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

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

OPINION AND ORDER

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

I. PROCEDURAL POSTURE[1]

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

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

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

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

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

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

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

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

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

<u>II.</u> <u>WITNESSES AT TRIAL</u>

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. <u>See</u> 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 <u>live</u> 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 <u>video deposition</u> 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 <u>live</u> expert witnesses:

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

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

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

III. TECHNOLOGY TUTORIAL

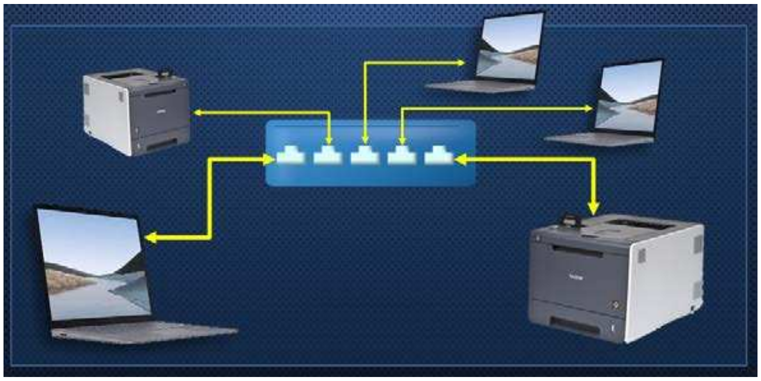
A. NETWORKING AND CYBERSECURITY TUTORIAL

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

i. Overview of Networking

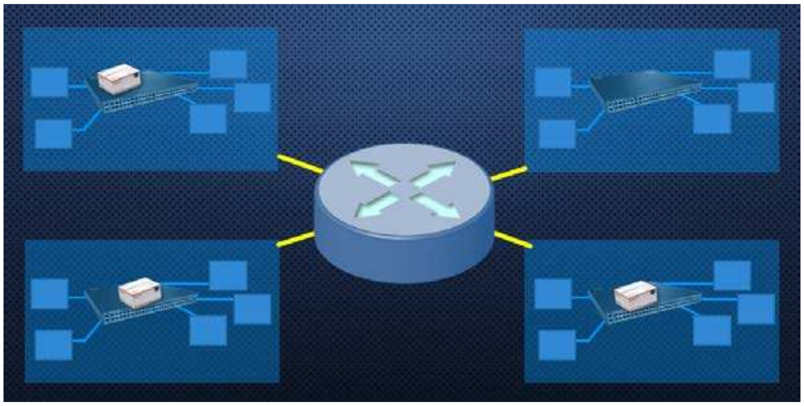
The three principal devices that comprise computer networks are switches, routers and firewalls. Tr. 20:5-10. Beginning with switches, Centripetal's expert Dr. Medvidovic used analogies to explain these complex network devices. He compared the operation of a switch to that of a telephone switchboard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

FIG. 1



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

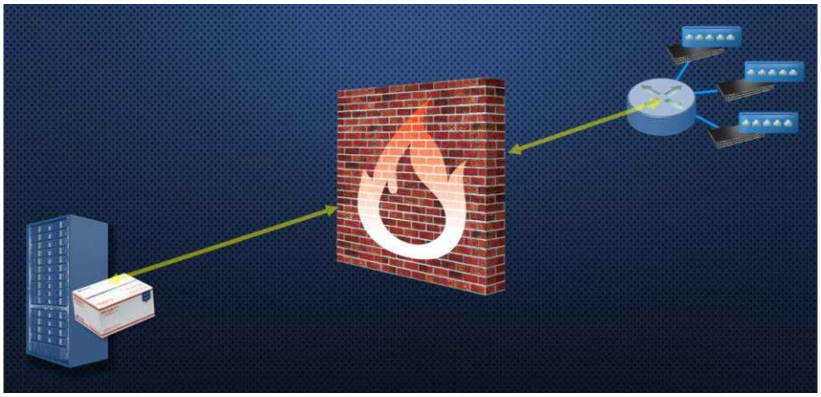
FIG. 2



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

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

FIG. 3



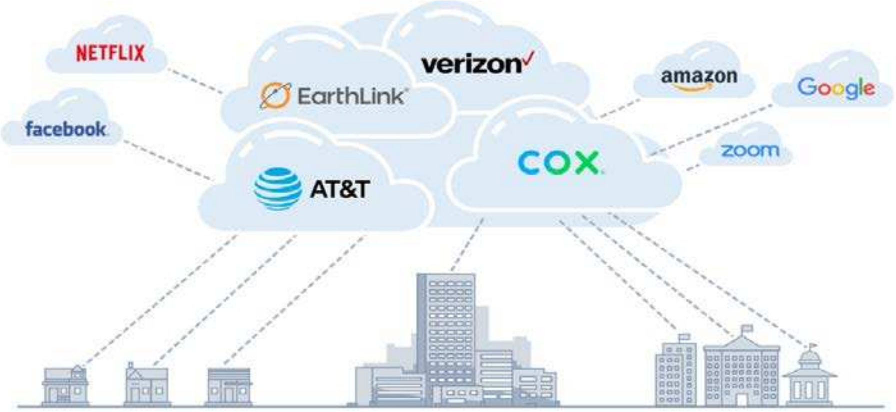
Dr. Medvidovic used video access to ESPN.com from a web server as an example of the operation of a firewall. He explained that:

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

Tr. 25:8-20. Accordingly, firewalls often sit at the edge of individual networks to control the entry of data from the internet. Tr. 26:1-12. As technology develops, firewall type functionality is often now included inside of other devices such as routers and switches. These devices may be located at different locations within a network – not just at the outside barrier. Tr. 82:8-18. This inclusion of firewall functionality in other devices is in contrast with older network technology where firewalls were responsible for the security of the network, by blocking malicious packets from entering it, while the routers and switches focused on speed and performance in the transmitting data. Tr. 26:16-22.

