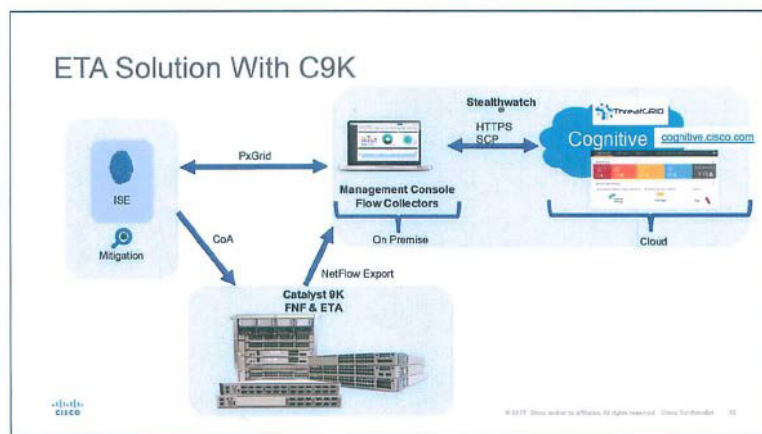
24. This process is shown by a Cisco technical demonstration of ETA provided in February of 2018. PTX-989. The title page and relevant page are shown below:

217a

Appendix E

PTX-989

**Cisco Encrypted Traffic Analytics Technical
Presentation from February of 2018**



Appendix E

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

Appendix E

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.

Appendix E

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.

Appendix E

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)).

Appendix E

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, 117 S.Ct. 1040, 137 L.Ed.2d 146 (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:

Appendix E

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.

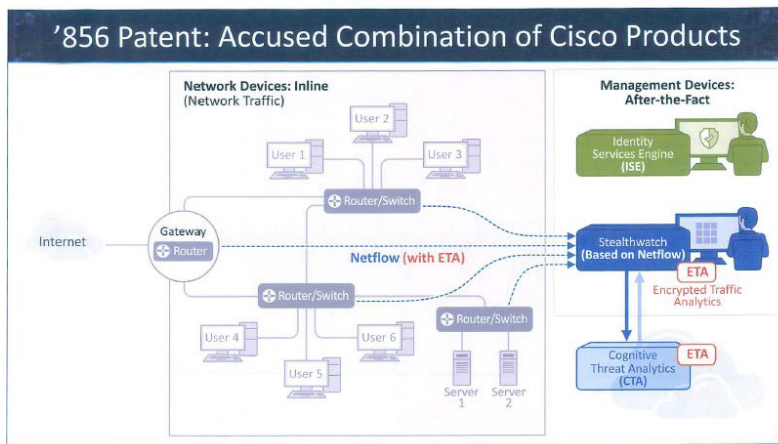
Tr. 1817:13-23. Dr. Schmidt opined that the '856 Patent is not-infringed on three different theories, First, Dr. Schmidt concludes that the current Cisco system is exclusively after the fact analysis and does not work on determined packets as required by the claims. Second, he states that the null interface 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:

224a

Appendix E

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.

Appendix E

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

Appendix E

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

Appendix E

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

Appendix E

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**

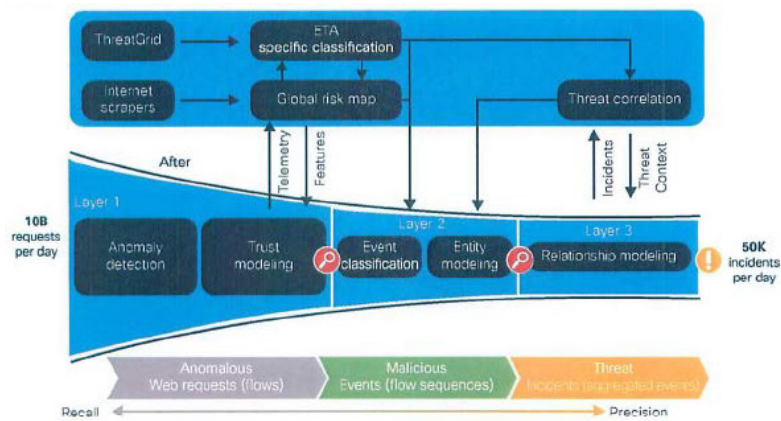
Cisco Stealthwatch uses NetFlow, proxy servers, endpoint telemetry, policy and access engines, and traffic segmentation as well as behavioral modeling and machine learning to establish baseline “normal” behavior for hosts and users across the enterprise. Stealthwatch can correlate traffic with global 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.

