APPENDIX

TABLE OF APPENDICES

Appendix A

UNITED STATES COURT OF APPEALS
FOR THE FEDERAL CIRCUIT

No. 21-1888

CENTRIPETAL NETWORKS, INC.,
Plaintiff-Appellee,
v.
CISCO SYSTEMS, INC.,
Defendant-Appellant.

Decided: June 23, 2022

Before: Dyk, Taranto, and Cunningham,
Circuit Judges.

OPINION

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

---

[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).

[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.

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 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. . . .

(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-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 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.

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

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

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 (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 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.*

---

[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.

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 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

---

[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

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.

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)).

---

statutory and non-statutory ethical principles that control the conduct of federal judges.").

[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).

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 (1990) (quoting *NLRB v. Food & Com. Workers*, 484 U.S. 112, 123 (1987)). "Our 'starting point is the language of the statute,'" *id.* (quoting *Schreiber v. Burlington N., Inc.*, 472 U.S. 1, 5 (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 (1989)); *see also K Mart Corp. v. Cartier, Inc.*, 486 U.S. 281, 291 (1988) (same).

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 (2018) (quoting *Perrin v. United States*, 444 U.S. 37, 42 (1979)); *see Mohamad v. Palestinian Auth.*, 566 U.S. 449, 454 (2012) (citing *FCC v. AT&T Inc.*, 562 U.S. 397, 403 (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 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. 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

---

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

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." 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

---

[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.").

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 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).

---

[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.

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.

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]

---

[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.

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. 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

---

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*, 137 S. Ct. 759, 779 (2017) (citing *Gonzalez v. Crosby*, 545 U.S. 524, 529 (2005)).

[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

we have here. The rulings at 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

---

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 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 Cont'l 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 (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 c[ould] be corrected on appeal and trial de novo in the County Court of Common Pleas").

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. *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 Int'l Bus. Machs. Corp.*, 618 F.2d 923, 932 (2d Cir. 1980) (adopting timeli- ness 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 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

[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.

from the previous trial. 11 Charles Alan Wright & Arthur R. Miller, *Federal Practice & Procedure* § 2922 n.19 (3d ed. 2022) (collecting cases).[13]

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 re- liance 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

---

[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 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.*

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 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

---

[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).

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 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

---

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

[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").

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 (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 (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 (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 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 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 dis- cussed 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 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 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).

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.

REVERSED IN PART, VACATED IN PART, AND REMANDED

---

[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.

Appendix B

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

No. 2:18cv94

CENTRIPETAL NETWORKS, INC.,
Plaintiff,
v.
CISCO SYSTEMS, INC.,
Defendant.

Decided: Oct. 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 conflict. The first disclosure came on March 2, 2020, where the Court's former law clerk, Neil McBride, entered the case on behalf of Cisco. The Court promptly notified the parties and disclosed that the Court had "visited Neil's home and he has visited mine and we have had family dinners together many times

over the years." Counsel for both parties responded that recusal was not necessary as a result of Mr. McBride's representation of Cisco. Next, during the pre-trial conference, the Court disclosed that it had purchased 200 shares of Zoom stock based on a recommendation by a service over the internet. At that time, neither party objected to the ownership of Zoom stock. Thereafter, the Court conducted a bench trial "spanning nearly eight weeks over Zoom, producing a 3,507-page record with twenty-six witnesses and over 300 exhibits." Doc. 564 at 2. As a result of an enormous variation in damages calculations by the opposing damages experts, the Court request additional data relevant to damages and after receipt of this information the Court heard final arguments on June 25, 2020.

On August 11, 2020, the Court's administrative assistant discovered during preparation of the Court's judicial financial disclosure reporting that the Court's spouse owned 100 shares of Cisco stock valued at $4,687.99 and advised the Court. The Court promptly investigated the issue and confirmed that the shares were purchased as a result of her brokers recommendation. The Court's spouse had no independent recollection of approving the transaction. The next day, August 12, 2020, the Court disclosed the existence of the shares to the parties. *See* Court's Email to Counsel [Attached as Ex. One]. The Court detailed that "full draft of my opinion had been prepared before I received this information yesterday. Virtually every issue was decided prior thereto." *Id.* Also explaining that the shares "did not and could not have influenced my opinion on any of the issues in this case." *Id.* Centripetal quickly notified the Court that it

had no objection based on the representations by the Court. Cisco responded, nine days later, by filing the instant motion for recusal. The Court ordered a response by Centripetal, if they be so advised. Centripetal responded by objecting to Cisco's motion and Cisco filed a rebuttal brief. The Court conducted a hearing on the motion and heard oral argument on September 9, 2020. At the hearing, the Court informed the parties that he had discussed the issue with his spouse and, as a result, the Court contacted their personal attorney to request the creation of a blind trust to divest the shares. The Court provided the completed trust documents to the parties at the hearing.

Moreover, at the hearing on Cisco's current motion, the Court disclosed a previous purchase by the Court and his spouse of 100 shares each of Crowdstrike stock. Similar, to Zoom, Crowdstrike was purchased on the basis of a recommendation of an internet service. The Court later discovered that Crowdstrike primarily engaged in the business of developing cybersecurity technology and had a previous intelligence sharing agreement with Centripetal. *See* PTX-1600. After learning of this information, the Court and his spouse divested their shares in Crowdstrike. Due to the indirect nature of Crowdstrike as a potential competitor of both parties, the Court did not disclose this transaction until the hearing date.

II. LEGAL STANDARD AND ANALYSIS

28 U.S.C § 455(a) requires that a judge of the United States "shall disqualify himself in any proceeding in which his impartiality might reasonably

be questioned." 28 U.S.C. § 455(a). The next section of the statute, 455(b) lays out specific circumstances where recusal is required. Section 455(b)(4) lays out one of these circumstances at issue here where:

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

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

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

In analyzing section 455, the Supreme Court in *Liljeberg v. Health Services Acquisition Corp.*, held that scienter is not a requirement of 455(a), but is a requirement of 455(b)(4*). Liljeberg v. Health Services Acq. Corp.*, 486 U.S. 847, 859 (1988). Therefore,

recusal under section 455(b)(4) imposes "actual knowledge" of the disqualifying financial interest. *C. Tel. Co. of Virginia v. Sprint Commun. Co. of Virginia. Inc.*, No. 3:09CV720, 2011 WL 6178652, at *5 (E.D. Va. Dec. 12, 2011) (collecting cases imposing the "actual knowledge" test), *aff'd*, 715 F.3d 501 (4th Cir. 2013) (on other grounds). However, the test for recusal under section 455(a), is "when a reasonable person, knowing the relevant facts, would expect that a justice, judge, or magistrate knew of circumstances creating an appearance of partiality." *Id.* at *7 (quoting *Liljeberg*, 486 U.S. at 850). Therefore, for section 455(a), "recusal is required even when a judge lacks actual knowledge of the facts indicating his interest or bias in the case if a reasonable person, knowing all the circumstances, would expect that the judge would have actual knowledge." *Liljeberg*, 486 U.S. at 860-61. The Court will first address recusal under 455(a) and then turn to 455(b)(4).

i. Section 455(a)

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

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

Centripetal, in opposition, responds that the facts presented would not lead a reasonable person to conclude that the Court knew of this interest but

proceeded despite that interest. Centripetal notes the "touchstone of the inquiry is reasonableness, not exhaustive and constant vigilance to the point of reviewing mail separately addressed to judges' spouses, as Cisco proposes." Doc. 564 at 8. Centripetal argues that the inquiry is judged on a reasonableness standard and reasonableness is confirmed by the legislative history of the section 455 highlighting that "the judge need not know what they are [his spouse's investments], but must merely make a *reasonable effort to inform himself of their investments*." *Id.* (quoting H.R. Rep. No. 93-1453 (1974), 1974 U.S.C.C.A.N. 6351, 6356) (emphasis added).[1] Accordingly, Centripetal concludes "[e]ither way, Cisco's unsupported insinuations do not establish an appearance of bias under Section 455(a)." *Id.* The Court agrees with Centripetal. The Court FINDS that a reasonable person would not conclude that the Court knew of his spouse's ownership and proceeded to hear the case nonetheless, where the Court avers he was notified about the stock during the preparation of his annual financial disclosures and immediately notified counsel.

---

[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.

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 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 teaming of his spouse's financial interest while preparing annual financial disclosures, the Court promptly notified counsel that he was unaware that his spouse had purchased shares of Cisco stock. A reasonable person would find it unlikely that a judge would now disclosure his spouse's

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

Furthermore, Cisco argues that the factual situation presented here is more akin to that in other cases where recusal was warranted. Specifically, Cisco argues that the reasoning in *Central Telephone* "cannot be reconciled with either *Chase Manhattan* or *Shell Oil*; each judge in those cases also 'brought [the] financial interest to the parties' attention Just after [they] discovered the ownership,' and would have been no more likely to 'run the risk of impeachment or perhaps prosecution for knowingly deciding a case from which he knew he should have recused himself"

However, the factual circumstances in both *Chase Manhattan* and *Shell Oil* are quite different than presented in this case.

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

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

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

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

> (1) sat on the Board of Trustees of an interested party, yet somehow forgot about its interest in land that was purchased for over $6 million dollars and stood to increase its value by 60% when the litigation arose;

> (2) attended a meeting discussing negotiations relevant to this interest days before the case was filed, which showed he had actual knowledge of the interest even if he later forgot;
>
> (3) despite ten years of regular Board meeting attendance, missed the one meeting at which his trial was discussed, and the other trustees remarkably chose not to "call to the judge's attention the obvious conflict of interest" of a University trustee presiding over this particular trial; and
>
> (4) failed to review the minutes mailed to him for that missed meeting, which would have revealed that the trial had been discussed.

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

Moreover, a reasonable observer would consider the Court's candor and history of disclosing possible conflicts in this case. As discussed supra, the Court has continually disclosed potential conflictual issues to counsel including Mr. McBride's representation of Cisco and ownership of Zoom stock. It is unreasonable to assume that this Court would be so forthcoming

regarding possible conflicts and at the same time conceal a more direct conflict of stock ownership of a named party. Therefore, a reasonable observer would weigh the Court's repeated candor in favor of a finding that it had no knowledge of its spouse's Cisco stock ownership. Furthermore, the Court evidenced its pattern of dealing with potential stock ownership conflicts by the manner in which it dealt with the Crowdstrike purchase. When the Court discovered that Crowdstrike may be a competitor in the similar cybersecurity technology with Cisco and Centripetal, the Court and the Court's spouse promptly sold their shares. Accordingly, it would an unreasonable presumption that a reasonable person viewing the facts would conclude that the Court would act any differently with knowledge of his spouse's ownership of Cisco.

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

ii. Section 455(b)(4)

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

In *Central Telephone*, the presiding judge found section 455(b)(4) to not apply to the facts because there was "no actual knowledge of the conflict." The conflict was discovered by the presiding judge "at a time when the preparation of the opinion on Sprint's

counterclaim was *underway* and when the presiding judge was preparing the annual financial disclosure statement required of federal judges . . ." *C. Tel. Co. of Virginia*, 2011 WL 6178652, at *1. Similarly, the Court only discovered the ownership during preparation of an annual financial disclosure report. However, here, the Court represented that every issue was "virtually" decided in this case before there was actual knowledge of the Cisco stock. Thus, in *Central Telephone*, the drafting of the presiding judge's decision was "underway," which is comparable to this Court's mostly drafted opinion. Moreover, this Court rests on the persuasive logic illustrated by the Ninth Circuit in *Davis V. Xerox*, 811 F.2d 1293, 1296 (9th Cir. 1987). There, the court noted that the right course under section 455(b) is:

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

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

iii. Divestment under 455(f)

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

divestment provision of Section 455(f). Section 455(f) states that

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

28 U.S.C. § 455(f). Therefore, the requirements for divestiture are met when "(i) the district judge devoted 'substantial judicial time' to the matter before 'appearance or discovery' of the conflict; (ii) his financial interest cannot be substantially affected by the outcome of the case; and (iii) he divested himself of the interest once he discovered it." *Chase Manhattan Bank*, 343 F.3d at 131. The Second Circuit has explained that this section "is meant to help judges strike a balance between the duty to recuse when their impartiality might reasonably be questioned and the need to resolve cases expeditiously and without undue collateral litigation." *Muchnick v.*

Thomson Corp. (In re Literary Works in Elec. Databases Copyright Litig.), 509 F.3d 136, 142 (2d Cir. 2007). It is undisputed in this case that there is substantial judicial time invested. The Court had devoted months of time into this matter engaging in ruling of pre-trial motions, holding a *Markman* hearing, conducting an almost six-week bench trial and drafting extensive findings of fact and conclusions of law in a 150-plus page opinion.

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

Additionally, Cisco notes that the interest held by the Court's spouse cannot fall under the divestiture provisions of section 455(f) because the interest would be substantially affected by the account where Centripetal has requested such a high amount of

damages. The Court finds the case *of Key Pharm., Inc. v. Mylan Laboratories Inc.*, 24 F. Supp. 2d 480, 483 (W.D. Pa. 1998) as persuasive on this issue. In that case, the judge found divesting 151 shares with a value of $10,185.18 "was an effective cure for the discovery of the interest, particularly where the investment had been in a Targe, publicly held corporation with diverse interests and revenues in the billions.'" Doc. 564 at 14 (quoting *Key Pharm.. Inc. v. Mylan Laboratories Inc.*, 24 F. Supp. 2d 480, 483 (W.D. Pa. 1998)). Here, the Court's spouse owned 100 shares of Cisco stock valued at $4,687.99. Cisco, similar to the company in *Key Pharm* is a large, publicly held corporation with billions in revenue. Therefore, the Court finds that divesture is appropriate under the circumstances. Cisco points to the previously discussed case of *Chase Manhattan* as an example that divestiture is unavailable in this case. As noted supra, that case has substantially different facts. In *Chase Manhattan*, the "disqualifying circumstances here appeared in 1997, [as such] they cannot be cured by a divestiture in 2000, long after the district judge's conduct of the bench trial, findings of fact, and issuance of judgment." *Chase Manhattan Bank*, 343 F.3d at 132. A three-year gap between identification of conflicting ownership and divestiture is drastically different than the less than a month gap presented in this case.

In light of this guidance, the Court's spouse has proceeded to divest the Cisco shares into a blind trust. Divestment to a blind trust is the proper remedy as the Court finds that an outright sale of the stock would undermine the purpose of section 455. Generally, section 455 "is designed to promote public confidence

in the impartiality of the judicial process . . . ." *Muchnick v. Thomson Corp. (In re Literary Works in Elec. Databases Copyright Litig.)*, 509 F.3d 136, 140 (2d Cir. 2007) (citing H.R. Rep. No. 93-1453. *reprinted in* 1974 U.S.C.C.A.N. 6351, 6355). Section 455(f) was incorporated for exactly the type of situations where the Court discovers an interest after substantial time and resources have been devoted to the case. *See Kidder, Peabodv & Co. v. Maxus Energy Corp.*, 925 F.2d 556, 561 (2d Cir. 1991) ("We think that section 455(f) directly applies to this situation. Nearly three years of the litigants' time and resources and substantial judicial efforts have been devoted to the litigation.")

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

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

The situation is somewhat of a reverse bias allegation as it is Cisco, in which the stock is owned, seeking recusal. Cisco's theory is that the Court would change its opinion to one less favorable to it in order to shore up its appearance of propriety. Such an allegation makes it difficult for the Court to consider

the outright sale of this stock. During the interim period between notification of counsel regarding the stock and the issuance of this opinion, the Court has performed no further work on its draft opinion on the merits. An outright sale of the stock would be inappropriate as the Court may appear to benefit itself in order to comply with the provisions of 455(f). Accordingly, the Court's spouse has divested her shares of Cisco stock by placing them in a blind trust to remove control from the Court and his spouse. This solution intends to abide by the statutory purposes of impartiality required by section 455 as well as the timely divestiture required by 455(f).

III. CONCLUSION

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

It is **SO ORDERED**.

/s/

Henry Coke Morgan, Jr.

Senior United States
District Judge

Appendix C

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

No. 2:18cv94

CENTRIPETAL NETWORKS, INC.,
Plaintiff,
v.
CISCO SYSTEMS, INC.,
Defendant.

Decided: Oct. 5, 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.

I. PROCEDURAL POSTURE[1]

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

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

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

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

5. Upon the motion of Centripetal, on September 18, 2019, the Court issued an order, lifting the stay in part with respect to patents and claims not currently subject to IPR proceedings and set the case for trial in

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

April 2020. Doc. 68. The parties later waived a jury trial following the jury trial limitations resulting from the COVID-19 pandemic.

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

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

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

II. WITNESSES AT TRIAL

9. During the twenty-two-day bench trial, and at a later hearing on damages evidence, both parties were given the opportunity to present their evidence live through a video platform approved by the Eastern District of Virginia after Court's staff was instructed in its operation. Cisco objected to proceeding through a video platform, and also objected to using the platform utilized in favor of its own platform. In its

order of April 23, 2020, the Court overruled Cisco's objections for the reasons stated therein. In light of the use of the video platform, the parties implemented specific trial protocols that are detailed in Appendix B. See Appendix B; Doc. 411 (Amended Pre-Trial Order). At the conclusion of the 22nd day of trial, the parties joined in congratulating the Court's staff for their handling of the trial evidence by means of the video platform.

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

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

- Mr. Steven Rogers – Founder and CEO of Centripetal. Tr. 228:8;

- Dr. Sean Moore – Chief Technology Officer and Senior Vice President of Research at Centripetal. Tr. 301:24-25. Dr. Moore is an inventor on all of the asserted patents in this case. Tr. 314:25, 315:1-2;

- Dr. Michael Mitzenmacher – an independent expert witness in cybersecurity who presented opinion testimony that the accused products infringe the '193 Patent, the '806 Patent and the '205 Patent. Tr. 431:16-23;

- Dr. Eric Cole – an independent expert witness in cybersecurity who presented opinion testimony that the accused products infringe the '856 Patent and the '176 Patent. Tr. 886:9-11, 975:19-21;

- Dr. Nenad Medvidovic – an independent expert witness in cybersecurity who opined about the importance of the patent technology in relation to the accused products. Tr. 1144:22-25, 1145:1-2;

- Mr. Jonathan Rogers – Chief Operating Officer at Centripetal. Tr. 1194:11;

- Mr. Christopher Gibbs – Senior Vice President of Sales at Centripetal. Tr. 1297:1-2;

- Dr. Aaron Striegel – an independent expert witness in computer networking who opined regarding apportionment and the top-level infringing functions of the accused products. Tr. 1337:19-23;

- Mr. Lance Gunderson – an independent expert witness in patent damages who opined regarding damages and a reasonable royalty. Tr. 1441:2-14;

- Mr. James Malackowski – an independent expert witness in business, intellectual property valuation and patent licensing who opined regarding the impact of the asserted infringement on Centripetal and damages going forward. Tr. 1573:14-19.

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

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

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

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

infringement, invalidity and damages of the '176 Patent. Tr. 2212:12-18;

- Dr. Mark Crovella – an independent expert witness in networking and network security who opined regarding non-infringement, invalidity and damages of the '193 Patent. Tr. 2349:18-24;

- Mr. Hari Shankar – Principal Engineer and Software Architect at Cisco who is responsible for the design of certain features of the accused products. Tr. 2500:3-5;

- Mr. Peter Jones – Distinguished Engineer in the Enterprise Network Hardware Group at Cisco. Tr. 2543:12-17;

- Dr. Narasimha Reddy – an independent expert witness in computer networking and computer security who opined regarding non-infringement, invalidity and damages of the '806 Patent. Tr. 2580:6-10;

- Mr. Matt Watchinski – a Cisco employee responsible for Cisco's Talos organization, which is Cisco's threat intelligence organization. Mr. Watchinski previously worked for Sourcefire. Tr. 2682:11-13;

- Dr. Kevin Jeffay – an independent expert witness in computer networks and network security who opined regarding non-infringement and damages of the '205 Patent. Tr. 2727:11-19;

- Mr. Timothy Keanini – Distinguished Engineer at Cisco involved with the Stealthwatch product line. Tr. 2810:4-6;

- Mr. Karthik Subramanian – Partner at a venture capital firm called Evolution Equity Partners. Mr. Subramanian previously led Cisco's Corporate Development Team for Cybersecurity for about four to four and a half years. Tr. 2827:23, 2828:17-18;

- Dr. Stephen Becker – an independent expert witness in economic damages analysis who opined regarding damages if the Court finds the Asserted Patents are infringed and valid. Tr. 2863:3-18.

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

- Mr. Douglas DiSabello;

- Mr. Haig Colter;

- Dr. Sean Moore;

- Mr. Jess Parnell;

- Mr. Justin Rogers;

- Mr. Christopher Gibbs;

- Mr. Gregory Akers.

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

- Dr. Alexander Orso – an independent expert witness in computer networking and security who opined regarding the validity of the '193 Patent and the '806 Patent. Tr. 2989:22-25;

- Dr. Trent Jaeger – an independent expert witness in computer and network security who opined regarding the validity of the '856 Patent and the '176 Patent. Tr. 3102:18-23;

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

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

III. TECHNOLOGY TUTORIAL

A. NETWORKING AND CYBERSECURITY TUTORIAL

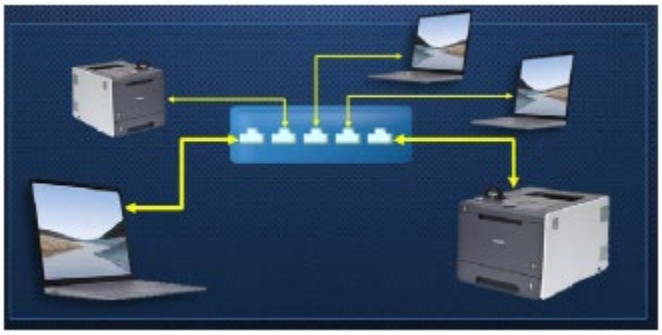
The asserted patents in this case deal with systems that engage in complex computer networking security functions. Accordingly, the Court heard detailed technological testimony regarding the structure and function of computer networks in general, as well as the specific processes employed to secure these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

findings by reciting a review of the presented technology tutorial.

i. Overview of Networking

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

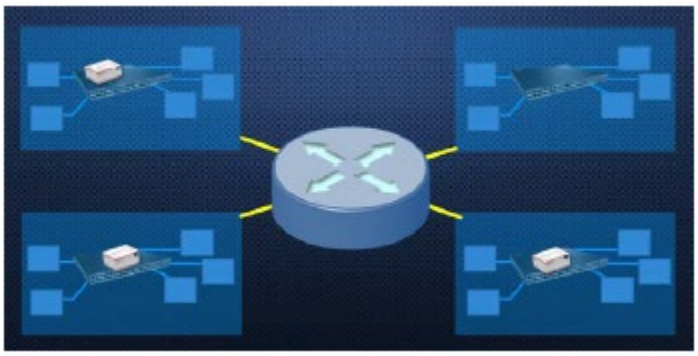
FIG. 1



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

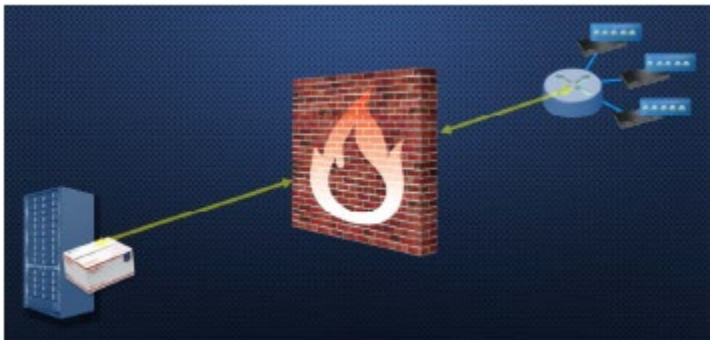
destination. Tr. 23:8-14. The combination of routers and switches are the fundamental building blocks of computer networks. Tr. 23:17-23. Together, switches connect local devices into small networks and routers operate to transmit data between these smaller networks—thus forming larger networks. Tr. 26:1-4; *see* Fig. 2.

FIG. 2



The next and final relevant device in computer networks is the firewall. Firewalls, in the context of computer networking, are similar to that of a firewall in an office building or hotel. Tr. 24:13-19. They operate to automatically put a "wall" between valuable assets and any potential danger. Tr. 24:13-19. Therefore, data entering a network is often transmitted in through a firewall and the firewall can perform a variety of functions, such as disallowing the data to enter the network by blocking it. Tr. 25:1-4; *see* Fig. 3.

FIG. 3



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

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

Tr. 25:8-20. Accordingly, firewalls often sit at the edge of individual networks to control the entry of data from the internet. Tr. 26:1-12. As technology develops, firewall type functionality is often now included inside of other devices such as routers and switches. These devices may be located at different locations within a

network—not just at the outside barrier. Tr. 82:8-18. This inclusion of firewall functionality in other devices is in contrast with older network technology where firewalls were responsible for the security of the network, by blocking malicious packets from entering it. while the routers and switches focused on speed and performance in the transmitting data. Tr. 26:16-22.

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

FIG. 4

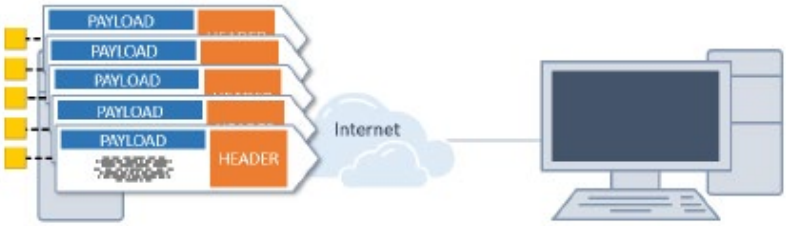
The international nature of the internet requires that the sending of data between all of these providers be based on uniformly developed standards that are globally applicable. Tr. 77:5-17. One such organization, the Internet Engineering Task Force ("IETF") is responsible for developing universal internet related standards. Tr. 77:5-17. There are many different standards that are developed to facilitate the transmission of data over the internet. Tr. 77:5-17. These standards are often in the form of protocols. Protocols are the rules of engagement for two computers that specify how the two computers can work together to communicate back and forth. Tr. 954:5-17. For example, the Hypertext Transfer Protocol ("HTTP") is used in web pages to transfer data over the internet from computer to computer, the Internet Protocol ("IP") is a building block in allowing data to use interconnected networks, and the Transmission Control Protocol ("TCP") is used to deliver information across the internet. Tr. 77:23-78:2, 89:18-21. These protocols are the methods by which data transfer is possible over nationwide and global networks. Tr. 88:19-21. This is a general "high level" overview of these networking concepts. Internet professionals and "experts" use the term "high level" to categorize these basic concepts involved in the transmission of data electronically, as well as the imposition of security upon such transmissions.

Moving into the specifics, the transmission of computing data through these devices is done in the form of a network packet or packets. Tr. 26:23-25. The packet is similar to that of a package sent through the United States Postal Service. Tr. 26:24-27:3, 89:2-3. For example, when a user on their computer attempts

to watch a video from ESPN.com, that video is a very large amount of information and cannot efficiently be sent in one package. It is, therefore, broken up into a number of smaller units known as packets. Tr. 27:3-14. The packet will flow from the internet and through multiple devices on the network and transmit the requested information to the end user. Tr. 88:1-14. At any time, there are trillions of packets being exchanged through global networks. Tr. 88:16-19.

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

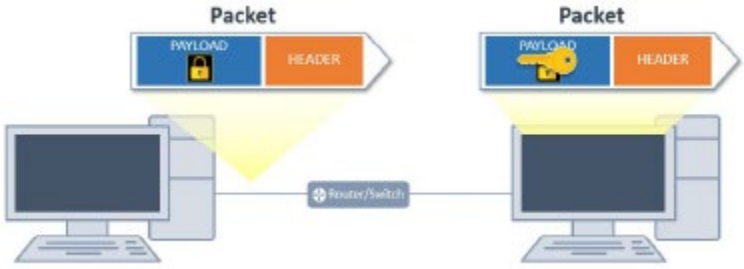
FIG. 5



The header contains information such as the source address, source port, destination address, destination port number, and the protocol being used to transmit the packets. Tr. 107:16-23. These five pieces of information are known as the "5-tuple." Tr. 108:4. The information contained in the header is inspected by the router or switch to determine where and how to send that individual packet. Tr. 108:7-16. This information can be thought of as a mailing label on a package which contains an individual's name and mailing address as well as a return address. Tr. 27:24-25. The payload is the portion of the packet that contains the actual content of the data. This information is similar to the content within a postal

package, such as a new football or baseball glove. In the ESPN video hypothetical, this would be the actual portion of the video sent by each individual packet. Tr. 28:4-10. This data in the payload part of the packet can be encrypted, meaning the information in the payload can be transmitted in code. Tr. 28:18-25. For example, the hypothetical video from ESPN.com would not usually be encrypted, but often data sent in a packet's payload containing sensitive information, such as banking or credit card data, will be encrypted. Encryption becomes vital so that this sensitive data is not stolen by bad actors hacking the network. Tr. 28:18-25. Encryption works to lock up the data in the payload section of the packet so it cannot be seen without decryption. Tr. 29:1-5. Consequently, just as with a sealed package, snoopers of network traffic would be unable to see what is in the packet unless it could be unlocked and opened, which is generally known as decrypting the data. But, even when a packet is encrypted, the header information, such as the source and destination, is not encrypted and is visible. Tr. 29:10-16; *see* Fig. 6.

FIG. 6



As previously noted, the hypothetical ESPN video is set in a collection of packets that comprise the video.

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

ii. Overview of Networking Security

As explained *supra*, the internet is a very large and complex organization of networks that utilize protocols to relay data from one network device to another resulting in the transmission of data to an end user. Tr. 112:1-6. As a result of the internet's complexity, there are many methods employed by cyber criminals to transmit malware and gain access to encrypted, secure and confidential information. Tr. 112:7-14. Cyber criminals can use malware or other methods to infect a network and steal data using a process known as exfiltration. Tr. 343:19-15. Exfiltration is the process by which cyber criminals "exfiltrate" data out of a network by stealing valuable confidential data. Tr. 343:19-15.[2] Therefore, to prevent malware and data exfiltration, cyber defense systems often use a concept known as defense-in-depth, the deployment of a variety of network security devices at different layers of the network, to protect sensitive network data. Cisco's expert, Dr. Almeroth, compared network defense-in-depth to that of the

[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.

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

Older security technology focused on a firewall at the border of the network to detect and block malicious packets from entering a network. Tr. 118:8-119:25. The process begins when a packet is sent from the internet to another smaller network. A firewall device, usually located at the entry of the network, operates by inspecting information in the packet to determine if that packet is malicious. Tr. 119:18-25. This process is completed by matching information from the header or payload of the packet to rules that are pre-enabled in the firewall type device. Tr. 119:18-25. These rules are comprised of previously known information about sources of malicious or otherwise unauthorized traffic.

Tr. 122:11. Thus, if information from a packet header is matched to a rule, then the packet is unauthorized to enter the network and is blocked/dropped.[3] Tr. 120:6-12. A blocked packet is virtually thrown away or could be re-routed to another location for additional inspection. Tr. 120:15-18. If there is no rule that matches the packet, the packet is allowed to proceed into the network and to its final destination. Tr. 120:2-5.

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

[3] Dropping and blocking can be used interchangeably as they have the same definition in the context of cybersecurity. Tr. 46623-467:4.

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 or destination points for data. Tr. 127:5-8. Therefore, firewall capable devices must be placed at all possible entry and destination points or risk that data could reach an improper destination without the application of updated rules. Tr. 127:5-8.

The older allow and detect model operates retroactively by monitoring the entry of packets into the network based upon prior threats to the network. Tr. 129:2-11. The flows are monitored by sensors in network devices and sent to another management device for review. Tr. 132:13-19. When malicious traffic is found, the devices can operate retrospectively, and update rules based upon information found in the forensic investigation. Tr. 133:2. Instead of blocking traffic at the gate, this method allows traffic to go through to its destination

and then performs post facto analysis on the flow of the information in the packet headers to determine if there was malicious activity afoot. Tr. 133:24-134:2. The challenges of this model include the lack of the ability to be proactive. It is different than an inline intrusion prevention system because malicious packets are still allowed into the network and then passed on to the destination without blocking. Tr. 141:11-14.

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

B. OVERVIEW OF THE ACCUSED PRODUCTS

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

i. Cisco's Switches

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

ii. Cisco's Routers

There are three different types of routers at issue. These routers are the 1000 series Aggregation Services Router ("ASR") and the 1000 / 4000 series Integrated Services Router ("ISR"). Tr. 54:22-25, 55:1-

2. Their purpose in the network is to provide performance, reliability, and integrate proactive security functionality within networks. Tr. 55:7-10. Like the switches, the routers contain functionality utilized by Cisco to integrate proactive security capabilities within the network.

iii. Cisco's Digital Network Architecture

Cisco's Digital Network Architecture ("DNA") operates as a network management device. Tr. 55:17-21. It operates to configure and troubleshoot problems in the network. Tr. 55:17-21. Therefore, the primary function is to interact and operate routers and switches. Tr. 55:17-21, 147:19-21. DNA may continually provision the routers and switches so they are capable of being used effectively in the operation of the network. Tr. 56:1-7. The DNA device uses advanced artificial intelligence and machine learning to observe past traffic on the network and has the capability to change configuration in the network in real time. Tr. 57:20-25. Accordingly, DNA takes that intelligence, operationalizes it, and turns it into rules and policies that Cisco's switches and routers use for security purposes. Tr. 451:3-24.

iv. Cisco's Stealthwatch

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

v. Cognitive Threat Analytics

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

vi. Identity Services Engine

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

vii. Encrypted Traffic Analytics

Encrypted Traffic Analytics ("ETA") is an element of the new Stealthwatch technology and also is embedded in Cisco's switches and routers. Tr. 61:17-24. ETA deals with the ability to track and analyze encrypted traffic in the network without decrypting said traffic. Tr. 61:19-21. ETA completes this objective by looking at non-encrypted information in the packet (i.e., header information, 5-tuple) in order to track and analyze particular packet flows. Tr. 62:1-5.

viii. Cisco's Firewalls

There are five different firewall products at issue. Tr. 63:10-17. First, there is the Adaptive Security Appliance ("ASA") with Firepower. Tr. 63:10-17. Then, there are the four series of firewalls: the 1000; 2100; 4100; and the 9300. Tr. 63:10-17. These devices are

newly equipped to operate proactively with packet filtering functionality. Tr. 151:23-25.

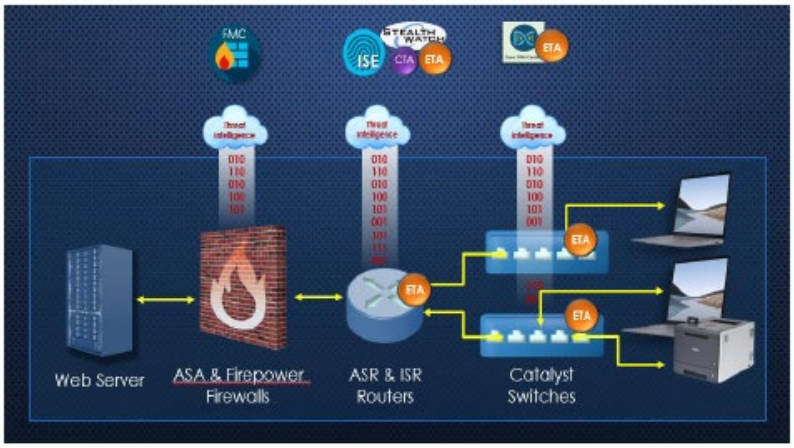
ix. Firepower Management Center

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

x. Complete Picture of a Cisco Network

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

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



A. THE PARTIES

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

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

IV. OVERVIEW OF THE EVIDENCE

As the technology at issue involves important cybersecurity technology, the Court endeavored to accommodate Centripetal's motion for an early trial date. The many requests for inter partes review, by necessity, delayed the trial. The Court, therefore, scheduled a trial on those asserted patent claims for

which such review had not been requested, as well as those which had survived this review process. Both parties' technologies are not only at the forefront in protecting intellectual property and confidential personal information, but also operate in the national defense context. With the rapidly developing technology in the field, the Court found it would not be in the public interest to delay the trial until the unknown time when courtrooms would open for traditional civil trials. Accordingly, the Court first scheduled the trial in April of 2020, then due to the restrictions imposed by the COVID-19 pandemic, finally scheduled it for May 8, 2020, to be heard on a court approved video platform. *See* Doc. 74; 328.

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

In the presentation of its infringement case, Centripetal called its top-level employees in person, Cisco employees by video deposition, and two expert witnesses. Centripetal presented numerous Cisco technical documents and other Cisco publications which postdated the alleged initial infringement date of June 20, 2017. Cisco's own documents from this time frame, and the evidence in general, strongly supported Centripetal's infringement case as to four of the five asserted patents. Therefore, the Court **FINDS**

that the '856 Patent, the '176 Patent, the '193 Patent, and the '806 Patent are valid and directly infringed. Cisco abandoned its claim that the '205 Patent was invalid, but argues that it was not infringed and the Court agrees and so **FINDS**.

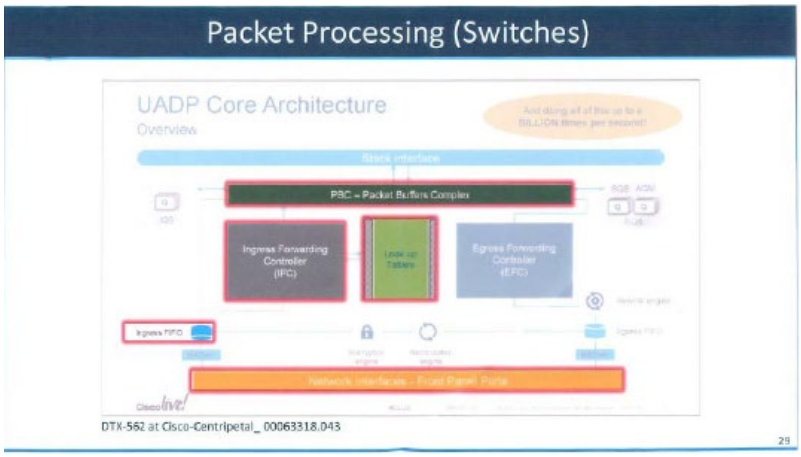
With regard to the infringement and validity claims, Cisco presented different independent experts witness as to each of the four. All four testified that based upon the infringement theories of Centripetal's experts, there was no infringement, but if the Court found infringement, that the asserted patents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

Moreover, Cisco's experts also testified that Cisco's products did not infringe any of the claims of any of the patents at issue, while focusing on distinct

elements of the claims. The testimony of these experts on infringement and validity all focused on old Cisco technology, as did most of the testimony of Cisco's employee witnesses. Cisco's lockstep strategy of denying any infringement of any of the elements of the four claims where infringement is found, and backstopping this position by contending that if the Court found infringement the patents were ipso facto invalid, led to a number of factual conflicts in its presentation of its evidence.

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

SLIDE 29 OF DR. REDDY'S PRESENTATION



> Q. And, Dr. Reddy, I would like to turn to an exhibit that the Court just saw with Mr. Jones. And I think Mr. Jones provided a pretty good explanation of this exhibit, but if

you could just focus on what we've highlighted in red and explain to the Court why that will be relevant to your opinions.

A. Okay. So the highlighted box at the bottom that says, "network interfaces," that's the box to which packets come into the switch, router, or the firewall. And in this example we're only talking about the switch here. And the packet, as it comes through the network interface, goes through the ingress FIFO, FIFO center, first-in-first-out, and from there the packet is moved into the packet buffers complex, on the top, and the header of the packet is given to the ingress forwarding controller, and the ingress forwarding controller consults the lookup tables, compares the packet header information, and makes decision about this packet; whether to allow this packet to go forward or to drop the packet or to take any other action at the level of the lookup table.