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

FIG. 4

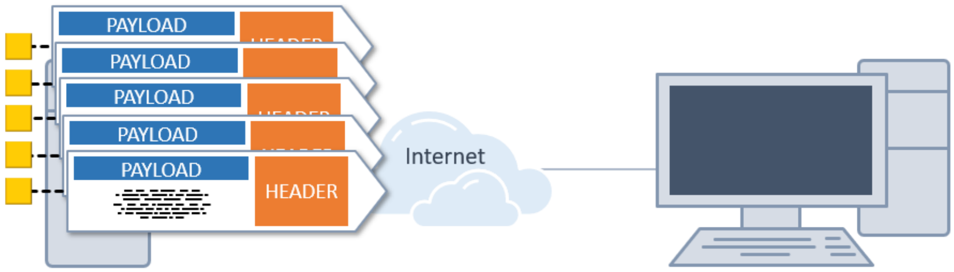


The international nature of the internet requires that the sending of data between all of these providers be based on uniformly developed standards that are globally applicable. Tr. 77:5-17. One such organization, the Internet Engineering Task Force ("IETF") is responsible for developing universal internet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

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

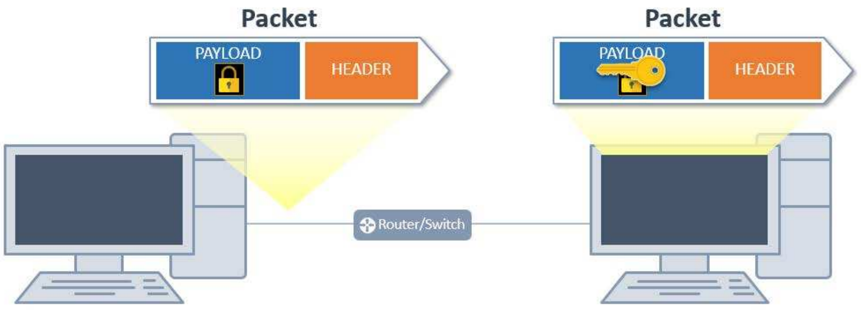
Packets consist of two different parts: the header and the payload; see Fig. 5.

FIG. 5



The header contains information such as the source address, source port, destination address, destination port number, and the protocol being used to transmit the packets. Tr. 107:16-23. These five pieces of information are known as the “5-tuple.” Tr. 108:4. The information contained in the header is inspected by the router or switch to determine where and how to send that individual packet. Tr. 108:7-16. This information can be thought of as a mailing label on a package which contains an individual’s name and mailing address as well as a return address. Tr. 27:24-25. The payload is the portion of the packet that contains the actual content of the data. This information is similar to the content within a postal package, such as a new football or baseball glove. In the ESPN video hypothetical, this would be the actual portion of the video sent by each individual packet. Tr. 28:4-10. This data in the payload part of the packet can be encrypted, meaning the information in the payload can be transmitted in code. Tr. 28:18-25. For example, the hypothetical video from ESPN.com would not usually be encrypted, but often data sent in a packet’s payload containing sensitive information, such as banking or credit card data, will be encrypted. Encryption becomes vital so that this sensitive data is not stolen by bad actors hacking the network. Tr. 28:18-25. Encryption works to lock up the data in the payload section of the packet so it cannot be seen without decryption. Tr. 29:1-5. Consequently, just as with a sealed package, snoopers of network traffic would be unable to see what is in the packet unless it could be unlocked and opened, which is generally known as decrypting the data. But, even when a packet is encrypted, the header information, such as the source and destination, is not encrypted and is visible. Tr. 29:10-16; see Fig. 6.

FIG. 6



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

ii. Overview of Networking Security

As explained supra, the internet is a very large and complex organization of networks that utilize protocols to relay data from one network device to another resulting in the transmission of data to an end user. Tr. 112:1-6. As a result of the internet's complexity, there are many methods employed by cyber criminals to transmit malware and gain access to encrypted, secure and confidential information. Tr. 112:7-14. Cyber criminals can use malware or other methods to infect a network and steal data using a process known as exfiltration. Tr. 343:19-15. Exfiltration is the process by which cyber criminals "exfiltrate" data out of a network by stealing valuable confidential data. Tr. 343:19-15.[2] Therefore, to prevent malware and data exfiltration, cyber defense systems often use a concept known as defense-in-depth, the deployment of a variety of network security devices at different layers of the network, to protect sensitive network data. Cisco's expert, Dr. Almeroth, compared network defense-in-depth to that of the security used by a federal courthouse, which contains a series of secured entry points to the building, a courtroom or a judge's chambers. Tr. 112:18-22. Consequently, just like any type of modern security system, there must be different layers of security in a network to be effective in preventing evolving methods of cyberattacks. Tr. 113:3-10, 51:17-21. Therefore, to maximize effectiveness, security measures are often placed at different devices/locations in a network, such as within a firewall, a security gateway, in routers and switches, and also within the end user's computer. Tr. 113:11-18. Dr. Almeroth outlined that there are multiple approaches used by cybersecurity professionals to effectively develop defense-in-depth security systems. Tr. 117:22-24. Two of the relevant approaches, for purposes of this trial, are known as detect and block through "inline" analysis and "out-of-band" also known as allow and detect. Tr. 118:2-7. These approaches can be used unilaterally or combined to create different styles of network security based on the needs of network administrators.