229a

Appendix E

Figure 3. Stealthwatch multi-layer machine learning

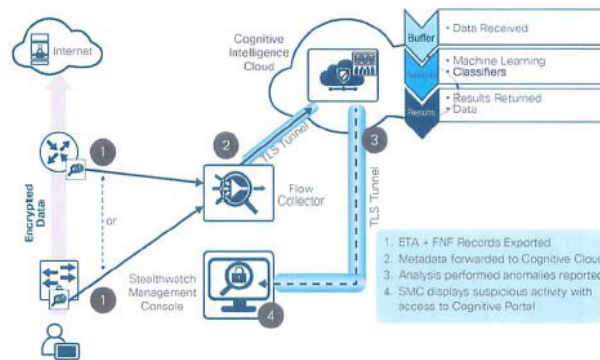


PTX-584 at 402.

PTX-570

Cisco Encrypted Traffic Analytics Technical Deployment Guide from July 2019

Figure 1. ETA malware detection in Cognitive Intelligence cloud



Appendix E

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?

Appendix E

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?

Appendix E

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

Appendix E

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.

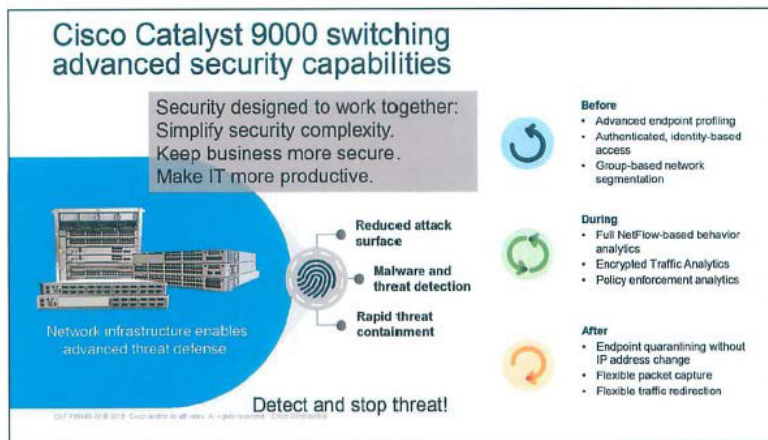
Tr. 1925:16-1927:21; *see* PTX-1287 at 028 (depicted below).

234a

Appendix E

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

Appendix E

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

Appendix E

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

Appendix E

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

Appendix E

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[d] 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

Appendix E

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

Appendix E

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:

Appendix E

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.

Appendix E

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

A. No, that's 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?

Appendix E

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 configured to establish the

Appendix E

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

Appendix E

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.

Appendix E

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

Appendix E

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.

Appendix E

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.

Appendix E

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.

*Appendix E**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, 99 S.Ct. 1804, 60 L.Ed.2d 323 (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

Appendix E

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

Appendix E

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

Appendix E

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

Appendix E

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

Appendix E

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

256a

Appendix E

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:

12/9/2019 Cisco unveils the network of the future | The Network

Home (Home)

The Network
(Home)

News Release (Press releases)

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 Geerkeleer, 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.
- **Insights:** 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.

<https://newsroom.cisco.com/press-release-content?type=webcontent&articleid=1854555>

1/8

CENTRIPETAL-CSCO 472946

Appendix E

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?

Appendix E

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.*

Appendix E

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

Appendix E

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

Appendix E

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.

262a

Appendix E

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

Appendix E

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.

Appendix E

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.

Appendix E

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

Appendix E

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

Appendix E

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.

Appendix E

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

Appendix E

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.

Appendix E

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 **PI**’ with **PI** (e.g., by determining that a portion of the data in entry 306 corresponds with data in entry 312). Similarly, packet cor-relator 128 may compare data in entry 308 with data in entry 314 to correlate **P2**’ with **P2**, packet correlator 128

Appendix E

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?