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

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

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

A. Yes, I have.

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

A. Okay.

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

THE WITNESS: Yes, Your Honor.

MR. JAMESON: This one here, Your Honor?

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

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

THE COURT: All right. Go on.

BY MR. JAMESON:

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

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

MR. JAMESON: Okay.

BY MR. JAMESON:

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

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

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

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

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

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

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

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

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

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

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

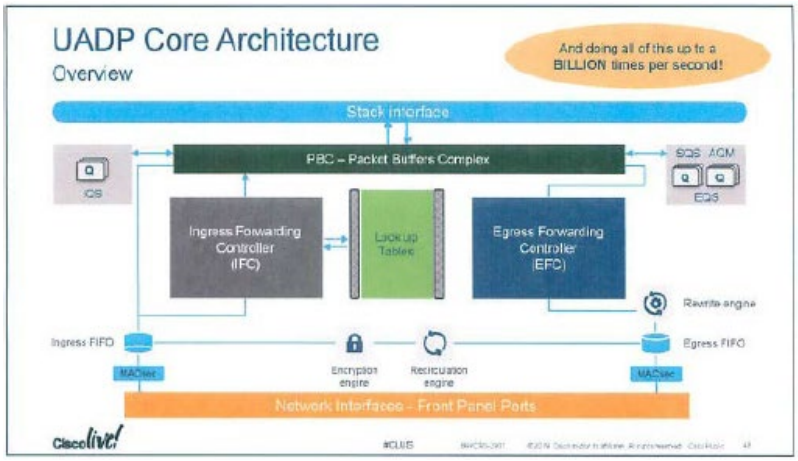
A. No, there is no notion of a cache here. Every packet is taking the same sort of steps. Whether the rule set is being swapped or during the normal course of action, the packets come though the network interface, into the ingress FIFO. From there, the

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

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

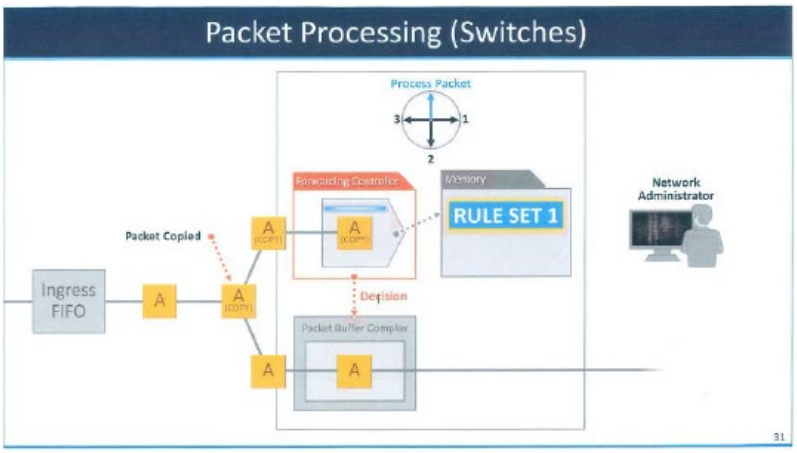
to the '806 Patent. Here is Cisco's technical diagram used by Mr. Jones in his testimony:

DTX-52



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

SLIDE 31 OF DR. REDDY'S PRESENTATION



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

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

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

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

A. THE '856 PATENT

i. Findings of Fact Regarding Infringement

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

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

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

4. Claim 24 is laid out below:

> A packet-filtering system comprising:
>
> at least one hardware processor; and memory storing instructions that when executed by the at least one hardware processor cause the packet-filtering system to:
>
> > receive data indicating a plurality of network-threat indicators, wherein at

least one of the plurality of network-threat indicators comprise a domain name identified as a network threat;

identify packets comprising unencrypted data;

identify packets comprising encrypted data;

determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;

filter, based on at least one of a uniform resource identifier (URI) specified by a plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules:

packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators; and

the determined packets comprising the encrypted data that corresponds to the

> one or more network threat indicators; and
>
> route, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.

JTX-5.

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

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.

---

[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.

Therefore, the '856 Patent deals specifically with Centripetal's threat filtering technology as applied to encrypted packets. Tr. 347:8-9.

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

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

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

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

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

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

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

> 1. **Sequence of Packet Lengths and Times** ("SPLT") – SPLT conveys the length (number of bytes) of each packet's application payload for the first several packets of a flow, along with the interarrival times of those packets.
>
> 2. **Initial Data Packet** ("IDP") – IDP is used to obtain packet data from the first packet of a flow. It allows extraction of interesting data such as an HTTP URL, DNS hostname and address, and other data elements.
>
> 3. **Byte Distribution** – The byte distribution represents the probability that a specific byte

> value appears in the payload of a packet within a flow.
>
> 4. **TLS Specific Features** – The TLS handshake is composed of several messages that contain interesting, unencrypted metadata used to extract data elements, such as cipher suite, TLS version, and the client's public key length.

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

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

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

15. After this determination, representations of information from the unencrypted portion of encrypted packets are sent up to Stealthwatch, which is running both ETA and Cognitive Threat Analytics

("CTA"). Tr. 910:15-911:9; PTX-989 at 033; PTX-578 at 061 (noting ETA "[m]akes the most out of the unencrypted fields" in the packet).

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

17. Using ETA and CTA, Stealthwatch analyzes the NetFlow from the packets and identifies malware threats in encrypted traffic without running any form of standard decryption. Tr. 910:15-911:9, 936:4-20, 941:4-8; PTX-989 at 033; PTX-1010 at 001 (stating Stealthwatch "can detect malware in encrypted traffic without any decryption using **Encrypted Traffic Analytics**.") (emphasis in original); PTX-1009 at 012 (Cognitive Threat Analytics technical release notes illustrating that ETA "[e]nhances existing Stealthwatch/CTA integration with malware detection capability for encrypted traffic without decryption.").

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

using the Global Risk Map to identify known malicious domain data).

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

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

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

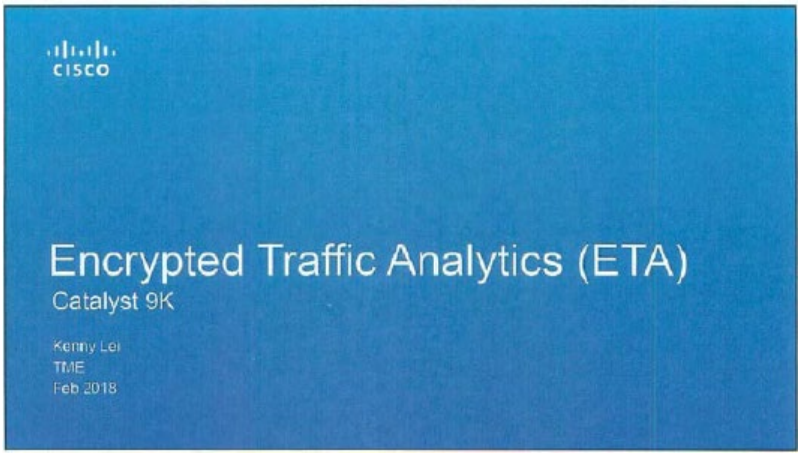
22. After this communication, ISE will provision rules or change of authorizations ("CoAs") to the switches and routers. The switches and routers operate inline and are able to drop incoming packets from the malicious source and outgoing packets containing sensitive data attempting to be exfiltrated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

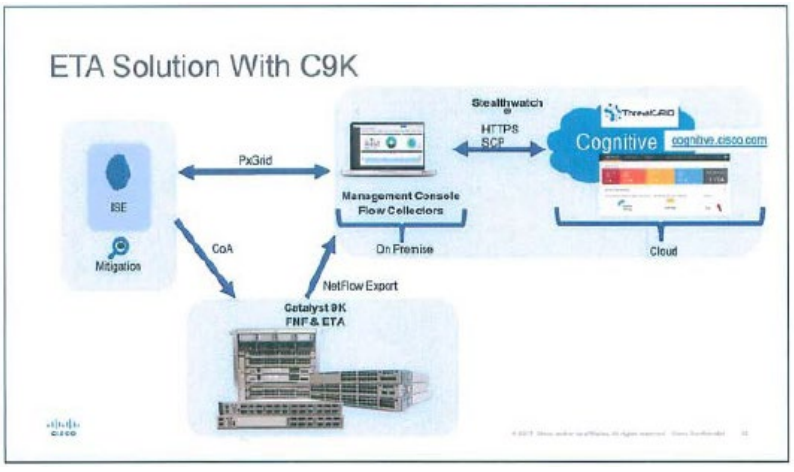
23. Blocked packets are routed to a proxy system, known as a null interface, that is used to drop packet traffic. Tr. 963:24-966:19; PTX-256 at 082,083; *see* Tr. 2199:21-2203:25.

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

PTX-989

CISCO ENCRYPTED TRAFFIC ANALYTICS TECHNICAL PRESENTATION FROM FEBRUARY OF 2018





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

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

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

ii. Conclusions of Law Regarding Infringement

The Federal Circuit has concisely stated that "[i]nfringement analysis is a two-step process: '[f]irst, the court determines the scope and meaning of the patent claims asserted . . . [and secondly,] the properly construed claims are compared to the allegedly infringing device.'" *N. Am. Container, Inc. v. Plastipak Packaging, Inc.*, 415 F.3d 1335, 1344 (Fed. Cir. 2005) (quoting *Cybor Corp. v. FAS Techs., Inc.,* 138 F.3d 1448, 1454 (Fed. Cir. 1998)).

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

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

	locators (URLs), or the like.
Packet security gateway	A gateway computer configured to receive packets and perform a packet transformation function on the packets.
Packets	Plain and ordinary meaning in the context of the claim in which the term appears.
Preambles	Preambles are limiting.
Proxy System	A proxy system which intervenes to prevent threats in communications between devices.
Responsive to correlating	Plain and ordinary meaning.
Rule	A condition or set of conditions that when satisfied cause a specific function to occur.
Security policy management server	A server configured to communicate a dynamic security policy to a packet gateway.

The Court has made one notable change from the previous claim construction order. The Court revises the construction of the term "configured to" from "Plain and ordinary meaning which requires that the

action actually do the function automatically" to "Plain and ordinary meaning which requires that the device be capable of configuring to do the function." *See* Tr. 1646:11-1647:1. This change is made in light of the Court's developing knowledge of the patented technology.

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

Literal infringement requires an accused product to embody each and every limitation of the patented claim. *V-Formation, Inc. v. Benetton Group SpA*, 401 F.3d 1307, 1312 (Fed. Cir. 2005). In contrast, "under the doctrine of equivalents, 'a product or process that

does not literally infringe upon the express terms of a patent claim may nonetheless be found to infringe if there is 'equivalence' between the elements of the accused product or process and the claimed elements of the patented invention.'" *W.L. Gore & Associates, Inc.*, 874 F. Supp. 2d at 541 (quoting *Warner-Jenkinson Co. v. Hilton Davis Chem. Co.,* 520 U.S. 17, 21 (1997)). A finding that the doctrine of equivalents applies requires either that "the difference between the claimed invention and the accused product or method was insubstantial or that the accused product or method performs substantially the same function in substantially the same way with substantially the same result as each claim limitation of the patented product or method." *Id.* (quoting *AquaTex Indus., Inc. v. Techniche Sols.*, 479 F.3d 1320, 1326 (Fed. Cir. 2007)).

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

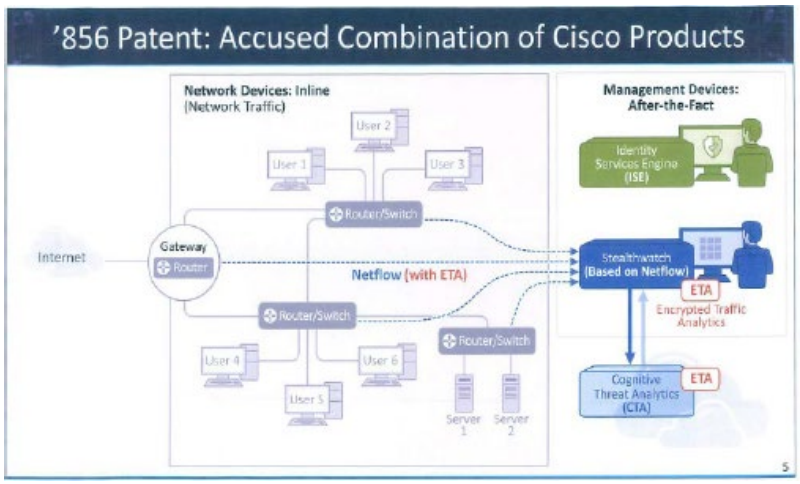
> I was asked to look first at whether or not the accused Cisco product suite infringed the '856 patent. I was also asked to opine on whether the '856 patent was valid relative to the prior art. And I was also asked to assume if, in fact, the patent was valid and the accused products infringed, what damages should be

> assessed, looking at this from a technical point of view of any benefit that the patent provided over what was already known in the prior art.

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

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

SLIDE FIVE OF DR. SCHMIDT PRESENTATION



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

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

Tr. 1815:10-18. Dr. Schmidt indicates throughout his testimony that the new Cisco system is all after the fact analysis and the system "doesn't work on determined packets." In his testimony and on slide

five, Dr. Schmidt opined that after the fact management devices include Identity Service Engine ("ISE"), Stealthwatch (based on NetFlow), and Encrypted Traffic Analytics ("ETA"). He opined:

> Q. The accused systems don't block.
>
> A. Again, don't block, don't block what? What are we talking about?
>
> Q. Don't block malware before it infects the host.
>
> A. I think my testimony this whole time has been that the accused products here, particularly the ones that are the after-the-fact ones, allow the information to go to the destination and then conduct so-called after-the-fact analysis in order to determine what issues have occurred and what remediations to take place.

Tr. 1923:14-23.

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

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

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

A. Uh-huh.

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

A. That's correct.

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

A. That's correct.

. . .

Q. It says, "Helps organizations get 360-degree view of their extended network." Now, what I want to focus on is at the bottom, where it says, "Simplify segmentation throughout your network with centralized control and policy enforcement and address threats faster, both proactively with threat detection and retroactively via advanced forensics." Now, Stealthwatch, working with other products in Cisco's Security Suite, in this case the Identity Services Engine, can proactively protect against threats, correct?

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

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

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

> Q. And you can address threats faster, you can proactively—both proactively with threat detection and retroactively via advanced forensics, correct?
>
> A. That's correct.

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

PTX-584

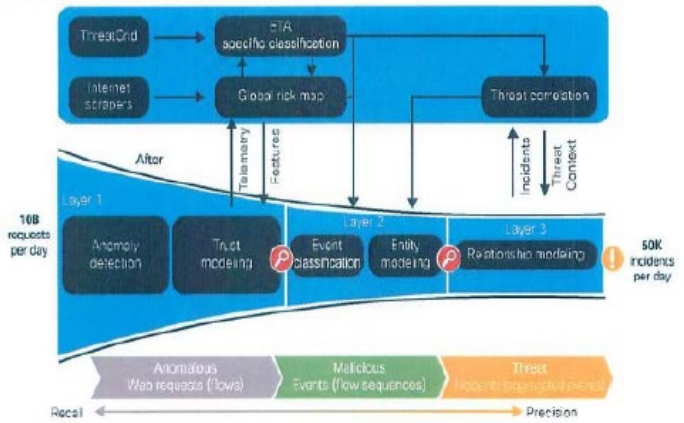
CISCO ENCRYPTED TRAFFIC ANALYTICS TECHNICAL WHITE PAPER FROM 2019

Cisco Stealthwatch

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

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

Figure 3. Stealthwatch multi-layer machine learning

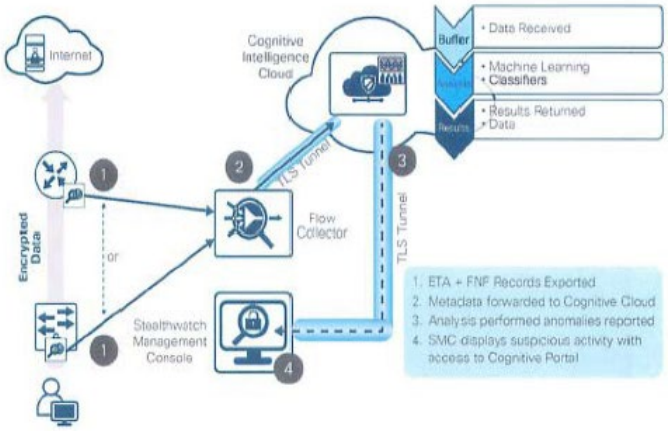


PTX-584 at 402.

PTX-570

CISCO ENCRYPTED TRAFFIC ANALYTICS TECHNICAL DEPLOYMENT GUIDE FROM JULY 2019

Figure 1. ETA malware detection in Cognitive Intelligence cloud



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

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

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

> Q. So we go to 1287. This is a document describing the Catalyst 9000 switch. "Foundation for a New Era of Intent-based Networking." Do you see that, Dr. Schmidt?
>
> A. I do.
>
> Q. Okay. You know Dr. Cole relied on this document in his direct testimony of infringement, correct?
>
> A. I believe so.
>
> Q. Okay. Now if we turn to Page 28 of that document ending in Bates Number 028, there's a graphic at the top here and it talks about the Catalyst 9000 Advanced Security Capabilities. Do you see that?
>
> A. I do.
>
> Q. And you recall Dr. Cole relying on this document, correct?
>
> A. Not particularly, no.
>
> Q. Okay. Well, if you look at the very bottom it says, "Detect and stop threats, exclamation point." Do you see that?
>
> A. I do.
>
> Q. And Dr. Cole used it to show that the Catalyst switches and the routers that have the same operating systems can detect and stop threats prospectively right? Or proactively, correct?
>
> A. I don't believe that that's what it says, no.

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

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

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

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

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

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

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

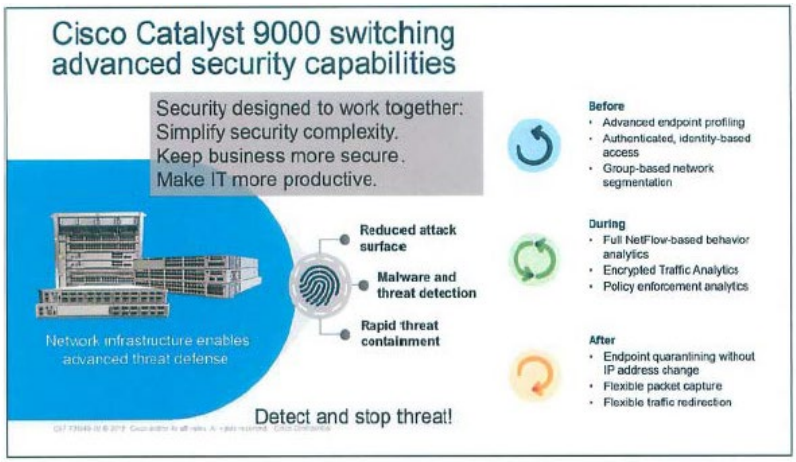
THE WITNESS: It looks like it's saying that—so it looks like it's talking about the fact it's possible to quarantine something, but I don't know how that refers to the—I don't know how that refers to the way in which it reads on the claims and whether what Dr.

> Cole was alleging has anything to do with what the claims are asserting.
>
> BY MR. ANDRE:
>
> Q. So when it says "During", during the packets coming in, Full NetFlow-based behavior analytics, Encrypted Traffic Analytics, Policy Enforcement Analytics. You don't have an understanding of what that's referring to?
>
> A. Again, this particular slide is coming out of thin air here, so I would have to spend a little bit of time looking at it to understand the way it's being used in this particular context.

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

PTX-1287

CISCO CATALYST 9000 SWITCHING TECHNICAL PRESENTATION FROM 2018



It's difficult to comprehend why Dr. Schmidt would state, in his rebuttal of Dr. Cole, that he cannot

understand a Cisco post 2017 document because it is "coming out of thin air." In his preparation for his expert testimony, the Court is unaware how or why he overlooked this crucial Cisco document. Dr. Schmidt, when questioned again about this point, stated:

> Q. When we talk about Stealthwatch, if we go to the next page, you keep talking about this after-the-fact stuff. On that table on the left there it says, "Real-time detection of attacks by immediately detecting malicious connections from the local environment to the Internet." Do you see that?
>
> A. I do.
>
> Q. So does that make you rethink your opinion that the real-time doesn't mean immediately?
>
> A. No, it does not.
>
> Q. So the word "immediately" doesn't mean immediately in that sentence?
>
> A. Again, immediately is always relative to something. We already know that the packets are always delivered to the destination by the time the work goes up, by the time the NetFlow goes up to Stealthwatch and Cognitive Threat Analytics. And so it will detect it as quickly as it can, but it doesn't say, it doesn't say before the packets are delivered to the destination, does it? It says real-time detection of attacks by immediately detecting malicious connections. But there's nothing there about it blocking the traffic, it just says it's detecting it.

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

> THE COURT: Why do you think it says "also" there?
>
> THE WITNESS: I think what it's talking about there, Your Honor, if you take a look, it says "You can determine where else it may have propagated." If you look at the—
>
> THE COURT: Do you think maybe it means you can do the things in the first two sentences and also do the thing in the third sentence? Do you think that's what "also" means?

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

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

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

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

> Q. And you actually cited to the specification to show that a proxy system, the analysis had to actually decrypt, correct? You said that this claim requires decryption. Do you recall that?
>
> A. I do.
>
> Q. All right. So let's go back to the patent. Column 10, line 15. 15 to 20. Now, this is the

point that's part of the specification you pointed to. Proxy device may receive the packet and decrypt the data in accordance with the parameters as in session 306. Do you see that?

A. I do.

Q. And you took that to mean that it must decrypt the data in accordance with the parameters, correct? Not that it may, that it must.

A. Well, so to be consistent, there's quite a number of places in columns, basically 8 through 12, where they talk about the role of proxy device, 112, which is the part here. And when they talk about proxy device 112, they're talking about it in the context, going back to figure 3B, where there is a SSL/TLS session set up that involves sending encrypted packets. And whenever they talk about it in all those different places in columns 8, 9, 10, 11, and 12, they always make it clear that proxy device 12 [sic] receives packets that are encrypted packets and then decrypts them, and then sends the unencrypted data to what they call the man in the middle RuleGate, which is RuleGate 124. And RuleGate 124 then, as it talks about just a little bit further down in the specification, it talks about actually doing the filtering. And it talks about filtering based on the URI, they talk about filtering based on the request, on the method, on the command and so on. And then right after that it talks

about how RuleGate 124 sends that information, which at that point is still decrypted—because of course we couldn't be analyzing it unless it was decrypted—it then sends it to proxy device 114. And as you read in the spec, it makes it very clear that proxy device 114 then re-encrypts the data and sends it on to the destination. So in all the cases where proxy system is disclosed—and like I said, there are three or four of them in the specification—it's always talked about in the context of receiving encrypted data and then proxy device 112 will decrypt it and then pass it on in some way. So those are the ways that proxy system are—proxy system is used in the spec. So that's where I come up with the reasoning that, A, proxy system is involving decryption and encryption, because it says so very clearly in the specification, and then reading claims F, F1 and F2, it's very clear that the analysis that's done to the filtering, for the most part can't be done unless the packets are decrypted.

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

BY MR. ANDRE:

Q. Okay. So I looked at this entire patent. I did a word search. The word "decrypt" shows

up one time in this entire patent. One single time. And it's right there.

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

Q. Doctor, you just said that—

A. —appears in multiple places.

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

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

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

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

Q. You just said that.

A. Well, that's not what I'm saying. What I'm saying here is very clear: The patent spec talks repeatedly, especially in reference to

> figure 3B, where information is being received from, I believe it's on session 306, I think it's from host 108, if I'm not mistaken, and that information is coming in over an encrypted session. And it makes it very clear in the patent spec that this is an encrypted session. And then it says proxy device 112 receives the encrypted data and then either decrypts it or they sometimes say then send on unencrypted data.
>
> . . .
>
> Q. Is there ever a disclosure of the proxy system in the specification that doesn't do any analysis at all; that just drops without first doing analysis?
>
> A. No.
>
> Q. And a null interface, does it do any analysis at all before it drops a packet?
>
> A. No, it does not.

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

> 5 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 con-
>
> figured 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 cor-

responding to the network-threat indicators, for example, by

correlating the packets with one or more packets previously

determined by packet-filtering system **200** to comprise data

corresponding to the network-threat indicators based on data

stored in logs **214** (e.g., log data generated by packet-

filtering system **200** in one or more of steps **#6, #7, #12,** or

#13), and one or more of log or drop the packets.

Responsive to receiving the packets from proxy device

114, host **142** may generate packets comprising data con-

Figured to establish the connection between proxy device

114 and host **142** (e.g., a TCP:SYN-ACK handshake mes-

sage) 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 previ-

ously determined by packet-filtering system **200** to comprise

data corresponding to the network-threat indicators based on

data stored in logs **214** (e.g., log data generated by packet-

filtering system **200** in one or more of step #s **6, 7, or 12-14),**

and one or more of log or drop the packets.

Responsive to receiving the packets from host **142,** proxy

device **114** may generate packets comprising data configured

to establish the connection between proxy device **114** and

host **142** (e.g., a TCP:ACK handshake message) and, at step

#16, may communicate the packets to host **142.** Rules **212**

may be configured to cause rule gate **128** to one or more of

identify the packets, determine (e.g., based on one or more

network addresses included in their network-layer headers)

that the packets comprise data corresponding to the network-

threat indicators, for example, by correlating the packets

with one or more packets previously determined by packet-

filtering system 200 to comprise data corresponding to the

network-threat indicators based on data stored in logs **214**

(e.g., log data generated by packet-filtering system **200** in

one or more of step #s **6, 7, or 12-15),** and one or more of

log or drop the packets.

> Referring to FIG. **3B,** proxy device **112** may receive the
>
> packets comprising data configured to establish the connection
>
> between proxy device **112** and host **106** communicated
>
> by host **106** in step **#14,** and connection **302** (e.g., a TCP
>
> connection) between proxy device **112** and host **106** may be
>
> established. Similarly, host **142** may receive the packets
>
> comprising data configured to establish the connection
>
> between proxy device **114** and host **142** communicated by
>
> proxy device **114** in step **#16,** and connection **304** (e.g., a
>
> TCP connection) between proxy device **114** and host **142**
>
> may be established.

JTX-5 at 724. Columns 9-12 of the specification all contain the same alternate phrase "or drop the packets." In fact, there is at least one mention of "or drop the packets" in each of columns 8-23 of the specification. These multiple references directly contradict Dr. Schmidt. Therefore, it is abundantly evident that Cisco's null interface serves as a proxy system because it prevents threats in communications between devices, and this type of dropping of packets is shown by the specification to be an alternative to

the further analysis of the packets. Therefore, the Patent does not require decryption as "or drop the packets" is already identified as an alternative.

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

The Stealthwatch user interface known as the Stealthwatch Management Console ("SMC") "provides a view of affected users identified by risk type." Tr. 1920:20-22 (Dr. Schmidt confirming that Stealthwatch may provide alarms and alerts based on views within Stealthwatch), 2205:25-2206:4 (Mr. Llewallyn, a Cisco engineer, confirming Stealthwatch triggers alerts). The SMC allows for the representation of packets currently being processed within the network to be filtered and ordered by

information within the unencrypted part of the packet such as protocol version, server name or domain name. Tr. 951:16-20; PTX-570 at 640. Dr. Cole highlights that this process meets the filter element because the Cisco system can identify and filter flows of packets that use certain versions of protocols that may be more vulnerable to malware incorporation. Tr. 953:22-954:2. For example, an outdated version 1.0 of a specific protocol such as TCP may be more vulnerable to be infected with malware than an updated and more secure version 2.0. *See* Tr. 953:22-955:24; *see* PTX-570 at 640. The Cisco system is able to filter the flows of packets to visualize outdated versions and filter flows based on outdated and vulnerable protocol versions. *See* Tr. 953:22-955:24. Seeing those packet flows, the system responds by implementing rules based solely on blocking an older protocol that may leave the network open to attack. Tr. 953:22-954:2, 2202:5-25 (Mr. Llewallyn highlighting that Stealthwatch and ISE can send rules to routers and switches based on identified packet information such as protocol). Additionally, besides protocol version, Stealthwatch can perform this filtering based on server name, a component embedded within a Uniform Resource Identifier ("URI"). Tr. 957:12-21; *see* PTX-996 at 005 (noting that server name is part of the Initial Data Packet sent up in a Flow Record to Stealthwatch). URI, like protocol version, can be used to design rules that prevent the exfiltration of packets to that identified destination server. Accordingly, Cisco's technical documents, as well as its own engineers, confirm that the Cisco system filters packets as required by the asserted claims of the '856 Patent.

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

iii. Findings of Fact Regarding Validity

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

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

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

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

32. The technical documents for the old Stealthwatch system contain no mention of the ability of determining network threat indicators with respect to encrypted packets or analyzing data with respect to

the unencrypted portion of encrypted packets, as it did not possess the functionality to determine what portion of the packets are unencrypted or encrypted. Tr. 3111:2-25.

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

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

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

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

iv. Conclusions of Law Regarding Validity

Patents and their claims are presumed to be valid. 35 U.S.C. § 282(a). This presumption may be rebutted by clear and convincing evidence that the patent at

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

Starting first with anticipation, in order to anticipate a claim, "a single prior art reference must expressly or inherently disclose each claim limitation." *Finisar Corp. v. DirecTV Group, Inc.*, 523 F.3d 1323, 1334 (Fed. Cir. 2008). This disclosure must go beyond a mere mention of each claim limitation, as anticipation "requires the presence in a single prior art disclosure of all elements of a claimed invention arranged as in the claim." *Id.* (emphasis in original).

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

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

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

PTX-1417 at 107. Dr. Schmidt's testimony on the Catalyst 9000 switches confirmed this technical

statement that the prior art system employed by Cisco, before ETA, required some form of decryption to detect threats in encrypted traffic. He testified:

> Q. Okay. Well, why don't we turn to Page Bates No. 107 of this document. I want to turn your attention to the second—this is talking about the Encrypted Traffic Analytics on the Catalyst switches. I want to turn your attention to the second paragraph. It states "Before the introduction of the Catalyst 9000 series, detecting attacks that hide inside encrypted sessions required unwieldy and expensive measures. In short, it meant installing decryption hardware in the middle of encryption flows." Do you see that?
>
> A. I do.
>
> Q. And you agree with that statement that's in the Catalyst manual?
>
> A. I think that's referring—I think that's contrasting the so-called inline systems which I believe the '856 patent to be focusing on with the after-the-fact analysis that they're talking about here. Because if you look, **"In short, it means installing decryption hardware in the middle of encrypted flows." I believe that's what a firewall does and that's what the prior art Cisco Systems did, and that's also of course what the '856 patent covers.**

Tr. 2100:24-2101:18 (emphasis added). Dr. Schmidt stated that he accepted Dr. Cole's construction of the claims to find that the prior art system performs all of the infringing functionality. Based on this testimony,

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

The technical documents confirm that Cisco represented it had solved the problems of expensive decryption by delivering "Encrypted Traffic Analytics (ETA) on Catalyst 9000 switches. ETA identifies malware communications in encrypted traffic via passive monitoring: no extra equipment is required and unnatural traffic redirection need not be performed." PTX-1417 at 107. Cisco completed malware identification in encrypted traffic by "ETA introducing new flow metadata to help it identify malicious activity hiding within an encrypted flow." PTX-1417 at 107. Cisco, through ETA, added both the "Initial Data Packer (IDP) and the Sequence of Packet Length and Times (SPLT)" to its use of NetFlow. PTX-1417 at 107. ETA was incorporated into all of the accused products in order to implement the functionality of detecting threats in encrypted traffic by using unencrypted portions of those packets. When asked about the functionality employed in the old

Stealthwatch technology, Dr. Schmidt asserted that the 2013 version of Stealthwatch was able to detect and stop threats in encrypted traffic without decryption:

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

Tr. 2110:17-2111-7 (emphasis added). This opinion is directly refuted by Dr. Schmidt's own prior testimony, Tr. 2100:24-2101:18, as well as the technical documents that describe the functionality of Stealthwatch. PTX-383, a Stealthwatch technical guide from 2018, incorporated language that the 2017 ETA solution enabled Stealthwatch as the "first and

only solution in the industry that can detect malware in encrypted traffic without any decryption using Encrypted Traffic Analytics." PTX-383 at 355. Dr. Schmidt continually attempts to characterize the ETA solution as enhancing previously existing technology to identify threats in encrypted traffic but cites to no Cisco documents pre-2017 showing that the older Stealthwatch system had the capability to do the same functionality as the ETA solution. The only technical documents that confirm this functionality are from later than the priority date of the '856 Patent. In this manner, the technical documents affirm that the infringing functionality was added after the priority date of the '856 Patent.

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

The Network

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 Goeckeler, senior vice president and general manager of networking and security. "ETA uses Cisco's Talos cyber intelligence to detect known attack signatures even in encrypted traffic, helping to ensure security while maintaining privacy."

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

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

Informed by context and powered by intent

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

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

The technologies that power the intuitive network

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

newsroom.cisco.com/press-release-content?type=webcontent&articleId=1854555 1/6

CENTRIPETAL-CSCO 472946

Dr. Schmidt testified to his characterization of these press releases:

> Q. But is it your testimony that Cognitive Threat Analytics was on Stealthwatch in 2013?

A. It was my testimony that Stealthwatch was capable of doing behavioral analytics, enabling it to be able to detect encrypted threat—encrypted threats—or threats in encrypted traffic without requiring decryption. That was my testimony when I talked yesterday.

Q. So all these testimony we, all this, the press releases, the documents about Encrypted Traffic Analytics, that's just all marketing puff; it was really not true, they could do it way before then, right?

A. I didn't say it was marketing puff, I said that the capabilities that were added with ETA, Encrypted Traffic Analytics, were very valuable, and the value came from the additional machine learning insights and classification capabilities that were added at that time frame. It was, in fact, possible for them to do it before that, but they were able to do it better now because they've added these additional capabilities.

Q. So when they said they solved the unsolvable problem, they had it solved years before, right?

A. Well, we don't know what the unsolvable problem is from that quote. It could very well have been solving it more precisely or solving it more efficiently or solving it more thoroughly. So the insurmountable or unsolvable problem, I never saw an actual definition of that term, so I'm simply assuming that what they meant was they

> could do a much better job now that they added these enhancements, but that in no way, shape or form means they couldn't do a good job before.

Tr. 2105:1-2106:4. This characterization by Dr. Schmidt of Cisco's language of "solving the unsolvable problem" as simply an improvement of a previous functionality is insupportable when compared with the technical documents. For all these reasons, Cisco has failed to present clear and convincing evidence that the '856 Patent is invalid for anticipation or obviousness. The prior art does not disclose the functionality to identify encrypted packets and then make determinations based on unencrypted information within those packet headers and flows.

The Court now turns to Cisco's written description argument. To meet the written description requirement, the patentee "must 'convey with reasonable clarity to those skilled in the art that, as of the filing date sought, he or she was in possession of the invention,' and demonstrate that by disclosure in the specification of the patent." *Idenix Pharms. LLC v. Gilead Scis. Inc.*, 941 F.3d 1149, 1163 (Fed. Cir. 2019) (quoting *Carnegie Mellon Univ. v. Hoffmann-La Roche Inc.,* 541 F.3d 1115, 1122 (Fed. Cir. 2008)); *see Hynix Semiconductor Inc. v. Rambus Inc.*, 645 F.3d 1336, 1351 (Fed. Cir. 2011); *Ariad Pharms., Inc. v. Eli Lilly & Co.,* 598 F.3d 1336, 1351 (Fed. Cir. 2010). The hallmark of the written description test is disclosure. Ariad, 598 F.3d at 1351. Therefore, the "test requires an objective inquiry into the four corners of the specification from the perspective of a person of

ordinary skill in the art." *Id.*; *see Idenix*, 941 F.3d at 1163.

Dr. Schmidt contends that the '856 Patent specification does not disclose any type NetFlow invention and, therefore, the claims fail for lack of written description. He opined that if the claims are infringed for filtering representation of packets, then the Patent is invalid for lack of written description because there is no disclosure of this type of scenario within the specification. Tr. 2067:6-25. The Court disagrees with Dr. Schmidt's conclusion. The specification specifically contains language that a "Packet-filtering system may be configured to correlate packets identified by the packet-filtering system with packets previously identified by packet-filtering system based on data stored in logs." JTX-5 col. 5 ln. 25-30. The specification continues to mention that:

> For example, for one or more packets logged by packet-
>
> Filtering system 200 (e.g., the packets comprising the DNS
>
> query or the packets comprising the reply to the DNS query),
>
> logs 214 may comprise one or more entries indicating one or
>
> more of network-layer information (e.g., information
>
> derived from one or more network-layer header fields of the
>
> packets, such as a protocol type, a destination network

address, a source network address, a signature or authentication

information (e.g., information from an Internet protocol

security (IPsec) encapsulating security payload (ESP)),

or the like), transport-layer information (e.g., a destination

port, a source port, a checksum or similar data (e.g., error

detection or correction values, such as those utilized by the

transmission control protocol (TCP) or the user datagram

protocol (UDP)), or the like), application-layer information

(e.g., information derived from one or more application-

Layer header fields of the packets, such as a domain name, a

uniform resource locator (URL), a uniform resource ident-

ifier (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

55 with but not solely derived from the packets themselves,

such as one or more arrival (or receipt) or departure (or

transmission) times of the packets . . .

JTX-5 col. 5 ln. 31-56; *see* Tr. 3144:3-21. This section of the specification clearly illustrates the '856 Patent invention discloses the logging of certain information from the packets by the packet filtering system. Dr. Jaegar confirmed that viewing this section of the specification as a person skilled in the art would disclose the information required to be used by the packet filtering system. Tr. 3144:3-21. This is the exact type of network information that is contained in NetFlow records. Therefore, looking at the four corners of the '856 Patent's specification, it is evident to a person skilled in the art that the '856 Patent made the required disclosure of the logging of information from packets to be used by the packet filtering system.

Accordingly, the Court **FINDS** that Cisco has not proven by clear and convincing evidence that the '856 Patent was anticipated, obvious or lacked adequate written description.

B. THE '176 PATENT

i. Findings of Fact Regarding Infringement

1. The '176 Patent has been informally known as the "Correlation" Patent.

2. The '176 Patent was issued on January 31, 2017. JTX-3. The '176 Patent was filed on May 15, 2015 as a continuation of application No.14/618,967, giving the '176 Patent a priority date of February 10, 2015. JTX-3.

3. The asserted claims of the '176 Patent are Claim 11 and Claim 21. Doc. 411. Claim 11 and Claim 21 are, respectively, a system and computer readable media claim.

4. Claim 11 is laid out below:

A system comprising:

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

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

5. Claim 11 is identical to Claim 21 in every respect except that Claim 21 is a computer readable media claim. Tr. 885:14-24. Claim 21 modifies the introductory preamble language of Claim 11 replacing "[a] system comprising: at least one processor; and a memory storing instructions that when executed by the at least one processor cause the system to:" with "[o]ne or more non-transitory computer-readable media comprising instructions that when executed by a computing system cause the computing system to:".

JTX-3. For purposes of infringement, the parties have treated the two claims as identical.

6. Dr. Moore, an inventor of the '176 Patent, describes the technology of the '176 Patent as the development of a system for identifying malware-infected computers through use of correlation. Tr. 341:3-15.

7. A single communication between two computers on different networks is often broken down into many different segments of packets. Tr. 340:20-341:2. These segments are compared to ascertain if they are a part of the same communications and then the system can make a determination that a computer within the network has been communicating with a computer of a cybercriminal. Tr. 341:3-15. Therefore, the correlation technology in the '176 Patent serves as a method to identify computers in a network that have been infected with malware. Tr. 341:18-19.

8. Centripetal accuses Cisco's Catalyst 9000 series switches, the Aggregation Services Router 1000 series routers and Integration Services Router 1000 and 4000 series routers in combination with Cisco's Stealthwatch of infringing Claims 11 and 21 of the '176 Patent. Tr. 975:19-21.