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

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

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

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

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

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

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

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

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

B. OVERVIEW OF THE ACCUSED PRODUCTS

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

i. Cisco's Switches

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

ii. Cisco's Routers

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

iii. Cisco's Digital Network Architecture

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

iv. Cisco's Stealthwatch

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

v. Cognitive Threat Analytics

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

vi. Identity Services Engine

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

vii. Encrypted Traffic Analytics

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

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

viii. Cisco's Firewalls

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

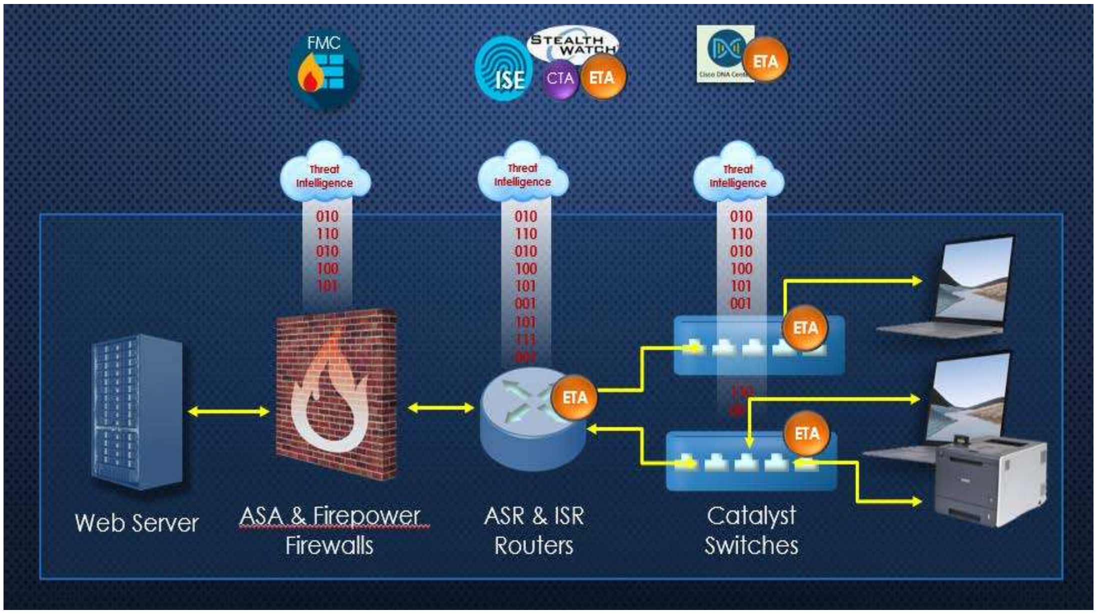
ix. Firepower Management Center

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

x. Complete Picture of a Cisco Network

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

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



C. THE PARTIES

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

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

IV. OVERVIEW OF THE EVIDENCE

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

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

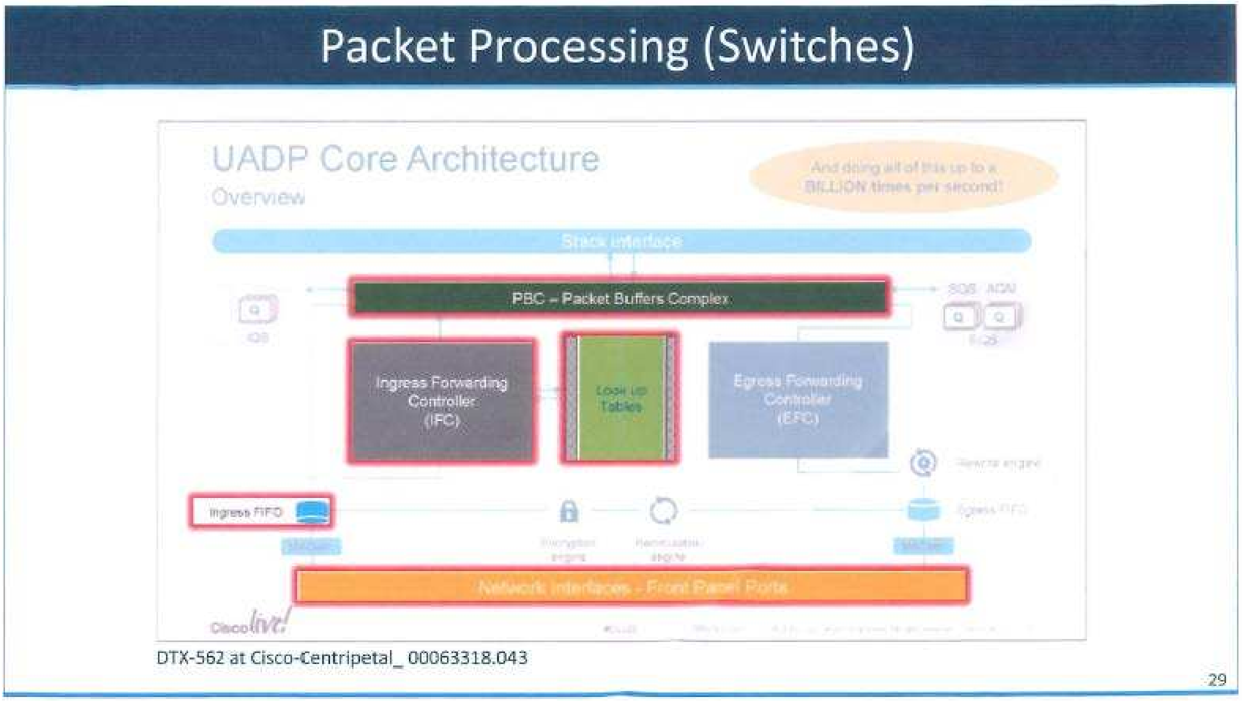
In the presentation of its infringement case, Centripetal called its top-level employees in person, Cisco employees by video deposition, and two expert witnesses. Centripetal presented numerous Cisco technical documents and other Cisco publications which postdated the alleged initial infringement date of June 20, 2017. Cisco's own documents from this time frame, and the evidence in general, strongly supported Centripetal's infringement case as to four of the five asserted patents. Therefore, the Court **FINDS** that the '856 Patent, the '176 Patent, the '193 Patent, and the '806 Patent are valid and directly infringed. Cisco abandoned its claim that the '205 Patent was invalid, but argues that it was not infringed and the Court agrees and so **FINDS**.

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

Moreover, Cisco's experts also testified that Cisco's products did not infringe any of the claims of any of the patents at issue, while focusing on distinct elements of the claims. The testimony of these experts on infringement and validity all focused on old Cisco technology, as did most of the testimony of Cisco's employee witnesses. Cisco's lockstep strategy of denying any infringement of any of the elements of the four claims where infringement is found, and backstopping this position by contending that if the Court found infringement the patents were ipso facto invalid, led to a number of factual conflicts in its presentation of its evidence.

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

SLIDE 29 OF DR. REDDY'S PRESENTATION



Packet Processing (Switches)

UADP Core Architecture
Overview
And doing all of this up to a BILLION times per second!
Stack interface
PBC – Packet Buffers Complex
SQS AQM
Ingress Forwarding Controller (IFC)
Look up Tables
Egress Forwarding Controller (EFC)
Rewrite engine
Ingress FIFO
Egress FIFO
Network interfaces – Front Panel Ports
Cisco live!

DTX-562 at Cisco-Centripetal_ 00063318.043

29

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

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

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

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

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

A. Yes, I have.

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

A. Okay.

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

THE WITNESS: Yes, Your Honor.

MR. JAMESON: This one here, Your Honor?

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

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

THE COURT: All right. Go on.

BY MR. JAMESON:

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

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

MR. JAMESON: Okay.

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

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

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

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

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

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

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

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

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

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

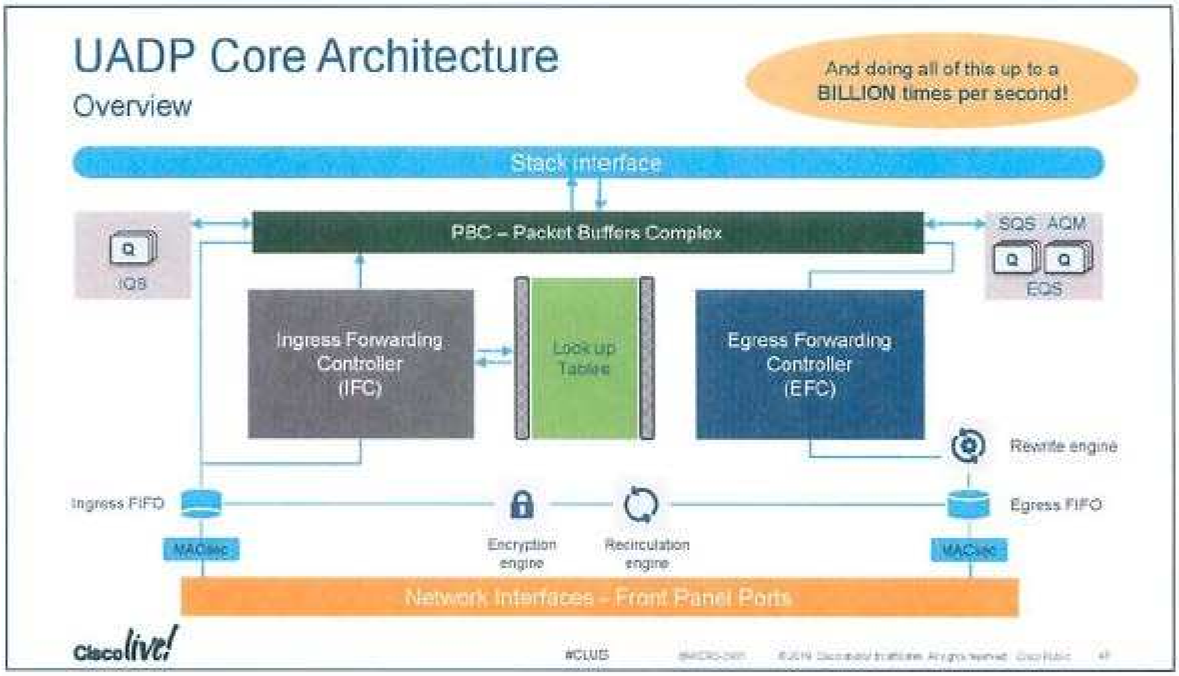
Q. And while the accused system is continuing to process packets with the old rule set, are packets moved into a cache?