Appendix E

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

Appendix E

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

274a

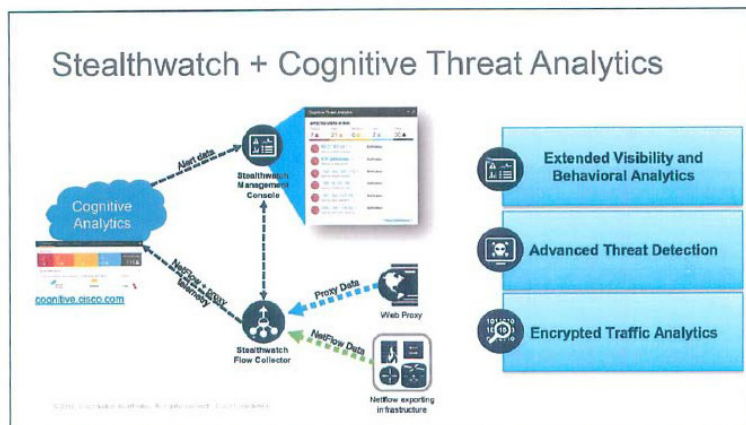
Appendix E

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**



Appendix E

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.

276a

Appendix E

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’.

Appendix E

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).

Appendix E

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).

Appendix E

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.

Appendix E

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:

Appendix E

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.

Appendix E

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 Adaptive 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

Appendix E

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

Appendix E

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:

Appendix E

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

Appendix E

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

Appendix E

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.

Appendix E

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 processors 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 processor 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

Appendix E

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 . . .”).

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.

Appendix E

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 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.

Appendix E

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

Appendix E

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.

Appendix E

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.

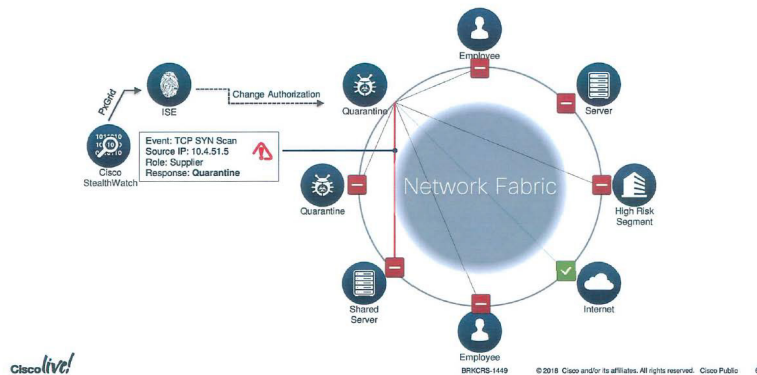
The Cisco packet-filtering system operates by using the Identity Services Engine to assign certain endpoint devices “roles” that determine what type of packets may be sent and/or received by that specific endpoint computer. PTX-1326. Therefore, the Identity Services Engine has the ability to monitor 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:

294a

Appendix E

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

Appendix E

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

Appendix E

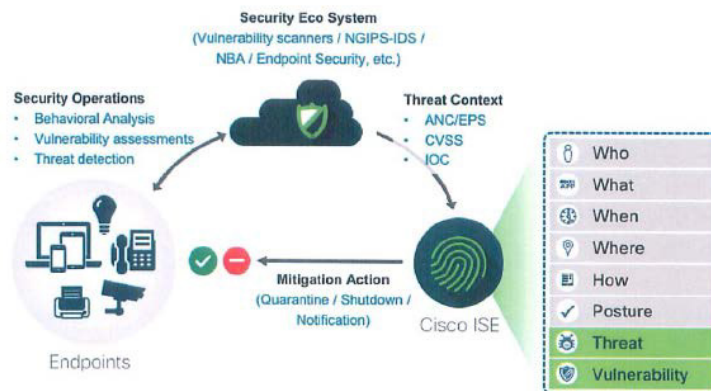
data while their users can keep working on less critical applications.” PTX-1326 at 011. Thus, the Cisco system operates by blocking packets affiliated with a particular type of data transfer to a protected resource, while allowing packets unaffiliated with a protected type of data transfer to be transmitted 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



Appendix E

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?

Appendix E

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-

Appendix E

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.

Appendix E

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,

Appendix E

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

Appendix E

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.

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.

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.