9. The accused Cisco's switches and routers share the same operating system known as IOS XE. Tr. 448:11-24; 449:19-450:4; PTX-242 at 816, 817.

10. The accused switches and routers contain processors and memory that stores software instructions. Tr. 477:12-478:14, 484:13-485:3; PTX-1303 at 056.

11. The accused Cisco switches and routers contain processors that function to transmit packets across different external and internal networks. Tr. 977:18-21.

12. Cisco has utilized its own proprietary packet logging technology known as NetFlow. Tr. 983:18-25; PTX-1060 at 008.

13. As packets are transmitted, the accused switches and routers generate NetFlow logs, which are summaries of information from the transmitted packets. Tr. 977:18-25; 984:7-13; PTX-1060 at 008. NetFlow includes information such as the source and destination IP address, the source and destination port, and the protocol being used. Tr. 984:7-13; PTX-1060 at 008.

14. The accused switches and routers are capable of generating NetFlow records for packets at both the ingress of the packet into the device and on egress out of the device. Tr. 986:18-987:1; PTX-1060 at 023 (showing that the Catalyst 9400 switch is capable of supporting 384,000 NetFlow entries—192,000 on ingress and 192,000 on egress); PTX-572 at 762; *see* Tr. 988:12-22 (Dr. Cole explaining PTX-572 showing "When you configure a flow record, you are telling the device to show all of the flow data traffic that enters"—which is ingress—"or leaves"—egress—"the device.").

15. These NetFlow records are sent up to Stealthwatch, which by 2018 was embedded with Cognitive Threat Analytics (CTA) that digests the information from the ingress and egress NetFlow records. PTX-1009 at 009; Tr. 1009:3-14. The new Stealthwatch with CTA also has the functionality to be sent data from proxy sources using another type of

logging called Syslog. PTX-1065 at 005; Tr. 1115:4-116:13 (noting the Stealthwatch "solution uses the Proxy ingestion feature to consume Syslog information . . .") Customers may use either NetFlow or Syslog data or both within Stealthwatch. PTX-1065 at 005.

16. Stealthwatch correlates NetFlow and/or Syslog information sent by devices on the network and correlates the information to provide a detailed overview of all traffic that is occurring on the network. PTX-1065 at 005. CTA, working within Stealthwatch, can leverage the correlations of NetFlow telemetry to detect malicious threats to the security of the network. PTX-1009 at 009; PTX-591 at 522 (using identical language to PTX-1009 in the Stealthwatch Release Notes); *see* Tr. 997 at 7-12 ("'telemetry' is just another word for the NetFlow log information. So the NetFlow telemetry, the NetFlow logs, these are all synonymous terms, so this is another way of referring to logs").

17. In response to these correlations, Stealthwatch creates a baseline of normal traffic behavior within the network. Based on these normal patterns and known threat indicators, Stealthwatch employs a funnel of analytical techniques to detect advanced threats. PTX-569 at 272; PTX-584 at 402.

18. Stealthwatch, in response to suspicious activity or threats, allows the Identity Services Engine or Stealthwatch Management Console to provision rules to proactively stop that threat. Tr. 1002:13-1003:21; PTX-1089 (showing the use of the Adaptive Network Control ("ANC") to implement rules). The ANC operates by applying new policies and changing individual user's authorization on the network

according to rules and policies configured by the Identity Services Engine in response to correlated threats on the network. PTX-595 at 179; Tr. 1005:10-19. Both the Identity Services Engine and the Stealthwatch Management Console operate in this fashion. Tr. 1006:19-1007:5. PTX-989.

ii. Conclusions of Law Regarding Infringement

Based on the Court's factual findings, Centripetal has proven by a preponderance of the evidence that Cisco's Catalyst 9000 series switches, the Aggregation Services Router 1000 series routers and Integration Services Router 1000 and 4000 series routers in combination with Cisco's Stealthwatch literally **INFRINGE** Claims 11 and 21 of the '176 Patent. Cisco's expert on the '176 Patent, Dr. Kevin Almeroth:

> was asked to offer opinions, after performing an analysis, on noninfringement as it related specifically to the '176 patent; similarly, to offer opinions about whether or not the '176 patent was valid; and then several additional opinions relating to the benefits of the patent, technical issues related to damages, and then also copying, to the extent it still exists in this trial.

Tr. 2212:12-18. Dr. Almeroth advanced two non-infringement theories. Tr. 2239:17-2240:14. First, that the accused system does not correlate a plurality of transmitted packets with a plurality of received packets as required by the asserted claims of the '176 Patent. Tr. 2247:18-2248:4. Second, that the accused system does not generate and provision rules in response to those claimed correlations. Tr. 2247:18-2248:4.

Turning to the first theory, Dr. Almeroth opined that Dr. Cole's infringement opinion relied on the systems' use of logs provided by Cisco's proprietary logging technology, NetFlow, as the logs outlined by the claim language. Dr. Almeroth construed the claims to require identification and generation of logs out of the same network device on ingress and egress. Therefore, Dr. Almeroth avers that the Cisco system cannot infringe, because in his opinion, the accused switches and routers do not generate NetFlow on both ingress into a device and egress out of one network device. Tr. 2249:4-18. Cisco's technical documents refute Dr. Almeroth's conclusion.

Dr. Cole pointed directly to PTX-1060, a Cisco technical document dated December of 2017, showing that the Catalyst switches have the ability to export NetFlow on ingress and egress. Tr. 986:18-987:1; PTX-1060 at 023 (showing that the Catalyst 9400 switch is capable of supporting 384,000 NetFlow entries—192,000 on ingress and 192,000 on egress). Dr. Almeroth, on cross-examination, even admitted that the accused switches and routers can be configured to export ingress and egress NetFlow.

> Q. Isn't it correct, Dr. Almeroth, that this Cisco document says right here that MPLS Egress and NetFlow Accounting feature can be used—being use to capture ingress and egress flow statistics for router B, one device. Is that correct?
>
> A. That's what it says. But my last answer was qualified for Stealthwatch. This document, at least what you're pointing me to here, does not mention Stealthwatch. And

> that was really my whole point: That you can certainly configure NetFlow ingress and egress, but when you get to troubleshooting Stealthwatch, it's considered an error within Stealthwatch.

Tr. 2286:10-19. In this exchange, Dr. Almeroth confirms that NetFlow can be configured on ingress and egress but shifts the crux of his non-infringement opinion to the fact that Stealthwatch produces an error based on producing both types of NetFlow. To support that claim, Dr. Almeroth relied solely on the presentation of source code from the 6.5.4 version of Stealthwatch that operated without enhanced NetFlow or the integration of Cognitive Threat Analytics (CTA). Tr. 2287:1-19; see DTX-1616 (showing source code from a previous 6.5.4 version of Stealthwatch that is not accused by Centripetal). He cites to no technical document that confirms that the accused/current version of Stealthwatch produces an error when exporting both ingress and egress NetFlow. In fact, the technical release notes for CTA, which was incorporated into Stealthwatch in 2018, support that CTA produced the ability for the correlation of NetFlow telemetry. PTX-1009 at 009.

Dr. Cole, in his infringement opinion on the "identify and generate" elements, relied on a similar claim scope as Dr. Almeroth to show that the claims required that one network device generate logs on a packets' ingress and egress out of the device. Moreover, Dr. Cole does not explicitly limit his construction of the asserted claims to the limitation of only ingress and egress out of one device. The Court **FINDS**, based on the testimony and technical

documents, that the accused switches and routers do identify and generate logs on ingress and egress. However, a look at the specification of the '176 Patent informs the Court that this is not the only construction that would infringe the asserted claims. These claim elements would also be met if there was identification, generation and correlation of logs from two different network devices on either ingress or egress. Column 8 line 46 of the specification highlights that:

> At step **16,** packet correlator **128** may utilize log(s) **142** to
>
> correlate the packets transmitted by network device(s) **122**
>
> with the packets received by network device(s) **122.** For
>
> example, packet correlator **128** may compare data in entry
>
> **306** with data in entry **312** (e.g., network-layer information,
>
> transport-layer information, application-layer information,
>
> or environmental variable(s)) to correlate **Pl'** with **Pl** (e.g.,
>
> by determining that a portion of the data in entry **306**
>
> corresponds with data in entry **312).** Similarly, packet cor-
>
> relator **128** may compare data in entry **308** with data in entry
>
> **314** to correlate **P2'** with **P2,** packet correlator **128** may

> compare data in entry **310** with data in entry **316** to correlate
>
> **P3'** with **P3,** packet correlator **128** may compare data in entry
>
> **318** with data in entry **324** to correlate **P4'** with **P4,** packet
>
> correlator **128** may compare data in entry **320** with data in
>
> entry **326** to correlate **PS'** with **PS,** and packet correlator **128**
>
> may compare data in entry **322** with data in entry **328** to
>
> correlate **P6'** with **P6.**

JTX-3 col. 8 ln. 46-63. This section of the specification indicates that the network device that generates the correlated logsmay be plural as well as singular. Additionally, this section is showing the correlation may occur between data entries that were processed through two different network devices. *Compare* JTX-3 col. 8 ln. 46-63 *with* JTX-3 Fig. 3. Dr. Almeroth, on cross examination, confirms that the use of "a network device" in the claim language may mean more than one network device:

> Q. And then you said this had to be a single network device, correct?
>
> A. Not quite. It says a network device here, and then later it's the network device. So it's the same network device across the limitations.

> Q. But you do understand that in a patent, when it says A, it can mean one or more; is that correct?
>
> A. That's my understanding.
>
> Q. So this could be more than one network device, correct?
>
> A. It could be.

Tr. 2278:11-20. Therefore, even if the Court were to accept Dr. Almeroth's conclusion that the accused devices do not process ingress and egress out of the same device, it would still find infringement on the basis that the Cisco system correlates logs between multiple devices within the network on either ingress or egress.

Moreover, Dr. Almeroth states that the accused system does not generate and provision rules in response to correlation performed as a result of Stealthwatch and CTA. Dr. Almeroth admits that Stealthwatch with CTA performs correlations, just not those required by the claim language. In explaining the diagram of PTX-1065, Dr. Almeroth opined:

> Q. Can you explain what's going on here, Dr. Almeroth?
>
> A. Yes. What's being shown here, if you start in the bottom, it shows two different sources of information that ultimately get correlated. There's proxy data and there's NetFlow data. And when Dr. Cole testified, he represented that that NetFlow data included ingress and egress records from the same device, which was actually not the case, as the evidence and the correct operation of the devices show. And

then from there, his analysis principally turned on the fact that these documents describe correlation. They absolutely use the word correlation, but it's not the correlation of the type required by the claims. And the example that's shown in this particular figure and what's described in the text below is that you're correlating NetFlow data, which is not the NetFlow data required by the claim for the reasons I've given, with other data. In this case, proxy data. And so even though these documents use the word correlate, what they're correlating is not the kind of correlation that's required by the claims.

Q. Okay. And if we look, Mr. Simons, at the text below?

BY MR. JAMESON:

Q. And I don't want to go through all of this, but is the same point made in the text below with respect to the comments you made, about the diagram?

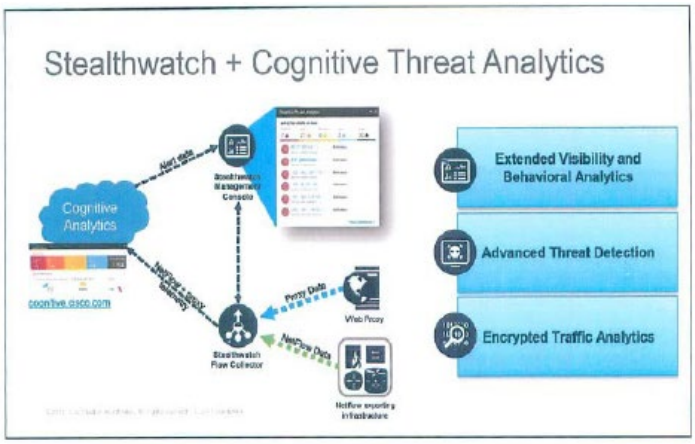
A. Yes. It's absolutely the case that Stealthwatch correlates I think what we've referred to as threat intelligence with NetFlow records. But what it is not comparing, what it is not correlating is it's not correlating the NetFlow records to themselves as required by the elements of the claims, because it tries to block or double count those NetFlow records. And so all of this evidence that Dr. Cole relied on that uses the word correlate, over and over again it describes correlation of threat intelligence

> with NetFlow data, which is not what the claim requires and also is not what the '176 patent is about.

Tr. 2256:3-2257:10.

PTX-1065

Cisco Technical Presentation Involving Operation of Stealthwatch in Combination with CTA in November 2017



Stealthwatch integrates with Cognitive Analytics ("CA" – aka Cognitive Threat Analytics). This involves the addition of a new information panel on the SMC's WebUI, and enhances Stealthwatch further by leveraging CA's cloud based analytics engine, that correlates threat behaviors seen in the enterprise with those seen globally. It uses machine learning and statistical modeling to learn from what it sees and adapt to changing network behavior over time.

The Court agrees with Dr. Almeroth's assessment that Stealthwatch correlates NetFlow and Syslog information with global threat indicators. PTX-202 states that Stealthwatch "correlates local traffic models with global threat behaviors to give you rich threat context around network traffic . . . and applies encrypted traffic analytics to enhance NetFlow analysis." PTX-202 at 242. Therefore, it is clear that Stealthwatch uses the NetFlow information within

the network to correlate those records to global threat indicators. However, this is not the only use of correlation that Stealthwatch uses in its operation. In order to make use of behavioral analytics, Stealthwatch correlates NetFlow that passes through network devices to create a baseline of normal types of traffic that would pass through the network. This correlation occurs between both NetFlow and other logs provided to Stealthwatch in the form of WebFlow telemetry through the use of Syslog. Therefore, along with matching threats to global threat indicators, Stealthwatch can also detect threats based on abnormal activity that occurs within the network. For example, a large amount of data being transported throughout the network at a time where an office is closed or not conducting business would send up an alert that something malicious may be afoot.

Cisco's technical guide for configuring Netflow and Stealthwatch, PTX-569, illustrates how Stealthwatch "[c]reates a baseline of normal behavior" and "correlates threat behaviors seen in the local environment with those seen globally."

PTX-569

Cisco Technical Guide for Configuring and Troubleshooting NetFlow for Cisco Stealthwatch from 2018*

Doc type
Cisco public

Stealthwatch Enterprise also integrates with a cloud based multi-stage machine learning analytics engine, that correlates threat behaviors seen in the local environment with those seen globally. It employs a funnel of analytical techniques to detect advanced threats.

Figure 3: Detect anomalies and threats

For more information about the Stealthwatch components and architecture, please refer to the Stealthwatch Enterprise Data Sheet.

*The heading in the bule box above states 'Collect and analyze telemetry'.

PTX-569 at 272. This process would require Stealthwatch to correlate NetFlow within the network between multiple devices in order to recognize normal traffic patterns within the network.

Accordingly, it is axiomatic that Stealthwatch could then provision rules to stop threats that are detected based on internal network NetFlow correlation with or without global threat indicators. PTX-595 at 179. Therefore, the Court **FINDS** by a preponderance of the evidence that Stealthwatch performs the exact type of correlation and

provisioning of rules in response to correlations required by the '176 Patent.

iii. Findings of Fact Regarding Validity

19. The priority date of the '176 Patent is February 10, 2015. JTX-4.

20. Sometime in 2012 or 2013, Cisco released and marketed a system known as the Cyber Threat Defense Solution. This system was a collection of Cisco switches and routers, the Identity Services Engine and Lancope's Stealthwatch. *Compare* Tr. 2430:1-3; DTX-311 *with* Tr. 2485:5-10; DTX-664 at 004.

21. Cisco asserts its Cyber Threat Defense Solution, using an older version of Stealthwatch, as the prior art that renders the '176 Patent invalid. DTX-311; DTX-312; DTX-343; DTX-463 (All documents from pre-2017).

22. The asserted prior art system leverages Cisco networking technology, including NetFlow, Identity Services Engine, and Stealthwatch. The Stealthwatch version asserted as prior art is version 6.5.4. Tr. 2344:22. This version of Stealthwatch incorporated Stealthwatch Labs Intelligence Center ("SLIC") threat intelligence information, which contained human collected threat indicators. Tr. 3153:14-19; DTX-312 at 001.

23. Old Stealthwatch was able to automatically respond to alarms generated by worms, viruses and internal policy violations. DTX-463 at 014 (noting Stealthwatch responds to alarms). There is no indication in the pre-2017 documents that Stealthwatch issued rules in response to correlations of NetFlow.

24. Cisco Stealthwatch incorporated Cognitive Threat Analytics in Stealthwatch in 2017. Tr. 2342:6-7. In version 7.0.0 of Stealthwatch released in 2019, CTA was improved with the ability to leverage threat detection from the analysis of WebFlow, produced by Syslogs, and NetFlow telemetry by correlating the data. PTX-1893 at 011.

25. In response to these correlations, new Stealthwatch creates a baseline of normal traffic behavior within the network. Based on these normal patterns and known threat indicators, Stealthwatch, using CTA, employs a funnel of analytical techniques to detect advanced threats. PTX-569 at 272; PTX-584 at 402 (post-2017 documents).

26. Stealthwatch, in response to suspicious activity or threats, allows the Identity Services Engine or Stealthwatch Management Console to provision rules to proactively stop that threat. Tr. 1002:13-1003:21; PTX-1089 (showing the use of the Adaptive Network Control ("ANC") to implement rules). The new ANC, which replaced the old quarantine functionality, operates by applying new policies and changing individual user's authorization on the network according to rules and policies configured by the Identity Services Engine in response to correlated threats on the network. PTX-595 at 179; Tr. 1005:10-19. Both Identity Services Engine and the Stealthwatch Management Console operate in this fashion. Tr. 1006:19-1007:5.

iv. Conclusions of Law Regarding Validity

Dr. Almeroth opined that the '176 Patent is invalid for anticipation, obviousness, and based on written description. Turning first to obviousness, Dr.

Almeroth averred, by using Dr. Cole's testimony, that all of the infringing functionality of the Cisco products is present in the prior art, particularly the Cisco Cyber Threat Defense System. Tr. 2304:9-20. Specifically, Dr. Almeroth contended that prior to the priority date of the '176 Patent, Stealthwatch was able to "raise alarms, and then be able to generate and provision rules [based on] the routers and switches exporting NetFlow in combination with Stealthwatch." Tr. 2305:2-5. The Court disagrees with Dr. Almeroth's characterization.

Dr. Jaegar, Centripetal's validity expert in his rebuttal testimony, highlights that the prior art confirms that the old Stealthwatch system is designed as a visibility system allowing administrators to view traffic in the network:

> Q. How do they characterize the old Stealthwatch Management Console?
>
> A. Well, I would characterize the old Stealthwatch systems, Stealthwatch Management Console, or SMC as its shown here, as the core visibility component of the old Stealthwatch system. This is the component that does the showing of information about flows in your network. And as you can see in the bottom paragraph, it talks about administrators, and so this SMC or Stealthwatch Management Console is designed for administrators to be able to look at what's going on in their networks.

Tr. 3152:13-22. The technical documents, from 2014, confirm Dr. Jaegar's opinion highlighting that [t]he Stealthwatch system by Lancope is a leading solution

for network visibility and security intelligence . . . ." PTX-343 at 001. Stealthwatch operates by providing "in-depth visibility and security context needed to thwart evolving threats . . . [and] quickly zooms in on any unusual behavior, immediately sending an alarm to the SMC . . . ." PTX-343.

Additionally, the old Stealthwatch operated in response to these alarms. Dr. Jaegar opined:

> Q. Could you give us your memory of Dr. Almeroth's testimony and why you disagree with it?
>
> A. My recollection is that he was saying that this shows that this adaptable mitigation that's responsive to alarms, this would satisfy the responsive to correlation limitation.
>
> Q. And why do you disagree with his interpretation of this?
>
> A. Well, it specifically says in the first sentence that "Lancope customers can direct the Stealthwatch appliance to automatically respond to alarms generated by worms, viruses and internal policy violations." And so this indicates that the, any—any addition or automation or—well, activation, I guess is the word I'm looking for—of these mitigation actions in the old Stealthwatch system is done in response to alarms being triggered and not in response to correlation of logs as is required by the claims. And my understanding is that previous *inter partes* reviews found that technology that only discloses being responsive to alarms rather than responsive to correlation of log entries as

> required by the claim elements, that doesn't satisfy the responsive to correlation claim element.

Tr. 3154:6-25; *see* DTX-463 at 014. The post-2017 documents illustrate that the generation of rules responsive to correlations was an added functionality with the addition of CTA into Stealthwatch. The release notes for Version 7.0.0 of Stealthwatch, PTX-1893, contain a section titled "What's New" which shows the additions made to Stealthwatch in this version. PTX-1893 at 011. In this section, the technical document indicates that "CTA can now leverage detections from the analysis of WebFlow telemetry to improve the efficacy of analyzing NetFlow telemetry from Stealthwatch. This is accomplished by the system through correlation of both telemetry types." PTX-1893 at 011 (a technical document from 2019 showing this type of correlation is an enhancement to the Cognitive engine). Cisco identifies that this technology increases the number of both confirmed and detected threats in the network. *Id.* Cisco's presentation on the incorporation of CTA into Stealthwatch shows that the technology "uses the Proxy ingestion feature to consume Syslog information sent from proxy sources . . . [and] then correlate the received syslog and relates it to the flows collected from network devices before and after the proxy . . . ." PTX-1065 at 005 (November 2017 document). This same document highlights that "[b]ringing CTA and Stealthwatch detection together gives us unique ability to combine our local and global detection capabilities." *Id.* In response to the local correlations of WebFlow and NetFlow, new Stealthwatch can provision Adaptative Network

Control policies based on the identification of behavioral anomalies. *See* PTX-569 at 272; PTX-595 at 179 (a technical document from 2019 showing how "ANC policies have replaced the previous quarantine and unquarantine feature"). Accordingly, Cisco has failed to present clear and convincing evidence that the "correlate" and "responsive to" functionality was in the Cisco prior art system. Therefore, the prior art does not render the asserted claims anticipated or obvious.

Switching to Cisco's argument regarding written description. Dr. Almeroth opined that the specification does not disclose to a person skilled in the art that the inventors were in possession of the invention that is covered by the scope of the claims that is alleged in Centripetal's infringement allegations. Tr. 2333:2-8. He avers that the '176 Patent is invalid because the specification of the '176 Patent contains no description of Cognitive Threat Analytics, machine learning, artificial intelligence, integrating threat feeds, or NetFlow. Tr. 2333:22-2334:12. The Court **FINDS** that both the challenged "correlate" and "responsive to" claim elements are adequately disclosed in the specification to meet the written description requirement.

Dr. Jaegar opined that a person skilled in the art would be able to look at column 8, lines 46 through 63 of the '176 Patent specification and determine that the invention "utilize[s] logs to correlate packets transmitted by one or more network devices with packets received by one or more network devices." Tr. 3155:16-18; *see* JTX-3 at col. 8 ln. 46-63. Additionally, for the "responsive to" element, Dr. Jaegar points to

column 12, line 55 through column 13, line 13. This section of the specification clearly shows that the invention identifies hosts associated with malicious entities and communicates messages identifying that host. JTX-3 at col. 12 ln. 55-col. 13 ln. 13. Further, the specification notes that this process occurs in response to the correlation of data, as described in column 8, lines 46 through 63 of the specification. Tr. 3156:9-3157:14. Based on these sections of the specification, the Court finds that a person skilled in the art would have been in possession of the invention at issue.

Accordingly, the Court **FINDS** that Cisco has not proven by clear and convincing evidence that the '176 Patent was anticipated, obvious or lacked sufficient written description.

C. THE '193 PATENT

i. Findings of Fact Regarding Infringement

1. The '193 Patent was informally known throughout the trial as the "Forward or Drop / Exfiltration Patent." Tr. 2356: 2-6.

2. The '193 Patent was issued on June 20, 2017. JTX-4. The '193 Patent was filed on February 18, 2015 as a continuation of application No.13/795,882, giving the '193 Patent a priority date of March 12, 2013. JTX-4.

3. The asserted claims of the '193 Patent are Claims 18 and 19. Doc. 411. Claims 18 and 19 are, respectively, a packet filtering system and computer readable media claim.

4. Claim 18 is laid out below:

A system comprising:

at least one processor; and

a memory storing instructions that when executed by the at least one processor cause the system to:

receive, from a computing device located in a first network, a plurality of packets wherein the plurality of packets comprises a first portion of packets and a second portion of packets;

responsive to a determination that the first portion of packets comprises data corresponding to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network, wherein the data indicates that the first portion of packets is destined for the second network:

apply, to each packet in the first portion of packets, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and drop each packet in the first portion of packets; and

responsive to a determination that the second portion of packets comprises data that does not correspond to the criteria, wherein the data indicates that the second portion of packets is destined for a third network:

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

JTX-4.

5. Claim 19 is identical to Claim 18 in every respect except it is a computer readable media claim. Claim 19 substitutes the introductory language of Claim 18, "A system comprising: at least one processor; and a memory storing instructions that when executed by the at least one processor cause the system to . . .", with "[o]ne or more non-transitory computer-readable media comprising instructions that when executed by one or more computing devices cause the one or more computing devices to: . . . ." JTX-4; *see* Tr. 472:21. For purposes of infringement, the parties treated Claims 18 and 19 the same.

6. Dr. Sean Moore, one of the inventors of the '193 Patent, testified that the technology claimed in the patent centered around preventing the exfiltration of confidential data by cyber criminals. Tr. 343:14-16.

7. Centripetal's expert, Dr. Mitzenmacher, defined the asserted claims of the '193 Patent as being related to the process of forwarding and dropping packets related to preventing exfiltrations. Tr. 465:18-

21. Additionally, Dr. Mitzenmacher opined that the '193 Patent applies to the prevention of many different types of data exfiltration. Tr. 467:14-468:17.

8. As previously noted, exfiltration can occur in the context of cyber criminals hacking into the network and stealing data, but it also can occur within networks internally. For example, within one large corporate network there are many different departments or subnetworks, such as finance and human resources. See Tr. 490:17-25. It is common within these multi-departmental companies that certain departments have access to confidential materials, while for others that access is restricted.

9. Accordingly, the network must restrict the ability of packets with this sensitive information to travel to unauthorized internal departments and external networks, while also allowing packets with no sensitive information to be freely transmitted to other employees within the network. Tr. 467:14-468:17. Therefore, the '193 Patent specifically identifies a process by which rules can be enabled to filter packets of data depending on the type of data transfer that is being transmitted throughout the network. Tr. 468:21-469:9.

10. Centripetal accuses Cisco's Catalyst 9000 series switches, the Aggregation Services Router 1000 series routers and Integration Services Router 1000 and 4000 series routers of infringing Claims 18 and 19 of the '193 Patent. Tr. 433:20-434:1.

11. The accused Cisco's switches and routers share the same operating system known as IOS XE. Tr. 448:11-24; 449:19-450:4; PTX-242 at 816, 817.

12. Cisco compiles the source code that operates the accused switches and routers in the United States. Tr. 462:5-463:18, 464:4-14; PTX-1409 at 5-6.

13. The accused switches and routers contain processors and memory that stores software instructions. Tr. 477:12-478:14, 484:13-485:3; PTX-1303 at 056. One of the processers within the accused Cisco devices are programmable Applied Specific Interred Circuits ("ASIC"), known as Unified Access Data Planes ("UADP"). Tr. 477:24-478:5; PTX-1262 at 994. This type of processer is commonly referred to as a UADP ASIC. Tr. 477:24-478:5; PTX-1262 at 994; PTX-1390 at 029.

14. In their operation, the processors work within the accused Cisco switches and routers to receive and transmit packets across a network. PTX-1276 at 216 (2011 Cisco document); Tr. 488:1-489:3. During the transmission of packets, the operating system ("IOS XE"), working in conjunction with UADP ASICs, apply a variety of different rules to packets to determine if the packet should be permitted or dropped. PTX-1276 at 215-16.[5]

15.Access Control Lists ("ACL") are often applied to packets on ingress into the device and egress out of the device. PTX-1276 at 215-16. To simplify the process of applying rules, Cisco's IOS XE utilizes a specific method where labels are applied to packets

[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

based on their source or destination. These labels are known as Secure Group Tag / Scalable Group Tag ("SGT").[6] Tr. 494:12-24; *see* PTX-1276 at 211.

16. SGTs are attached to categorize packets into different numerical groupings based on information such as the packet's source IP, destination IP and/or both. PTX-1280 at 021. SGT can also be based on other information that is included in the 5-tuple, such as source port, destination port and protocol. Tr. 2400:24-25 (Dr. Crovella, Cisco's expert witness, highlighting that a quarantine rule has the ability to look at all information in the 5-tuple),2404:4 ("[t]he quarantine rule only looks at the 5-tuple . . .").

17. As packets enter the switch and router, they perform an initial check to see if there is a specific source SGT attached to each packet that is entering through the switch or router. Tr.2421:2-8.

18. After the initial check, the switch and/or router applies an initial collection of rules known as a Group Access Control List ("GACL").A Security Group ACL ("SGACL")is an 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-

---

[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.

1288 at 012 (showing input GACL applied based on ingress client); *see also* PTX-1276 at 216; PTX-1390 at 86 (2019 document).

20. On a packet's egress out of a device, the switch and/or router applies an output SGACL based upon the SGT associated with the source, and drops or transmits packets based upon the destination of the packets. Tr. 2389:15-19; *see* PTX-1288 at 012 (showing output GACL applied based on egress client); *see also* PTX-1276 at 216; PTX-1390 at 86 (2019 document).

21. Cisco's expert, Dr. Crovella, confirms that SGACLs are applied on a packet ingress into the switch and/or router and applied on a packet's egress out of the router and/or switch. Tr. 2389:15-19, 2399:22; PTX-1288 at 012.

22. This SGACL rule-based packet blocking by comparing SGTs is more commonly referred to by Cisco as the quarantine rule. Tr. 2383:12-19, 2423:9-15 (Dr. Crovella noting that other ACLs besides the SGACL are not accused).

23. The quarantine rule operates to block or allow packets that are being transmitted throughout the network. Tr. 494:3-495:14, 496:17-497:13, 536: 24-25, 2419:3-15; *see* PTX-1262 at 999.

24. The switch and/or router determines whether the packet should be permitted or blocked based on the SGT assigned to that particular source. Tr. 535:10-17; PTX-1280 at 21; *see* PTX-1262 at 999. This process is completed by the switch and/or router by applying operators, such as permit or deny, to incoming and exiting packets based upon their assigned SGT. Tr. 531:18-21; PTX-1280 at 021. 22.

25. If a packet's SGT is not correlated to a SGACL rule on either ingress or egress, then a permit operator is applied to the packet, and it is permitted to be transmitted through the router or switch on to its destination. Tr. 542:17-24; PTX-1288 at 012. But if an SGT matches one of the SGACL rules because of an unpermitted source or destination, a deny operator is applied, and subsequently the packet will be blocked. Tr. 545:8-546:12, 548:11-19; PTX-1288 at 012.

26. In their presentation of evidence, Cisco has failed to cite any technical document produced post June 20, 2017. Cisco relies on ex post facto animations which were designed for litigation, and do not accurately portray the current functionality of the accused products.

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

ii. Conclusions of Law Regarding Infringement

Based on the Court's factual findings, Centripetal has proven by a preponderance of the evidence that the Cisco's Catalyst 9000 series switches, the Aggregation Services Router 1000 series routers and Integration Services Router 1000 and 4000 series routers literally **INFRINGE** Claims 18 and 19 of the '193 Patent. Cisco's expert on the '193 Patent, Dr. Mark Crovella testified:

> I was asked to consider whether the '193 patent was infringed by the accused Cisco technology, I was asked whether it should be considered valid in light of the prior art, and I was also asked about potential damages if we were to assume that it were valid and

> infringed, whether there were significant benefits over the prior art.

Tr. 2349:18-24. Dr. Crovella advanced two theories in his non-infringement opinion. First, that the function which is referred to as a "quarantine" blocks all traffic from a source computer and does not block a "particular data transfer," as required by the language in the claim. Second, he averred that Stealthwatch, using NetFlow, cannot identify exfiltrations until it is too late to drop the packet.

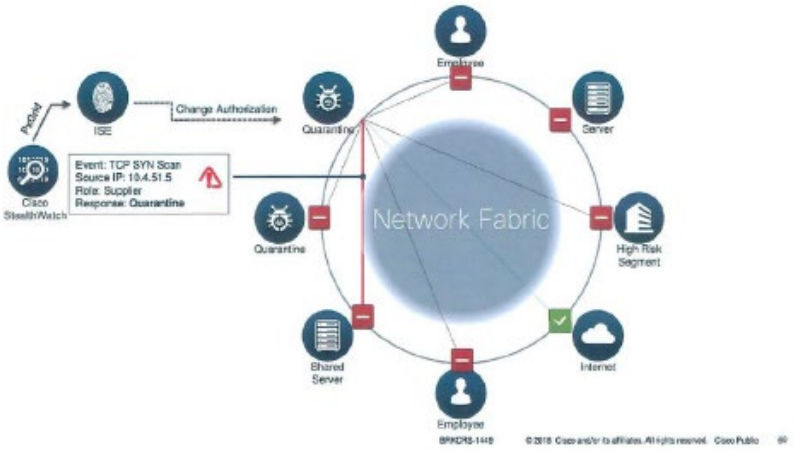
As to the first theory, Dr. Crovella admits on cross examination to the "two stage" process. This testimony, coupled with Cisco's technical information from PTX-1284 and PTX-1326, prove that the accused switches and routers have been aided with Cisco's Identity Services Engine to measure the vulnerability level of individual network risk and assign roles to certain devices based on this analysis. Walking through the operation of the accused products illustrates that the Cisco system operates in a two-stage process that meets the functionality required by the asserted claims.

The Cisco packet-filtering system operates by using the Identity Services Engine to assign certain endpoint devices "roles" that determine what type of packets may be sent and/or received by that specific endpoint computer. PTX-1326. Therefore, the Identity Services Engine has the ability to monitor levels of vulnerabilities based on the packets that are being transmitted by switches and routers in the network, and to adjust the permissions based on real-time network operations. As a general example, the Cisco system operates by limiting a computer located in a

first network from accessing sensitive data in a protected network, while simultaneously allowing unsensitive data to be accessed. In this manner, packets from the computer in the first network may be allowed to access unprotected resources on the larger internet, but would be restricted from transmitting packets containing secure information. This is shown by Cisco's technical demonstration, PTX-563:

PTX-563

Cisco Technical Presentation on Rapid Threat Containment from 2018



The accused switches and routers are the specific network devices used to institute this packet filtering system. In their operation, the accused products receive different portions of packets from a first computing network. PTX-1276 at 216. Upon entry into an accused device, each packet is assigned a Scalable/Security Group Tag ("SGT"). The SGT that is attached to each packet is based on the role and/or privileges that is assigned to that specific endpoint computer. Therefore, SGTs, at their most basic level,

are assigned to packets based on where the packet is being transmitted from and/or the destination of the transmitted packet. In this manner, the 5-tuple information in the header of the packet, such as the source of the packet's origin and/or the destination to which it is being transmitted, is the operative data being used to determine the packet's SGT. This assignment of SGT to packets as they enter the switch or router is the first step in the operation of the quarantine process.

After SGT attachment, the switches and routers execute the second stage. The accused devices utilize specialized rules, known as SGACLs, that deal specifically with forwarding and dropping packets based on what type of SGT is attached to the packet. SGACLs are applied to packets on both ingress in and egress out of switch and/or router. *See* PTX-1390 at 86. On ingress, the device looks at the SGT that is associated with the source of the packets. This application of SGACLs by the device determines whether packets are allowed to be transmitted by this specific SGT. If packets are allowed to be transmitted by the specific SGT, the packets are permitted into the device where the packets would be subject to another set of SGACLs on egress. On egress, different SGACLs are applied based on the packet's destination. Egress SGACLs determine if packets associated with this SGT can be sent to the specific destination.

Centripetal's expert, Dr. Mitzenmacher, used PTX-1326 to confirm that Cisco's quarantine rule operates with this rule-based blocking functionality. Moreover, technical documents, such as Cisco's Rapid Threat Containment Guide, confirm that switches and

routers are programmed to "manually or automatically change your user's access privileges when there's suspicious activity, a threat or vulnerabilities discovered." Tr. 527:4-17; PTX-1326 at 011. Accordingly, the accused Cisco system attaches SGT to packets, and then uses the SGACL quarantine functionality within the switches and/or routers to contain malware infected computers by blocking "access to critical data while their users can keep working on less critical applications." PTX-1326 at 011. Thus, the Cisco system operates by blocking packets affiliated with a particular type of data transfer to a protected resource, while allowing packets unaffiliated with a protected type of data transfer to be transmitted to their final destination. In this manner, the technical documents confirm that the accused products utilize "packet filtering-rules" that operate to prevent "a particular type of data transfer" from a first to second network. This functionality is shown by text and diagram included in Cisco's technical document that outlines the operation of the quarantine feature:

PTX-1326

Cisco Identity Services Engine Technical Ordering Guide from August 2019

With integrated network access control technology, you can manually or automatically change your users' access privileges when there's suspicious activity, a threat or vulnerabilities discovered. Devices that are suspected of being infected can be denied access to critical data while their users can keep working on less critical applications.

1.6.2 How does Rapid Threat Containment work

See PTX-1326 (showing infected endpoints can be denied access to certain types of data while being allowed access to other types of data).

This functionality confirms the accused devices operate in the "two-stage" process outlined by both the claims and the specification of the '193 Patent. The accused products perform a two-stage process by first assigning SGT to packets, based upon the source and/or destination of the packets, and then applies different "operators" or functions, such as permit/deny, to those packets based on the associated packet SGT. Cisco's infringement expert, Dr. Crovella, on cross examination confirmed that the accused products perform all the functionality required to infringe the claims:

> Q. . . .So we have multiple steps. First, the SGT tag is checked to see if it's present, right?

A. That's right.

Q. Then, if the SGT tag is present and it says, "quarantine," then a quarantine policy is applied, correct?

A. That's right.

Q. If the quarantine policy is applied, you check the destination, and if the destination is a protected resource in which it says, do not allow this packet to go there, it will prevent the data transfer from going to that destination, correct?

A. That is, in fact, the quarantine policy. In other words, there's not two steps there. A quarantine policy is, in fact, checking the destination.

Q. Okay. And if it says, block the packet, it will be prevented from the data transfer going there, right?

A. That's right.

Q. If it's not in there, and if there is a—it's able to go through to a permitted network or permitted resource, then the packet would be allowed to go through by the switch or the router. Isn't that right?

A. That's right.

Tr. 2423:19-2424:15; *see* PTX-563; PTX-1326. Dr. Crovella even concedes that the '193 Patent requires a device to "block some communication between the two networks but allow other communication to flow." Tr. 2400:8-10. This is the exact functionality outlined by the asserted claims.

This described system, without the use of Stealthwatch, can identify exfiltrations and drop packets as a result. Therefore, the Court **FINDS** that Cisco's second theory of non-infringement is irrelevant to the Court's determination because the accused system operates to block packets based on the particular type of data transfer as required by the claims. Cisco's technical documents, such as PTX-1294 and PTX-1326, demonstrate that Stealthwatch is not involved in the two stages of the infringing functionality. Accordingly, any evidence regarding Stealthwatch has no bearing on infringement for the '193 Patent. Based on its analysis, the Court **FINDS** that the packet filtering system instituted by the accused products infringes Claim 18 and 19 of the '193 Patent.

iii. Findings of Fact Regarding Validity

28. The priority date of the '193 Patent is March 12, 2013. JTX-4.

29. Sometime in 2012 or 2013, Cisco released and marketed a system known as the Cyber Threat Defense Solution. This system was a collection of Cisco switches and routers, the Identity Services Engine and Lancope's Stealthwatch. *Compare* Tr. 2430:1-3; DTX-311 *with* Tr. 2485:5-10; DTX-664 at 004.