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

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

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

DTX-562



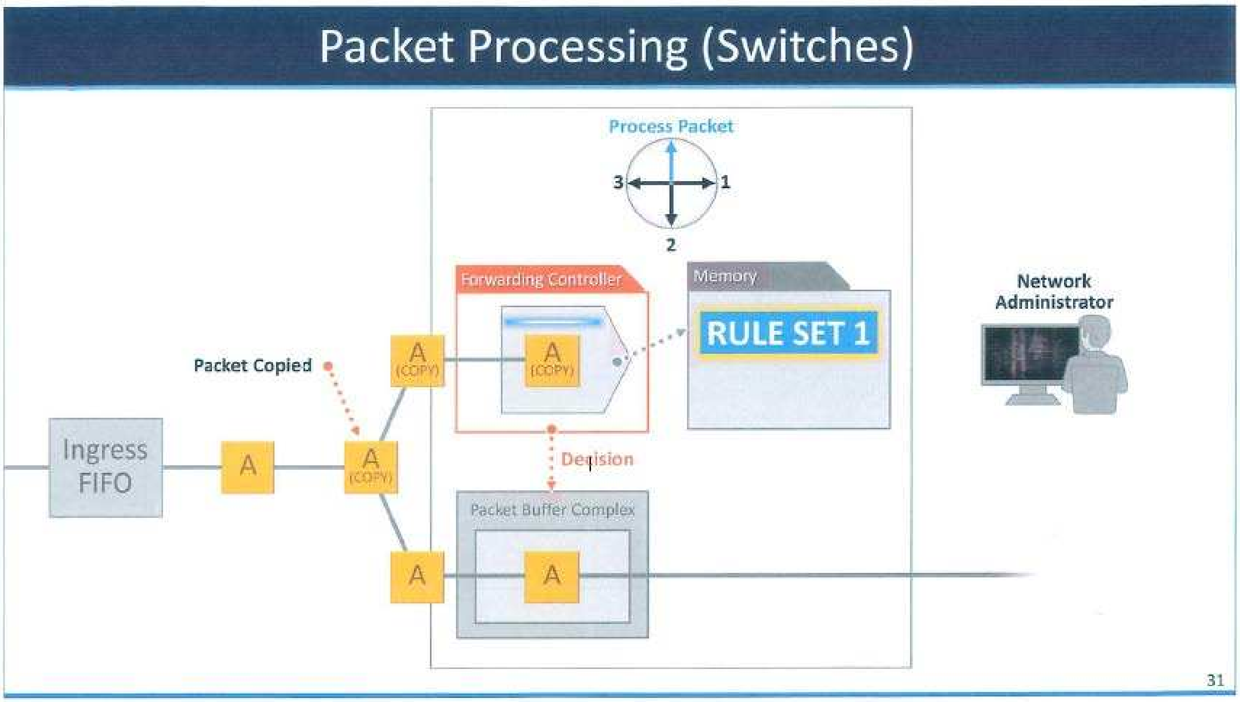
UADP Core Architecture

Overview

And doing all of this up to a BILLION times per second!

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


Packet Processing (Switches)

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

Cisco's experts attempted to challenge every element of all of the claims at issue in its non-infringement case. However, the Court **FINDS** that Centripetal has proven the direct infringement of each element of the asserted claims in the '856 Patent, the '176 Patent, the '493 Patent, and the '806 Patent by a preponderance of the evidence. Most of Cisco's challenges amounted to no more than conclusory statements by its experts without evidentiary support. Accordingly, in its findings of fact and conclusion of law, the Court has focused on only those elements cited by Cisco's infringement experts in their patent by patent outlines of noninfringement theories. The Court will analyze each patent individually, and outline all relevant findings of fact and conclusions of law regarding infringement, validity, and damages. The Court will address the patents in the following order: the ‘856 Patent; the ‘176 Patent; the ‘193 Patent; the ‘806 Patent; and the ‘205 Patent.

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

A. THE ‘856 PATENT

i. Findings of Fact Regarding Infringement

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

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

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

4. Claim 24 is laid out below:

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

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

JTX-5.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

<u>Analytics</u>.") (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; <u>see</u> 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.