Appendix E

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;

Appendix E

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.

Appendix E

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

Appendix E

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

Appendix E

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 Jones⁸, a distinguished Cisco engineer responsible for building the switching, routing and

8. Mr. Jones was one of the architects for the design of the UADP processor 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.

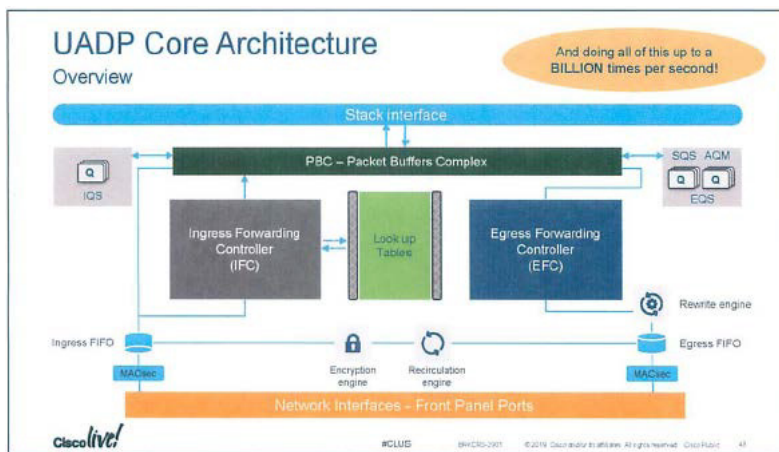
Appendix E

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:

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

Appendix E

(“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

Appendix E

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:

311a

Appendix E

PTX-1195 AT 003

**Cisco FED 2.0 Hitless ACL Update Software
Functional Specification⁹ 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.

Appendix E

With the new 2.0 Hitless ACL Update:

PTX-1195 AT 003**Cisco FED 2.0 Hitless ACL Update Software
Functional Specification from July 2017¹⁰****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.

Appendix E

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

Appendix E

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).

Appendix E

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

Appendix E

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

Appendix E

. . . [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,

Appendix E

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

Appendix E

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.

*Appendix E**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.

Appendix E

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.

*Appendix E**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

Appendix E

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.

Appendix E

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 configured 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;

Appendix E

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

Appendix E

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.

Appendix E

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

Appendix E

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 known 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

Appendix E

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

Appendix E

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?

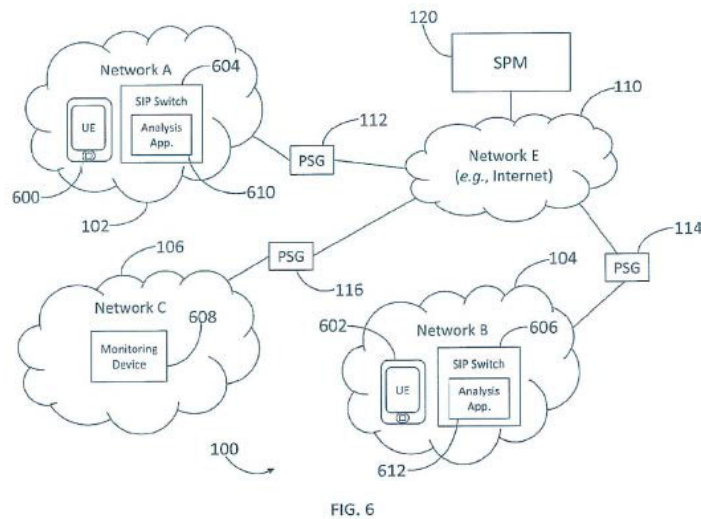
A. Well, in my report I documented several disputes, but in the interest of time, we’re going to focus on two here, and these are the two that I think are the easiest to see. And the first one is really sort of a black/white issue; that Centripetal’s theory of infringement focuses on the blocking of packets. And blocking has really been the key to most of this case; that

Appendix E

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



Appendix E

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

Appendix E

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.

Appendix E

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

Appendix E

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

Appendix E

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.

Appendix E

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.

*Appendix E***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, 6 S.Ct. 934, 29 L.Ed. 954 (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

Appendix E

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

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).

Appendix E

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.

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

Appendix E

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.

Appendix E

(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

Appendix E

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

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.