30. Cisco asserts the Cyber Threat Defense Solution as the prior art that renders the '193 Patent invalid. DTX-311.

31. Switches and routers within Cisco's Cyber Threat Defense Solution both received packets and created records of packet flows using Cisco's proprietary logging system known as NetFlow. DTX-311 at 004.

32. The Cyber Threat Defense Solution operates by analyzing NetFlow data and inspecting that data for exfiltrations in the network. DTX-588 at 002.

33. The Cyber Threat Defense Solution contained a quarantine function. At that time, the quarantine function operated by completely isolating a source computer by blocking all packets sent from the computer into the network. Tr. 3011:1-9; DTX-711 at 002. Within this quarantine functionality, there is no mention of allowing access to certain resources while denying access to others. Tr. 3012:1-2.

34. The prior art does not contain any mention of Secure Group Tags or Identity Service Engine's role-based quarantine functionality. *See* DTX-588; PTX-1193.

35. The prior art does not contain any mention of the application of operators to filter packets based on the attachment of Secure Group Tags. Tr. 3015:11-18, 3016:10-21, 3017:4-10; *see* DTX-588.

36. The prior art does not contain any information showing the application of SGACL to filter packets in the same manner shown by Cisco's technical documents produced after March 12, 2013. *Compare* PTX-1276 at 211, 216 (showing the application of Secure Group Tags and SGACLs by the IOS-XE operating system) *with* PTX-1193 at 007 (showing the same diagram, but failing to make mention of any rules attached and filters based on the application of Secure Group Tags).

iv. Conclusions of Law Regarding Validity

For the '193 Patent, Cisco contends it is invalid based on anticipation by the prior art under 35 U.S.C.

§ 102, and based on obviousness in view of the prior art under 35 U.S.C § 103. First, Cisco has presented no compelling evidence that the alleged prior art system, the Cisco Cyber Threat Defense Solution, operates in a two-stage filtering process, as illustrated by the claims of the '193 Patent. *See* DTX-311. The most complete version of prior art, the Cisco Cyber Threat Defense Solution 1.0 Design and Implementation Guide, makes no mention of the attachment of Secure Group Tags or the application of operators to filter portions of packets based on that packet information. Throughout Dr. Crovella's testimony, there is clear reliance on multiple prior art references to prove the invalidity case. For those reasons, it is apparent that a single prior art fails to contain all elements of the claimed invention, and Cisco has failed to show anticipation by clear and convincing evidence.

Turning to obviousness, the prior art references advanced by Cisco do not show that a skilled artisan would have been able to combine the teachings in these technical documents and produce the patented invention. Cisco argues that the '193 Patent must be invalid because the previous system, that includes older versions of similar switches, routers, ISE and Stealthwatch, has had some method of quarantining and blocking functionality. However, the Court rejects Cisco's contention that these products have operated in the same manner and functionality just because the system had preexisting baseline functionality and consistent nomenclature. The prior art makes no mention of the infringing packet filtering process. Dr. Crovella relies on PTX-588, DTX-711, DTX-311, and PTX-1193 to contend that a person skilled in the art

would have combined these references in order to teach the functionality outlined in the claims of the '193 Patent. A review of the asserted prior art shows no mention of the Identity Services Engine packet filtering system that utilizes switches and routers to attach Secure Group Tags, apply operators and then allow certain packets to be transmitted while other packets are subsequently blocked.[7] It is that system which contains the functionality taught by the claims of the '193 Patent. Cisco's own technical documents that were used to show infringing functionality are all from post-2013. *See* PTX-1288 at 012; PTX-1276 at 216; PTX-1280 at 21; PTX-1294; PTX-1326. Not one selection of asserted prior art shows the infringing switch and router functionality was embedded in any of the Cisco products before the '193 Patent's priority date. These conclusions allow the Court to infer that the infringing functionality was added as a result of newly designed versions of the accused products that occurred after March of 2013.

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.

D. THE '806 PATENT

i. Findings of Fact Regarding Infringement

1. The '806 Patent was informally known throughout the trial as the "Rule Swap Patent."

2. The '806 Patent was issued on December 1, 2015. JTX-2. The application for the '806 Patent was filed on January 11, 2013.

3. The asserted claims of the '806 Patent are Claim 9 and Claim 17. Doc. 411. Claim 9 and Claim 17 are, respectively, a system and computer readable media claim.

4. Claim 9 is laid out below:

A system comprising:

a plurality of processors; and

a memory comprising instructions that when executed by

at least one processor of the plurality of processors cause the system to: receive a first rule set and a second rule set; preprocess the first rule set and the second rule set to optimize performance of the system for processing packets in accordance with at least one of the first rule set or the second rule set;

configure at least two processors of the plurality of processors to process packets in accordance with the first rule set; after preprocessing the first rule set and the second rule set and configuring the at least two processors to process packets in

> accordance with the first rule set, receive a plurality of packets;
>
> process, in accordance with the first rule set, a portion of the plurality of packets; signal, each processor of the at least two processors, to process packets in accordance with the second rule set; and
>
> configure, each processor of the at least two processors to, responsive to being signaled to process packets in accordance with the second rule set: cease processing of one or more packets; cache the one or more packets; reconfigure to process packets in accordance with the second rule set;
>
> signal completion of reconfiguration to process packets in accordance with the second rule set; and
>
> responsive to receiving signaling that each other processor of the at least two processors has completed reconfiguration to process packets in accordance with the second rule set, process, in accordance with the second rule set, the one or more packets.

JTX-2.

5. Claim 9 is identical to Claim 17 in every respect except that Claim 17 is a computer readable media claim. JTX-2. Claim 17 substitutes the introductory language of Claim 9, replacing "[a] system comprising: a plurality of processors; and a memory comprising instructions that when executed by at least one

processor of the plurality of processors cause the system to:" with "[o]ne or more non-transitory computer-readable media comprising instructions that when executed by a computing system cause the computing system to:" JTX-2. For purposes of infringement, the parties treated Claims 9 and 17 the same.

6. Dr. Moore, one of the inventors of the '806 Patent, defined the technology in the '806 Patent as a process by which a network device could perform a live swap of rules without sacrificing any security concerns or dropping packets. Tr. 338:22-339-2.

7. Cyber threat intelligence is often changing, so the rules that are embedded in switches and routers need to be continually updated. Tr. 339:5-10. Therefore, the rules that are being applied need to be continually swapped out from old rules to new rules. Tr. 339:13-25. The most efficient way to do this is by swapping rules while live traffic is going through the device and without any packets being dropped. Tr. 339:13-25.

8. Centripetal accuses Cisco's Catalyst 9000 series switches, the Aggregation Services Router 1000 series routers and Integration Services Router 1000 and 4000 series routers in combination with Cisco's Digital Network Architecture of infringing Claims 9 and 17 of the '806 Patent. *See* PTX-1263 at 180 (highlighting Cisco networks are intent-based networks which provide "[p]erimeter-based, reactive security that has been supplanted by network-embedded, content-based security that reaches from the cloud to the enterprise edge") (2019 document).

9. Additionally, Centripetal accuses Cisco's Adaptive Security Appliance 5500 series with Firepower services and Cisco's Firepower Appliance 1000, 2100, 4100, and 9330 series that run Firepower Threat Defense ("Cisco's Firewalls") with Firepower Management Center infringe Claims 9 and 17 of the '806 Patent. *See* PTX-1291 at 668 (noting the rule swapping procedures of the Cisco firewall products) (September 2017 document).

10. Cisco compiles source code for the accused switches, routers, and firewalls in the United States. Tr. 462:5-463:18, 464:4-14; PTX-1409 at 5-6. The accused products have a plurality of processors and computer memory which stores software instructions. Tr. 573:8-575:6, 642:4-647:11.

11. Cisco's Digital Network Architecture ("DNA Center") is the management structure that allows the system to take in or utilize threat intelligence, operationalize it, and turn it into rules and policies that Cisco's switches and routers use for security purposes. Tr. 451:3-24.

12. The DNA Center receives rule sets from various sources and preprocesses the rule sets to create optimized policies which are distributed to Cisco's switches and routers. Tr. 575:15-577:8, 579:18-580:24, 584:14-585:4, 586:15-587:18, 588:12-589:18, 2571:12-2573:8; PTX-992 at 2; PTX-1294 at 3 (2019 document).

13. Similar to the DNA Center, Firepower Management Center's Threat Intelligence Director receives rule sets from various sources and preprocesses the rule sets to create optimized policies which are distributed to firewalls. Tr. 655:10-656:20,

673:21-675:5, 680:11-681:10; *see* Tr. 2537:3-7, 2539:11-17.

14. When new rules are available and sent to Cisco's switches and routers by the DNA Center, the switches and routers will perform a rule swap without dropping any packets. Tr. 597:10-601:8, 606:15-608:14, 633:24-634:14; *see also* Tr. 2571:12-2573:8; PTX-1915; PTX-1195 at 001, 003-04.

15. Similarly, when new rules are available and sent to Cisco's firewalls from the Firepower Management Center, Cisco's firewalls will perform a rule swap without dropping any packets. PTX-1196 at 001, 007; Tr. 694:22-696:12, 698:8-22, 705:15-707:1.

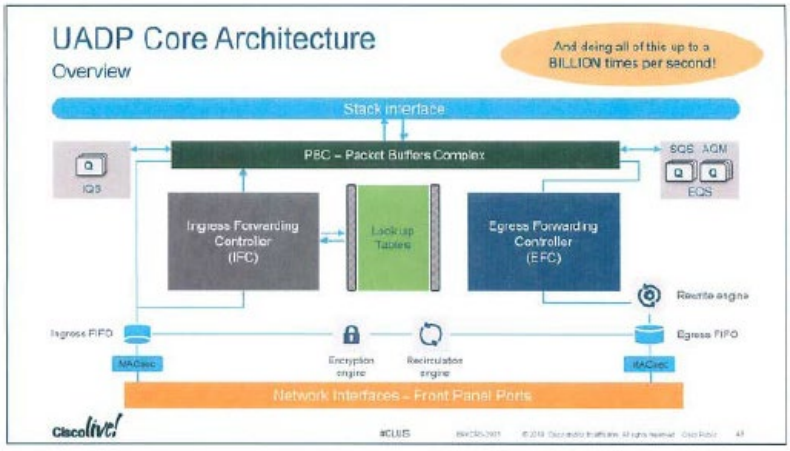
16. Mr. Peter Jones[8], a distinguished Cisco engineer responsible for building the switching, routing and enterprise network, explained in detail how the accused products process packets and swap rules. Tr. 2543:9-11, 2561:25-2562:1.

17. Mr. Jones explained that the architecture that enables packet processing functionality within the switch and/or router is the Uniform Access Data Plane ("UADP") processor. Tr. 2562:10-18; DTX-562 at 043. The figure below shows the core architecture in detail:

[8] Mr. Jones was one of the architects for the design of the UADP processer used by Cisco's accused switches and routers. Tr. 2549:10. He also provided multiple technical presentations regarding the operation of the UADP at many Cisco events. *See* DTX-562 at 006.

DTX-562

Cisco Technical Presentation on UADP Core Architecture in 2019



18. Mr. Jones noted that as packets arrive into a router and/or switch, they enter through the front panel ports and head into the Media Access Control Security ("MACSec"). Tr. 2567:18-25. The MACSec serves as an encryption block. Tr. 2567:23.

19. The packet then moves into the Ingress FIFO. The FIFO, or First In First Out, is a small buffer that serves to order packets as they enter the device. Tr.2567:23-2568:3.

20. After the FIFO, the payload of the packet is then sent to the Packet Buffer Complex ("PBC") for storage. Tr. 2568:4. Simultaneously, the header and address of the packet is sent to the Ingress Forwarding Controller.

21. The Ingress Forwarding Controller processes the packet by matching the header information to a variety of Access Control Lists ("ACL") that are stored in the look-up tables. Tr. 2568:10-16. Based on those

ACLs, the Ingress Forwarding Controller then decides to either drop the packet or transmit it forward. Tr. 2568:10-16.

22. Mr. Jones explicitly noted that if the packet is to be forwarded, it is sent to the Egress Forwarding Controller. Tr. 2568:21-24. He highlighted that the Egress Forwarding Controller operates identically to the Ingress Forwarding Controller. Tr. 2568:21-24. Therefore, for a second time on exit, the payload of the packet is sent to an egress Packet Buffer Complex while the header is sent to the Egress Forwarding Controller. Tr. 2568:21-24; PTX-1390 at 86.

23. It is in the Egress Forwarding Controller that the packet headers are again compared to ACLs that are located in the look-up tables. Tr. 2568:21-24. On egress, the packet can be dropped or further transmitted. Tr. 2568:21-24; PTX-1390 at 86.

24. If the packet is transmitted, it goes through an Egress FIFO, an Egress MACSec, and then out a port on the device. Tr. 2569:1-4.

25. Mr. Jones noted that the UADP operates on its own fixed time pipeline, meaning there will be a packet processed every two or four internal clock periods. The internal clock periods are not set to a normal time scale, but operate in milliseconds. Tr. 2554:22-24.

26. The accused products contain a new FED 2.0 Hitless ACL update. Tr. 3550:18-25. Mr. Jones testified that before the 2.0 Atomic Hitless feature was added to the accused products, performing rule swaps often resulted in a discard of a number of packets. Tr. 2552:20-23. Therefore, the new 2.0 Hitless version updated the products so that new ACLs can be placed

into the device and be activated without displacing packet processing. Tr. 2551:2-5; PTX-1303 at 073. Compare the older ACL Process:

PTX-1195 at 003

Cisco FED 2.0 Hitless ACL Update Software Functional Specification[9] from July 2017

2.1 Current ACL Change Flow

Currently whenever there is a change to the ACE in an ACL, the data will drop packets during the change to hardware programming.

This is the sequence of events today:

1. ACE added, removed, modified or re-sequenced
2. An ACL Class Group (CG) change event is sent to FED
3. FED CFM is updated with new Policy CG information
4. All features using this Policy CG are updated
   a. Create new Policy to use temporarily
   b. Generate a new VMR list
   c. Merge and Optimize new VMR list
   d. Write the Drop Policy label to every LE attached to the old Policy
   e. Remove existing TCAM entries
   f. Overwrite old Policy with new Policy in SDK
   g. Delete new Policy
   h. Write new TCAM entries
   i. Validate which will write the Policy label back into all LE attached to Policy
   j. Return SUCCESS

On ERROR returned from writing entries into TCAM:

- If TCAM is full then leave with Drop Policy label programmed (UNLOADED)
- Display UNLOADED or ERROR message to console to indicate hardware was not programmed with new Policy
- Drop all packets for this protocol type, in this direction on the interface
- Return ERROR

PTX-1195 at 003.

With the new 2.0 Hitless ACL Update:

---

[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.

PTX-1195 at 003

Cisco FED 2.0 Hitless ACL Update Software Functional Specification from July 2017[10]

2.2 Hitless (Atomic) ACL Change Flow

For this new feature Hitless (Atomic) ACL Change, no packets should drop while programming the new TCAM entries. To allow this to happen a new policy will be created and attached to the interface before deleting the existing policy.

This will always be enabled for all features that set the flag acknowledging support for hitless acl change; and is only available to features that go through ACL common code.

This is the new sequence of events:

1. ACE added, removed, modified or re-sequenced
2. An ACL Class Group (CG) change event is sent to FED
3. FED CFM is updated with new Policy CG information
4. All features using this Policy CG are updated
5. Generate a new VMR list
6. Merge and Optimize new VMR list
7. Verify if feature supports hitless ACL change
   - If supported, continue to Step 8
   - If not, use old method starting at Section 2.1 step 4d
8. Add new VCUs into hardware
9. Add new TCAM entries
10. Delete old entries from TCAM
11. Return SUCCESS

On ERROR returned from either of the new steps 7 or 8 will cause it to go back to use the old method of programming described in Section 2.1 starting with step 4d. So then, it will no longer be hitless.

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 ne installed before the old entries are deleted." *See* PTX-1195 at 003. Here is a copy of those Software Requirements:

---

[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.

PTX-1195 at 003

Cisco FED 2.0 Hitless ACL Update Software Functional Specification from July 2017

3 Software Requirements

The label will not be changed on the Policy. Just as the current Hitless QoS feature does, the new entries will be added with the existing label and there will be a short period where both sets of VMR entries will be installed before the old entries are deleted.

This will only be supported for these ACL features:

PACL, RACL, VACL, CGACL, and SGACL

27. ACLs are sent to switches and/or routers from a variety of sources - including Cisco's Digital Network Architecture. Tr. 2571:12-17. In order to use the rules, the switches and routers must compile them. Tr. 2571:18-21. Accordingly, the DNA Center begins the process by signaling the switches and routers to perform a swap from old to new ACLs. Tr. 2572:14-17.

28. While the ACLs are being compiled within the device, the device uses the old rule set to process packets. Tr. 2571:22-2572:1. The device, after compilation is finished, then signals the processor to begin processing packets with the new updated ACL rule set. Tr. 2572:2-6.

29. This swap of ACL rules within the device occurs in the middle of the two to four clock cycles, when the device is operating in idle and there is no processing of packets. Tr. 2572:10-13. Accordingly, there is a short period where the VMR contains both sets of new and old rules will be installed before the old rules are cleared. *See* PTX-1195 at 003-04.

30. After the swap is complete, the device performs a memory write and shows a return success function to the end user. Tr. 2573:5-8.

31. After the return is complete, packets are then processed with the newly updated second rule set. Tr. 2572:14-17.

32. Cisco's expert has failed to cite any technical document produced post June 20, 2017. Cisco's expert witness relies on animations, produced ex post facto, which were designed for litigation and do not accurately portray the current functionality of the accused products. Exhibit DTX-562, which was altered from its original form as cited by Cisco's employee Mr. Jones, had emphasis added to it to exclude egress from the presentation of Cisco's expert Dr. Reddy. *See supra* sec. *IV. Overview of the Evidence* (discussing Dr. Reddy's animations).

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

ii. Conclusions of Law Regarding Infringement

Based on the Court's factual findings, Centripetal has proven by a preponderance of the evidence that the Cisco's Catalyst 9000 series switches, the Aggregation Services Router 1000 series routers and Integration Services Router 1000 and 4000 series routers in combination with Cisco's Digital Network Architecture literally **INFRINGE** Claims 9 and 17 of the '806 Patent. Additionally, the Court **FINDS** Cisco's Adaptive Security Appliance 5500 series with Firepower services and Cisco's Firepower Appliance 1000, 2100, 4100, and 9330 series that run Firepower Threat Defense ("Cisco's Firewalls") with Firepower Management Center literally **INFRINGE** Claims 9 and 17 of the '806 Patent.

For Cisco, Dr. Narasimha Reddy testified regarding the '806 Patent as to infringement, validity and damages. Dr. Reddy opined that:

> The accused product combinations do not infringe the '806 [P]atent. Secondly, if the Court were to find that the accused product combinations infringe, the asserted claims are invalid on existing prior art of Cisco before the patents were filed. And for damages, assuming that the products are found to be infringing and that the claims are valid, the contribution of the patent claims are minimal.

Tr. 2580:15-23. Dr. Reddy advances three theories of non-infringement for the '806 Patent. He avers that the accused products: (1) do not cease processing of packets responsive to a signal; (2) do not cache the packets responsive to a signal; and (3) do not reprocess packets according to a second rule set. To prove that the products do not perform this functionality as required by the claims, Dr. Reddy relied on an animation produced for litigation that directly contradicts Cisco's own employee testimony and Cisco's own technical documents. Using this animation, Dr. Reddy opined that the Cisco products never cache or cease processing packets during a rule swap. Tr. 2610-2-8.

Turning to the first theory, Cisco employee, Peter Jones, testified that in the operation of packet processing, Cisco's switches and routers will store packets in a part of the UADP ASIC processor known as the Packet Buffer Complex ("PBC"). The PBC operates as a holding spot for the data in the payload

of the packet while the header information is forwarded to another part of the processor for the application of rules. This operation in the Cisco switches and routers is designed to maximize the speed and efficiency of packet processing through software. Tr. 622:16-18. Dr. Mitzenmacher highlights that computer scientists use the term buffer and cache interchangeably as a word denoting the use of memory to hold packets for a short period of time. Tr. 628:7-25. Dr. Mitzenmacher referenced that a buffer is a "memory that holds something . . . [o]ften for future use." In reference to the Court's question about defining a cache, Dr. Mitzenmacher gave a similar definition of cache in the following exchange:

> Q. What's a cache?
>
> A. A cache is also often used, is used in the same way as a memory for holding things. They're very similar. And with a cache you don't typically or necessarily have an ordering associated with it. I mean, it can have an ordering, but it doesn't have to. But a cache is typically used as a memory that holds information that you expect to be using in the near future.

Tr. 836:17-23. Martin Hughes, a Cisco Engineer, confirmed Dr. Mitzenmacher's opinion that a packet buffer is a cache. Mr. Hughes was asked:

> Q. When the router products receive a packet, do router products store the packet in the cache?
>
> A. All products have packet buffers where packets are stored before processing.

DTX-1650; *see* Tr. 628:3-25, 866:8-22. Based on this testimony, it is apparent that the Packet Buffer Complex within the accused switches and routers clearly acts as a memory storage to hold packet information for further use, and therefore performs the same function of a cache, however, Cisco uses a different nomenclature, calling it a packet buffer. Tr. 836:17-23. Accordingly, in the course of packet processing, the accused devices store packets in a cache as required by the claims.

As their second theory of non-infringement, Cisco advances that the accused products do not cease processing of packets in response to a rule swap. Mr. Jones, a Cisco Engineer, testified contrary to this assertion. He explained that the newly compiled rules are swapped for the old rules in-between the two to four clock periods that occur within the switches and routers. This swap occurs directly during an idle period where the accused switches and routers are not processing any packets. Tr. 2572:10-20. Therefore, it is apparent that the switches and routers do cease packet processing, at least momentarily, to implement the newly compiled rule set.

With regard to both of these theories, Cisco argues that because this process is the normal processing functionality of the accused products, Cisco cannot in theory infringe the claims of the '806 Patent. The Court disagrees with Cisco's argument. It is true that the Cisco products do cache and cease processing packets during their normal packet processing operation. However, Cisco has implemented the rule swap functionality outlined in the '806 Patent to greatly improve the security functionality of its

products without dropping packets. The devices, in response to an initial signal, operate to stop processing packets during an idle period, and during the idle period, unprocessed packets are cached within the Packet Buffer Complex. This process is the exact functionality as described by the cease and cache elements of the '806 Patent.

Lastly, Cisco argues that packets are not reprocessed by a second rule set as required by the claims. First, Cisco is incorrect when it states the claims require a reprocess of packets. The claims clearly state that all that is required is a process through a second rule set. JTX-2. In other words, packets must just be processed by the second rule set—not processed a first time then reprocessed as Cisco suggests. Second, Cisco's non-infringement expert, Dr. Reddy, does not opine upon or even discuss the egress portion of a packet's transmission through a switch, router or firewall. Mr. Jones and Cisco's technical documents confirm that the accused devices apply rules on both ingress into the device and on egress out of the device. Therefore, in their operation, the devices are configured to apply one set of rules on ingress while the very same packet would be subject to a second set of rules on egress within the same device. This process would meet the claim language of the '806 Patent to process packets with a first rule set and then in accordance with a second rule set.

Accordingly, the accused products practice every claim limitation in Claims 9 and 17 of the '806 Patent. Therefore, the Court **FINDS** the rule swap system instituted by the accused Cisco products literally infringe Claims 9 and 17 of the '806 Patent.

iii. Findings of Fact Regarding Validity

34. The priority date of the '806 Patent is January 11, 2013.

35. Cisco asserts the functionality from a previous Cisco switch, the Catalyst 6500, and the Cisco Prime Network Control System as prior art for the '806 Patent. Tr. 3023:23-25.

36. The prior art functionality asserted within the Catalyst 6500 contains the older version of the Atomic ACL Hitless Update.

37. The Atomic ACL Hitless Update, within the Catalyst 6500 switch, operates by adding a new Access Control List ("ACL") in the Ternary Content-Addressable Memory ("TCAM") alongside the old ACL, and merging the two lists together. DTX-686 at 001. This process often overwhelms the TCAM and causes packets to be unintentionally dropped. *See* DTX-686 at 037-038.

38. The Atomic ACL Hitless Update was updated to the FED 2.0 version in 2017. PTX-1195 at 001; Tr. 3036:12-3037:4. The FED 2.0 Hitless Atomic ACL Update Software Functional Specification shows the differences between the older version of Hitless and the new 2.0 version. PTX-1195 at 002-03; Tr. 3040:2-3042:20. The newer version is accused of infringement by Dr. Mitzenmacher within the Catalyst 9000 switches and accused routers. Tr. 3035:15-25.

39. The older version of Hitless operated by completely stopping the system, eliminating ACLs, merging and replacing those ACLs, then reactivating the processing system. Tr. 3034:23-3035:2. This system resulted in overlap between the old rules and

the new rules within the TCAM. This caused packets to be dropped because old ACLs were being applied alongside the new ACLs, causing conflict and disruption. Tr. 3035:3-15, 3040:2-12; *see* PTX-1195 at 003.

40. The 2.0 Atomic ACL Hitless Update modified the process by eliminating the overlap and implementing rapid swap and replacement of the old ACLs with updated ACLs. Tr. 3041:7-18; *see* PTX-1195 (technical document from July 2017).

41. Cisco Prime Network Control System's Release Notes show that Prime operated by monitoring and troubleshooting support for a maximum of packets through the 5000 series Cisco Catalyst switches, allowing viability into critical performance metrics for interfaces, ports endpoints, users and basic switch inventory. DTX-525 at 002. The Release Notes for Prime and Dr. Reddy's testimony contains no mention of the preprocessing of rules or allowing switches to receive rules sent by Prime. Tr. 3043:10-24; *see* DTX-525 at 002. There is no evidence that the predecessor 6500 series switch, aided with Cisco Prime, could swap new rules for the old, as opposed to merging old and new rules together.

iv. Conclusions of Law Regarding Validity

Cisco asserts that the asserted claims of the '806 Patent are anticipated and/or are obvious based on the Atomic ACL Hitless Update in the Cisco Catalyst 6500 Supervisor Engine 2T and the Cisco Prime Network Control System. Tr. 2656:5-2657:22. Cisco's invalidity expert, Dr. Reddy, presented various documents opining that the functionality of Claims 9 and 17 of the '806 Patent was included within the prior art. This

Court disagrees with the conclusions of Dr. Reddy and **FINDS** the '806 Patent valid.

First, the Atomic ACL Hitless Update embedded within the Catalyst 6500 was an older and different functioning process than that which was embedded within the accused switches and routers. The accused devices contain a FED 2.0 version of the Atomic ACL Hitless Update. As evidenced by Centripetal's expert, Dr. Orso, and PTX-1195, this 2.0 version provided a meaningful update to the system by which old ACLs were *swapped* for new ACLs. *See* PTX-1195, Tr. 3040:2-3042:20. The older version of the Hitless Update, embedded in the 6500, involved *merger and application* of old and new ACLs that resulted in disruption of packet processing and the unintentional dropping of packets. This rule swapping technique outlined by the '806 Patent solved the problem that the old Hitless Update was having. *See* JTX-2 col. 1 (noting that the '806 Patent was addressing the problems faced by network devices "processing packets in accordance with an outdated rule set"). Therefore, it is axiomatic that the claimed invention would have not been obvious in the prior art because the '806 invention of rule swapping was the solution to the exact problem outlined by the original Hitless Update.

Second, the Cisco Prime technical documents do not contain any functionality of the asserted claims for the '806 Patent. The only document presented by Dr. Reddy identifies that Prime provided monitoring and troubleshooting support for Cisco's switches. There is no clear and convincing evidence from Dr. Reddy's testimony, or this one document offered by Cisco, that

Prime served a similar function as Cisco's Digital Network Architecture. Accordingly, there is not clear and convincing evidence for the Court to find that Prime caused the Cisco devices to receive first and second rule sets as required by the claims. Therefore, both asserted prior art references fail to teach the invention as described by Claims 9 and 17 of the '806 Patent. Accordingly, the Court **FINDS** that Cisco has not proven by clear and convincing evidence that the '806 Patent was anticipated or obvious.

E. THE '205 PATENT

i. Findings of Fact Regarding Infringement

1. The '205 Patent has been commonly known as the "dynamic security policy" Patent. Tr. 432:17-20.

2. The '205 Patent was issued on September 15, 2015. JTX-1. The application for the '205 Patent was filed on October 22, 2012. JTX-1.

3. The asserted claims of the '205 Patent are Claims 63 and 77 of the '205 Patent. Claims 63 and Claim 77 are, respectively, a system and computer readable media claim.

4. Claim 63 is laid out below:

> A system, comprising:
>
> a security policy management server; and one or more packet security gateways associated with the
>
> > security policy management server, wherein each packet security gateway of the one or more packet security gateways comprises computer hardware and logic

configure to cause the packet security gateway to:

receive, from the security policy management server, a dynamic security policy comprising at least one rule specifying a set of network addresses and a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI);

receive packets associated with a network protected by the packet security gateway;

perform, on the packets, on a packet by packet basis, at least one packet transformation function of multiple packet transformation functions specified by the dynamic security policy;

encapsulate at least one packet of the packets that falls within the set of network addresses and matches the SIP URI with a header containing a network address that is different from a destination network address specified by the at least one packet and that corresponds to a network device configured to copy information contained in the at least one packet and to forward the at least one packet to the destination network address; and

route, based on the header, the at least one packet to the network address that is

> different from the destination network address.

JTX-1.

5. Claim 63 is identical to Claim 77 in every respect, except that Claim 77 is a computer readable media claim. Claim 77 substitutes the introductory language of Claim 63, replacing "[a] system, comprising: a security policy management server; and one or more packet security gateways associated with the security policy management server, wherein each packet security gateway of the one or more packet security gateways comprises computer hardware and logic configured to cause the packet security gateway to" with "[o]ne or more non-transitory computer-readable media having instructions stored thereon, that when executed, cause each packet security gateway of one or more packet security gateways associated with a security policy management server to:." JTX-1. For purposes of infringement, the parties have treated the two claims as identical.

6. Dr. Moore, the inventor of the '205 Patent, characterizes the technology in the '205 Patent as Centripetal's network protection system that enforces threat intelligence policies on network traffic.

7. Dr. Moore identified that there is a thriving ecosystem of companies that observe behavior on the internet and collect information on who are the cyber criminals, what computers are being controlled, and what types of attacks are being implemented. This information is collected and turned into threat intelligence.

8. Dr. Moore specifically credits the technology in the '205 Patent as a system for operationalizing threat

intelligence into policies of rules that are uploaded into network devices to block dynamic threats. Tr. 321:5-9, 320:16-25.

9. Cisco's expert on the '205 Patent, Dr. Kevin Jeffay, challenges Dr. Moore's characterization by noting that the specific claims at issue have no relation to the blocking of malicious traffic. Instead, Dr. Jeffay characterizes the claims at issue as dealing with the encapsulation, copying and forwarding of voice traffic over the internet. Tr. 2727:11-19, 2732:2-19. More generally, Dr. Jeffay describes the claims at issue as enabling law enforcement to potentially wiretap internet calls. Tr. 2732:13-16.

10. Centripetal accuses Cisco's Catalyst 9000 series switches, the Aggregation Services Router 1000 series routers and Integration Services Router 1000 and 4000 series routers, in combination with Cisco's Digital Network Architecture, of infringing Claims 63 and 77 of the '205 Patent. Additionally, Centripetal accuses Cisco's Adaptive Security Appliance 5500 series with Firepower services and Cisco's Firepower Appliance 1000, 2100, 4100, and 9330 series that run Firepower Threat Defense ("Cisco's Firewalls") with Firepower Management Center of infringing Claims 63 and 77 of the '205 Patent. Tr. 7235:16-20.

11. The accused switches, routers and firewalls have the ability to act as packet security gateways. Tr. 732:24-734:22, 735:15-20, 737:24-738:5.

12. Cisco's Digital Network Architecture Center serves as the "foundational controller . . . at the heart of Cisco's intent-based network . . . [and] provides a single dashboard for every fundamental management task." PTX-1294. Accordingly, both the DNA Center

and Cisco's Firepower Management Center manage and update security policies that are employed by the accused devices. Tr. 728:21-730:9; 736:3-13; PTX-1294 at 15.

13. The accused devices process a certain type of network traffic sent by Session Initiation Protocol ("SIP"). Tr. 739:13-18, 2782:12-17; PTX-1408 at 19. SIP is one of the many protocols that is used to transmit information over the internet. Tr. 739:5-9. SIP is primarily used for the sending of voice data, but can be used for video and instant messaging. Tr. 739:5-9, 741:15-24, 2729:13-19.

14. Each device, when making a call using SIP, has a unique identifier know as a SIP Uniform Resource Identifier ("SIP URI") that functions similarly to a telephone number. Tr. 2729:16-23. SIP URI is embedded within SIP traffic to identify the party to the call. Tr. 2729:16-23.

15. Cisco's expert, Dr. Kevin Jeffay, opined that a SIP URI consists of SIP and then a unique identifier of the individual device that is being called. Tr. 2739:1-7. He provided an example of a SIP URI as sip:jeffay@unc.edu. Tr. 2739:8-10.

16. Dr. Jeffay's opinion is confirmed by the Internet Engineering Task Force's Request for Comment ("RFC") 3261 that outlines the procedures for the SIP protocol. RFC 3261 confirms that a SIP URI contains the word SIP, and the document provides a specific example as "sip:user:password@host:port;uri-parameters?headers." DTX-1296 at 148. RFC 3261 contains many examples of SIP URIs that all contain the word sip. DTX-1296

(listing examples of SIP URIs such as "sip:alice@atlanta.com.").

17. Centripetal's expert, Dr. Michael Mitzenmacher, presented that the Firepower Management Center enables the network firewalls to monitor traffic sent by SIP for network exploits. Tr. 748:6-13; PTX-1289 at 912. The technical documents confirm that if any SIP traffic is found to be a threat to the network, rules may be created to prevent any dangers to the network. Tr. 748:19-24; PTX-1289 at 912.

18. The accused products have the capability to handle SIP traffic and can block that traffic that is determined to be malicious. Tr. 750:11-17.

19. However, Dr. Mitzenmacher presented no technical documents that confirm that the accused firewalls have specific rules that contain both a network address and a SIP URI. Tr. 2756:18-2757:2. Furthermore, no Cisco technical document confirms that the accused switches and routers have any rules that contain both a network address and a SIP URI. Tr. 2756:18-2757:2.

20. Dr. Mitzenmacher and Cisco's technical documents do confirm that the accused switches, routers and firewalls can forward and block packets. Tr. 754:11-756:7; PTX-1276 at 216; PTX-1493 at 009.

21. The accused devices can encapsulate and route packets. Tr. 756:8-758:21, 760:5-764:16; PTX-1262 at 994; PTX-524 at 309; PTX-1229 at 69; PTX-1293 at 062. However, Dr. Mitzenmacher presented no evidence that the accused devices perform a "copying" of information contained in the packets. Tr. 2749:24-2750:4 (Dr. Jeffay confirming no testimony or evidence on copying).

ii. Conclusions of Law Regarding Infringement

Cisco expert, Dr. Jeffay, opined that the '205 Patent was not infringed for two distinct reasons. First, he opined that Centripetal's infringement theory relies on the "blocking" of packets, but the asserted claims of the '205 Patent require encapsulation and forwarding. Second, he averred that Centripetal has not asserted any proof that the accused products have "at least one rule specifying a set of network addresses and a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI)," as required by the claims. The Court agrees with Dr. Jeffay on both of his non-infringement theories. The Court affirms Dr. Jeffay's characterization that the '205 Patent teaches a method of tapping internet-based phone communications and potentially video via the internet. It may be characterized as a method of spying upon or "hacking" internet communications, which is the converse of the four previous patents that are found as valid and infringed, the function of which is to provide network security.

On his first theory, Dr. Jeffay outlined the main focus of the invention in the '205 Patent is on Voice over IP traffic and the encapsulation and forwarding of data. He opined:

> Q. And turning to slide 5, how many disputes—on the infringement issue, how many major disputes do you intend to focus on today?
>
> A. Well, in my report I documented several disputes, but in the interest of time, we're going to focus on two here, and these are the two that I think are the easiest to see. And

> the first one is really sort of a black/white issue; that Centripetal's theory of infringement focuses on the blocking of packets. And blocking has really been the key to most of this case; that the accused products block packets. But the '205 [P]atent is not about blocking packets, it's about precisely the opposite. It's about doing things that we'll come to see are called encapsulation and forwarding, but the point here is that we want the packets to go through to their destination. We're going to see that the patent is really about enabling law enforcement to potentially wiretap phone calls, so we want the package to go through. And so the '205 claims are really about the opposite of what we've heard in this case; they're about letting packets make it to their destination.

Tr. 2731:24-2732:19. Dr. Jeffay explained in detail Figure 6 of the '205 Patent, walking through the major outline of the invention, as described by the claims:

FIG. 6 from the '205 Patent

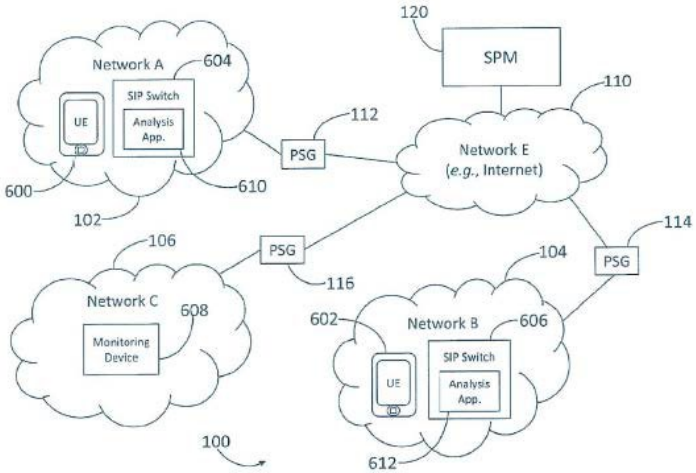


FIG. 6

Q. We've got figure 6 up now. Dr. Jeffay, could you, using figure 6, walk the Court through the major components of the claimed invention.

A. Sure. So this is the world—this a version of the world in which the claimed invention would operate. So let's focus first on network A, which is in the upper left-hand corner. And in network A there is a device, UE 600. Now, UE in the patent stands for User Equipment, but what I'd like the Court to think of it—think of it as a phone. And you can kind of see it's drawn kind of like an iPhone. So it's a phone. And what's going to happen here is that this user in network A is going to make a phone call, a Voice over IP phone call, to a user in network B. So let's highlight network B, which is on the lower right. And we can see

that also there's a UE 602, User Equipment, just basically another phone, that's in network B. So a user in network A makes a call to a user in network B, and what the patent is about is using an SPM 120—SPM is going to stand for Security Policy Management server; this is the entity that creates security policies. The SPM is going to send a policy that contains a rule to a packet security gateway 112. So the packet security gateway is the thing that actually looks at the packets. Now the rule—the policy contains a rule, and the rule that's going to be sent to the packet security gateway is going to contain information to allow the packet security gateway to identify the packets corresponding to this Voice over IP phone call. And when it identifies the right kind of packets, what it's going to do is a little unusual. It's going to let the packets go through. It's not going to block the packets, but it's not going to send the packets to their intended destination, which is network B. It's going to send them to network C, which is shown on the lower left. And in network C you can see that there's a monitoring device, and what's going to happen is the packets are going to be routed from the packet security gateway, to network C, to this monitoring device. The monitoring device is then going to copy some information from the packets. It's going to keep that copied information, because, in theory, that's what law enforcement wants to see, but then we need

> the call to go through, so it's—the network device 608 is going to unencapsulate the packet, get the original packet, and send it on its way back to network B.