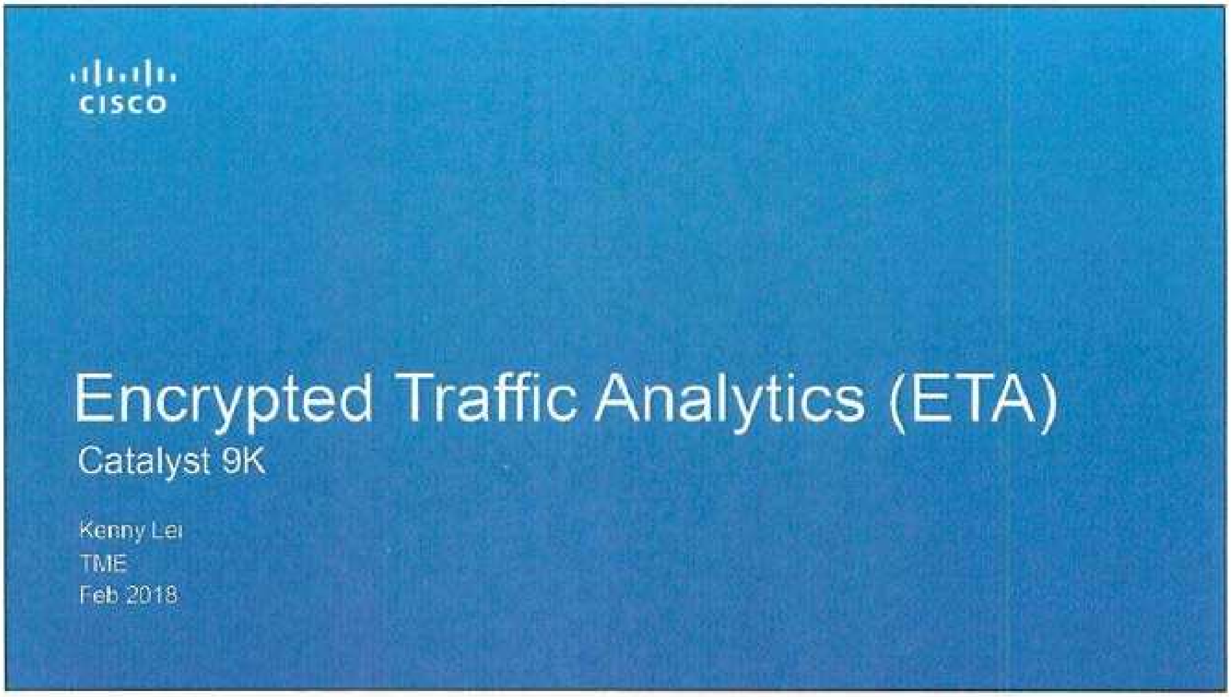
22. After this communication, ISE will provision rules or change of authorizations ("CoAs") to the switches and routers. The switches and routers operate inline and are able to drop incoming packets from the malicious source and outgoing packets containing sensitive data attempting to be exfiltrated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

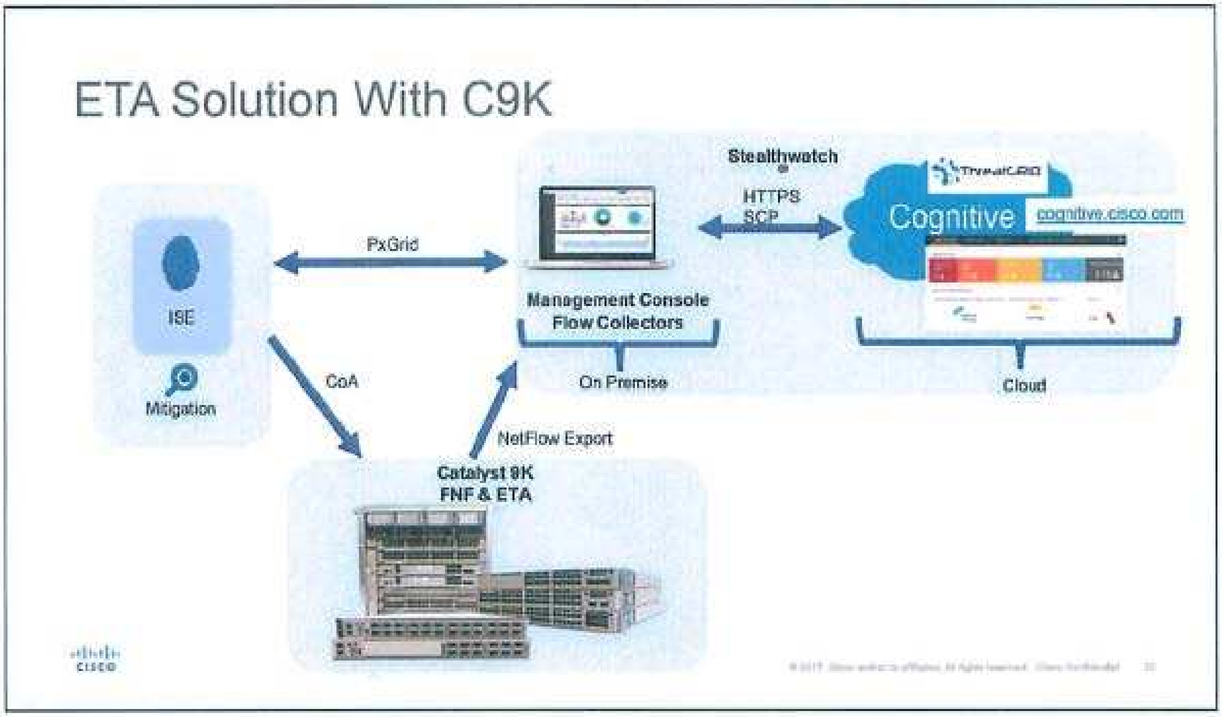


cisco

Encrypted Traffic Analytics (ETA)

Catalyst 9K

Kenny Lei
TME
Feb 2018



ETA Solution With C9K

ISE
Mitigation
PxGrid
CoA
NetFlow Export
Catalyst 9K
FNF & ETA
Management Console
Flow Collectors
On Premise
Stealthwatch
HTTPS
SCP
ThreatGRID
Cognitive
cognitive.cisco.com
Cloud
cisco

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)).

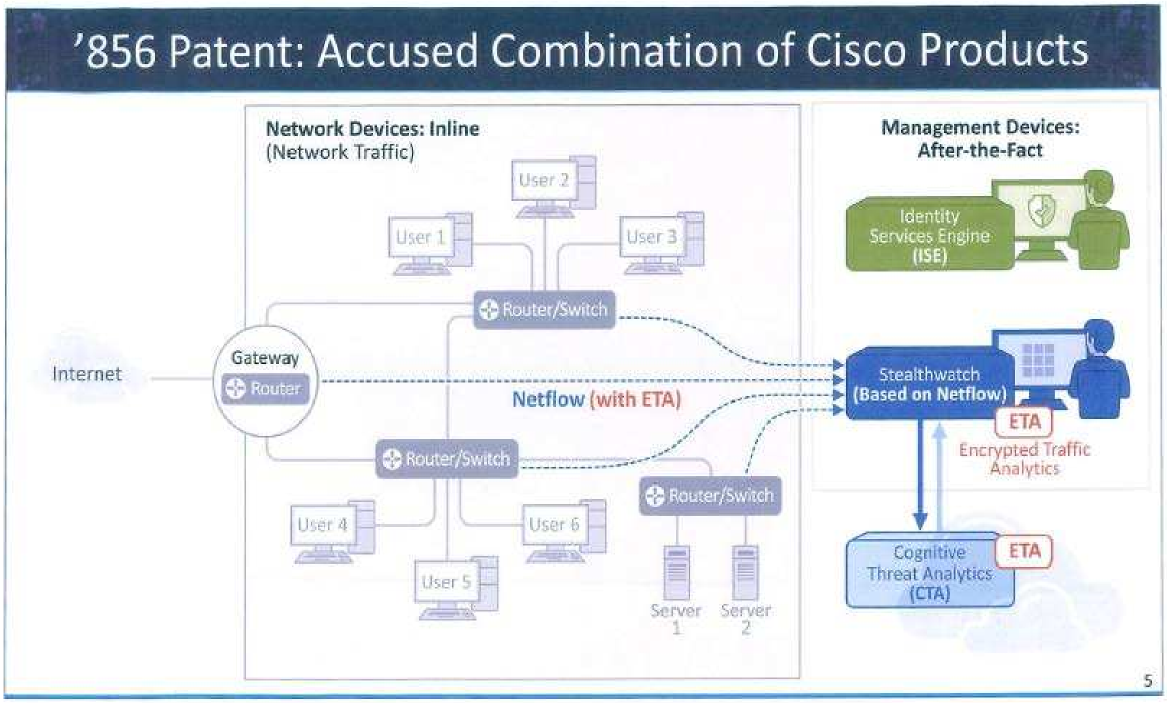
Based on the Court's factual findings, Centripetal has proven by a preponderance of the evidence that Cisco's Catalyst 9000 series switches, the Aggregation Services Router 1000 series routers and Integration Services Router 1000 and 4000 series routers in combination with Cisco's Stealthwatch and Identity 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