Appendix E

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 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

Appendix E

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

Appendix E

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).

Appendix E

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

Appendix E

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").

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

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. Stahl 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)).

Appendix E

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

Appendix E

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, 53 S.Ct. 736, 77 L.Ed. 1449 (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%

351a

Appendix E

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.

352a

Appendix E

3/24/2020 Cisco Catalyst 9000 - The best keeps getting better. - Cisco Blogs

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

<https://blogs.cisco.com/networking/cisco-catalyst-9000-the-best-keeps-getting-better>

2/10

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

Appendix E

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

Appendix E

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.

355a

Appendix E

12/9/2019 Cisco unveils the network of the future | The Network

CISCO The Network
(http://www.cisco.com) (home)

Home (home)

News Release (Press Releases)

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 Geoeckeler, 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., Scentay, 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/en/usa/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 as digital speed.

<https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1854555>

1/6

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

Appendix E

(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:

Appendix E

Product	Increase in Revenues %	Increase in Revenues \$ (in millions)
Switches	40.9%	\$3,973.4
Routers	13.2%	501.5
Adaptive 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 Architecture¹⁴	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. 2621:5-10, 2634:14-18 (showing how ASICs process packets

14. There is 100% revenue increase for the Digital Network Architecture, as this product was released in mid-2017, and had no defined predecessor.

358a

Appendix E

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**



Appendix E

Speed & Scale

- Centripetal's patented filter algorithms eliminate the speed & scalability problem.
- The computational problem.
 - I/O of 30 million packets per second
 - Filter against 5 million+ complex IOCs
 - Process for host ID
 - Append IOC meta-data
 - Capture & Record PCAP content
 - Take non-binary action




 Confidential & Proprietary Cisco-CNI NDA
 7

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

Appendix E

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

Appendix E

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. Striegel’s testimony, Cisco objected to Dr. Striegel’s apportionment opinion on the basis that his opinions do not satisfy the essential requirement for reliability under *Daubert*. Additionally, Cisco’s

Appendix E

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):

Appendix E

[illegible]

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.

Appendix E

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):

Appendix E

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%
Firepower / ASA (including Firepower Management Center)	13	7 ['806 Patent] ¹⁶	54%

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.

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

Appendix E

Digital Network Architecture	10	3 ['806 Patent]	30%
Stealthwatch	5	4 ['806 Patent]	80%
Identity Services Engine	1354%	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).

Here is a reproduction of the apportionment percentages applied to Cisco's gross revenues from June

for products where the apportionment was based on the '205 Patent. *See* Doc. 488, Ex. 7.

367a

Appendix E

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, 2020¹⁷	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

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).

Appendix E

Identity Services Engine	\$497,000,709	38%	\$188,860,269
TOTAL	\$21,467,079,878 (billion)		\$7,558,085,447 (billion)

Accordingly, based on Mr. Gunderson and the Court's analysis, the Court **FINDS** that the correct apportioned royalty base is \$7,558,085,447¹⁸ 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.

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.

Appendix E

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.

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.

Appendix E

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 Oppenheime & 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

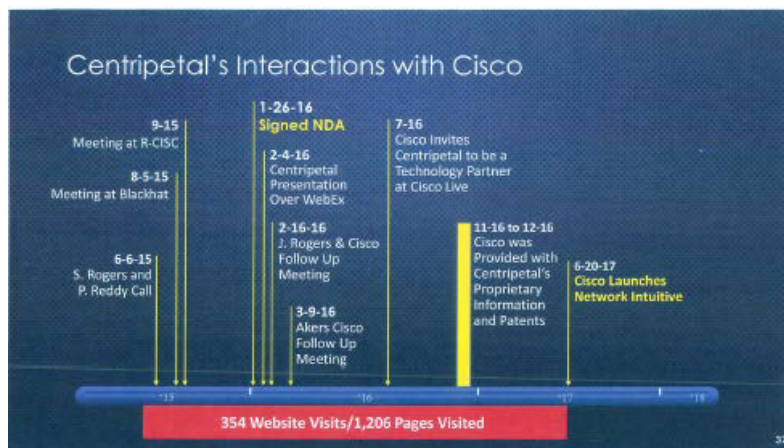
371a

Appendix E

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 accurately reflects the evidence presented at trial surrounding the events of Centripetal and Cisco's relationship¹⁹.