Tr. 2735:5-2736:24. In this explanation of the claims, Dr. Jeffay noted explicitly that the claims do not require the blocking of packets because "[i]f the call is blocked, then the packets would be dropped at the packet security gateway 112, and there would be nothing to monitor." Tr. 2742:19-21. Based on an independent reading of the claims, the Court agrees with Dr. Jeffay that the scope of the asserted claims of the '205 Patent deal specifically with the functionality to encapsulate, copy and then forward on packets to a different network.

To prove infringement, Centripetal's expert Dr. Mitzenmacher specifically identified the '205 Patent as:

> Q. If we can go to your demonstrative, can you briefly explain what this is showing, in terms of the '205 [P]atent, with the dynamic security policy?
>
> A. As we've seen for all of these systems, they will be given threat intelligence, or gather or absorb threat intelligence, and they can use that to update the rules. In particular, just generally, they have dynamic security policies. They're constantly getting new information, and over time, they will often update the rule sets in order to deal with new threats accordingly.

Tr. 726:21-727:5. Dr. Mitzenmacher, in his infringement opinion, specifically focused on the use

of threat intelligence being used to block malicious traffic in the network. In his testimony, Dr. Mitzenmacher confirms that the accused products can perform the encapsulation of packets. Tr. 756:8-758:21, 760:5-764:16. This is confirmed by the Cisco technical documents. PTX-1262 at 994; PTX-524 at 309; PTX-1229 at 69; PTX-1293 at 062. But the encapsulation of packets described by Dr. Mitzenmacher and the technical documents is not all that is required by the asserted claims. This element of the claim reads:

> encapsulate at least one packet of the packets that falls within the set of network addresses and matches the SIP URI with a header containing a network address that is different from a destination network address specified by the at least one packet and that corresponds to a network device **configured to copy information** contained in the at least one packet and to forward the at least one packet to the destination network address . . .

JTX-1 (emphasis added). Dr. Mitzenmacher presented no testimony or technical documents that confirmed that the accused products are "configured to" or have the ability to copy information, as outlined by the asserted claims. Tr. 2749:24-2750:4; see PTX-1262 at 994; PTX-524 at 309; PTX-1229 at 69; PTX-1293 at 062. Additionally, there is no evidence in the documents presented by Dr. Mitzenmacher that the encapsulated packets are those that "fall within the set of network addresses and matches the SIP URI with a header containing a network address . . . ." See

PTX-1262 at 994; PTX-524 at 309; PTX-1229 at 69; PTX-1293 at 062. For these reasons, Centripetal has failed to prove by a preponderance of the evidence that the accused products embody each and every limitation of the patented claim. See V-Formation, Inc. v. Benetton Group SpA, 401 F.3d 1307, 1312 (Fed. Cir. 2005).

Turning to the second theory, Dr. Mitzenmacher presented no document that specifies that the accused products contain" at least one rule specifying a set of network addresses and a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI)," as required by the claims. For the accused routers and switches, Dr. Mitzenmacher points to a presentation, PTX-1408, that shows that SIP traffic passes through Cisco's products. This document's mere mention of SIP traffic is not compelling evidence that Cisco's routers and switches have rules that contain SIP URI and network addresses. See Tr. 2756:18-2757:2. PTX-1408. Similarly, for the accused firewalls, Dr. Mitzenmacher turns to PTX-1289 to show that the Cisco firewalls have four SIP keywords that allow the user to monitor SIP traffic for exploits. PTX-1289 at 808. This document contains no mention of having specific rules that contain SIP URIs in combination with network addresses. Viewing all of the documents and testimony presented by Dr. Mitzenmacher, there is sufficient evidence to conclude that the accused products process SIP traffic. However, there is no compelling evidence to show that the accused products have rules that possess both a SIP URI and a network address, as required by the claims. See Tr. 2756:18-2757:2.

Additionally, the Court **FINDS** that there is no infringement of the '205 Patent under the doctrine of equivalents. Dr. Mitzenmacher, in his equivalents testimony, stated:

> Q. So, go ahead. Can you, please, explain for the Court how the switches, routers, and firewalls perform substantially the same function.
>
> A. Certainly. So it provides substantially the same function, which is to block potentially malicious network traffic that's been determined or related to a Session Initiation Protocol URI. It does this in the same way; by specifying a rule that would block this corresponding traffic. It may do so—it does so by establishing a rule containing relevant SIP information, such as a domain or an IP address, and it achieves substantially the same result, which is to block that potentially—or create rules which would either block or monitor, or whatever action you want to take, on the corresponding Session Initiation Protocol traffic.

Tr. 774:23-775:12. The Court has already determined that the asserted claims cover the encapsulation, copying and forwarding of packets. Blocking packets, as identified by Dr. Mitzenmacher, would not perform substantially the same function in substantially the same way as encapsulation, copying and forwarding. Accordingly, there is no infringement under the doctrine of equivalents.

For both of these reasons, the Court **FINDS** that Centripetal has not met its burden to prove by a

preponderance of the evidence that the accused products infringe Claims 63 and 77 of the '205 Patent literally or under the doctrine of equivalents.

iii. Validity

During trial, Cisco withdrew its claim that the '205 Patent was invalid. Tr. 2795:16-24. Therefore, this Court will not address the validity of the '205 Patent as it is not required to rule upon the validity of a patent which has not been found infringed.

VI. FINDINGS OF FACT AND CONCLUSIONS OF LAW REGARDING DAMAGES

A. PAST DAMAGES

i. Findings of Fact and Conclusions of Law Regarding Reasonable Royalty Base and Rate

"Upon finding for the claimant the court shall award the claimant damages adequate to compensate for the infringement, but in no event less than a reasonable royalty for the use made of the invention by the infringer, together with interest and costs as fixed by the court." *Lucent Techs., Inc. v. Gateway, Inc.*, 580 F.3d 1301, 1324 (Fed. Cir. 2009) (quoting 35 U.S.C. § 284). In awarding damages under the governing statute, 35 U.S.C. §284, "a reasonable royalty is the minimum permissible measure of damages." *Deere & Co. v. Int'l Harvester Co.*, 710 F.2d 1551, 1558 n.9 (Fed. Cir. 1983). The Supreme Court has framed reasonable royalty damages achieved through litigation as a court's duty to assess "the difference between [the patentee's] pecuniary condition after the infringement, and what his condition would have been if the infringement had not occurred." *Yale Lock Mfg. Co. v. Sargent,* 117 U.S. 536,

552 (1886). The burden of proving damages as a result of infringement falls on the patentee. *Lucent Techs., Inc.*, 580 F.3d at 1324. The Federal Circuit has determined two acceptable "alternative categories of infringement compensation." *Id.* The first category is based on a patentee's lost profits. *Id.* To recover lost profits, "a patent owner must prove a causal relation between the infringement and its loss of profits." *Shockley v. Arcan, Inc.*, 248 F.3d 1349, 1362 (Fed. Cir. 2001). The patentee is required to "show a reasonable probability that 'but for' the infringing activity, the patentee would have

made the infringer's sales." *Id.* The four-factor test for utilizing the lost profit model is laid out in *Panduit Corp. v. Stahlin Bros. Fibre Works, Inc.*, 575 F.2d 1152, 1156 (6th Cir. 1978).[11] The lost profits method is not at issue in this case since Centripetal has not presented any evidence of a causal relationship between suspected lost profits and Cisco's sales of the infringing technology. The second category, which the Court adopts in this case, is based on the "the reasonable royalty . . . [the patentee] would have received through arms-length bargaining." *Lucent Techs., Inc.*, 580 F.3dat 1324.

In determining this reasonable royalty, patentees have primarily used two distinct methods of

[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).

calculation. "The first, the analytical method, focuses on the infringer's projections of profit for the infringing product." *See id.* (citing *TWM Mfg. Co. v. Dura Corp.,* 789 F.2d 895, 899 (Fed. Cir. 1986) (describing the analytical method as "subtract[ing] the infringer's usual or acceptable net profit from its anticipated net profit realized from sales of infringing devices")). Here, there was insufficient evidence submitted to the Court based on the infringer's profit projections and thus this method is inappropriate for calculating damages. "The second, more common approach, called the hypothetical negotiation or the 'willing licensor-willing licensee' approach, attempts to ascertain the royalty upon which the parties would have agreed had they successfully negotiated an agreement just before infringement began." *Id.* The date used for the occurrence of the hypothetical negotiation is the date that infringement began. *Wang Labs., Inc. v. Toshiba Corp.*, 993 F.2d 858, 870 (Fed. Cir. 1993). The evidence at trial supports a first infringement date of June 20, 2017. The Court **FINDS** the reasonable royalty method to be appropriate based on the evidence presented by both Centripetal and Cisco.

To determine a reasonable royalty, the Court bases its economic analysis on the factors laid out in *Georgia-Pacific Corp. v. U.S. Plywood Corp.*, 318 F. Supp. 1116, 1120 (S.D.N.Y. 1970). Determining a reasonable royalty involves the Court's analysis into each of the relevant *Georgia-Pacific* factors:

> (1) Any royalties received by the licensor for the licensing of the patent-in-suit, proving or tending to prove an established royalty.

(2) The rates paid by licensee to license other patents comparable to the infringed patents.

(3) The nature and scope of the license, as exclusive or non-exclusive, or as restricted or non-restricted in terms of its territory or with respect to whom the manufactured product may be sold.

(4) The licensor's established policy and marketing program to maintain its right to exclude others from using the patented invention by not licensing others to use the invention, or by granting licenses under special conditions designed to preserve that exclusivity.

(5) The commercial relationship between the licensor and the licensee, such as whether or not they are competitors in the same territory in the same line of business.

(6) The effect of selling the patented product in promoting other sales of the licensee; the existing value of the invention to the licensor as a generator of sales of its non-patented items; and the extent of such collateral sales.

(7) The duration of the infringed patents and the term of the license.

(8) The established profitability of the product made under the infringed patents; its commercial success; and its popularity.

(9) The utility and advantages of the patented invention over the old modes or devices, if any, that had been used for achieving similar results.

(10) The nature of the patented invention; the character of the commercial embodiment of it as owned and produced by or for the licensor; and the benefits to those who have used the invention.

(11) The extent to which the infringer has made use of the invention; and any evidence that shows the value of that use.

(12) The portion of the profit or of the selling price that may be customary in the particular business or in comparable businesses to allow for the use of the invention or analogous inventions.

(13) The portion of the profit that arises from the patented invention itself as opposed to profit arising from unpatented features, such as the manufacturing process, business risks, or significant features or improvements added by the accused infringer.

(14) The opinion testimony of qualified experts.

(15) The amount that a licensor (such as Centripetal) and a licensee (such as Cisco) would have agreed upon (at the time the infringement began) if both sides had been reasonably and voluntarily trying to reach an agreement; that is, the amount which a prudent licensee—who desired, as a business proposition, to obtain a license to manufacture and sell a particular article embodying the patented invention—would have been willing to pay as a royalty and yet be able to make a reasonable profit and which

> amount would have been acceptable by a patentee who was willing to grant a license.

See Georgia-Pacific Corp. v. U.S. Plywood Corp., 318 F. Supp. 1116, 1120 (S.D.N.Y. 1970), *modified sub nom. Georgia-Pacific Corp. v. U.S. Plywood-Champion Papers, Inc.*, 446 F.2d 295 (2d Cir. 1971). The Court will examine each of the relevant *Georgia-Pacific* factors that guide its determination of a proper reasonable royalty rate.[12]

Beginning with *Georgia-Pacific* factors one and two, the only comparable license of the patents-in-suit is the Confidential Binding Term Sheet agreed to in a previous case tried by this Court—*Centripetal Networks, Inc., v. Keysight Technologies, Inc. and Ixia*, Case No. 2:17-cv-383 (E.D Va.). The Court is limited to this license granted by Centripetal as the only comparable license, as neither party presented any comparable licenses for similar patented inventions or similar infringing products. Tr. 1498:2-10. Although Cisco licensed Stealthwatch for a period of years from Lancope before Cisco acquired the company in 2013, neither Centripetal nor Cisco presented evidence of this or any other license in which Cisco was involved, and the Keysight agreement is the only licensing agreement in which Centripetal has been involved. The Keysight agreement was entered into by Centripetal and Keysight/Ixia during trial to settle the

---

[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 for qualified experts) to support its analysis of the other factors.

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 comparable because Keysight was a direct competitor in the threat intelligence gateway market, and Cisco is not. Although Centripetal does not market and sell switches and routers, Cisco has embedded the patented software functionality from the Centripetal patents into the infringing switches and routers that provides the same functionality as the RuleGate

product. Centripetal does market and sell firewalls. Accordingly, the Court **FINDS** that Centripetal and Cisco are direct competitors with respect to the infringing software, as well as firewalls. This incorporation of infringing functionality persuades the Court that the infringing Cisco products are more comparable to the 10% royalty on competing products than the 5% royalty for non-competing products in Keysight. Accordingly, the 10% royalty on directly competing products in the Keysight case provides a comparable baseline license from which the Court can determine a reasonable royalty in this case.

The Court recognizes that the Keysight license was obtained in the coercive environment of litigation and not the result of open negotiation. *See LaserDynamics, Inc. v. Quanta Computer, Inc.*, 694 F.3d 51, 77 (Fed. Cir. 2012) (highlighting that "[t]he notion that license fees that are tainted by the coercive environment of patent litigation are unsuitable to prove a reasonable royalty is a logical extension of *Georgia-Pacific* . . ."). Generally, these types of settlement agreements "should not be considered evidence of an established royalty." *Id.* (citing *Hanson v. Alpine Valley Ski Area, Inc.,* 718 F.2d 1075, 1078-79 (Fed. Cir.1983). However, the Federal Circuit has recently permitted reliance on such agreements "under certain limited circumstances." *Id.* In the case of *ResQNet.com, Inc. v. Lansa, Inc.*, the Federal Circuit "permitted consideration of the settlement license on remand" because the "settlement license to the patents-in-suit in a running royalty form was 'the most reliable license in [the] record.'" *Id.* (discussing and quoting language from *ResQNet*); *see*

ResQNet.com, Inc. v. Lansa, Inc., 594 F.3d 860, 872 (Fed. Cir. 2010).

Similarly, here, the Court, has only one comparable license in the form of a settlement agreement from the Keysight case. The Court, in its use of this license to determine a reasonable royalty, heeds the guidance of the Federal Circuit to "consider the license in its proper context within the hypothetical negotiation framework to ensure that the reasonable royalty rate reflects "the economic demand for the claimed technology." *Id.* Therefore, the Court will analyze the Keysight rate in the context of the other *Georgia-Pacific* factors to account for the similarities and differences in the Keysight license and the facts present in this case. *See AstraZeneca AB v. Apotex Corp.*, 782 F.3d 1324, 1335 (Fed. Cir. 2015) (finding no error when the district court accounted for similarities and differences between past negotiations and the hypothetical negotiations); *see also Elbit Sys. Land & C4I Ltd. v. Hughes Network Sys., LLC*, 927 F.3d 1292, 1300 (Fed. Cir. 2019) (collecting cases that show it is appropriate to rely on prior licenses, even in a settlement context, when they are sufficiently compared to the facts and circumstances of the case at issue).

Turning to *Georgia-Pacific* factor three, the scope and nature of the Keysight license weighs in favor of reducing the baseline royalty percentage, because the license presented to Cisco would be limited to the infringing patents instead of a full patent portfolio that was granted in Keysight. Consequently, the Court agrees with Dr. Becker that this factor promotes in favor of a royalty rate reduction. Tr. 2869:2-12.

Georgia-Pacific factor four has some influence on the royalty figure. The Court can infer that Centripetal was at least willing to license its patent portfolio to Keysight, for the terms outlined in the agreement, in order to settle ongoing litigation. This comparable license shows that Centripetal may have been willing to license the asserted patents to Cisco. It is a consideration that would sway the Court to adjust the royalty somewhat in a downward direction. The license is a major consideration in Centripetal's request for injunctive relief.

Georgia-Pacific factor five has minimal impact on the royalty figure. This factor asks the Court to inquire into the commercial relationship of the parties at the hypothetical negotiation. The Court notes that Centripetal has presented evidence that Cisco's incorporation of the patented functionality into its products would result in substantial lost profits from the competing RuleGate product. Generally, this fact would weigh in favor of increasing the royalty as Centripetal, in the hypothetical negotiation, would consider the substantial loss that may be attributed to licensing the patented technology.[13] From Cisco's

[13] "It is a step further, and we think a necessary one, to say that, when the patentee's business scheme involves a reasonable expectation of making future profits by the continuing sale to the purchaser of the patented machine, of supplies to be furnished by the patentee, which future business he will lose by licensing a competitor to make the machine, this expectant loss is an element to be considered in retroactively determining a reasonable royalty." *Panduit Corp. v. Stahlin Bros. Fibre Works, Inc.*, 575 F.2d 1152, 1163 (6th Cir. 1978) (quoting *Egry Register Co. v. Standard Register Co.*, 23 F.2d 438, 443 (C.C.A. 6th Cir. 1928)).

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 software technology to Cisco in order to take advantage of Cisco's substantial market share. *See* Tr. 1449:17-1451:2. The Court **FINDS** that all these considerations generally neutralize each other and warrant no variance to the royalty number.

Georgia-Pacific factor six does call for some upward influence. Cisco has incorporated the patented software functionality into a variety of its routers, switches and firewalls in its network security system. Therefore, the effect of the sales and the profits therefrom are promoted by Centripetal's software. The

upward influence is somewhat offset by the apportionment analysis of Centripetal's experts. There was no evidence presented that the infringing products contributed to increased sales of any of Cisco's other non-infringing products.

Georgia-Pacific factor seven inquires as to the duration of the patent and terms of the license. The Court's inquiry into the length of the license is more appropriately construed in terms of an ongoing royalty, and will be addressed in that portion of the Court's findings.

Georgia-Pacific factor eight deals with the profitability of products made under the patent and the commercial success of those products. One of Centripetal's damages experts, Mr. Gunderson, presented detailed evidence of Cisco's profitability of the infringing products. The Federal Circuit has expressly noted that "anticipated incremental profits under the hypothesized conditions are conceptually central to constraining the royalty negotiation . . . [and] . . . [e]vidence of the infringer's actual profits generally is admissible as probative of his anticipated profits." *Aqua Shield v. Inter Pool Cover Team*, 774 F.3d 766, 772 (Fed. Cir. 2014); *see Sinclair Refining Co. v. Jenkins Petroleum Process Co.,* 289 U.S. 689, 698 (1933) (noting "[e]xperience is then available to correct uncertain prophecy"). In the context of the hypothetical negotiation, "the core economic question is what the infringer, in a hypothetical pre-infringement negotiation under hypothetical conditions, would have anticipated the profit-making potential of use of the patented technology to be, compared to using non-infringing

alternatives." *Aqua Shield*, 774 F.3d at 770-71 (emphasis in original) (noting that "[i]f a potential user of the patented technology would expect to earn X profits in the future without using the patented technology, and X + Y profits by using the patented technology, it would seem, as a prima facie matter, economically irrational to pay more than Y as a royalty—paying more would produce a loss compared to forgoing use of the patented technology").

As probative evidence of anticipated profits, Mr. Gunderson provided percentages of Cisco's actual gross profit in the infringed products from June 20, 2017 to December 31, 2019:

Product	**Gross Profit %**
Catalyst Switches	67.8%
Aggregation Services Router	79.2%
Integration Services Router	82.0%
Adaptive Security Appliance	56.6%
Firepower Appliance	71.1%
Firepower Management Center	76.5%
Stealthwatch	81.4%
Identity Services 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

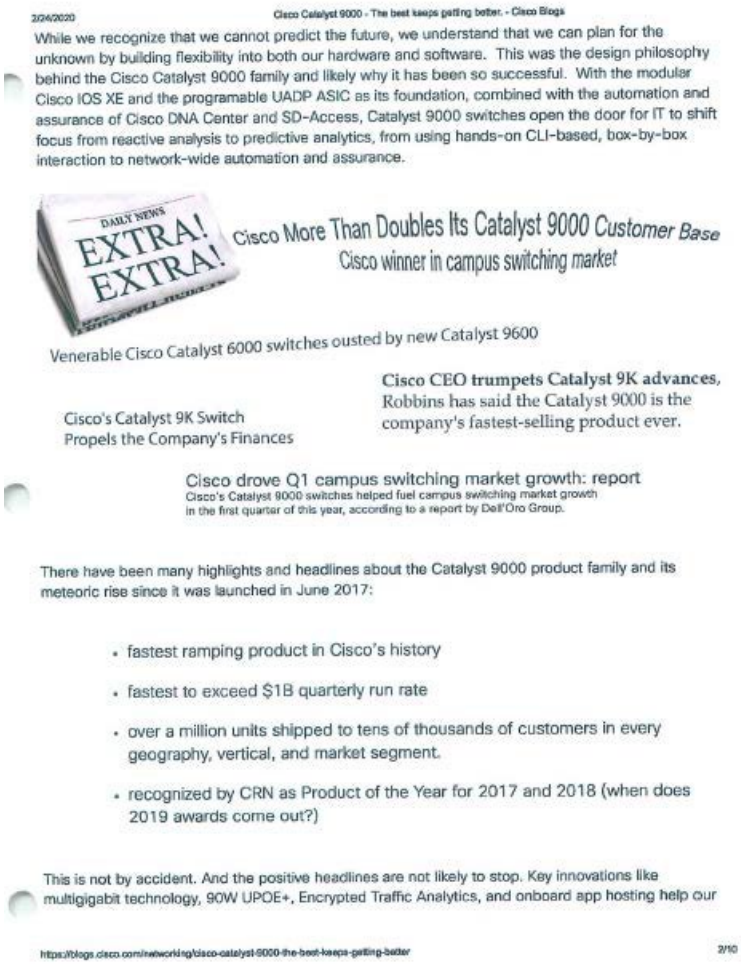
Cisco Article Published on Website from November 7, 2019

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.



2/24/2020 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.

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 functionality as incorporated in the patented technology. *See* Tr. 1602:8-16 (Mr. Malackowski noting that "Cisco did not suggest or offer any alternatives or even what it would cost to come up with alternatives"). Therefore, at a hypothetical

negotiation, Centripetal would hold a considerable advantage due to the lack of non-infringing alternatives and the ability for Cisco to make large profits from the use of the technology. This evidence of high profits and lack of alternatives supports a higher reasonable royalty rate. *See Lucent Techs., Inc.*, 580 F.3d at 1335 (noting that approximately 70-80% profit margin of the products at issue supports a higher versus a lower reasonable royalty).

Additionally, Mr. Malackowski, Centripetal's expert on patent evaluation, testified to his understanding that the Keysight license was structured in the manner it was due partly to the fact that Keysight had no available alternative to infringing the patent technology. *See* Tr. 1602:8-23. Accordingly, the 10% rate on competing products in the Keysight license had incorporated Keysight's necessity of using the infringing technology. Here, similar circumstances would be prevalent at the hypothetical negotiation, such as Cisco's "anticipated" profit margins in using the patented functionality and also the fact that there are no suitable alternatives available. Consequently, this factor supports the Court's imposition of a higher royalty rate.

Georgia-Pacific factor nine asks the Court to look at the utility and advantages of the patented property over the old modes or device. When developing its cybersecurity software system, Cisco repeatedly spent considerable monies to acquire smaller companies that produced software security technology. From 2013 to 2015, Cisco acquired Sourcefire for $2.7 billion, Lancope for $435 million and ThreatGRID for an undisclosed amount. *See* Tr. 1605:6-15.

Combinations of technology acquired from these companies form the basic elements of the older Cisco technology which preceded the infringing systems. *See* Tr. 1605:6-23. Cisco took the acquired technology and came up with what it described as the first cybersecurity solution of its type in the industry by adding Centripetal's patented functionality. Accordingly, these dollar amounts that Cisco paid to acquire two of the three companies is compelling evidence that the underlying older components of the infringing system needed enhancement by adding the infringing functionality from Centripetal to become the industry leader in this new technology as it claims to be.

During trial, each of Cisco's experts on infringement, validity, and damages testified that the patented inventions add minimal value to the products. Their testimony is in direct conflict with Cisco's technical and marketing documents which contribute the addition of the infringing functionality as a "breakthrough" in building "an intelligent platform with unmatched security." PTX-1135 (Cisco Press Release from June 20, 2017, reproduced below); PTX-963.

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

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

News Release (/Pressreleases)

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

June 20, 2017

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

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

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

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

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

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

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

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

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

Informed by context and powered by intent

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

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

The technologies that power the intuitive network

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

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 (David Goeckeler, Cisco's Senior Vice President of Sales, representing Cisco's new technology). Additionally, these representations made by as dominant a company as Cisco would have

a devastating impact upon Centripetal as the original inventor of the technology. Therefore, under factor nine, Cisco's technical and marketing documents, as well as previous business acquisitions, support a higher royalty rate, as the addition of the infringing technology greatly improved Cisco's sales and the profitability of its new infringing versions of the products over older models. *See Deere & Co. v. Int'l. Harvester Co.*, 710 F.2d 1551, 1558 (Fed. Cir. 1983) (supporting a higher royalty rate in light of descriptions that the infringing product had a "bright future").

Cisco's representations are confirmed by the increase in revenues from previous non-infringing versions of the products vs. the new infringing models. Moreover, the increase in revenues can be analyzed under Georgia-Pacific factor eleven to show the great extent which Cisco has made use of the patented invention. The Court, at the end of the trial, requested both parties to supplement their damages reports with revenue data from the predecessor products compared to the infringing products. *See* Tr. 2967:17-2973:5. This table summarizes Centripetal's estimates regarding Cisco's revenue increase for the infringing products, after the date of first infringement, as compared to the predecessor products sales for the fiscal year before June 20, 2017:

Product	**Increase in Revenues %**	**Increase in Revenues $ (in millions)**
Switches	40.9%	$3,973.4
Routers	13.2%	501.5

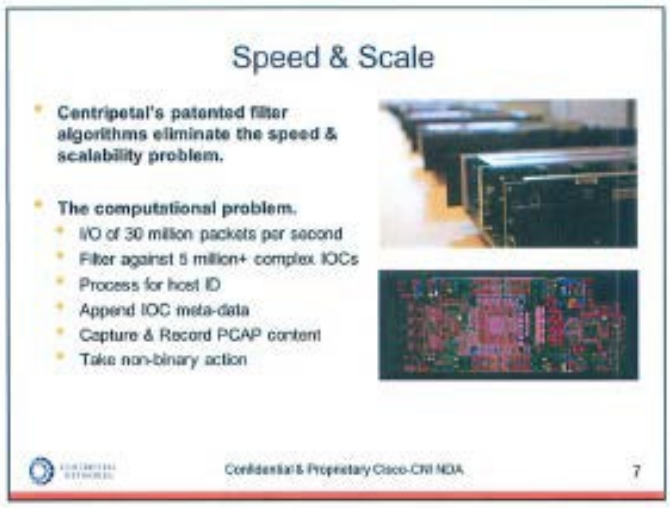
Adaptative Security/Firepower	29.5%	550.4
Stealthwatch	36.0%	70.2
Firepower Management Center	3.5%	1.7
Identity Services Engine	52.0%	225.3
Digital Network Architecture[14]	100%	252.9
Total Increases		5,575.4

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 at high speeds and how Centripetal's rule swap technology aids that process and is disclosed in the '806 Patent); *see* PTX-547.

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

PTX-547

Centripetal Demonstrative Presentation Presented to Cisco About Patented Technology



Viewing both Cisco's technical documents, marketing representations and the sales data, the Court **FINDS** that the patented functionality added very significant

value to the older technology. Therefore, this factor supports a substantially increased royalty figure.

Accordingly, based upon its analysis of the Georgia-Pacific factors, the Court determines that the weight of the factors as a whole strongly favors Centripetal. As a result, the Court **FINDS** that the Keysight royalty rate of **10%** of the apportioned value of its infringed technology is a reasonable royalty rate to compensate Centripetal for Cisco's past infringement. This figure is supported both by the comparable factors in the Keysight license and the weight of the Georgia-Pacific factors. Now that the Court has determined a reasonable royalty rate, it must determine the proper royalty base to which to apply the rate in order to reach the final lump sum pretrial damages.

Georgia-Pacific factor thirteen looks at the portion of the profit that arises from the patented invention itself as opposed to profit arising from unpatented features, such as the manufacturing process, business risks, or significant features or improvements added by the accused infringer. Therefore, instead of having a primary effect on the royalty rate, this factor is often used to determine the royalty base to which the rate is applied.

With regard to the proper royalty base, the Federal Circuit has noted that patent damages awarded for infringement "must reflect the value attributable to the infringing features of the product, and no more." *Commonwealth Sci. & Indus. Research Org. v. Cisco Sys., Inc.*, 809 F.3d 1295, 1301 (Fed. Cir. 2015) (quoting *Ericsson, Inc. v. D-Link Sys., Inc.,* 773 F.3d 1201, 1226 (Fed. Cir. 2014)). When an infringing

product is comprised of multiple components, the infringing portions must be apportioned to represent the value contributed by solely the infringing functionality. *See id.* "The patentee must 'give evidence tending to separate or apportion the [infringer]'s profits and the patentee's damages between the patented feature and the unpatented features, and such evidence must be reliable and tangible, and not conjectural or speculative.'" *Finjan, Inc. v. Blue Coat Sys., Inc.,* 879 F.3d 1299, 1310 (Fed. Cir. 2018). The Federal Circuit has recognized "there may be more than one reliable method" in order to prove proper damages in an apportionment case. *Id.* at 1302. Therefore, the apportionment can be done by various ways including "by careful selection of the royalty base to reflect the value added by the patented feature, where that differentiation is possible; by adjustment of the royalty rate so as to discount the value of a product's non-patented features; or by a combination thereof." *Ericsson, Inc. v. D-Link Sys., Inc.*, 773 F.3d 1201, 1226 (Fed. Cir. 2014).

This flexibility in methodology is centered on "the difficulty that patentees may face in assigning value to a feature that may not have ever been individually sold." *Virnetx, Inc. v. Cisco Sys., Inc.*, 767 F.3d 1308, 1328 (Fed. Cir. 2014). Therefore, the integral inquiry is "whether the data utilized in the methodology is sufficiently tied to the facts of the case." *Finjan, Inc.*, 879 F.3d at 1301-02 ("[C]ourts must be proactive to ensure that the testimony presented—using whatever methodology—is sufficiently reliable to support a damages award."). Sufficient reliability has "never required absolute precision in this task; on the contrary, it is well-understood that this process may

involve some degree of approximation and uncertainty." *Virnetx, Inc.*, 767 F.3d at 1328.

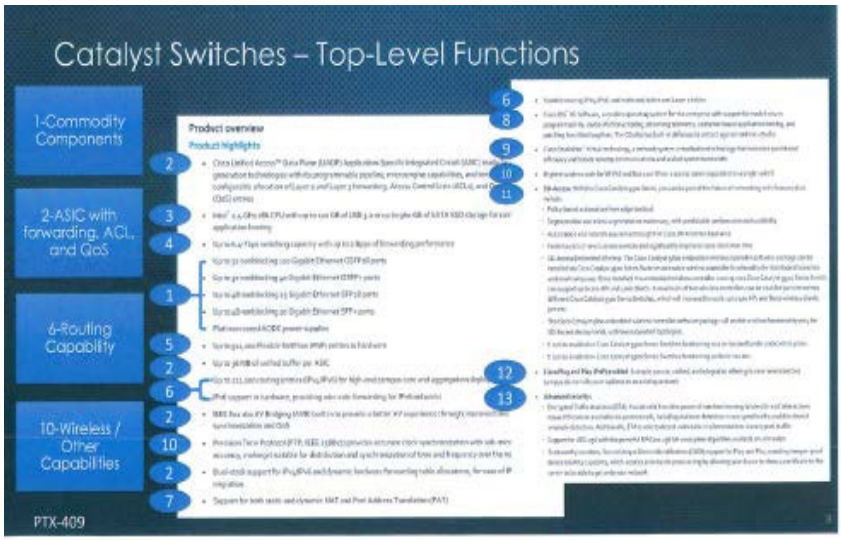
Here, Centripetal presented extensive apportionment evidence of the infringing products using the analysis of their apportionment expert, Dr. Striegel. Tr. 1337:19-1342:14. Before Dr. Streigel's testimony, Cisco objected to Dr. Streigel's apportionment opinion on the basis that his opinions do not satisfy the essential requirement for reliability under *Daubert*. Additionally, Cisco's expert, Dr. Becker, contends that "Dr. Striegel didn't do an incremental value analysis," and simply checked off functions as infringing that did not provide "any improvement to that aspect of the products." The Court disagrees on both grounds.

This is exactly the type of apportionment analysis that was performed in *Finjan, Inc. v. Blue Coat Sys., Inc.*, for which the Federal Circuit found the jury was entitled to rely upon as substantial evidence to support damages. *Finjan, Inc.*, 879 F.3d at 1313-14. In *Finjan*, Finjan's expert, Dr. Layne-Farrar, used the defendant's technical documents to separate the functionality of the accused product. *Id.* She assumed each box in a diagram of the product "represented one top level function and that each function was equally valuable." *Id.* Dr. Layne-Farrar relied on deposition testimony from defendant's employees and discussions with Finjan's technical expert, who "identified certain components within the diagram that did and did not infringe." *Id.* at 1313.

Here, Dr. Striegel performed an almost identical type of apportionment analysis to that of Dr. Layne-Farrar in *Finjan*. Using Cisco's technical specification

of each of the products, Dr. Striegel identified the top-level functions of each of the products. Tr. 1337:21-23; *see* PTX-409. Dr. Striegel's process of identifying the top-level functions by using Cisco's technical documents is shown by slide eight from his demonstratives (using Catalyst Switches Product Overview, PTX-409, as an example for the analysis done with each product):

SLIDE 8 FROM DR. STRIEGEL PRESENTATION



See PTX-409 (for clear image of technical features). He then identified which of those top-level functions for each product are implicated by the asserted patents and their asserted claims. *See* PTX-1931. In order to analyze and present this technical apportionment, Dr. Striegel highlighted all of the materials he relied upon in this analysis:

> I looked at both public documentation as well as confidential documents including various

> articles, various videos, various tutorials. I also browsed through numerous depositions. I did have the opportunity to go and browse through the source code on-site. And then I also had discussions with our two other infringing technical experts, Dr. Cole and Dr. Mitzenmacher.

Tr. 1338:9-15. This is exactly the type of materials relied upon by Dr. Layne-Farrar in the *Finjan* case, where the Federal Circuit determined that the jury was entitled to rely upon such information as substantial evidence to support a damages award. Accordingly, the Court **FINDS** that Dr. Striegel's analysis is admissible as "reliable and tangible" evidence of apportionment of the infringing products. *See Ericsson, Inc.*, 773 F.3d at 1226 (highlighting that a court or jury must "apportion the defendant's profits and the patentee's damages between the patented feature and the unpatented features" using 'reliable and tangible' evidence"). Accordingly, the Court **FINDS** Dr. Striegel's apportionment evidence and analysis to be a reliable method to determine a royalty base.

As shown *supra*, Dr. Striegel opined on each of the infringing products, and determined how many of the top-level functions were implicated by infringement of the asserted patents. Dr. Striegel then determined an apportionment percentage for each of the infringing products based off this analysis. PTX-1931 is a summary of those findings made by Dr. Striegel (recreation of PTX-1931):

Product	**Total # of Top-Level Fun-ctions**	**# Infringing Top-Level Functions**	**Apportion-ment %**
Catalyst Switches	13	6 [‘856 and ‘193 Patent] 5 [‘176 Patent] 4 [‘806 Patent]	31%[15]
Integrated Services Routers	9	4 [All Patents]	44%
Aggregated Services Routers	8	2 [All Patents]	25%

[15] Even though Dr. Striegel found that six of the thirteen functions were infringed by the ‘856 Patent and ‘193 Patent, he relied on the lower apportionment percentage of 31%. Therefore, the Court adopts that number for its determination of the royalty base in lieu of the 46% alternative based on the ‘856 Patent and the ‘193 Patent.

Firepower /ASA (including Firepower Management Center	13	7 ['806 Patent][16]	54%
Digital Network Architecture	10	3 ['806 Patent]	30%
Stealthwatch	5	4 ['806 Patent]	80%
Identity Services Engine	13	5 ['856 Patent]	38%

After Dr. Striegel's technical apportionment, Centripetal's expert on patent evaluation, Mr. Gunderson, applied these apportionment percentages to total sales revenues from the infringing products since the date of first infringement, June 20, 2017, through December 31, 2019. At the final damages hearing, these figures were updated through Cisco's sales data ending on June 20, 2020 and totaled $21,467,079,878.00 billion. *See* Doc. 488, Ex. 7 (updated version produced at damages hearing). The Court adopts Centripetal's exhibits outlining the sales revenues of Cisco. Cisco presented a patent by patent

[16] Since the '205 Patent was found to not infringe the higher number of infringing functionalities found for the '806 Patent is used for the Firepower / ASA because this would be the most accurate apportionment ratio. The Court has removed the '205 Patent from Dr. Striegel's chart and applied a 54% apportionment for products where the apportionment was based on the '205 Patent. *See* Doc. 488, Ex. 7.

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 20, 2017 through June 20, 2020, by using Centripetal's update to PTX-1629, Doc. 488, Ex. 7:

Product	Invoice Gross Revenue June 20, 2017 – June 20, 2020[17]	Apportionment Factor Percentage	Apportioned Revenue June 20,2017 – June 20, 2020
Catalyst Switches	$11,839,742,927	31%	$3,670,320,307
Integrated Services Routers	$2,375,633,299	44%	$1,045,278,652
Aggregated Services Routers	$3,456,557,172	25%	$864,139,293
Firepower Appliance (plus subscription)	$2,283,221,005	54%	$1,232,939,343
Adaptative Security Appliance (plus subscription)	$428,380,587	54%	$231,325,517
Firepower Management Center	$67,635,757	54%	$36,523,309
Digital Network Architecture	$252,855,962	30%	$75,856,789
Stealthwatch	$266,052,460	80%	$212,841,968
Identity Services Engine	$497,000,709	38%	$188,860,269
TOTAL	$21,467,079,878 (billion)		$7,558,085,447 (billion)

17

[17] As stated, *supra*, Centripetal's exhibit outlining the sales revenues of Cisco goes from June 20, 2017 to June 20, 2020. *See* Doc. 488, Ex. 7 (updated version produced at damages hearing).

Accordingly, based on Mr. Gunderson and the Court's analysis, the Court **FINDS** that the correct apportioned royalty base is $7,558,085,447[18] for all of the infringing products based upon gross revenue through June 20, 2020. Doc. 488, Ex. 7. Moreover, as determined *supra* based on the Georgia-Pacific factors and the analysis of a hypothetical negotiation, the Court **FINDS** a **10%** royalty is appropriate in this case. Accordingly, before the Court adjusts for enhanced damages, the total past damages award is $755,808,545 million (10% royalty rate applied to $7,558,085,447 million royalty base).

ii. Findings of Fact Regarding Willful Infringement and Enhanced Damages

1. Centripetal's RuleGate product practices the patents found to be infringing in this case. Centripetal marks its RuleGate product with the patents that it practices. Tr. 1203:12-1204:3; PTX-528; Tr. 1383:18-1385:15; PTX-1215.

2. In 2015, Centripetal CEO Stephen Rogers had a meeting with Pavan Reddy, a Cisco employee, where Mr. Rogers disclosed Centripetal product offerings and the effectiveness of their solutions. Mr. Reddy and Mr. Rogers had a follow-up meeting in 2015, where Centripetal provided a demonstration of their system and explained why it was an effective method of cyber defense. Tr. 256:8-257:12.

---

[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.

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.

5. After the WebEx meeting, Cisco's Engineer, TK Keanini, who attended the WebEx meeting, wrote an internal email, stating the team should "look at these algorithms" that Centripetal had and "study their [patent] claims." Tr. 1128: 8-1129:5; PTX-134 at 3.