’856 Patent: Accused Combination of Cisco Products

Network Devices: Inline
(Network Traffic)

Management Devices:
After-the-Fact

Internet

Gateway
Router

Router/Switch

Router/Switch

Router/Switch

User 1

User 2

User 3

User 4

User 5

User 6

Server 1

Server 2

Netflow (with ETA)

Identity Services Engine (ISE)

Stealthwatch (Based on Netflow)

ETA

Encrypted Traffic Analytics

Cognitive Threat Analytics (CTA)

ETA

5

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:

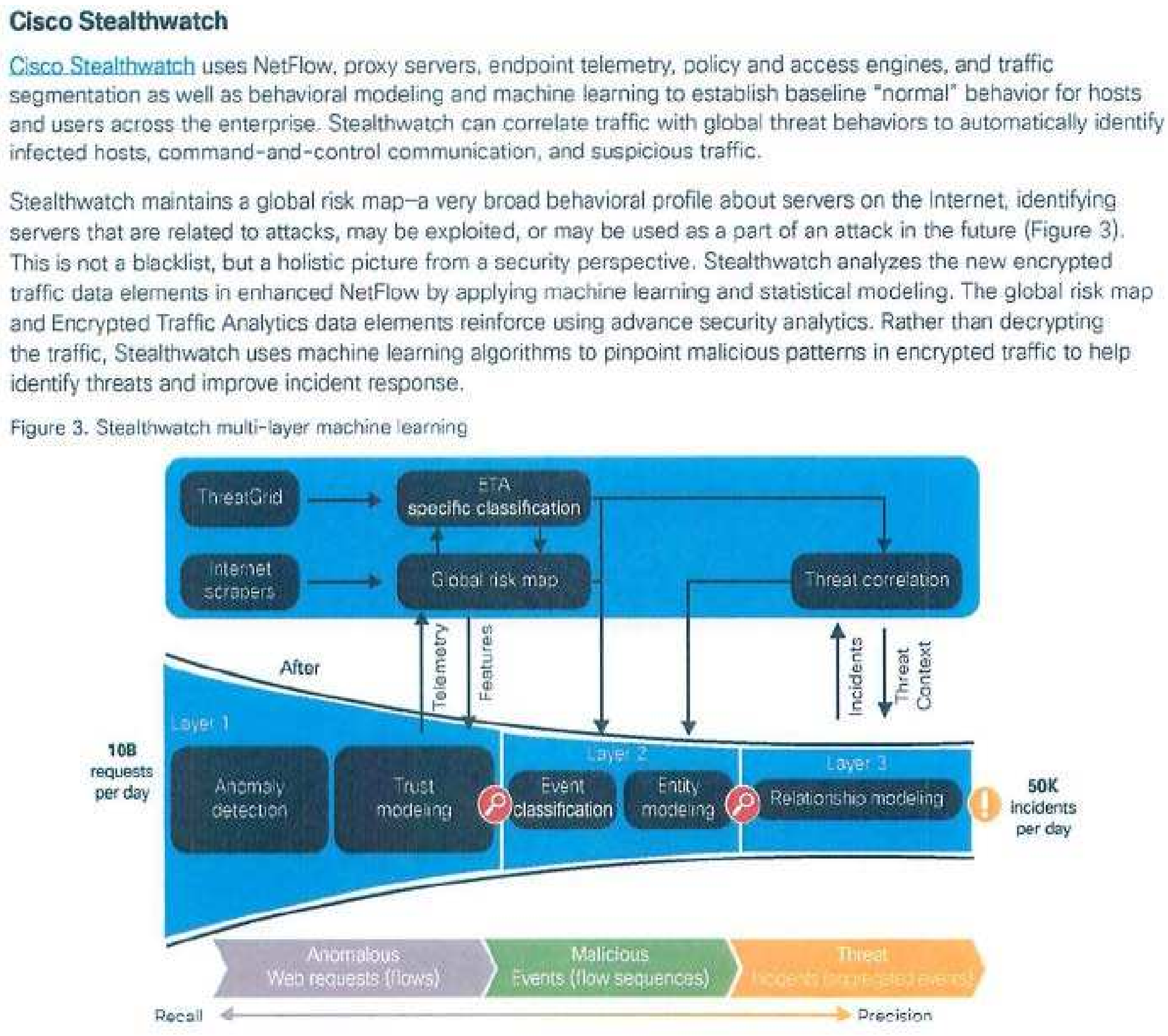
> Q. Do you see this is a Cisco Stealthwatch document? It looks like it's "At a Glance." Do you see that?
>
> A. Yes.
>
> Q. And there's a copyright date on the bottom there of 2017. It might be hard to see, but I'll pull it up. This is a 2017 document?
>
> A. Uh-huh.
>
> Q. Now, you talked about how 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.