SLIDE 37 FROM CENTRIPETAL'S OPENING STATEMENT



19. This slide does not attempt to reflect the numerous “hits” on Centripetal's website by Cisco's employees.

*Appendix E**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.*, — U.S. —, 136 S. Ct. 1923, 1931, 195 L.Ed.2d 278 (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

Appendix E

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, 472 F.Supp.3d 377, 382–84, 2020 U.S. Dist. LEXIS 122276, at *11 (E.D. Mich. 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

Appendix E

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

Appendix E

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*, 472 F.Supp.3d at 384–85, 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:

Appendix E

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

Appendix E

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)

Appendix E

(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.

Appendix E

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

Appendix E

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.*, 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

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.

Appendix E

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 (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

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.

Appendix E

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 WL 6840353, at *7, 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,

Appendix E

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, 103 S.Ct. 2058, 76 L.Ed.2d 211 (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, 103 S.Ct. 2058. 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, 103 S.Ct. 2058. In determining the rate of pre-judgment interest,

Appendix E

“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

23. This was calculated using a simple interest formula - $I = P \times R \times T$ ($27,243,850 = 755,808,545 \times .0121 \times 3$).

Appendix E

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 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, 126 S.Ct. 1837, 164 L.Ed.2d 641 (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, 130 S.Ct. 2743, 177 L.Ed.2d 461 (2010) (citing *Weinberger v. Romero-Barcelo*, 456 U.S. 305, 311-12, 102 S.Ct. 1798, 72 L.Ed.2d 91 (1982)). “If a less drastic remedy . . . [is] sufficient to redress [Proponents’] injury,

Appendix E

no recourse to the additional and extraordinary relief of an injunction [is] warranted.” *Id.* at 165-66, 130 S.Ct. 2743. 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 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

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.

Appendix E

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, 1297 (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.*

Appendix E

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,

Appendix E

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 successors²⁵.

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.

*Appendix E***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.

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.
HENRY COKE MORGAN, JR.
SENIOR UNITED STATES DISTRICT JUDGE

October 5, 2020
Norfolk, Virginia

*Appendix E***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

Appendix E

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

Appendix E

SGT	Security Group Tag
SPLT	Sequence of Packet Lengths and Times
SIO	Security Intelligence Operations
SIP	Session Initiation Protocol
Stealth-watch	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 E

APPENDIX B

OUTLINE OF COURT'S PROTOCOLS FOR TRIAL

A. 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 efforts to resolve the objections to each other's proposed exhibits.

*Appendix E***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

Appendix E

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 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.

26. All times identified herein are Eastern Time.

Appendix E

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.

Appendix E

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 prima facie 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

Appendix E

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-designations²⁷, 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

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.

Appendix E

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 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

Appendix E

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.

**APPENDIX F — OPINION AND ORDER OF
THE UNITED STATES DISTRICT COURT FOR
THE EASTERN DISTRICT OF VIRGINIA,
NORFOLK DIVISION, FILED OCTOBER 2, 2020**

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
NORFOLK DIVISION

Civil Action No. 2:18cv94

CENTRIPETAL NETWORKS, LLC,

Plaintiff,

v.

CISCO SYSTEMS, INC.,

Defendant.

Signed October 2, 2020

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

Appendix F

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

Appendix F

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.

*Appendix F***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

Appendix F

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, 108 S.Ct. 2194, 100 L.Ed.2d 855 (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, 108 S.Ct. 2194). 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, 108 S.Ct. 2194. 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

Appendix F

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

Appendix F

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

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.

Appendix F

“[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 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

Appendix F

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 disclose 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.

Appendix F

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*.

Appendix F

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.

Appendix F

Finally, Cisco frequently cites *Liljeberg v. Health Services Acq. Corp.*, 486 U.S. 847, 108 S.Ct. 2194, 100 L.Ed.2d 855 (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, 108 S.Ct. 2194). The totality of the circumstances present

Appendix F

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 be 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.

Appendix F

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.

Appendix F

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

Appendix F

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

Appendix F

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 divestiture 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

Appendix F

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 divestiture 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.

Appendix F

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

421a

Appendix F

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

Norfolk, Virginia
October 2, 2020