6. The next day, on February 5, 2016, Centripetal's Jonathan Rogers sent an e-mail to Cisco summarizing the WebEx meeting, noting that Cisco "seemed to hone in on our filter technology and algorithms. The algorithms are a significant networking technology with broad application that we've productized for security. There were also a few

questions on our patents..." Tr. 1226:10-1227:18; PTX-102; PTX-1046

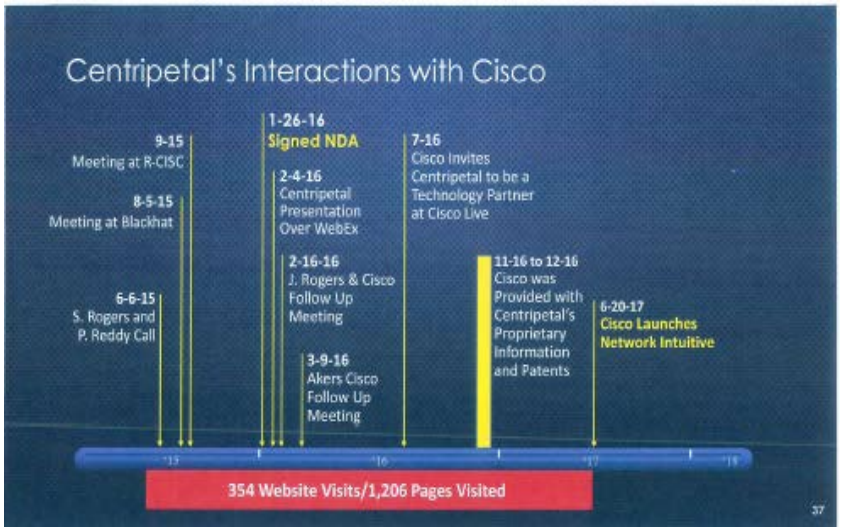
7. There were a number of follow up meetings with Cisco, including a request from Cisco's security architect, Joseph Muniz, who was very interested in Centripetal's patented technology. He requested and received a demonstration of Centripetal's patented RuleGate product, which he described in an online blog that educates Cisco employees entitled "Cool Tool: Centripetal Networks RuleGate—Threat Intelligence Tool," and where he stated, "I found this tool to be a pretty cool new approach to leveraging threat data." Tr. 1299:16-1300:7; 1308:5-15; PTX- 548, PTX-550 at 647-49, 51.

8. In November and December 2016, Cisco had several meetings with Oppenheimer & Co., Inc. about Centripetal, pursuant to Centripetal's engagement with Oppenheimer to evaluate companies who were interested in making a strategic investment in Centripetal. In December 2016, Oppenheimer presented to Cisco additional information about Centripetal, including a list of Centripetal's patents issued at the time, product offerings that practice the patents, and a highly sensitive, detailed technical disclosure which detailed the core RuleGate functionalities covered by the Asserted Patents. Tr. 1235:11-20, 1237:25-1238:9, 1242:17-1243:11; DTX-1270 at 1, 25-28, 30.

9. After all of these detailed meetings with Centripetal, Cisco released its "network of the future" products on June 20, 2017, which incorporated Centripetal's patented technology. See PTX-1135. Below is Centripetal's demonstrative, Slide 37,

presented during opening statements which accurate reflects the evidence presented at trial surrounding the events of Centripetal and Cisco's relationship[19].

SLIDE 37 FROM CENTRIPETAL'S OPENING STATEMENT



iii. Conclusions of Law Regarding Willful Infringement and Enhanced Damages

Under the patent damages provisions of 35 U.S.C. § 284, a court "may increase the damages up to three times the amount found or assessed." *Halo Elecs., Inc. v. Pulse Elecs., Inc.*, 136 S. Ct. 1923, 1931 (2016) (quoting 35 U.S.C. § 284). The use of "may" in the statute indicates that enhancement under § 284 is within the discretion of the district court. *Id.* The Supreme Court in *Halo Elecs., Inc. v. Pulse Elecs., Inc.*, explicitly noted that a court exercising discretion to

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

award enhanced damages merits an analysis of "the particular circumstances of each case" unencumbered by the "inelastic constraints" of a rigid framework. *Id.* at 1932. Although the statute does not include a "precise rule or formula" for an enhanced damages award, the "court's discretion should be exercised in light of the considerations underlying the grant of that discretion." *Id. Halo*, additionally, mandated that the award of enhanced damages is governed by a preponderance of the evidence standard. *Id.* at 1934.

Historically, enhanced damages have been reserved for infringement behavior that was found to be "egregious." *Id.* (explaining "through nearly two centuries of discretionary awards and review by appellate tribunals, "the channel of discretion ha[s] narrowed . . . so that such damages are generally reserved for egregious cases of culpable behavior"). The Halo decision highlights that enhanced damages are warranted as a "punitive" or "vindictive" sanction for egregious conduct described as "willful, wanton, malicious, bad-faith, deliberate, consciously wrongful, flagrant or—indeed—characteristic of a pirate." *Id.* at 1932.

Additionally, the Supreme Court noted that even if these types of conduct traditionally underlie enhanced damages, there is no requirement that the court find egregious conduct to award enhanced damages. *Id.* at 1933. Accordingly, in deciding to award enhanced damages, a court, in its discretion, "should take into account the particular circumstances of each case," while remembering the historical underpinnings that enhanced damages should

generally "be reserved for egregious cases typified by willful misconduct." *Id.* at 1933-34.

The factors laid out in *Read Corp. v. Portec, Inc.*, 970 F.2d 816, 826-827 (Fed. Cir. 1992), *overruled on other grounds by Markman v.Westview Inst. Inc.*, 52 F.3d 967 (Fed. Cir. 1995), have been used post-Halo to aid a district court's determination of whether a case's circumstances warrant enhanced damages. *See Mich. Motor Techs. LLC v. Volkswagen Aktiengesellschaft*, No. 19-10485, 2020 U.S. Dist. LEXIS 122276, at *11 (E.D. Mich. July 13, 2020) (noting that the *Read* factors are a useful guide, but stating that *Halo* has eliminated "any rigid formula or set of factors"). These factors are not an exhaustive list, but provide a meaningful guide to determine if the infringer's conduct was "willful, wanton, malicious, bad-faith, deliberate, consciously wrongful, or flagrant." *See id.*; *Finjan, Inc. v. Blue Coat Sys., Inc.*, 13-CV-03999-BLF, 2016 WL 3880774, at *16 (N.D. Cal. July 18, 2016) (applying the Read factors to determine if the infringing conduct warrants enhanced damages). The *Read* factors are:

(1) deliberate copying;

(2) defendant's investigation and good faith-belief of invalidity or non-infringement;

(3) litigation behavior;

(4) defendant's size and financial condition;

(5) closeness of the case;

(6) duration of the misconduct;

(7) remedial action by the defendant;

(8) defendant's motivation for harm; and

(9) attempted concealment of the misconduct.

Green Mt. Glass LLC v. Saint-Gobain Containers, Inc., 300 F. Supp. 3d 610, 628 (D. Del. 2018) (citing *Read Corp.*, 970 F.2d at 816, 826-27). The Federal Circuit in *WBIP, LLC v. Kohler Co.*, distinctly declined to interpret Halo as changing the requirement that willfulness should be decided by the finder of fact before the court determines whether enhanced damages are warranted as a matter of law. *See WBIP, LLC v. Kohler Co.*, 829 F.3d 1317, 1341 (Fed. Cir. 2016). Therefore, the Court, as fact-finder, will address the issue of willful infringement and enhanced damages in tandem, as the *Read* factors adequately address both issues.

Moreover, the Federal Circuit has outlined that "[k]nowledge of the patent alleged to be willfully infringed continues to be a prerequisite" to the court finding that enhanced damages are warranted. *Id.* Therefore, prior knowledge of the patents at issue appears to be "a necessary but not sufficient condition for an award of enhanced damages." *Mich. Motor Techs. LLC*, 2020 U.S. Dist. LEXIS 122276, at *11-13 (collecting cases noting pre-suit knowledge of the patent is not alone sufficient to uphold a finding of willfulness and requires more factual allegations to meet *Halo*'s egregious conduct standard). Accordingly, in light of this guidance, the Court will first determine if Cisco has pre-suit knowledge of the patents at issue. Second, the Court will use the *Read* factors to aid its analysis of whether infringement of the patents was willful, and to what degree enhanced damages should be assessed under the circumstances. The Court **FINDS** that Cisco willfully infringed the '856 Patent,

the '176 Patent, the '193 Patent, and the '806 Patent, therefore enhanced damages are warranted under the evidence.

The facts illustrate that Cisco had pre-suit knowledge of Centripetal's asserted patents. First, after signing an NDA, Centripetal presented a detailed PowerPoint presentation to Cisco employees that laid out their patented technology. PTX-547 at 389-91; Tr. 258:21-25, 260:2-18; 1220:1-1222:25. This meeting was presented by Jonathan Rogers, who testified that, at this meeting, he:

> highlighted the technologies that were patented. We had a number of questions there, and I was offering to have additional discussion on that, as well, if it would be helpful.

Tr. 1227:15-18. Contemporaneous emails sent by Jonathan Rogers to the Cisco team state that he was willing to share more information on the patented technology, as the group asked, "a few questions on our patents." PTX-102. This knowledge of the patents is confirmed by internal emails of Cisco's engineer, TK Keanini, which detailed the type of functionality covered by Centripetal's intellectual property and expressing interest in "study[ing] their claims." PTX-134 at 3; *see* Tr. 1128:8-1129:5. Moreover, a third-party firm, Oppenheimer, met with Cisco to discuss Centripetal's product offerings that practice the patents, and presented a highly sensitive, detailed technical disclosure, which detailed the core RuleGate functionalities covered by the Asserted Patents. Tr. 1235:11-20, 1237:25-1238:9; 1242:17-1243:11; DTX-1270 at 1, 25-28, 30.

Second, Centripetal has marked its RuleGate product with a notice indicating the patents practiced by the device. PTX-528 (showing a photograph of the RuleGate device clearly marked with the asserted patents). The evidence presented at trial indicates that the RuleGate device was presented and demonstrated to Cisco employees, indicating that they had direct contact with the label showing the practiced patents. *See WBIP, LLC*, 829 F.3d at 1342 (noting the marking of a device with the asserted patents is supporting evidence that the infringer knew of the patents). Accordingly, the pre-infringement events indicate that Cisco had direct knowledge of the asserted patents and the functionality of the claims. The Court broadly considers all the circumstances of the case, but several of the *Read* factors are particularly instructive in the Court's analysis of enhanced damages.

Turning to the *Read* factors, factor one inquires whether there was deliberate copying of the "ideas and design" of the elements of the claim or the commercial embodiment of the patent. *See Read*, 970 F.2d at 827 n.7; *Arctic Cat Inc. v. Bombardier Recreational Prods., Inc.*, 198 F. Supp. 3d 1343, 1350 (S.D. Fla. 2016), *aff'd*, 876 F.3d 1350 (Fed. Cir. 2017). The case of *Arctic Cat Inc. v. Bombardier Recreational Products, Inc* has similar factual relation to the case here. There, defendant BRP had multiple meetings with Arctic Cat, including testing and demonstrations of its patented embodiment. *Id.* After meetings and testing, BRP stated that they were not interested in the technology and stopped negotiations with Arctic Cat. *Id.* Then, four years later, BRP began infringing Arctic Cat's patents after abandoning its own process. *Id.*

The district court found that BRP's development of "a very similar system under these circumstances [was] strong evidence of copying and favor[ed] enhancing damages." *Id.* Similarly, here, Cisco had multiple meetings with Centripetal employees and provided detailed presentations of the patents and their functionality. *See Georgetown Rail Equip. Co. v. Holland L.P.*, 6:13-CV-366, 2016 WL 3346084, at *17 (E.D. Tex. June 16, 2016), *aff'd*, 867 F.3d 1229 (Fed. Cir. 2017) (showing disclosure of patented systems under a non-disclosure as evidence of copying).

As detailed in the Court's factual findings, Cisco was provided with demonstrations of the product and confidential information regarding Centripetal's proprietary algorithms. Within a year of these meetings, Cisco released the "network of the future," involving the release of older products embedded with new software functionality that was outlined and detailed to them by disclosure of the patents and multiple technical discussions and demonstrations. The fact that Cisco released products with Centripetal's functionality within a year of these meetings goes beyond mere coincidence. Therefore, the fact that Cisco's system mirrors the functionality of the Centripetal patents is compelling evidence that damages should be enhanced for copying. *See Crane Sec. Techs., Inc. v. Rolling Optics AB*, 337 F. Supp. 3d 48, 57 (D. Mass. 2018) ("The Court observes that the similarities of RO's technology to Crane's patented invention, coupled with RO's extensive knowledge of Crane's intellectual property rights and products, support the inference of copying that favors enhancement.")

The second *Read* factor is "whether the infringer, when he knew of the other's patent protection, investigated the scope of the patent and formed a good-faith belief that it was invalid or that it was not infringed." *Read*, 970 F.2d at 827. Cisco presented no evidence of any such investigation and its own technical and marketing documents suggest it would have been difficult to form such a belief.

With respect to *Read* factor three, Cisco's trial attorneys' hands were tied by Centripetal's use of Cisco's own technical documents, coupled with the adverse testimony of Cisco engineers. Cisco had to shield the engineers who authored its current technical documents and the executives who praised its new security functionality for "solving problems previously thought unsolvable" from answering to their own writings and statements.

On the other hand, while Cisco objected to trying the case on a video/audio platform, and specifically the platform upon which the Court's staff was trained, its counsel teamed with Centripetal's counsel to formulate protocols which expanded and improved upon the Court's standard protocols to promote a more reliable and efficient trial by remote means. Counsel for both parties faithfully followed all of the protocols, were both very well prepared, were mostly courteous to one another and joined in congratulating the Court's staff on its efficient handling of the trial. Accordingly, while this factor favors enhanced damages, it is mitigated by the professional performance of its trial counsel.

The fourth *Read* factor looks at the infringer's size and financial condition. Cisco represents itself as the

largest provider of network infrastructure and services in the world. PTX-570 at 991. As discussed *supra*, Cisco saw an increase of approximately $5.575 billion dollars over three years by adding the infringing functionality to the predecessor non-infringing product lines. Additionally, Cisco had substantial profit margins during the infringing period from 52% to 92% on the infringing products.[20] *See Creative Internet Advert. Corp. v. Yahoo! Inc.*, 689 F. Supp. 2d 858, 866 (E.D. Tex. 2010) (showing high profit margins as evidence that favors enhanced damages). Accordingly, for a company as large as Cisco with these levels of revenues and profits, an enhanced damages award would not "unduly prejudice [Cisco's] non infringing business." *Georgetown Rail Equip. Co.*, 2016 WL 3346084, at *19 (quoting *Creative Internet Advert. Corp.*, 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

[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.

Cisco's employee witnesses. Cisco avoided calling the authors of its technical documents as well. There was no testimony that Centripetal attempted to broaden the reach of the four infringed patents, thus opening the door to additional prior art. *See 01 Communique Lab., Inc. v. Citrix Sys.*, 889 F.3d 735, 742 (Fed. Cir. 2018). Nonetheless, Cisco, in its invalidity case, cited its old technology as prior art, while claiming its new technology did not infringe. This led to many inconsistencies in its evidence, on both issues. Of course, Cisco could not rely upon its own documents, as they proved Centripetal's case.[21] Therefore, this factor weighs heavily in favor of enhanced damages.

Read factor six addresses the duration of the misconduct and *Read* factor seven weighs the remedial action taken by the infringer. While *Read* factor nine looks at whether the infringer attempted to conceal any misconduct.[22] The infringing conduct has been continuous and unabated without any form of remedial action from June 20, 2017 to the present time. *See Acantha LLC v. Depuy Synthes Sales, Inc.*, 406 F. Supp. 3d 742, 761 (E.D. Wis. 2019) (citing *Broadcom Corp. v. Qualcomm Inc.*, No. SACV 05-467-JVS, 2007 U.S. Dist. LEXIS 62764, 2007 WL 2326838, at *3 (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*

[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.

Optics AB, 337 F. Supp. 3d 48, 59 (D. Mass. 2018) (no remedial action supporting treble damages). Moreover, Cisco, through its course of conduct, continually gathered information from Centripetal as if it intended to buy the technology from Centripetal. Cisco, then, appropriated the information gained in these meetings to learn about Centripetal's patented functionality and embedded it into its own products. *See Liqwd, Inc. v. L'Oréal USA, Inc.*, No. 17-14-JFB-SRF, 2019 U.S. Dist. LEXIS 215668, at *21 (D. Del. Dec. 16, 2019) (noting how the defendants "concealed their misconduct in gathering information from the plaintiffs so as to create the infringing products" and weighing this factor in favor of enhanced damages). Therefore, all three of these factors weigh in favor of enhanced damages.

The Court **FINDS** that Cisco did not advance any objectively reasonable defenses at trial as to the four infringed and valid patents including the '856 Patent, the '176 Patent, the '193 Patent, and the '806 Patent. Its non-infringement case was grounded upon their old technology. The infringing functionality was added to their accused products post June 20, 2017, and resulted in a dramatic increase in sales which Cisco touted in both technical and marketing documents.

Cisco's invalidity evidence often contradicted its non-infringement evidence and failed to recognize the new functionality which it copied from Centripetal during and after the Nondisclosure Agreement. PTX-99. It embedded the copied software functionality from the patents in its post June 20, 2017 switches, routers and firewalls and then ignored the accused products while claiming its pre-June 20, 2017 technology as

prior art. Moreover, its damages evidence was deeply flawed in attempting to base its calculations on each patent separately instead of considering its own sales of the infringing products. Again, the increase in its sales of the accused products illustrates how completely unrealistic its damages evidence was compared to the reality of the marketplace. Accordingly, in the exercise of its discretion, the Court considers the sound legal principles underlying the history of enhanced damages and **FINDS** this is an egregious case of willful misconduct beyond typical infringement. *Halo Elecs., Inc.*, 136 S. Ct. at 1935.

However, there are other considerations. Cisco did prevail as to one of the patents. In considering the cases awarding enhanced damages, and comparing these cases to this case, the Court **FINDS** that enhancing the damages by a factor of 2.5 is appropriate. Accordingly, the Court's past damages award of $755,808,545 is properly enhanced by a multiple of 2.5 times to award lump sum past damages of $1,889,521,362.50.

iv. Pre-judgment Interest

35 U.S.C. § 284 grants the Court discretionary authority to award interest and costs. 35 U.S.C. § 284; *see General Motors Corp. v. Devex Corp.,* 461 U.S. 648, 653 (1983). The Supreme Court has interpreted the interest provision of section 284 and has instructed courts that pre-judgment interest should ordinarily be awarded, "absent some justification for withholding such an award." *Id.* at 657. The Supreme Court determined that the "fixed by the court" language in section 284 leaves the court's some discretion in awarding pre-judgment interest. *Id.* at 656-57. In

determining the rate of pre-judgment interest, "the district court has the discretion to determine whether to use the prime rate, the prime rate plus a percentage, the U.S. Treasury rate, state statutory rate, corporate bond rate, or whatever rate the court deems appropriate under the circumstances." *Century Wrecker Corp. v. E.R. Buske Mfg. Co.*, 913 F. Supp. 1256, 1280 (N.D. Iowa 1996) (citing *Allen Archery, Inc. v. Browning Manuf. Co.,* 898 F.2d 787, 789 (Fed. Cir. 1990)).

Here, the Court will use the statutory post-judgment rate from the date of first infringement June 20, 2017, of 1.21%. See 28 U.S.C. § 1961. The Court calculates simple interest at the 1.21% rate over the infringement period of three years from June 20, 2017 to June 20, 2020 using the award of damages (excluding enhanced damages) of $755,808,545. This calculation makes an interest determination of $27,243,850.[23] The Court divides this number by two to account for the fact that infringement occurred over this three-year period. Accordingly, the total interest number awarded by the Court is $13,717,925. This interest is added to the final damages award, including the damages enhancement, to reach a final past damages award of $1,903,239,287.50.

B. FUTURE DAMAGES

"There are several types of relief for ongoing infringement that a court can consider: (1) it can grant an injunction; (2) it can order the parties to attempt to negotiate terms for future use of the invention; (3) it

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

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 (2006). "[A]n injunction is a drastic and extraordinary remedy, which should not be granted as a matter of course." *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 165 (2010) (citing *Weinberger v. Romero-Barcelo*, 456 U.S. 305, 311-12 (1982)). "If a less drastic remedy . . . [is] sufficient to redress [Proponents'] injury, no recourse to the additional and extraordinary relief of an injunction [is] warranted." *Id.* at 165-66. If the Court were to grant an injunction, it would do so

on every infringing product and not solely on Cisco's firewalls, as Centripetal originally requested.[24] Moreover, the test for injunctive relief is not met in this case. Cisco's switches, routers, and firewalls make up large portions of the global internet infrastructure. These products are components of both civilian and military networks. Therefore, granting an injunction on the infringing products will likely cause massive adverse effects on the functional capabilities of Cisco's customers and have an adverse ripple effect on national defense and the protection of the global internet.

Therefore, as to factor two, monetary damages are more appropriate to compensate Centripetal for patent infringement. The Keysight license shows that Centripetal is willing to patent its technology to direct competitors. Courts have stated that an injunction is improper where a patent owner has shown that they are willing to accept monetary damages. *See EcoServices, LLC v. Certified Aviation Servs., LLC*, 340 F. Supp. 3d 1004, 1023 (C.D. Cal. 2018); *Cave Consulting Grp., LLC v. Optuminsight, Inc.*, No. 5:11-CV-00469-EJD, 2016 WL 4658979, at *21 (N.D. Cal. Sept. 7, 2016) (finding that where a patent holder is willing to "forego its patent rights for compensation," "monetary damages are rarely inadequate"); *see also Advanced Cardiovascular Sys., Inc. v. Medtronic Vascular, Inc.*, 579 F. Supp. 2d 554, 560 (D. Del. 2008) ("The fact that [plaintiff] was selective regarding its licensing compensation—exchanging its technology

[24] Centripetal later expanded its request for injunctive relief to additional projects. While *EBay* factor one has been clearly proven, factor two has clearly not.

only for other licenses to competing technology—does not rectify the fact that [plaintiff] was willing, ultimately, to forego its exclusive rights for some manner of compensation. Money damages are rarely inadequate in these circumstances."). As to factor three, the greater hardship would clearly impact Cisco. Factor four, the public interest, does not support injunctive relief for the same reasons outlined as to factor two. Accordingly, for these reasons, the Court **FINDS** that an injunction is not an appropriate legal remedy for Cisco's infringement.

ii. Ongoing Royalty

Rather, the Court **FINDS** that an ongoing royalty is proper in this case. An ongoing royalty is essentially a compulsory license for future use of the patented technology during the life of the patents. Indeed, pre-verdict and post-verdict royalties are "fundamental[ly] differen[t]." *XY, LLC v. Trans Ova Genetics*, 890 F.3d 1282, 1397 (Fed. Cir. 2018). When setting an ongoing royalty for future use, the district court should consider "the change in the parties' bargaining positions, and the resulting change in economic circumstances." See id., ("When patent claims are held to be not invalid and infringed, this amounts to a 'substantial shift in the bargaining position of the parties.'") (quoting *ActiveVideo Networks, Inc. v. Verizon Commc'ns, Inc.,* 694 F.3d 1312, 1342 (Fed. Cir. 2012)). Such differences include a Court's determination that certain of the patents at issue are valid, enforceable, and would be infringed by the accused products. *See id.*

The Court should analyze future royalties in the context of the *Georgia-Pacific* factors. Indeed, this is

the approach adopted by other district courts, after modifying the *Georgia-Pacific* analysis to resolve any uncertainty as to whether the accused product will infringe the patent claims, whether the asserted patents are enforceable, and whether the asserted patent claims are valid. *See Creative Internet Advert. Corp. v. Yahoo! Inc.*, 674 F. Supp. 2d 847, 860 (E.D. Tex. 2009); *Paice LLC v. Toyota Motor Corp.*, 609 F. Supp. 2d 620, 623-24 (E.D. Tex. 2009); *Boston Sci. Corp. v. Johnson & Johnson*, No. C 02-00790 SI, 2009 WL 975424 (N.D. Cal. Apr. 9, 2009). As discussed *supra*, this Court has analyzed the *Georgia-Pacific* factors in the context of past damages. The Court, here, incorporates its analysis of the previous Keysight license but takes into consideration the distinct differences in determining a past damages award as opposed to an ongoing royalty. Therefore, as it did before, the Court **FINDS** the Keysight license as a comparable license for use in determining ongoing royalties. In light of that, the Court **FINDS** an appropriate future royalty is ***10%*** **on the APPORTIONED REVENUES OF THE INFRINGING PRODUCTS FOR THREE (3) YEARS**, beginning June 21, 2020 and payable annually beginning June 20, 2021, without interest. The revenues shall be apportioned in the same manner as the pre-judgment damages, and shall apply to the infringing technology as described in the Court's Findings of Fact and Conclusions of Law. Successor products to the infringing product shall pay the same percentage royalty on sales revenue as applied to the current infringing products, so long as the successor products contain any technology found to infringe in this Opinion and Order. As to the four patents

infringed, assigning different nomenclature to infringing products, or to Cisco's software technology found to infringe, shall not relieve Cisco of its obligation to pay its royalty. After this three-year term, the Court **FINDS** the royalty should be decreased to ***5%*** **FOR ANOTHER THREE (3) YEAR TERM**. Due to Cisco's dominant position in the cyber security software and firewall markets and the resulting damage to Centripetal as the first inventor the Court **FINDS** a six year term is called for in lieu of the three year term agreed upon in Keysight. Similar to the Keysight license, the Court imposes a minimum and maximum on the imposed ongoing royalty. For the **first three-year term at 10%,** such annual royalty **shall not be less than $167,711,374.10** and **shall not be more than $300,076,834.** For the **second three-year term at 5%,** such annual royalty **shall not be less than $83,855,867.00** and **shall not be more than $150,038,417**. The maximum and minimum of each year is based upon the highest and lowest years of apportioned revenues per a full year of infringement from the 2017-2020 time frame. *See* Doc. 411 Ex. 7. Similarly, the maximum and minimum is reduced by one-half during the second three year term to reflect the reduced royalty rate. *See id.* At the conclusion of this second term of three years, there shall be no further monetary payments or other relief for the sale or use of the infringing products or their successors[25].

[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

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

It is **SO ORDERED**.

/s/

Henry Coke Morgan, Jr.
Senior United States
District Judge

October 5, 2020
Norfolk, Virginia

annual revenue of $300,076,834.00 for the period of June 20, 2018 to June 20, 2019.

APPENDIX A
EXPLANATION OF ABBREVIATIONS

Computer engineers use abbreviations to describe basic functionality as well as to describe the specific functionality of individual patented technology. To assist with interpreting their testimony and documents, the Court has compiled a list of the abbreviations used in the testimony and documents cited in this opinion.

ACL	Access Control List
ACE	Access Control Entry
ANC	Adaptive Network Control
ASA	Adaptive Security Appliance
ASDM	Adaptive Security Device Manager
ASR	Aggregation Services Router
ASIC	Application-Specific Integrated Circuit
CLI	Command Line Interface
CPU	Central Processing Unit
CRM	Computer-Readable Media
CSIRT	Computer Security Incident Response Team

CTA	Cognitive Threat Analytics
CTI	Cyber Threat Intelligence
DNA	Digital Network Architecture
DNS	Domain Name Server
DOE	Doctrine of equivalents
ETA	Encrypted Traffic Analytics
FC	Flow Collector
FMC	Firepower Management Center
GACL	Group Access Control List
HTTP/HTTPS	HyperText Transfer Protocol (Secure)
ISE	Identity Services Engine
IDP	Initial Data Packet
IDS	Intrusion Detection System
IOS-XE	Internetwork Operating System-XE
IT Manager	Information Technology Manager
ISR	Integrated Services Router
IP	Internet Protocol

IPR	*inter partes* review
IPS	intrusion prevention system
IDS	intrusion detection system
ML	Machine Learning
NAT	network address translation
NSEL	NetFlow Secure Event Logging
PBC	Packet Buffer Complex
PTAB	Patent Trial and Appeals Board
SD-Access	Software Defined Access
SGACL	Security Group Access Control List
SGT	Security Group Tag
SPLT	Sequence of Packet Lengths and Times
SIO	Security Intelligence Operations
SIP	Session Initiation Protocol
Stealthwatch	Stealthwatch Enterprises
SLIC	Stealthwatch Management Console
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 D

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

No. 2:18cv94

CENTRIPETAL NETWORKS, INC.,
Plaintiff,
v.
CISCO SYSTEMS, INC.,
Defendant.

Decided: Mar. 17, 2021

OPINION AND ORDER

Defendant, Cisco Systems, Inc. ("Cisco") filed a Rule 59(a)(2) motion for a new trial regarding the Court's rulings as to the '176 Patent and the '806 Patent as well as a new trial as to willfulness and damages. Cisco simultaneously filed a Rule 52(b) motion regarding direct infringement, damages, and an amended judgment as well as a Rule 54(b) request for partial judgment. There are overlapping findings of fact and conclusions of law applicable to Cisco's several motions and the Court will therefore rule upon all of Cisco's motions in this opinion and order.

For the reasons that follow, the Court **DENIES** each of Cisco's motions.

I. INTRODUCTION

As to infringement and validity, Centripetal and its experts relied on 1) Cisco's technical documents as interpreted by Centripetal' s experts, 2) admissions in Cisco' s pleadings, and 3) the testimony of Cisco's own engineers, principally Mr. Llewallyn and Mr. Jones, Cisco's distinguished engineers. Cisco attempts to classify the Court's rulings as sua sponte, however, the most compelling evidence originated in Cisco's own technical documents introduced at trial by Centripetal and thus are anything but sua sponte. Cisco attempted to avoid the impact of its own technical publications by using animations prepared solely for trial as the basis for its expert testimony. The Court found that the animations misrepresented the functionality of the infringing products and found Cisco's retained experts' testimony unpersuasive as to infringement and validity as well as damages.

The four Centripetal patents which the Court found Cisco infringed, when combined, cover a broad spectrum of security software which promoted Cisco's security products from an also ran to a leader in the security marketplace. *See* PTX-1460. Cisco portrays itself as "the largest provider of network infrastructure and services for many years before any of the patents issued." Cisco's Reply Brief in Support of 59(a)(2) at 17[1]. This was probably accurate as to hardware, but not as to the software required to

[1] The Court is citing to the page numbers listed at the bottom of the briefs, not the page numbers assigned to the document by the Clerk's office.

operate it until Cisco began infringing the Centripetal patents on June 20, 2017.

The Centripetal '193 Patent, referred to at trial as the "FORWARD OR DROP EXFILTRATION PATENT," the technology from which is embedded in Cisco's switches and routers, enabled Cisco to proactively search for bad actors attempting to exfiltrate confidential data from the switches and routers which operate its networks. The '856 Patent, referred to at trial as the "ENCRYPTED TRAFFIC PATENT," the technology from which is also embedded in Cisco's switches and routers, enabled Cisco to proactively search for and find bad actors and malware in the unencrypted portion of encrypted packets without decrypting them. Cisco repeatedly claimed that it was the first to possess this technology, but in fact it copied the technology from Centripetal. *See e.g.*, PTX-383; PTX-569; PTX-1009.

The '176 Patent, referred to at trial as the "CORRELATION PATENT," the technology from which is also embedded in its switches and routers, enabled Cisco to correlate its NetFlow intelligence with proxy data from multiple third party sources as well as to correlate intelligence from multiple sources within NetFlow. This enabled Cisco to proactively obtain up to date intelligence data for use in its infringing security software embedded in its switches and routers.

The '806 Patent, referred to at trial as the "RULE SWAP PATENT," the infringing technology from which is also embedded in its switches, routers and firewalls enabled Cisco to more efficiently and proactively transform up to date data and collate this

intelligence into rules which are then used to detect and stop malware, bad actors (i.e. hackers) and exfiltration.

Accordingly, the patent claims within Centripetal's patented technology work in combination with one another on Cisco's hardware to transform the obsolete portions of Cisco's software from reactive to proactive. The four infringed patents then work together to furnish Cisco's customers with proactive security software throughout its network hardware, thereby contributing to Cisco's goal of transforming itself from a hardware supplier to a full-service network security supplier.

Although Cisco began infringing on June 20, 2017, it continued its copying of Centripetal's patents through 2019 and later, as is illustrated by its technical documents introduced at trial by Centripetal.

II. JUNE 20, 2017 AS THE DATE OF FIRST INFRINGEMENT AND A BASELINE TO COMPARE SALES

Cisco alleges that the Court ruled sua sponte in fixing the date of Cisco's first infringement. The evidence contradicts this claim. In determining the damages based on a reasonable royalty, the Court employed the hypothetical negotiation approach. Also known as the "willing licensor-willing licensee" approach, this calculation "attempts to ascertain the royalty upon which the parties would have agreed had they successfully negotiated an agreement just before infringement began." *Lucent Techs., Inc. v. Gateway, Inc.,* 580 F. 3d 1301, 1324 (Fed. Cir. 2009). "The date used for the occurrence of the hypothetical negotiation

is the date that infringement began." *Centripetal Networks, Inc. v. Cisco Sys., Inc.,* 2: l 8-CV-94, 2020 WL 5887916, 56 (E.D. VA Oct. 5, 2020) (citing *Wang Labs., Inc. v. Toshiba Corp.,* 993 F. 2d 858, 870 (Fed. Cir. 1993)) [hereinafter October 5, 2020 Opinion]. Cisco stated in its opening statement that Encrypted Traffic Analytics, an infringing technology, came to the marketplace in June of 2017. *See* Trial Transcript [Docket Nos. 496-550] [hereinafter Tr.] at 221:19. As per PTX-1135, Cisco's own press release from June 20, 2017 marked the date of first infringement. Lance Gunderson, Centripetal's damages expert, explained why this date should apply to all four patents:

> "[T]hese patents really work in concert. They work together. They provide this operationalization of threat intelligence, this new concept that was a new and innovative concept brought about by Centripetal. So they really kind of worked together.
>
> . . . [T]hey have equal weight, each of them adds an important element to this operationalization .... [I]t seems like that they work in concert, and it's my opinion that any negotiation would have negotiated a license to all of the patents. Even some of the patents that actually issued afterwards. My understanding is the patents were actually filed for prior to this hypothetical negotiation, they would have been known, and these reasonable actors would have licensed everything." Tr. 1445:14- 1446:2.

Cisco's damages expert, Dr. Stephen Becker, agreed that June 20, 2017 would be about the date of

the hypothetical negotiation. *See* Tr. at 2993. Further, Becker agreed that the date of first infringement for at least some of the patents at issue would be June 20, 2017:

> Q: And you agree that the start date of damages for purposes of this case, as it relates to the various [four] patents, begins starting June 20 of 2017; is that right?
>
> A: Yes. It's not every single patent and every single product, but generally that's when it starts. Tr. 2964:4-8 (cross-examination by Ms. Kobialka).

The Court found the date of first infringement to be June 20, 2017. *See* Tr. 725:3-8 (Dr. Michael Mitzenmacher stating this as the date of first infringement); *see also,* Tr. 1534: 17 (Cisco cross-examining Mr. Gunderson and confirming his stated date of first infringement was June 20, 2017). The damages are calculated by positing what would be agreed upon at a hypothetical negotiation. *See Lucent* at 1324. Because all the infringing patents work in concert-and because three of the four infringed patents had been granted and the fourth filed for prior to June 20, 2017 and would have been known-it is reasonable to determine that all four patents would be negotiated for licensing at the same time. *See* Tr. at 1445:14-1446:2. As Mr. Gunderson stated in his testimony:

> You look for the date of first infringement. You have a variety of patents, it's the same month that the ' 193 Patent was issued. There were also some accused products that were

> sold that month. So there's not a lot of dispute about this date that I'm aware of. They would negotiate a reasonable royalty for all [four] patents, in my opinion, at this time. Tr. 1444:24-1445:5. (direct examination by Ms. Kobialka).

This date was put forth by Centripetal, based upon a Cisco Publication PTX-1135, acknowledged by Cisco' s own damages expert during his trial testimony, and certainly was not a *sua sponte* ruling of the Court as claimed by Cisco.

III. DAMAGES - GENERALLY

In its damages case Centripetal relied upon 1) an apportionment formula approved by the Federal Circuit, 2) the only royalty rate cited by either party previously utilized in an infringement claim relating to the same family of patents, and 3) sales data obtained from Cisco which corroborated the damages claimed by Centripetal and accorded with economic reality.

Cisco presented a damages expert whose theory lacked any precedential or evidentiary support in patent law, and was completely devoid of economic reality.

The Court found Centripetal's evidence on infringement, validity, and damages credible and persuasive. The Court found Cisco's defenses objectively unreasonable and in many areas not credible, as well as finding its conduct willful and egregious in infringing the four patents. The Court found that Centripetal did not prove by a preponderance of the evidence that the '205 Patent was infringed by Cisco. The '205 Patent dealt

primarily with a method of 'tapping' telephones and was used mostly by law enforcement to record such calls. This is the opposite of the functionality of the infringing products, Cisco never claimed the ability to make, use or sell products based upon the '205 Patent technology. The '205 Patent had no impact upon the Cisco sales data analyzed by the Court or the Court's computation of any form of damages.

IV. MAKING, SELLING AND USING THE INFRINGING PRODUCTS IN COMBINATION IN THE UNITED STATES AND ELSEWHERE AND DAMAGES

Cisco challenged the Court's calculation of damages in both its Rule 52(b) and 59(a)(2) motions. In the introduction to its brief in support of its Rule 52(b)/54(b) motion, Cisco argued the following: "It is undisputed that the accused products are sold separately and that (for instance) Cisco switches, routers or firewalls may be bought and used without buying the other products in the combined systems found to infringe." Cisco' s Brief in Support of its Rule 52(b) Motion [Docket No. 628) at 2. "Centripetal did not show, and the Court did not find, that every one of the accused products would meet claims' limitations when sold or used by themselves." Doc. 628 at 11. The evidence demonstrates that the accused products were made and sold to be used in the United States embedded with and in combination with the infringing technology.

Cisco's hardware—i.e., switches, routers, and firewalls—cannot operate without software, and the software that constituted Cisco's operating systems contained Centripetal's patented technology, which

Cisco thereby infringed. Further, Centripetal's experts testified that it was Cisco's post June 20, 2017 infringing software that was embedded in Cisco's switches, routers, and firewalls. Multiple technical documents introduced in evidence by Centripetal, but published and circulated by Cisco itself, illustrated in diagrams and explained in text precisely how the infringing software functioned in the Cisco networks, which operated through its switches, routers, and firewalls. Thus, Centripetal presented credible and persuasive evidence of infringement corroborated by Cisco's own technical publications and the testimony of its own employees; including Mr. Llewallyn and Mr. Jones who were designated "distinguished engineers," as well as by Dr. Schmidt, a retained Cisco expert. Cisco for its noninfringement evidence relied upon animations created for trial, upon which their independent experts in turn relied in forming their opinions. The Court found the animations misrepresented the functionality of the infringing technology and found the testimony of Cisco's independent experts unpersuasive and in many instances not credible, resulting in a finding that Cisco's defenses were objectively unreasonable.

Cisco did not present any evidence that contradicted its own documents, employees, and Centripetal's experts. In fact, none of the authors or presenters of its technical documents were called as witnesses. Instead, Cisco tried to avoid responding to its own publications by creating misleading animations for use at trial. Cisco presented the testimony of Dr. Becker on its "lack of product combination" defense. Dr. Becker, its damages expert, testified as follows:

Q. And just to be clear for the record, does that $13.4 billion represent the revenue from Cisco customers who purchased the required combination of products for the '856?

A. No. No. In fact it's, it is all of the revenue from all 98,800 customers, which we could see from looking at the StealthWatch data we know that the vast, vast majority of those customers just have the switch. They're just using the switches and routers, they're not also using this Cisco security product in the form of this, of Stealth Watch.