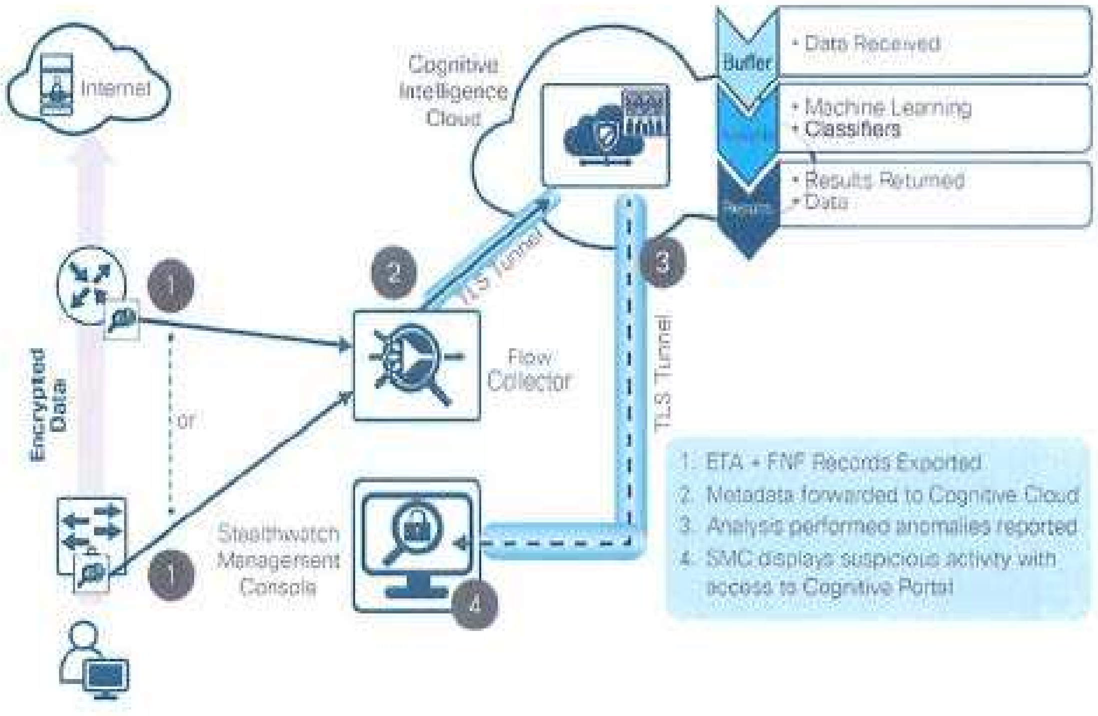
Figure 3. Stealthwatch multi-layer machine learning

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



1. ETA + FNF Records Exported
2. Metadata forwarded to Cognitive Cloud
3. Analysis performed anomalies reported
4. SMC displays suspicious activity with access to Cognitive Portal

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.

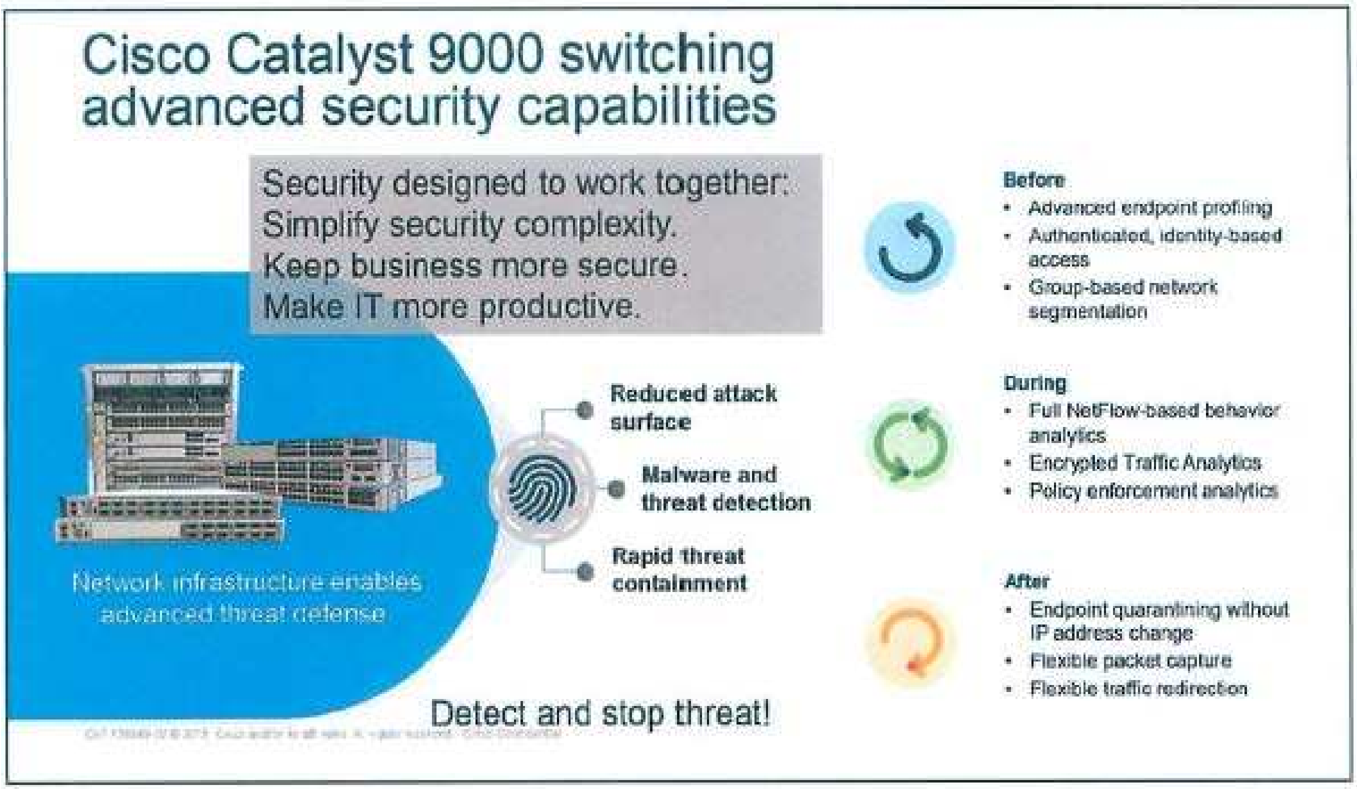
Q. I’m asking about your opinion now. When it says, “Detect and stop threats,” does that mean it’s detecting and stopping the threat before they get to the host?

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



Cisco Catalyst 9000 switching advanced security capabilities

Security designed to work together:
Simplify security complexity.
Keep business more secure.
Make IT more productive.

Network infrastructure enables advanced threat defense

Reduced attack surface

Malware and threat detection

Rapid threat containment

Before
- Advanced endpoint profiling
- Authenticated, identity-based access
- Group-based network segmentation

During
- Full NetFlow-based behavior analytics
- Encrypted Traffic Analytics
- Policy enforcement analytics

After
- Endpoint quarantining without IP address change
- Flexible packet capture
- Flexible traffic redirection

Detect and stop threat!

[illegible]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Q. Doctor, you just said that –

A. -- appears in multiple places.

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

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

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

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

Q. You just said that.

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

> . . .
>
> Q. Is there ever a disclosure of the proxy system in the specification that doesn't do any analysis at all; that just drops without first doing analysis?
>
> A. No.
>
> Q. And a null interface, does it do any analysis at all before it drops a packet?
>
> A. No, it does not.