Q. Did Mr. Gunderson account for the fact that the accused switches and routers "can" be sold separately from the other products required for these accused combinations?

A. No.

Q. Do you know whether Mr. Gunderson had access to the same data that you had with respect to these revenue figures?

A. He did. He has all the same data that I have and he could have looked at these combinations and didn't.

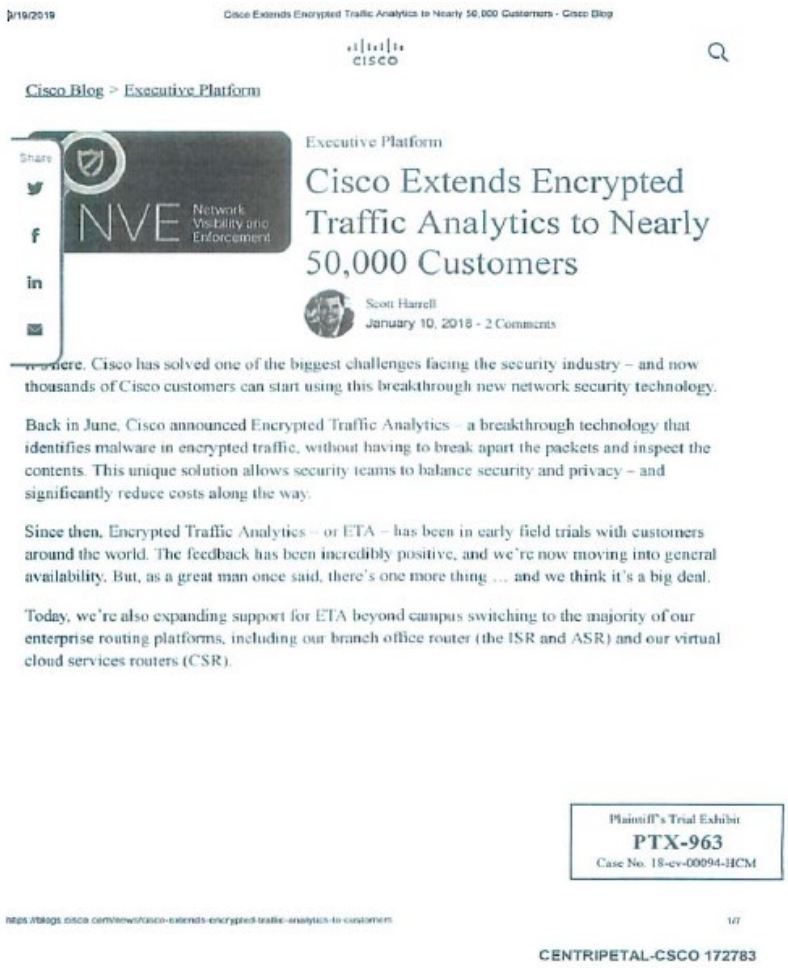
Q. If Mr. Gunderson had considered the required combination of products, what would that have done to his royalty base in your view?

A. Well, I think we know that mathematically his base would have been a very, very small fraction of what it was since well-less than five percent of the customers, the data would indicate, have the combination that's

> required. Trial Tr. 2879:5-2880:3 (Dr. Stephen Becker's testimony) (emphasis added).

However, testimony from Cisco's first independent expert to testify, Dr. Doug Schmidt, contradicts Dr. Becker's damages theory. Dr. Schmidt's factual testimony confirmed explicitly that ETA was embedded in Cisco's Accused Switches:

> THE COURT: Well, I read something that said ETA was embedded in the switch. What does that mean?
>
> THE WITNESS: That's correct. That's what it just said here at the bottom. The last sentence that's on the screen right now says that.
>
> BY MR. GAUDET (Cisco counsel):
>
> Q. What part of ETA is embedded in the switch?
>
> A. The part that collects the Initial Data Packet and the Sequence of Packet Length and Times.
>
> Q. Is that what it says in this document?
>
> A. That's exactly what it says in this document, yes. Trial Tr. 2131: 12-22. See also PTX-963 illustrated.



1/19/2019 Cisco Extends Encrypted Traffic Analytics to Nearly 50,000 Customers - Cisco Blog

Cisco Blog > Executive Platform

Share

NVE Network Visibility and Enforcement

Executive Platform

Cisco Extends Encrypted Traffic Analytics to Nearly 50,000 Customers

Scott Harrell
January 10, 2018 - 2 Comments

Here. Cisco has solved one of the biggest challenges facing the security industry – and now thousands of Cisco customers can start using this breakthrough new network security technology.

Back in June, Cisco announced Encrypted Traffic Analytics – a breakthrough technology that identifies malware in encrypted traffic, without having to break apart the packets and inspect the contents. This unique solution allows security teams to balance security and privacy – and significantly reduce costs along the way.

Since then, Encrypted Traffic Analytics – or ETA – has been in early field trials with customers around the world. The feedback has been incredibly positive, and we're now moving into general availability. But, as a great man once said, there's one more thing … and we think it's a big deal.

Today, we're also expanding support for ETA beyond campus switching to the majority of our enterprise routing platforms, including our branch office router (the ISR and ASR) and our virtual cloud services routers (CSR).

Plaintiff's Trial Exhibit
PTX-963
Case No. 18-cv-00094-HCM

https://blogs.cisco.com/news/cisco-extends-encrypted-traffic-analytics-to-customers 1/7

CENTRIPETAL-CSCO 172783

Dr. Schmidt additionally confirmed in his factual testimony that Cisco's infringing products were sold in combination:

BY MR. GAUDET (Cisco counsel):

Q. Let's be clear: Does Cisco have any customers who would only buy this product and not have the other products that are

> actually designed to prevent malicious packets from coming in?
>
> MR. ANDRE: Objection. Lacks foundation. He doesn't know.
>
> THE WITNESS: I do know.
>
> BY MR. GAUDET:
>
> Q. Do you know that, Dr. Schmidt?
>
> A. Yes, of course. Only if those customers are extremely looking forward to having their networks hacked. Good network administration, Your Honor, relies on what's called layered defense, where you have firewalls, you have tools like Stealth Watch. This is a comprehensive technique. Comprehensive set of products. Trial Tr. 2130:7-20.

While the Court rejected Dr. Schmidt's expert opinion on infringement and invalidity, when reckoning with competing testimony it is within the purview of the Court as the trier of fact to determine which witnesses and what testimony or portions thereof are to be accepted as credible. *See Sartor v. Arkansas Natural Gas Corp.*, 321 U.S. 620, 627 (1944) ("The rule has been stated that if the Court admits the testimony, then it is for the [trier of fact] to decide whether any, and if any what, weight is to be given to the testimony.") (internal quotations removed); *see also, In re Methyl Tertiary Butyl Ether (MTBE) Prod Liab. Litig.*, 139 F. Supp. 2d 576,604 (S.D.N.Y. 2010) ("In general, a [factfinder] is not required to choose between adopting or rejecting an expert's testimony wholesale; it is free to accept or reject expert's opinions

in whole or in part and to draw its own conclusions from it.")

Of course the software programs, such as Stealth Watch, "can" be sold separately, as the sales data twice supplied by Cisco illustrates clearly. Customers who already owned Cisco hardware, as well as the outdated Cisco software such as the older versions of Stealth Watch, would only need to purchase the newer infringing software so long as the customer's existing hardware was compatible. The Court found that the preponderance of the evidence established that the sales data for the switches, routers, and firewalls, produced during pretrial discovery and again in more detail at the damages hearing, listed by Cisco were embedded with software which infringed the four Centripetal patents. Cisco was asked to produce sales data on its "accused products," which Centripetal proved were "embedded with its patented software." Dr. Becker's testimony did not refer to the sales data produced in response to the Plaintiffs and the Court's requests for sales data of the "accused products." Cisco never produced any other evidence that its "accused products," as identified in its pretrial sales data production or its second production at the Court's damages hearing, did not contain the infringing software, while Centripetal presented a preponderance of evidence that it did. The Court inferred that Cisco's failure to produce such evidence, even when Dr. Becker was invited to do so by the Court, is proof that the sales data twice presented by Cisco did contain the infringing software. At no time did the Court request that Cisco produce the sales data for all Cisco's hardware and software, as Dr.

Becker's testimony might suggest, but rather sales data relating to the "accused products."

Not only is Dr. Becker's testimony contrary to the preponderance of the evidence in the case, but he also misrepresents the testimony of Centripetal's expert, Mr. Gunderson who stated as follows:

> BY MS. KOBIALKA (Centripetal's counsel):
>
> Q. And can we go to Slide 45? And can you just provide your key takeaways in terms of your opinion for the hypothetical negotiation?
>
> A. It's my belief that the Centripetal/Keysight patent license is the best available information we have and it's something that I did use. The asserted functionalities are contained within the switches, the routers, firewalls and the other accused products and they work in concert. And apportionment method needs to measure value provided to Cisco, and so that's what I believe happened with Dr. Striegel's analysis. The asserted functionalities are of critical importance to Cisco and endusers, and I think we went through a series of schedules that showed that importance. And finally, I believe that Georgia-Pacific factors support the royalty and are consistent with the Keysight license agreed rate.[2] Trial Tr. 1525:10-25 (Lance Gunderson's testimony).

---

[2] Centripetal analyzed its damages using the *Georgia-Pacific* factors, and, under those parameters, Keystone was the only license transaction in which Centripetal had been involved. It sought additional licensing information from Cisco, but none was

Q. "ETA Impact on Security Bookings." And if you can explain here how this informed your opinion?

A. So it says "We're also embedding it in our products right and you can look at like when we acquire Stealth Watch. It's now part of what we're doing at Cat 9000." So this is really talking about the importance of ET A and the fact that it impacts their bookings. And bookings, I think, means their sales, essentially. And it's really a revenue impactor, is what they're saying. Trial Tr. 1472:17-25 (Lance Gunderson's testimony); *see* PTX-31 at Bates No. 006.

Q. Okay. I'd like to turn to the royalty base, and we can go to Slide 36. What did you use for coming up with your royalty base?

A. Well, again, in terms of the royalty base we need to look at what is infringing, and we have to start out with what constitutes infringing. And my understanding of the

---

forthcoming. In answering Centripetal's interrogatory, Cisco stated that it was "not presently aware of any patent license agreements that relate to the functionality of accused instrumentalities, nor is Cisco aware of any other license relevant to the evaluation of a reasonable royalty of damages in this case." Trial Tr. 1478:23-1479:2 (Mr. Gunderson quoting Cisco's interrogatory response). However, Cisco's exhibit, DTX-729 at page 5, shows that Cisco had licensed Stealth Watch from Lancope for approximately two years before Cisco purchased Lan cope in 201 5. It is not clear if Cisco was contending that the Old Stealth Watch was not comparable to the post-2017 7 .0 version of Stealth Watch or what the reason was for omitting the Stealth Watch license.

statute is, making it, using it, importing it, offering it for sell, and selling. Those are the—that's the way the statute reads. And so I always keep that in the back of our mind as we're looking at what the royalty base is. No. 2, the asserted patents are system claims, and so they're for a system comprising a variety of different things. And they're computer-readable medium claims which, in my mind, is software. It's really software that's on the system that makes the patents go, essentially. And then thirdly, the asserted functionalities are embedded in the switches, routers, and firewalls through this source code. This infringing code that is throughout the system. Trial Tr. 1499:18-1500:10 (Lance Gunderson's testimony).

Q. And the 9300 Series the first—it looks like it's always included Encrypted Traffic Analytics, and that's the first model to do so?

A. Yep. The way it's sold here is that it's always included, yep.

Q. And in addition there was other evidence at trial, you also saw that ETA was also part of the Catalyst 9000 switches?

A. Yes. Trial Tr. 1461:20-1462:2 (Lance Gunderson's testimony).

MS. KOBIALKA: If we could look at PTX-1507?

BY MS. KOBIALKA:

Q. Mr. Gunderson, can you describe what that document is?

A. It's a very simple—excuse me --

THE COURT: Let me get to that.

MS. KOBIALKA: Sorry. Maybe we can highlight the date at the bottom.

THE COURT: This is 2017?

MS. KOBIALKA: That's correct.

THE COURT: All right. You may proceed.

BY MS. KOBIALKA:

Q. Mr. Gunderson, could you tell us what this document is?

A. It's very similar to the last document that we had. Last document was talking about switches, this is talking about routers. Integrated Services Router. And it has a couple of different generations of routers, and then it's comparing it to the Cisco 4000 Series of routers. And it's an attempt to upsell, to get the current clients of Cisco to buy this new and innovative router that has this great technology on it.

Q. Okay. And I see a blue button up on top, says "How To Buy". Do you see that as well?

A. Yes.

Q. Okay. So this is evidence of how Cisco offers to sell and sells its routers, right?

A. Yes. They point out the benefits, and they're trying to get their existing customers to upgrade and put in a Cisco 4000 Series router.

MS. KOBIALKA: Okay. Now if we could highlight the second row, which is Cisco IOS XE Open operating system all the way across. Then if we could go down to couple it says Cisco DNA Center[3], Centralized Management.

BY MS. KOBIALKA:

Q. And could you just explain what we're seeing here with the check box under the 4000 Series for these?

A. So it shows no checks on the first two generations and then it had a check box that says that's included. So it's got the new IOS that's being accused here as the DNA Center, Centralized Management System. So there's a check box there. It has - you know, you look further down it says Cisco DNA Assurance Network Monitoring. It has a variety of the accused functionality that is included in the Cisco 4000 Series.

Q. If we could turn to the next page of this document? I'd like to just point out the two rows at the bottom. Says "Cisco Stealth Watch Enterprise and Encrypted Traffic Analytics." Does this show that also those things come with the Cisco 4000 Series Integrated Services Router?

---

[3] There is a glossary of abbreviations attached as Appendix A of the Court's Opinion and Order dated October 5, 2020.

> A. Yes. You can see that those check boxes are there and they come with it, it appears, automatically.
>
> Q. Is this just one example like the other one with the switches of what you have seen in terms of how Cisco sells and offers to sell these products?
>
> A. Yeah. So even though they might have a separate charge, sometimes for StealthWatch, for example, they're selling it as one product. These all work together. And that goes to my point: This is, they're really—they're really trying to sell everything together and to sell a solution rather than just sell individual products. Even though they might charge differently for them, they're selling them together. Trial Tr. 1462:5-1464:13.

The Court found this testimony presented by Centripetal credible, persuasive, and in accord with the preponderance of the evidence. Mr. Gunderson relied to a great extent upon Cisco's own publications, which corroborated his opinions. There is no equivalent corroboration from any source for Dr. Becker's opinions, which the Court rejected. In addition to the evidence Centripetal presented relative to the accused technology being embedded in Cisco' s switches, routers and firewalls, Cisco effectively admitted as much in its discovery responses. When asked to produce data regarding its sales of accused products it included specific amounts for its switches, routers, and firewalls through December 31, 2019 in response to Centripetal's

pretrial discovery. In its attempt to tailor its damage awards to the evidence, the Court requested that Cisco refine its sales data to a month to month outline and update it to begin in July of 2016 and extend it through the trial which began on May 8, 2020. The Court also invited Cisco's damage witness, Dr. Becker, to furnish any data supporting his damage theory, where at one point he stated that less than five percent of all sales involved sales in infringing combinations. The Court rejected his five percent figure since Cisco offered no sales data to support it, and it conflicted with Centripetal's evidence to the contrary that the Court found reliable. Cisco's sales data produced for pretrial discovery was the same data produced when the Court requested updated sales records. Cisco merely updated the sales records. At no point did Cisco dispute which accused products should have been included or excluded, nor did they at trial contradict with evidence to Centripetal' s characterizations that the accused products contained in the sales data infringed.

With regard to damages, the Court accepted Centripetal's theory of damage calculations which was based upon Dr. Striegel's apportionment and Mr. Gunderson's and Mr. Malackowski's application of the financial data. The Court did not base its damages calculations upon the comparative sales data before and after June 20, 2017 produced at the June 25, 2020 Court hearing on damages, but upon the *Finjan* and *Ericsson* cases in which the Federal Circuit expressly approved the damages theory employed by Centripetal. *See Finjan, Inc.* v. *Blue Coat Sys., Inc.*, 879 F. 3d 1299, 1310 (Fed. Cir. 2018); *Ericsson, Inc.* v. *D-Link Sys., Inc.*, 773 F. 3d 1291, 1266 (Fed. Cir.

2014). The Court also analyzed the *Georgia-Pacific* factors in its opinion. *See* October 5, 2020 Opinion at 126-49; 164-65.

The Court did seek further evidence supporting damages from both parties in an attempt to resolve the vast difference in the approaches and results presented by the opposing parties. The request by the Court to Dr. Becker began on Trial Tr. 2968:1 and continued through Trial Tr. 2979:5. The Court only had six (6) months of sales data, beginning January 1, 2017, preceding the June 20, 2017 date of first infringement. The Court found that an additional six (6) months of sales data would assist it in determining whether the data would support Centripetal' s theory of damages or that of Cisco. The key portions of the Court's request for additional data is set forth as follows:

> THE COURT: All right, Dr. Becker. With respect to that data, what the Court needs, to try to figure out what's going on between these various opinions, is the sales of the products in the '176, the '193, the '205, and the '806. I need the monthly sales of those products beginning in 2016, June of 2016. You can't begin them in the middle of a month, so let's say you'll begin them July '16, July of 2016, with those four patents. I want the monthly sales of the predecessor products for the period of one year prior to June 20, 2017, so that would include the entire month of June, for the predecessors of the accused products because the products are accused beginning June 20th. And when I say, "the

> accused products," I want to include the sales of all products after that date, on a month-to-month basis, which included the products - all the features accused by the plaintiff. Trial Tr. 2968: 17-2969:7.

The Court then asked Dr. Becker to furnish the sales figures based upon his damages theory:

> THE COURT: . . . Then I'd like for you to do the same thing with what you considered to be the relevant products, which—and you didn't consider, for example, in some cases, the routers and switches to be relevant products, so I just want the sales of what you considered to be the relevant products, which included, for example, StealthWatch in some instances, but it didn't include the routers and switches. Trial Tr. 2970:23-2971 :4.

Cisco only produced one set of documents in response to the Court's request. It did not produce any compilation of sales figures to support Dr. Becker's theory of damages.

The Court dealt specifically with the '856 Patent because it was granted after June 20, 2017.

> THE COURT: All right. And for the '856 Patent, that patent—well, I would really just ask for the same data on the '856 Patent, but the patent wasn't granted until after the relevant date. It was granted in '18, and the relevant date is June 20 of '17, so just get me the same figures for that patent on a monthly basis.

> THE WITNESS: Right. I think, to the extent that—the data that's collected for these other four patents will—just glancing at the list, I think it will overlap with the '856, and I think, to the extent that we are able to collect the data and get it to you related to the other four, it will cover everything you're asking for on the '856. Trial Tr. 2973:5-16 (Dr. Stephen Becker's testimony).

In its Reply (Rebuttal) brief in support of its Rule 59(a)(2) motion on Doc. 635 p. 15, Cisco stated:

> Likewise, the Court put strict limits on this follow-up testimony from Dr. Becker, instructing Dr. Becker that he was "not to discuss your testimony with anyone between now and the time that you're prepared to deliver the data to the Court," and cautioning Cisco's counsel that it was "to use good faith in limiting themselves to just furnishing the source of the data." Trial Tr. 2978:4-25.

What Cisco describes as "strict limits" applied to barring new damages theories (models). There were no limits on the data to be supplied.

> THE WITNESS: Yes. There's a particular model, for example, that I think the record would show doesn't actually—won't work with any of the security products, but I think I have an understanding of what you want, and we will work to get that done.
>
> THE COURT: Well, and you're not limited by what I ask for.
>
> THE WITNESS: I understand.

> THE COURT: If there's something else along these lines—you know what I'm thinking about—that you think would be helpful, go ahead and include it. But I've got to resolve this tremendous difference in --
>
> THE WITNESS: I understand.
>
> THE COURT:—what each side is coming up with, and I'm trying to think how I can best do that. Trial Tr. 2977:2-17 (Dr. Stephen Becker's testimony).

What the Court requested and received was updated sales data through June 2020 plus comparative data for the year preceding the date of the alleged first infringement on June 20, 2017. The sales data, if any, which Dr. Becker used in his damages calculations was not furnished. The Court already had the total sales of the accused products from January 1, 2017 to December 31, 2019.

On page 9 of Doc. 626, its initial memorandum in support of its Rule 59(a)(2) motion, Cisco states:

> In its Opinion and Order, the Court used the sales data from June 2016-June 2017 in a way that Centripetal never had. The Court set forth a table summarizing "Centripetal's estimates regarding Cisco's revenue increase for the infringing products, after the date of first infringement, as compared to the predecessor products sales for the fiscal year before June 20, 2017." Order at 139-140.
>
> And further stated on page 10 of Doc. 626:
>
> Comparing product sales from June 2016 - June 2017 to product sales over the

> subsequent three-year period was not a damages model that Centripetal presented to the Court. Nor was it a model that Centripetal (via its damages experts Mr. Gunderson or Mr. Malackowski) had ever suggested would be appropriate.

These allegations are not supported by the evidence.

As previously noted, comparative sales before and after June 20, 2017 was not the damages model the Court utilized. It was evidence, which along with Cisco' s marketing documents, corroborated the enormous increase in sales resulting from Cisco embedding Centripetal' s software in its switches, routers, and firewalls. The Court also considered sales data as corroborating evidence in accord with *Georgia-Pacific* factor number 11, the comparison which originated with Centripetal's damages expert, James Malackowski, who stated:

> I calculated the averages sales for the predecessor products; I set that as the baseline; and then I calculated everything that was above the baseline for the accused sales to show you the rate of growth. Trial Tr. 3437:16-19

Centripetal electronically filed a group of seven (7) exhibits outlining the data which was the basis for his above quoted testimony at the damages hearing. Mr. Malackowski received the underlying data from Cisco on June 18th and 19th, 2020. Cisco never objected to the Court's request for this data at trial, nor did it object to the manner in which the data was utilized during the damages hearing at which

Centripetal compared the dollar amounts of sales of the predecessor products with the dollar amounts of the alleged sales ofinfringing products. Cisco's only objection to the data was the manner in which the sales of the predecessor switch products were computed.

> BY MR. JAMESON (Cisco counsel):
>
> Q. And, Dr. Becker, was there daylight between you and Mr. Malackowski with respect to what constituted the predecessor products to the 9000 series one?
>
> A. Yes. There's substantial—there's a substantial difference. Set aside this question of the update between June 18th and June 19th, the slides that Mr. Malackowski just presented, which have the updated data in them, are comparisons that only treat the Cisco 3000 series switches as predecessors to the Catalyst accused 9000 series switches, and that is just—frankly, it's inconsistent with the facts and, I think, creates a very significant difference in the picture that is painted with respect to the sales of the predecessor switches versus the accused switches. Trial Tr. 3441:14- 3442:1.

As the Court noted in its opinion, the technical predecessor issue may have been caused by Cisco arguing at trial that the 3000 series of switches, not the 6000 series, was the "design" predecessor to the 9000 series. However, as to damages, the 6000 series should be treated as a predecessor product. The Court reduced the differential by approximately $200,000, but the differential in sales of the infringing Cisco

products was nonetheless $5,575.4 billion, which corroborates Centripetal' s apportionment theory and royalty rate for damages. The $5,575.4 billion is not an exact figure, but it was only used to corroborate the multi-billion dollar damages figure claimed by Centripetal, not to actually compute damages.

Dr. Becker's bottom line was to value all five (5) patents then in issue at $3,014,561.00. It is instructive to compare this number with PTX-584, a Cisco technical document from 2018 that states the average cost of a single data breach is $3.86 million, which is more than Dr. Becker's value for all of the patents combined. However, the cost of a data breach helps to explain why Cisco's customers paid it over twenty (20) billion dollars for its infringing security products for the period from June of 2017 to June of 2020.

Very shortly before the Court's damages hearing on June 25, 2020, Cisco filed sales data separating sales in the United States from overseas sales in an effort to reduce the royalty base. This deepens the enigma Cisco created by its tactics in producing sales data in the United States and overseas while denying that any sales of accused products have been proven by Centripetal.

Cisco took similarly inconsistent positions during the trial regarding infringement and validity attempting to use the case of *01 Communique Lab., Inc. v. Citrix Sys., Inc.,* 889 F. 3d 735, 742-43 (Fed. Cir. 2018) to support its arguments. The *01 Communique* case did not support Cisco's inconsistent positions on infringement and invalidity then or on damages now. Cisco has cited no other authority that supports the inconsistent positions regarding its sales data and

making, using, and selling the accused products which it attempts to argue.

The authority cited by Cisco in support ofits defense to damages based upon the worldwide sales of the accused products is inapposite. In fact, the case relied upon by Cisco *(Power Integrations, Inc.* v. *Fairchild Semiconductor Int'l., Inc.,* 711 F. 3d 1348, 1371 (Fed. Cir. 2013)) makes clear that where products are made in the United States, the patent owner is entitled to damages for direct infringement based on overseas sales. *Power Integrations* discusses whether a party is entitled to damages for infringement that occurs outside of the United States. *See* 711 F. 3d at 1371 ("[T]he underlying question here remains whether Power Integrations is entitled to compensatory damages for injury caused by infringing activity that occurred outside the territory of the United States."). As the court in *Power Integrations* notes, infringement cannot happen entirely outside of the United States: "[T]he entirely extraterritorial *production,* use, or sale of an invention patented in the United States is an independent, intervening act that, under almost all circumstances, cuts off the chain of causation initiated by an act of domestic infringement." *Id.* (emphasis added). Centripetal, however, did not seek damages for extraterritorial products. Thus, *Power Integrations'* only value in this instance would be to show that the sales for infringing products *produced* in the United States but used or sold extraterritorially do indeed infringe.

There is support for the Centripetal' s damages award for worldwide sales due to direct infringement under § 271(a). The Supreme Court's decision in

WesternGeco LLC v. *ION Geophysical Corp* allowed damages for foreign sales when there is infringement under subsection § 27l(f)(2). 138 S.Ct. 2129, 2139 (2018). As the Supreme Court states, "Taken together, § 271(f)(2) and§ 284 allow the patent owner to recover for lost foreign profits . . . when the patent owner proves infringement under § 271(f)(2)." *Id.* *WesternGeco* suggests that a similar act of infringement under§ 271(a), where an infringing product was made in the United States but sold internationally, would qualify a plaintiff to the same damages for foreign sales set forth under § 271(f)(2). *See, e.g., Plastronics Socket Partners, Ltd. v. Dong Weon Hwang,* No. 218CV00014JRGRSP, 2019 WL 4392525, at **5* (E.D. Tex. June 11, 2019) ("[T]hese instances would constitute infringement under§ 27l(a), and thus, under the reasoning of *WesternGeco,* would be compensable even if the sale causing damage ultimately occurred abroad.").

Cisco never offered any persuasive evidence to counter Centripetal's proffered testimony and its own response to requests for admissions evidencing that the accused products were made, used, and sold in the United States and the Court found for Centripetal on this issue. *See* Opinion at 32, 86, and 100; *see also,* PTX-1409 at 5-6; PTX-1932. Further Cisco never offered evidence to rebut Centripetal's preponderance of the evidence that its infringing software was not embedded in its traditional hardware and sold in combination with it and when it was asked in pre-trial discovery and later by the Court to produce the data explaining the sales of its "accused products" it produced sales data which included "accused products" containing the infringing technology. Cisco's

only response to Centripetal's evidence was to say it's hardware "can" be sold separately, which is insufficient to challenge Centripetal' s comprehensive presentation.

Accordingly, the Court **FINDS** that Centripetal has proven that the sales data of the "accused products" which it produced was embedded with and sold in combination with the infringing technology continued Centripetal's Patents '806, '856, '176 and' 193. The Court further **FINDS** that Centripetal accurately computed its damages based upon the correct data supplied by Cisco using a proper model including apportionment and the *Georgia-Pacific* factors approved by the Federal Circuit, and that Centripetal is entitled to damages based upon worldwide sales as Centripetal proved direct infringement of the four patents remaining in issue. Insofar as Cisco's Rule 59(a) and 52(b) and 54(b) motions relied upon arguments to the contrary they are denied.

V. MR. LLEWALL YN'S AFFIDAVIT AND PATENT '856

Cisco's motion pursuant to Rules 52(b) and 54(b) challenged the Court's finding that the '856 Patent was directly infringed. Cisco attached affidavits from Mr. Daniel Llewallyn and Mr. Peter Jones, its distinguished engineers, to its initial Rule 59(a)(2) motion for a new trial. Llewallyn's affidavit and its attachments were marked as Exhibit A to Doc. 625. Cisco presented Mr. Llewallyn at trial in its defense of the claimed infringement of the '856 Patent. Centripetal relied on Llewallyn's trial testimony in its infringement case particularly regarding Patent '856

referred to at trial as the Encrypted Traffic Patent. In its post-trial Rule 59(a)(2) motion Cisco seeks to use Llewallyn's affidavit to support its noninfringement argument with regard to the '176 Patent which was referred to at trial as the Correlation Patent. Trial Tr.884:25.

However, Llewallyn's expertise was related primarily to the old StealthWatch which he helped develop while employed by Lancope, which was purchased by Cisco. Cognitive Threat Analysis (CTA) was later integrated with an updated version of Stealth Watch in 2017, and Mr. Llewallyn had only a basic familiarity with Encrypted Traffic Analysis (ET A) or CTA at the time of his trial testimony.

BY MR. BAIRD (Cisco counsel):

Q. Okay. Now we're showing this with Cognitive Threat Analytics integrated with Stealth Watch. When did that happen?

A. The Cognitive Threat Analytics integration was in 2017. It was in version 6.10.3.

THE COURT: This represents Version 10.3 of Stealth Watch?

THE WITNESS: 6.10.3, I'm sorry.

THE COURT: 6.10.3?

THE WITNESS: That's correct.

BY MR. BAIRD:

Q. So this is --

THE COURT: What do all those numbers stand for?

THE WITNESS: Oh, that's just our numbering system. We have like our release levels. We'll call it 6.10, 6.11 as we move on. But if you have a minor release in between the bigger releases, that's where the third number comes in. So we had a 6.10.1, a 6.10.2. That's just our numbering system for our releases.

THE COURT: And each of those, the last number would be a minor release; the one before that would be a major release, is that it?

THE WITNESS: Exactly. Exactly. And if it's a really, really big change we would change this to 7.0.

THE COURT: Okay. When did you get to level 6?

THE WITNESS: That was in around 2012 I think it is when we started shipping 6.0.

THE COURT: And when did you get to 6.10?

THE WITNESS: That was in the 2017 time frame.

THE COURT: Okay. You may proceed. Trial Tr. 2148:8-2149:11.

Mr. Llewallyn testified that he had never heard of Centripetal:

BY MR. BAIRD:

Q. Okay. Last question or set of questions:

Had you ever heard of a company called Centripetal Networks before this lawsuit?

A. I had not.

> Q. In developing Stealth Watch, have you ever referred to or relied on anything in any way, shape, or form from Centripetal?
>
> A. I have not. Trial Tr. 2196:2-9.

Therefore he would not have been involved in the exchange of technology between Cisco and Centripetal which resulted in integrating the new version of StealthWatch with CTA. He confirmed this on his cross examination by Centripetal:

> BY MR. ANDRE (Centripetal counsel):
>
> Q. You don't know what goes on over in Cognitive Threat
>
> Analytics, do you?
>
> A. I do not, just the big picture. Trial Tr. 2205:20-22.

Cisco continued to improve its security software after the June 20, 2017 transformation from manual after the fact security software to Centripetal's patented proactive machine learning security software. Llewallyn's testimony and PTX-569 illustrate the transition:

> BY MR. ANDRE:
>
> Q. I'm not asking about automatic. I'm just saying can the switches and routers - and particularly the Catalyst 9000 switches and the same routers—can they block bad traffic from coming in based on Stealth Watch intelligence that it gives to them via the ISE?
>
> A. That's correct. If the manual quarantine is fired, then the result is those switches or routers do initiate the rerouting of this IP

address's traffic into a quarantined area, yeah.

Q. And so the switches and routers would not let this bad website get to the host, right, if Stealth Watch gives it the information?

A. Well, yes. It's more like the host is quarantined, so it won't be able to reach that host anymore. The host is kind of segmented off into an area that can do no harm.

Q. And in that way, StealthWatch is being proactive in prohibiting the attack, correct?

A. I don't know about the word "proactive. 11 It's just—it's the result of the manual operation of the ISE quarantine. You can call that proactive, I guess, but it's in response, though, to me. You're implying to me that it's—"proactive" to me means before, you know. This is after the fact. Trial Tr. 2202:5-2203:2.

and:

BY MR. ANDRE:

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

A. That's correct.

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

A. That's correct.

Q. Okay. Let's go to Page Bates number 803 of this document. And in the left-hand column, there's a paragraph next-from-the-

last on the bottom. It says, "Integration of Cisco Stealth Watch with Cisco's Identity Services Engine." Do you see that?

A. Yes, sir.

Q. It says, "Helps organizations get 360-degree view of their extended network." Now, what I want to focus on is at the bottom, where it says, "Simplify segmentation throughout your network with centralized control and policy enforcement and address threats faster, both proactively with threat detection and retroactively via advanced forensics." Now, StealthWatch, working with other products in Cisco's Security Suite, in this case the Identity Services Engine, can proactively protect against threats, correct?

A. Well, it's based on a manual operation, though. Trial Tr. 2198:15-2199:13.

Llewallyn describes a manual operation and he also states that there is no correlation between StealthWatch alarms and CTA alarms. However, Cisco examined Mr. Llewallyn regarding PTX-569, a 2018 Cisco technical document, as follows:

BY MR. BAIRD (Cisco counsel):

Q. And so, Mr. Llewallyn, is it true that this is a 2018 document?

A. Yes, it is.

Q. Okay. And what is this document? Is the document still used today for—by Cisco?

A. Yes, it is. It's on the Cisco website in the public area.

Q. Okay. And what is this document?

A. It's basically how to configure your switches or routers and exporting devices to work more effectively with StealthWatch. And it also has some troubleshooting issues that you can refer to when working with Stealth Watch if you see problems. Trial Tr. 2178:8-21.

Exhibit PTX-569 contains the following language:

"Cisco Stealth Watch Enterprise Cisco StealthWatch is a security analytics solution that leverages enterprise telemetry from the existing network or public cloud infrastructure. It provides advanced threat detection, accelerated threat responses and simplified network segmentation using multi-layer machine learning and entity modeling. With a single, agentless solution, you get visibility across the extended network including endpoints, branch, data center and cloud. And it is the only product that can detect malware in encrypted traffic and ensure policy compliance, without decryption.

It consumes information about the traffic that is passing through the devices in the network such as routers, switches, and firewalls. Stealth Watch can analyze enterprise telemetry from any source (NetFlow, IPFIC, sFlow, other Layer 7 protocols) across the extended network, to provide real time visibility into assets that are using the network, while profiling each of these assets. It provides visibility into the east-west traffic

> in an enterprise network (in addition to north-south traffic) and analyzes network behavior to detect policy violations, anomalies as well as data consumption in the network. This document covers Stealth Watch configuration for NetFlow enabled network devices.
>
> Aggregation and correlation
>
> The flow or telemetry represents unidirectional accounting information about the traffic that is passing through a network device and is stored at the level of the flow capable device for a period of time until timeout or until flow ends. This flow will them be exported into Stealth Watch that will correlate flows from multiple devices and interfaces and perform stitching and de-duplication action to provide a single bidirectional flow of the traffic end-to-end." PTX-569 at Bates No. 270.

Cisco's counsel did not identify the foregoing language from PTX-569, but they did question Llewallyn about certain other language.

> "The Flow Collector usually only needs ingress export from all interfaces on the exporter to create interface traffic data for inbound and outbound traffic. For devices that use logical interfaces enabling both may cause the Flow Collector to double report traffic stats in noninterface documents. We usually ask the Customer to choose which data set is most important." PTX-569 at Bates No. 282.

> However, Llewallyn also testified:
>
> BY MR. BAIRD:
>
> Q. Okay. Have you done anything in the code to deal with that problem?
>
> A. I have. Some customers do export ingress/egress for their own reasons, and I've added the ability to configure the Stealth Watch Flow Collector to ignore the egress side. Trial Tr. 2173:4-8.

The above testimony confirms that the egress portion of the infringing technology is also used by his customers.

Paragraph 9 of the Llewallyn affidavit is troublesome. It describes proxy as a device and a different type of equipment, when in reality proxy is more correctly classified as a software feature achieved by combining Stealth Watch and CT A. The proxy sources are identified as Cisco USA, Bluecoat proxy, Squid and McAfee Web Gateway which are sources of intelligence transmitted over the internet by subscription. The Cisco product described in PTX-569 does not require any additional device or equipment to consume this data as the capability is contained in the Centripetal software embedded in Cisco's hardware as shown in the Cisco diagram in PTX-1065 attached to Llewallyn's affidavit. *See* PTX-1065, Attachment 1 to exhibit A of Cisco's Motion for a New Trial, Doc. 625. This Cisco diagram is also cited by the Court on p. 76 of the October 5, 2020 Opinion.

Paragraph 11 of the Llewallyn affidavit says the third-party intelligence data does not originate in the switches and routers, which is true, but misleading.

Instead this outside the network third party data enters as proxy data which is then forwarded via the switches and routers which utilize Centripetal software to correlate the proxy data with the NetFlow data thereby creating the data to be analyzed by cognitive (threat) analysis as shown in the diagram on page 5 of the Llewallyn affidavit. Llewallyn described the diagramed process in his trial testimony:

> BY MR. BAIRD:
>
> Q. Okay. Mr. Llewallyn, can you just briefly orient the Court about how this relates to the demonstrative that we were using earlier? Let's just start on the left side. What's this client server and this switch-router?
>
> A. The client server equates to computer A and computer B and the other screens. So the client is sending a request to the server above, and it's going through a switch or router to do that. As it passes through the switch or router, the NetFlow is exported to the Flow Collector to make Stealth Watch flow out of it, like we were saying, and that copy of the StealthWatch flow is sent to CTA in the cloud for analysis, and then the same copy is sent to the database below for the Flow Collector, and CT A analyzes it, and it reports back to the Stealth Watch Management Console anything that it discovered in terms of maliciousness. The Stealth Watch user on the right, Adam the Analyst, he's using the user interface provided by the StealthWatch Management Console. Trial Tr. 2189:10-2090:4.

By 2018 Cisco had replaced Adam the Analyst with Centripetal's machine learning as previously explained by PTX-569.

The balance of the Llewallyn affidavit repeats Cisco's contentions that it didn't make, use, offer to sell or sell infringing products from 2017 through June of 2020. In their invalidity evidence Cisco nonetheless claimed they possessed and offered for sale the infringing technology in 2014 and earlier which conflicts with Mr. Llewallyn's and Mr. Jones' trial testimony as well as with multiple Cisco technical and marketing documents. In its Rule 52(b)/54(b) motion alleges that Centripetal did not prove that Cisco directly infringed the '856 Patent. For the reasons stated in this Section V and in Section IV supra the Court FINDS that Cisco did so infringe and **DENIES** this portion of Cisco's motions based upon its claimed noninfringement of the '856 Patent.

VI. MR. JONES AFFIDAVIT AND PATENT '806

The conflict between Cisco distinguished engineer Mr. Peter Jones' trial testimony and Cisco's presentation of its expert trial testimony was a subject of the "Overview of the Evidence" beginning on page 22 of the October 5, 2020 Opinion. Cisco now seeks to supplement or perhaps to change or obfuscate his trial testimony through one of its sua sponte arguments in both its Rule 52(b)/54(b) and 59(a) motions. Initially, the Court observes there is no persuasive authority presented in support of supplementing his testimony posttrial via affidavits. However, an examination of the Jones affidavit's content discloses that it did not change his description of the functionality of Cisco's accused products, which infringe the claims in the '806

Patent referred to at trial as the "Rule Swap Patent." As the Court noted in its opinion, at trial Cisco attempted to contradict its own distinguished engineer Jones' testimony through its retained expert, Dr. Reddy. However, the Court rejected Reddy's testimony and accepted Jones' explanation, which was in accord with the other evidence introduced by Centripetal and its experts.

Jones defines the Access Control List (ACL) as a set of rules:

> BY MR. POWERS (Cisco counsel):
>
> Q. Okay. Could you briefly explain to the Court what an Access Control List is?
>
> A. An Access Control List is basically a set of rules. Each rule contains criteria to compare a packet against and an [sic] action. Something to do. Simple actions are either to permit or deny, allow a packet to proceed forward or to throw it away. Trial Tr. 2549:24-2550:4.

The UADP is the Cisco diagram illustrated on page 28 of the October 5, 2020 Opinion (DTX-562 at Bates No. 043). Mr. Jones thoroughly explained this Cisco software which the Court found infringed the '806 Patent in DTX-562 as follows:

> By MR. POWERS (Cisco counsel):
>
> Q. Okay. Now, just to the left, there's something called the egress forwarding controller. Please tell the Court what the forwarding controller is.

A. It looks at the headers of the packets, applies the rules to them. It decides the fate of the packets.

Q. And just above that, there's something called the PBC, packet buffers complex. Do you see that?

A. I do.

Q. And could you give the Court an overview of what that component is and how it's used during packet processing?

A. That is where the packets stay, waiting for the results from the ingress forwarding controller.

Q. Do all packets pass through that buffer complex?

A. They do.

Q. Please explain any relationship between the packet buffers complex and the hitless ACL rule update technique that we talked about yesterday.

A. There is no relationship.

Q. Now, if we go to the bottom left-hand corner, there is something called ingress FIFO.

THE COURT: What is that packet buffers complex? What is that?

THE WITNESS: It is a storage place. So as packets arrive in from ports, the packet headers are sent to the ingress forwarding controller. The packet itself goes into the packet buffers complex.

THE COURT: What goes there?

THE WITNESS: I'm sorry. Could you repeat yourself, Your Honor?

THE COURT: What goes from the ingress forwarding controller to the packet buffers complex? What goes there?

THE WITNESS: The results of all the rule settings, so the instructions for what to do with the packet. A simple case would be throw the packet away. Another one would be send it to the stack interface or the ingress forwarding controller.

THE COURT: The second one would be what, now?

THE WITNESS: A very simple answer would be if the rule set at the ACL says to discard the packet, the instruction would go from the ingress forwarding controller to the packet buffer to discard the packet.

THE COURT: And you said the second alternative was what?

THE WITNESS: It would be to send the packet forward, to send it out to a different forwarder or switch so it could leave.

THE COURT: So it could what?

THE WITNESS: A way to describe this would be the results of like a—of an ACL could be either to admit or deny. The ingress forwarding controller processes those rules. It may send an instruction to the packet buffers complex to discard the packet, or it may send

an instruction to tell the packet buffers complex where that packet should leave the system.

THE COURT: So if it goes to the packet buffers complex, it's not going to reach its destination—

THE WITNESS: Let me clarify.

THE COURT:—its original destination; is that right?

THE WITNESS: Let me clarity. The packet buffers complex is where the packet stays waiting for results from the ingress forwarding controller. It may be dropped, or it may be sent on to its destination. For instance, you will see on the right-hand side there's links from the packet buffers complex to the egress forwarding controller. This is the part in which the packet can leave the system.

THE COURT: Well, when you say, "leave the system," that means it's been blocked; is that right?

THE WITNESS: No, that does not mean it's been blocked. If it has been blocked, it is discarded. If we forward the packet, it will leave out another port on the system. It's an example of the path on which it would leave.

THE COURT: But there might be different paths that it would follow. Is that right?

THE WITNESS: So we have a number of these complexes inside the system. This would describe when the ingress port and the

egress port were on the same UADP. The block at the top—you see it's called "stack interface"—this is how we link together multiple UADPs inside the system. So the results of the ingress forwarding controller can include a set of destinations that the packet needs to leave the system.

THE COURT: Well, suppose it was going to go to its destination, initial destination. Where would it go from the packet buffers complex? Would it go through the ingress forwarding controller?

THE WITNESS: No. If you see, it would not-it would leave through the egress forwarding controller. We tend to have—the ingress forwarding controller is the processing we do on packets as they arrive. The egress forwarding controller is the process we do on the packets as they leave the system.

THE COURT: Well, maybe I'm not understanding what it means to leave the system. When you say, "leave the system," where does it go when it leaves the system?

THE WITNESS: It will go out one of the ports. On the front of the switch, you'll see a whole set of ports. So packets arrive through a port and are processed. While they're waiting for the result, they sit in the packet buffers complex. Once we have the results, which could either be throw the packet away or forward the packet, it will leave out through one of our egress forwarding controllers out to a port.

THE COURT: And will it go from the egress forwarding controller to the original destination?

THE WITNESS: Yes. Trial Tr. 2563:2-2567:8.

Jones repeated this same explanation a second time in his direct testimony:

By MR. POWERS(Cisco counsel):

Q. And, Mr. Jones, could you just remind us what FIFO is?

A. It's called a first-in-first-out buffer. It's a small queue.

The packet is then sent into the PBC for storage.

Q. What is the PBC?

A. Yes.

Q. Could you—packet buffers complex?

A. Packet buffers complex.

Q. Thank you.

A. At the same time, the packet headers, the addresses of the packets, are sent into the ingress forwarding controller. The ingress forwarding controller processes the packet according to the rules that are in the lookup tables. The result is then sent to the packet buffers complex, and it instructs the packet buffers complex what to do with the packet. A simple example would be to throw the packet away. Another example would be to send it out a port. If the packet is to be sent out a port, it's sent from the packet buffers complex to the egress forwarding controller. The

> egress forwarding controller also runs rules, including Access Control Lists. When the packet is finished going through the egress forwarding controller, it could also be dropped, or it could be sent out a port. It goes via the rewrite engine, which makes modifications to the packets. It goes through the egress FIFO, again, a small shallow buffer, the block level MACSec, Media Access Control Security—it's an encryption block—and the packet would leave the front panel port. So it comes in on the left side, circles around, and goes out on the right side. Trial Tr. 2568:1- 2569:9.

And again repeated the same explanation during his very brief cross examination by Centripetal:

> BY MR. HANNAH (Centripetal counsel):
>
> Q. Thank you, Your Honor. Good morning, Mr. Jones.
>
> A. Good morning.
>
> Q. My name is James Hannah. I'll be asking you some questions this morning. I want to talk about the Catalyst switches that you've been discussing and, in particular, the 9000 series of switches, okay?
>
> A. Yes.
>
> Q. Now, the Catalyst switches, they can receive rule sets from a variety of sources; isn't that right?
>
> A. That is correct.

Q. And one of those sources can be the DNA center; isn't that right?

A. Yes, they may receive rules from the DNA center.

Q. And, now, the way the Catalyst processes these rules, in order to process these rules, the Catalyst switch must compile them, right, in order to implement the rules?

A. That is correct.

Q. And in doing this compiling, it compiles these rules while the old rule set is still processing packets, while the old rules are still being applied to packets; isn't that right?

A. That is correct.

Q. Now, once the compilation is complete, a signal is sent to the processor to stop processing packets with the old rule set and to start processing packets with the new rule set; isn't that right?

A. That is correct.

Q. And then during the two to four clock periods that you mentioned yesterday, when there's no processing of packets, the rules are swapped; isn't that right?

A. That is correct. There is—the processing of packets continues. Packets are processed at a maximum frequency of two to four clock periods. So we don't stop processing the packets, there's just an idle period between two packets.

Q. But there's a signal that's sent to say, stop processing packets with the old rule set and start processing packets with the new rule set, correct?

A. Yes, we swap from the old to the new.

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

A. Right.

Q. Now, once that process is complete, the system signals that the swap has been complete, and then the new rule set will be applied to any subsequent packet; isn't that right?

A. We don't—we don't signal that a swap is complete, we just instruct the swap to happen.

Q. Well, there's a return success that happens after the swap is complete, correct?

A. There's really not. We just do a write of the new value. So it's a memory write.

Q. A memory write, okay. But in the document, it actually says that you return success. That's how you represent that memory write, correct?

A. Yes.

MR. HANNAH: No further questions, Your Honor. Trial Tr. 2571 :2-2573:9

Mr. Jones affidavit in paragraphs 8-12 outlines what "he could have testified to." While no persuasive authority is cited for such content to be considered,

there is nothing in paragraphs 8-12 to contradict what "he did testify to" at trial. As it did during trial with its expert witness, Dr. Reddy, Cisco is attempting to contradict or obfuscate Jones' trial testimony upon which the Court relied. Cisco's principal defense to infringement of the '806 Patent during the trial was that it's accused products neither cached (stored) the packets nor subjected them to two sets of rules during processing. Jones' trial testimony, which is not contradicted in his affidavit, confirms that Cisco's accused products "store packets in the buffer" (the same function is referred to in the trial as "caches") between subjecting each packet to a first set of rules on ingress and a second on egress.

As is explained in more detail in its October 5, 2020 Opinion, Jones' testimony corroborated Centripetal's own expert testimony and the Court accordingly DENIES both Cisco's Rule 52b/54b and its 59(a)(2) motion insofar as they are based upon its alleged noninfringement of the '806 Patent.

VII. CISCO'S ADDITIONAL EVIDENCE

Centripetal has cited multiple circuits and other federal courts that have refused to accept additional evidence of the nature proffered by Cisco before this Court in post-trial motions, and Cisco has not cited any applicable authority to the contrary. Nonetheless, the Court has reviewed and considered the affidavits of Mr. Llewallyn and Mr. Jones and finds that there is no content therein or content in the attachments to Mr. Llewallyn's affidavit that would change the Court's interpretation of their trial testimony and the inferences to be drawn therefrom. Cisco has also cited testimony from the trial in its briefs, much of which

the Court rejected and instead adopted testimony presented by Centripetal to the contrary. In addition, in numerous portions of their opening and Reply (Rebuttal) briefs, Cisco presents testimonial statements, without reference to trial testimony or exhibits that the Court admitted. Such testimonial statements are given no weight by the Court, as there are no evidentiary references to support the same.

As Centripetal argued, with supporting authorities, in its brief: Cisco cannot simply add evidence that was not introduced at trial. *See Goldblum v. Klem,* 510 F.3d 204,226 n.14 (3d Cir. 2007) ("Evidence is not 'new' if it was available at trial, but a petitioner merely chose not to present it to the jury."); *see also, Amrine v. Bowersox,* 238 F.3d 1023, 1029 (8th Cir. 2001), cert. denied, 534 U.S. 963 (2001) (approving district court's determination on remand that "evidence is new only if it was not available at trial and could not have been discovered earlier through the exercise of due diligence"); *United States* v. *Starr,* 275 F. App'x 788, 790 (10th Cir. 2008) ("[T]he district court correctly found that this evidence was available before trial, and in fact had been discovered by defense counsel. Thus Starr's claim is not based on 'new' evidence, but rather on evidence that could have been presented at trial.").

Numerous federal trial courts cited by Centripetal have come to the same conclusion. *See, e.g., Berlinger* v. *Wells Fargo,* N.A., No. 2:11-cv-459-FtM-29CM, 2016 WL 11423815, at *1 (M.D. Fla. Sept. 6, 2016); *Guisao* v. *Secretary, Dep't of Corr.,* No. 8:15-cv-9-T35AAS, 2018 WL 10883771, at *2 (M.D. Fla. Mar. 26, 2018); *Lorme v. Delta Air Lines, Inc.,* No. 03-cv-5239 (GBD),

2005 WL 1653871, at *5 n.6 (S.D.N.Y. July 13, 2005); *Watkins v. Casiano,* No. CCB-07-2419, 2009 WL 2578984, at *3 (D. Md. Aug. 17, 2009), aff'd, 413 F. App'x 568 (4th Cir. 2011); *Connelly* v. *Blot,* No. 1:16-cv-1282 (AJT/JFA), 2017 WL 11501501, at *3 (E.D. Va. Oct. 18, 2017). Cisco has not provided any authority to the contrary. The one case cited by Cisco, *Twigg v. Norton Co.,* 894 F .2d 672, 675-676 (4th Cir. 1990), does not support the admissibility of the Llewallyn affidavit or its attachments, the Jones affidavit, or the testimonial statements in Cisco memoranda, and accordingly this Court **FINDS** that such evidence is not admissible for purposes of the Cisco motions ruled upon in this opinion and order. In its October 5, 2020 Opinion the Court found direct infringement of the four (4) patents based upon Centripetal's evidence. It further found that the functionality explained in Cisco's own evidence as to the '806 Patent based upon Mr. Jones' testimony and Cisco's documents would also support infringement under Centripetal's evidence. It was not a sua sponte finding as Cisco's purported defense amounted to an admission of infringement set forth by its own distinguished engineer, Mr. Jones and corroborated by Cisco's technical publications.

In its other motion under Rules 52(b) and 54(b), Cisco claims that Centripetal did not prove Cisco's hardware was embedded with Centripetal's technology or sold in combination with same. Interestingly, Cisco states in its Reply (Rebuttal) brief in support of its Rule 52(b)/54(b) motion "... but Cisco only admitted that it loaded software onto "some" of the accused firewalls in the United States," which is, of course, all Centripetal has to prove in the making,

using, and selling factor of its infringement case against the firewalls. The factor of sales of the accused products embedded and used in combination as for damages is analyzed in Section IV of this opinion. Accordingly, the Court **DENIES** Cisco's motion insofar as it is based upon the noninfringement of the '806 Patent as argued in both Rule 59(a)(2) and 53(b)/54(b) motions.

VIII. THE '193 PATENT

Cisco challenges the Court's finding that the accused products directly infringed the' 193 Patent in its Rule 52(b)/54(b) motion. It alleges in its motion that the Court's finding of direct infringement depends upon the theory that the Identity Services Engine (ISE) device must be found to infringe. The use of the word engine may suggest that ISE is a "device," but in reality it is a part of Cisco's infringing software. The Court did describe ISE as a "device" in patent jargon on Page 19 of the October 5, 2020 Opinion.

Cisco states "However, Centripetal's infringement proof also relied extensively on ISE to establish infringement of the '193 Patent." Doc 628 at 9. Actually, Centripetal's expert Dr. Mitzenmacher's testimony was to the contrary.

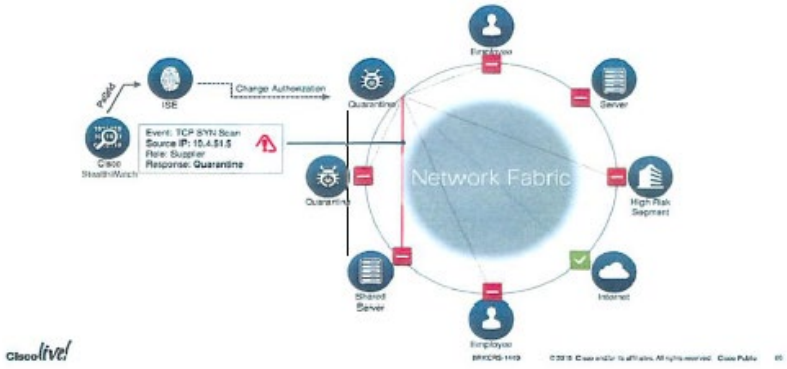
BY MR. GAUDET (Cisco counsel):

> Q. Dr. Mitzenmacher, you didn't undertake any analysis to figure out how many of Cisco's router and switch customers also buy Stealth Watch or also buy Cognitive Threat Analytics or also buy the Identity Services Engine. You don't know any of those numbers. Is that fair?

> A. I certainly couldn't recite them to you. Off the top of my head, I don't know them, but, again, since these are both system claims and computer-readable medium claims, which relate to the code on the switches and the performance of the switches and all our end routers, and all of these devices have the code there to do these things, as I've described, I just am not clear why that would specifically be relevant for me, but... Trial Tr. 804: 11-23.

Cisco also states: "Again, the Court did not find that Cisco's switches and routers are only ever used with ISE, and the record would not support such a finding." Doc. 628 at 9.

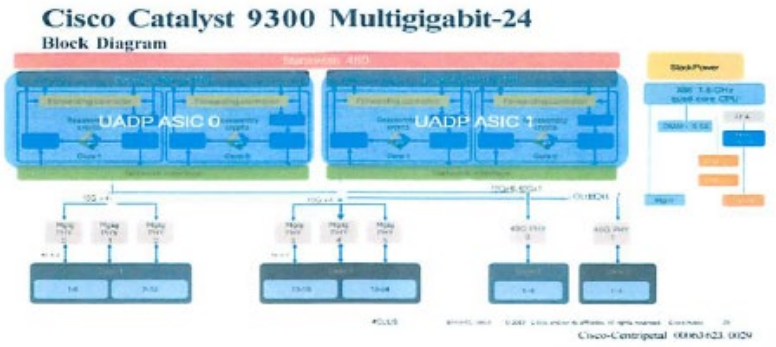
While it is not clear to the Court precisely what this sentence means, Ex. PTX-563, a Cisco technical document introduced by Centripetal during the testimony of Dr. Mitzenmacher (Tr. At 500) at Page Bates No. 415, diagrams Stealth Watch forwarding data to ISE which in turn forwards data to the switches and routers in which the infringing software is embedded as explained by Dr. Mitzenmacher.

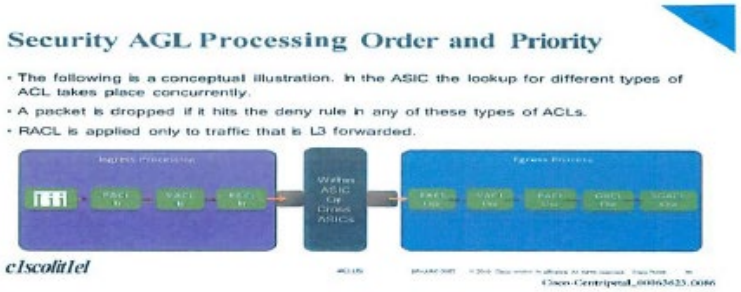


The language from PTX-1280, also a 2018 Cisco technical document introduced by Centripetal during the testimony of Dr. Mitzenrnacher, contains the following language confirming that the switches and routers perform a two stage process as opposed to only one stage which was Cisco's defense to infringement at trial:

> "Notice above that rapid threat containment is seamless in SD-Access fabric, as the endpoint continues to be operational in the employee VLAN and the IP address remains unchanged. However, the SGT assignment has changed from 4 to 255, which is the quarantine SGT.
>
> Fabric edge devices will then download SGACL permissions specific to SGT 255, which will limit the endpoint's network address access until a successful remediation is performed." PTX-1280 at Bates No. 21.

Exhibit PTX-1390, a 2019 Cisco technical document, introduced by Centripetal, illustrates at Bates No. 029 how the packets are buffered between being subjected to the two-step process and at Bates No. 086 how the packets are subjected to one set of ACLs (rules) at stage one and, after being placed in the buffer, another set of ACLs on egress at stage two. As to the '193 Patent, this exhibit corroborates the infringing software embedded in Cisco's switches and routers processes the data sent to them by ISE and Stealth Watch via a two stage process.





As it did at trial, Cisco attempts to ignore the content of its technical documents that Centripetal introduced in evidence as well as the clear inferences to be drawn from them. In its Reply (Rebuttal) brief in support of its 59(a)(2) motion, Cisco argues that " . . . Cisco also would have offered factual testimony from the many Cisco technical witnesses that were the original architects of the relevant products." Doc. 635 at 15, line 20. The Court repeatedly observed in the October 5, 2020 Opinion that Cisco failed to call such technical witnesses to respond to its technical documents which Centripetal presented as exhibits. The Court inferred in its October 5, 2020 Opinion on page 159 that Cisco wished to protect such witnesses

from Centripetal's cross examination. Cisco goes on to argue in its Reply (Rebuttal) brief in Doc. 635 page 15 line 22, "For example, Cisco would have elicited testimony confirming that - contrary to the Court's findings (Order at 140-141) the increase in sales was impacted by the addition of numerous non-accused features, and had nothing to do with Centripetal's claimed technology." Cisco's marketing documents raved about its increased sales based upon the functionality of the accused products. If Cisco actually had evidence of such new and non-accused features in its hardware or in its own software, why would it not present it at trial?

FRCP 52(b) motions should not attempt to relitigate a theory available at trial. The rule states that a party may make a motion requesting the Court "amend its findings-or make additional findings-and . . . amend the judgment accordingly." "The purpose of motions to amend is to correct manifest errors of law or fact or, in some limited situations, to present newly discovered evidence." *Fontenot v. Mesa Petroleum Co.,* 791 F.2d 1207, 1219 (5th Cir. 1986) (quoting *Evans, Inc. v. Tiffany & Co.,* 416 F. Supp. 224, 244 (N.D. Ill. 1976)). "This is not to say, however, that a motion to amend should be employed to introduce evidence that was available at trial but was not proffered, to relitigate old issues, to advance new theories, or to secure a rehearing on the merits." *Id.* (citing *Evans, Inc. v. Tiffany & Co.,* 416 F. Supp. 224, 244 (N.D. Ill. 1976)). Additionally, as Centripetal argues in its opposition brief, a Rule 52(b) motion should not be granted when it "constitute[s] nothing more than an invitation to the district court to reverse itself." *Weatherchem Corp. v. J.L. Clark, Inc.,* 163 F.3d

1326, 1336 (Fed. Cir. 1998) (denying motion). Doc. 630 at 4. Accordingly insofar as its Rule 52(b)/54(b) motion relies on Centripetal's alleged failure to prove direct infringement of the '193 Patent, such motion is **DENIED.**

IX. THE '176 PATENT

Cisco challenged the Court's ruling that the '176 Patent was infringed by the accused products in both its Rule 52(b)/Rule 54(b) motion and its Rule 59(a)(2) motion. The '176 Patent was referred to during the trial as the "Correlation Patent."

In its Rule 52(b)/54(b) Reply (Rebuttal) brief there is only a single paragraph referencing the '176 Patent. The argument is based upon Cisco's made, used, or sold in combination argument which the Court analyzed in Section IV of this opinion. Again, Cisco begins its argument in its Rule 59(a)(2) opening brief by stating "The Court sua sponte adopted a new claim construction and infringement theory with regard to the '176 Patent." Doc. 626 at 2. Cisco argues that Dr. Cole limited his infringing testimony to a single switch or router. Dr. Cole's cross examination testimony does not support Cisco's claim; indeed it may suggest exactly the opposite:

> BY MR. JAMESON (Cisco counsel):
>
> Q: Now Dr. Cole, this is claim 11 [of the '176 Patent], all right?
>
> A: Once again we have the same caveat that this is the exact wording from the patent and nothing's been altered or modified.

> Q: Okay. And if you look at the elements B1 through 84, there is a reference to a network device in each of those elements, right?
>
> A: That is correct. There is a network device listed in each of those elements.
>
> Q: And the network device is the router or switch, right?
>
> A: Once again, we're not infringing individual components, it's the entire system, but the *component* in this case that's receiving and transmitting those packets is the router or switch. Trial Tr. 1101: 1-13 (emphasis added).

In any event Centripetal dealt directly with this point when Cisco's expert witness on the '176 Patent, Dr. Almeroth testified during his cross examination as follows:

> BY MR. KASTENS (Centripetal counsel):
>
> Q. And then you said this had to be a single network device, correct?
>
> A. Not quite. It says a network device here, and then later it's the network device. So it's the same network device across the limitations.
>
> Q. But you do understand that in a patent, when it says A, it can mean one or more; is that correct?
>
> A. That's my understanding.
>
> Q. So this could be more than one network device, correct?
>
> A. It could be. Trial Tr. 2278: 11-20.

Mr. Llewallyn also corroborated Centripetal's claim that multiple switches and routers are utilized in Cisco's infringing network:

> BY MR. BAIRD:
>
> Q. Now, this slide just showed one router or switch. Mr. Llewallyn, is it correct that the flow collector could be getting Netflow records from other switches and routers along the path between the two computers that aren't shown here?
>
> A. That's correct. And it's also most common. It's very rare to get it from just one. Trial Tr. 2149:12-18.

The multiple device language also appears in the patent specification. *See* '176 Patent col.2 1.58-63 (filed Jan. 31, 2017) ("Network device(s) **120** may include one or more devices (e.g., servers, routers, gateways, switches, access points, or the like) that interface hosts **108, 110, and 112** with network **106.** Similarly, network device(s) **122** may include one or more devices that interface hosts **114, 116,** and **118** with network **106**."). Therefore, it was Centripetal and its exhibits that introduced the multiple device argument, not the Court sua sponte. Notably "devices" as used in the patent means; servers, routers, gateways, switches, access points (another name for firewalls) or the like, all expressed in the plural.

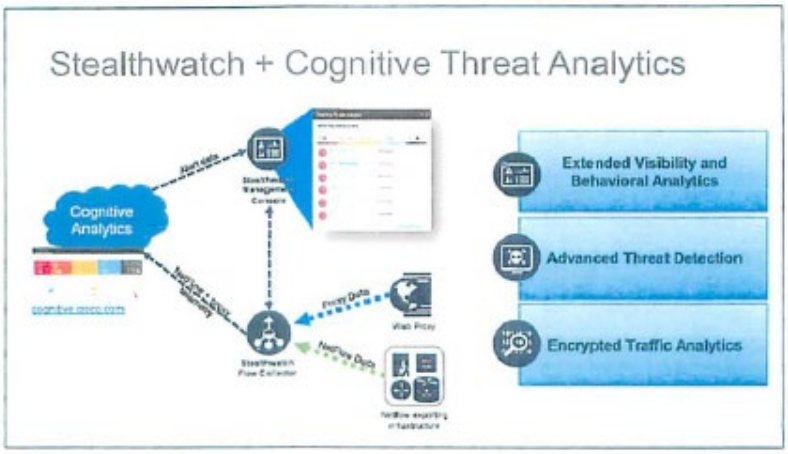
Cisco's repeated references to sua sponte seems to suggest that the Court must somehow limit its analysis to the testimony of Centripetal' s experts. The Court again observes that Cisco's own documents contradict its arguments, in particular PTX-1065 a November 2017 Cisco technical document which is

Exhibit A to Mr. Llewallyn's affidavit Doc. 635, Ex. A, Attachment 1.

Compare Cisco's argument in its "Reply" (Rebuttal) brief:

> "Had Centripetal or its infringement expert relied on a "one or more" construction of the phrase "a network device," then Dr. Almeroth would have explained why that theory breaks down as well-namely that the claims would still require correlation of packets received into a set of switches or routers with packets transmitted by the *same* set of devices; not just any "correlation" generically with other data. Finding a document with the word "correlation" in it is not good enough; the claims requires correlation of packets entering with packets exiting the same thing. Had Centripetal accused a group of switches or routers, Dr. Almeroth could have responded accordingly. But because Centripetal did not raise the Court's new theory, Cisco had no notice of it and no opportunity to present responsive evidence at trial.
>
> Finally, Centripetal's suggestion that its expert Dr. Cole testified regarding correlation of logs from multiple devices is incorrect. *See* Opp. at 10. Centripetal cites a brief discussion of Syslog data in Dr. Cole's redirect examination, which contains no suggestion that Stealth Watch can correlate logs from multiple switches or routers. Trial Tr. 1 114:24-1116:20. More importantly, the cited

testimony actually shows that Dr. Cole *does not* use Syslog as evidence of infringement. Dr. Cole testified: So customers can just use NetFlow by itself to do that correlation. It does not need to use the proxy data." *Id.* at 1116:12-13. When asked what this means for infringement, Dr. Cole testified "This shows that the claim language says *it must be able to correlate the two NetFlows.* So this is confirming that it can correlate NetFlow by itself which would consist of ingress and egress Netflow." *Id.* at 1116:23-1117:1 (emphasis added). In sum, Dr. Cole never opined that correlation of Syslogs is infringing; his infringement theory relied entirely on correlation of NetFlow data." Doc. 635 at 6.



Stealthwatch integrates with Cognitive Analytics ("CA"—aka Cognitive Threat Analytics). This involves the addition of a new information panel on the SMC's

> WebUI, and enhances Stealthwatch further by leveraging CA's cloud based analytics engine. that correlates threat behaviors seen in the enterprise with those seen globally. It uses machine learning and statistical modeling to learn from what it sees and adapt to changing network behavior over time.

Compare the foregoing argument by Cisco with its 2017 technical document PTX-1065. The explanatory text contains the following language which explains the functionality of the diagrammed Cisco network which infringes as made, used, and sold by Cisco and contradicts its arguments:

> " . . . and enhances StealthWatch further by leveraging CA's cloud based analytics engine, that correlates threat behaviors seen in the enterprise with those seen globally. It uses machine learning and statistical modeling to learn from what it sees and adapt to changing network behavior over time . . .
>
> . . . This solution uses the Proxy ingestion feature to consume Syslog information sent from proxy sources, integrating it into StealthWatch's flow visibility ...
>
> . . . This Syslog information contains details similar to what a flow record contains: Source IP, destination IP, Source Po1t, Destination Port, URL, Username . . .
>
> . . . StealthWatch will then correlate the received Syslog and relates it to the flows collected from network devices before and

> after the proxy, providing deeper visibility into customers web traffic . . .
>
> . . . Customer may use either Netflow or Proxy data, or both . . . " PTX-1065 at Bates No. 005.

In support of its arguments Cisco attacks a part of PTX-1065 in the text of Mr. Llewallyn' s affidavit at Paragraph 11 on Page 5, Doc. 626-1. The explanatory language which appears immediately below the diagram in PTX-1065 as it was introduced at trial contains the foregoing explanatory language that directly contradicts both Mr. Llewallyn's affidavit and Cisco's argument in its Reply (Rebuttal) brief as well as the testimony of Dr. Almeroth, Cisco's expert witness on the '176 Patent. (Exhibit 1065 in its entirety is attached to Cisco' s brief Doc. 626-1 as Exhibit A).

Attachments 2 and 3 of Mr. Llewallyn's affidavit amount to no more than a play on words. These exhibits use the term "de-duplicated," which is a function performed by a previous form of StealthWatch when Lancope was still a separate company, as if it described the accused technology, which it does not. De-duplication is only one of the many functions of the post June 20, 2017 infringing software. The term de-duplication does not even appear in the diagram or the text explaining the diagram. Likewise, the Llewallyn affidavit states that "proxy data" in PTX-1065 is not "generated" by Cisco's switches and routers, which is correct, but, again, misleading. The proxy data, which is intelligence data usually generated by third parties, arrives at Cisco's network via the internet whereupon Cisco switches and routers (single as shown in the diagram, or

multiple), embedded with Centripetal's infringing technology, feed it to StealthWatch which correlates it and sends it to Cognitive Analysis (aka Cognitive Threat Analysis) and the correlated intelligence data generate rules which are utilized to process such data in its infringing network of switches, routers and, in some instances, firewalls as well. Clearly there is more going on in Cisco's post June 20, 2017 network than "de-duplicating" as described in attachments 2 and 3.

The diagram's explanatory text demonstrate that the StealthWatch and Cognitive Threat Analysis contain either correlation from a single source through a single router (i.e. Netflow Data to Stealth Watch Flow Collector) which processes ingress, correlation and egress through a single switch (i.e. NetFlow to Stealth Watch Flow Collector to Cognitive Analysis) or multiple switches, Proxy Data (such as Syslog and NetFlow Data to StealthWatch Flow Collector or Collectors to Cognitive Analysis). *See* PTX-1060.

However, PTX-1060, a Cisco technical document introduced by Centripetal during Dr, Cole's testimony, demonstrates that as of December 2017 Cisco was having scalability issues which indicate the need for multiple StealthWatch Flow Collectors describing multiple switches as follows:

> "The Catalyst 9400 series of switches supports analysis of up to 3500 flows per second for ETA and are capable of up to 384,000 NetFlow entries per switch (128K per ASIC); 192,000 ingress and 192,000 egress based on the installed supervisor regardless of the number of linecards installed. At 3500 FPS for ET A, it is recommended that it only

> be configured when the Catalyst 9400 is used as an access switch and not in distribution or core of the network. As with the Catalyst 9300, ET A on the 9400 when exceeding 3500 flows per second may miss exporting ET A records for some flows, causing incomplete ETA fields in flow analysis.
>
> In addition to the Catalyst 9300 and 9400 specification, you need to carefully consider the number of StealthWatch Flow Collectors required to support the Catalyst 9300s with ET A configured and the flows per second reaching the Flow Collectors." PTX-1060 p. 23.

Centripetal's demonstrative exhibit PTX-547 explains that its software technology solves Cisco's speed and reliability problems. PTX-547, page 141 of the October 5, 2020 Opinion.

Cisco argues that "Finding "a" document with the word correlation is not good enough." (emphasis added) In addition to PTX-1065, which both diagrams and explains in depth how the '176 Patent is infringed through correlation, the following Cisco technical publications post June 20, 2017 explain the correlation feature in whole or in part; PTX-584 at Bates No. 402, PTX-1009 at Bates No. 409, PTX-591 at Bates No. 522, PTX-202, PTX-569 at Bates No. 272 and PTX-1893 at Bates 011. Pre June 20, 2017 older versions of StealthWatch also used the term "correlate" (DTX-343 Bates No. 002), however, the technology at that time relied upon manual responses from Adam the Analyst and therefore operated only retroactively;

> "The Stealth Watch System quickly zooms in on any unusual behavior, immediately sending an alarm to the SMC with the contextual information necessary for security personnel to take quick, decisive action to mitigate any potential damage." DTX- 343 at Bates No. 001 (a 2014 document).

Cisco technical documents also illustrate that Cisco's products continued to rely on manual software referred to as "Adam the Analyst" until it copied Centripetal's machine learning software. PTX-1089 at Bates No. 239.

Cisco did not successfully copy all of Centripetal's technology at one time, rather it did so over a period of years. It now claims the ability to process billions of packets, where it formerly claimed hundreds of thousands.

Cisco cannot credibly argue that it was taken by surprise (i.e. sua sponte) by its own technical documents or by the patent itself, both of which refer to multiple devices and both of which were introduced by Centripetal during trial. Accordingly what Cisco attempts to classify as sua sponte originated in the patent itself, was the subject of cross examination of Cisco' s retained expert Dr. Almeroth as well as Cisco's direct examination of its distinguished engineer, Mr. Llewallyn, and was corroborated by Cisco's own published documents and explanatory text. The Court **DENIES** both Cisco's Rule 59(a)(2) motion and its Rule 52(b)/54(b) motion insofar as each motion relies upon its claim that Centripetal failed to prove infringement of the '176 Patent.

X. WILLFULNESS

While Cisco did not directly address willfulness in its brief in support of its Rule 59(a)(2) motion, it did argue the point in its Reply (Rebuttal) brief. The Court addressed willfulness in its October 5, 2020 Opinion in Pages 149-161 as well as on Page 166.

Cisco is particularly critical of the Court's analysis of *Read* factor four, Cisco's "size and financial condition." Cisco does not dispute the significance of its "size and financial condition, as it portrays itself as "the largest provider of network infrastructure and services for many years before any of the patents issued." Doc. 635 at Page 17.

In reviewing Cisco's marketing documents, the Court observes the repeated claims that it had "solve[d] a network security challenge previously thought to be unsolvable" (PTX-452 at Page 648) and was the "Industry's first network with the ability to find threats in encrypted traffic without decryption." (PTX-989 at Page 4); *see also,* PTX-383 ("Stealthwatch is the first and only solution in the industry that can detect malware in encrypted traffic without any decryption using Encrypted Traffic Analysis."); PTX-561; PTX-963; PTX-1004; PTX-1010; PTX-1136; PTX-1417. All the while Cisco knew that Centripetal had solved the challenge and was providing the software needed to deal with encrypted traffic, based upon information it obtained from Centripetal during the Nondisclosure Period. The Nondisclosure Agreement was signed and effective on January 26, 2016 (PTX-99) and confidential information was shared for approximately one and a half years thereafter. Thus, Cisco utilized its footprint in the marketplace and

financial prowess to the detriment of Centripetal and its conduct was willful and egregious.

XI. FINAL ORDER

The Court has undertaken to analyze each issue raised by Cisco in both of its motions individually and collectively. The Court **DENIES** the relief sought in Cisco's Rule 59(a) as it **FINDS** no merit in any of the grounds upon which Cisco relies. The Court also **FINDS** no merit in any of the grounds raised in support of its Rule 52(b)/54(b) motion when considered individually and collectively and accordingly **DENIES** that motion.

With regard to Cisco's motion as it separately relates to Rule 54(b) the Court **FINDS** that Cisco's request is mooted by the Court's Order of November 19, 2020 **GRANTING** the joint motion of the parties to dismiss, without prejudice, all remaining claims not addressed in its Order of October 5, 2020.

Therefore the Court enters **FINAL JUDGMENT** in favor of Centripetal Networks, Inc. against Cisco Systems, Inc. for the reasons and upon the terms set forth in its October 5, 2020 Order as well as in this Order.

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

It is **SO ORDERED.**

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

March [handwritten: 17], 2021
Norfolk, Virginia

Appendix E

RELEVANT STATUTORY PROVISION
28 U.S.C. §455

(a) Any justice, judge, or magistrate judge 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:

(1) Where he has a personal bias or prejudice concerning a party, or personal knowledge of disputed evidentiary facts concerning the proceeding;

(2) Where in private practice he served as lawyer in the matter in controversy, or a lawyer with whom he previously practiced law served during such association as a lawyer concerning the matter, or the judge or such lawyer has been a material witness concerning it;

(3) Where he has served in governmental employment and in such capacity participated as counsel, adviser or material witness concerning the proceeding or expressed an opinion concerning the merits of the particular case in controversy;

(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;

(5) He or his spouse, or a person within the third degree of relationship to either of them, or the spouse of such a person:

(i) Is a party to the proceeding, or an officer, director, or trustee of a party;

(ii) Is acting as a lawyer in the proceeding;

(iii) Is known by the judge to have an interest that could be substantially affected by the outcome of the proceeding;

(iv) Is to the judge's knowledge likely to be a material witness in 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.

(d) For the purposes of this section the following words or phrases shall have the meaning indicated:

(1) "proceeding" includes pretrial, trial, appellate review, or other stages of litigation;

(2) the degree of relationship is calculated according to the civil law system;

(3) "fiduciary" includes such relationships as executor, administrator, trustee, and guardian;

(4) "financial interest" means ownership of a legal or equitable interest, however small, or a relationship as director, adviser, or other active participant in the affairs of a party, except that:

(i) Ownership in a mutual or common investment fund that holds securities is not a "financial interest" in such securities unless

the judge participates in the management of the fund;

(ii) An office in an educational, religious, charitable, fraternal, or civic organization is not a "financial interest" in securities held by the organization;

(iii) The proprietary interest of a policyholder in a mutual insurance company, of a depositor in a mutual savings association, or a similar proprietary interest, is a "financial interest" in the organization only if the outcome of the proceeding could substantially affect the value of the interest;

(iv) Ownership of government securities is a "financial interest" in the issuer only if the outcome of the proceeding could substantially affect the value of the securities.

(e) No justice, judge, or magistrate judge shall accept from the parties to the proceeding a waiver of any ground for disqualification enumerated in subsection (b). Where the ground for disqualification arises only under subsection (a), waiver may be accepted provided it is preceded by a full disclosure on the record of the basis for disqualification.

(f) Notwithstanding the preceding provisions of this section, if any justice, judge, magistrate judge, or bankruptcy judge to whom a matter has been assigned would be disqualified, after substantial judicial time has been devoted to the matter, because of the appearance or discovery, after the matter was assigned to him or her, that he or she individually or as a fiduciary, or his or her spouse or minor child residing in his or her household, has a financial

interest in a party (other than an interest that could be substantially affected by the outcome), disqualification is not required if the justice, judge, magistrate judge, bankruptcy judge, spouse or minor child, as the case may be, divests himself or herself of the interest that provides the grounds for the disqualification.