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

> and one or more of log or drop the packets.
>
> Responsive to receiving the packets from proxy device **112,** host **106** may generate packets comprising data configured to establish the connection between proxy device **112** and host **106** (e.g., a TCP:ACK handshake message) and, at step **#14,** may communicate the packets to proxy device **112.** Rules **212** may be configured to cause rule gate **120** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on data stored in logs **214** (e.g., log data generated by packet-filtering system **200** in one or more of steps **#6, #7, #12,** or **#13),** and one or more of log or drop the packets.
>
> Responsive to receiving the packets from proxy device **114,** host **142** may generate packets comprising data conFigured to establish the connection between proxy device **114** and host **142** (e.g., a TCP:SYN-ACK handshake message) and, at step **#15,** may communicate the packets to proxy device **114.** Rules **212** may be configured to cause rule gate **128** to one or more of identify the packets, determine (e.g., based on one or more network addresses included in their network-layer headers) that the packets comprise data corresponding to the network-threat indicators, for example, by correlating the packets with one or more packets previously determined by packet-filtering system **200** to comprise data corresponding to the network-threat indicators based on

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

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:

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

> Q. But is it your testimony that Cognitive Threat Analytics was on Stealthwatch in 2013?
>
> A. It was my testimony that Stealthwatch was capable of doing behavioral analytics, enabling it to be able to detect encrypted threat -- encrypted threats -- or threats in encrypted traffic without requiring decryption. That was my testimony when I talked yesterday.
>
> Q. So all these testimony we, all this, the press releases, the documents about Encrypted Traffic Analytics, that's just all marketing puff; it was really not true, they could do it way before then, right?
>
> A. I didn't say it was marketing puff, I said that the capabilities that were added with ETA, Encrypted Traffic Analytics, were very valuable, and the value came from the additional machine learning insights and classification capabilities that were added at that time frame. It was, in fact, possible for them to do it before that, but they were able to do it better now because they've added these additional capabilities.
>
> Q. So when they said they solved the unsolvable problem, they had it solved years before, right?
>
> A. Well, we don't know what the unsolvable problem is from that quote. It could very well have been solving it more precisely or solving it more efficiently or solving it more thoroughly. So the insurmountable or unsolvable problem, I never saw an actual definition of that term, so I'm simply assuming that what they meant was they could do a much better job now that they added these enhancements, but that in no way, shape or form means they couldn't do a good job before.

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

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

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

> For example, for one or more packets logged by packet-Filtering system **200** (e.g., the packets comprising the DNS query or the packets comprising the reply to the DNS query), logs **214** may comprise one or more entries indicating one or more of network-layer information (e.g., information derived from one or more network-layer header fields of the packets, such as a protocol type, a destination network address, a source network address, a signature or authentication information (e.g., information from an Internet protocol security (IPsec) encapsulating security payload (ESP)),

> or the like), transport-layer information (e.g., a destination port, a source port, a checksum or similar data (e.g., error detection or correction values, such as those utilized by the transmission control protocol (TCP) or the user datagram protocol (UDP)), or the like), application-layer information (e.g., information derived from one or more application-Layer header fields of the packets, such as a domain name, a uniform resource locator (URL), a uniform resource identifier (URI), an extension, a method, state information, media-type information, a signature, a key, a timestamp, an application identifier, a session identifier, a flow identifier, sequence information, authentication information, or the like), other data in the packets (e.g., payload data), or one or more environmental variables (e.g., information associated with but not solely derived from the packets themselves, such as one or more arrival (or receipt) or departure (or transmission) times of the packets . . .

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

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

B. THE ‘176 PATENT

i. Findings of Fact Regarding Infringement

1. The ‘176 Patent has been informally known as the “Correlation” Patent.

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

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

4. Claim 11 is laid out below:

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

> provision a device located in the first network with the one or more rules configured to identify packets received from the host located in the first network.

5. Claim 11 is identical to Claim 21 in every respect except that Claim 21 is a computer readable media claim. Tr. 885:14-24. Claim 21 modifies the introductory preamble language of Claim 11 replacing "[a] system comprising: at least one processor; and a memory storing instructions that when executed by the at least one processor cause the system to:" with "[o]ne or more non-transitory computer-readable media comprising instructions that when executed by a computing system cause the computing system to:". JTX-3. For purposes of infringement, the parties have treated the two claims as identical.

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

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

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

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

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

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

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

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

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

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

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

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

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

18. Stealthwatch, in response to suspicious activity or threats, allows the Identity Services Engine or Stealthwatch Management Console to provision rules to proactively stop that threat. Tr. 1002:13-1003:21; PTX-1089 (showing the use of the Adaptive Network Control ("ANC") to implement rules). The ANC operates by applying new policies and changing individual user's authorization on the network according to rules and policies configured by the Identity Services Engine in response to correlated threats on the network. PTX-595 at 179; Tr. 1005:10-19. Both the Identity Services Engine and the Stealthwatch Management Console operate in this fashion. Tr. 1006:19-1007:5. PTX-989.

ii. Conclusions of Law Regarding Infringement

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

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

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

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

Dr. Cole pointed directly to PTX-1060, a Cisco technical document dated December of 2017, showing that the Catalyst switches have the ability to export NetFlow on ingress and egress.

Tr. 986:18-987:1; PTX-1060 at 023 (showing that the Catalyst 9400 switch is capable of supporting 384,000 NetFlow entries – 192,000 on ingress and 192,000 on egress). Dr. Almeroth, on cross-examination, even admitted that the accused switches and routers can be configured to export ingress and egress NetFlow.

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

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

Dr. Cole, in his infringement opinion on the "identify and generate" elements, relied on a similar claim scope as Dr. Almeroth to show that the claims required that one network device generate logs on a packets' ingress and egress out of the device. Moreover, Dr. Cole does not explicitly limit his construction of the asserted claims to the limitation of only ingress and egress out of one device. The Court **FINDS**, based on the testimony and technical documents, that the accused switches and routers do identify and generate logs on ingress and egress. However, a look at the specification of the ‘176 Patent informs the Court that this is not the only construction that would infringe the asserted claims. These claim elements would also be met if there was identification, generation and correlation of logs from two different network devices on either ingress or egress. Column 8 line 46 of the specification highlights that:

> At step **16,** packet correlator **128** may utilize log(s) **142** to correlate the packets transmitted by network device(s) **122** with the packets received by network device(s) **122.** For example, packet correlator **128** may compare data in entry **306** with data in entry **312** (e.g., network-layer information, transport-layer information, application-layer information, or environmental variable(s)) to correlate **Pl'** with **Pl** (e.g., by determining that a portion of the data in entry **306** corresponds with data in entry **312).** Similarly, packet correlator **128** may compare data in entry **308** with data in entry **314** to correlate **P2'** with **P2,** packet correlator **128** may compare data in entry **310** with data in entry **316** to correlate **P3'** with **P3,** packet correlator **128** may compare data in entry **318** with data in entry **324** to correlate **P4'** with **P4,** packet correlator **128** may compare data in entry **320** with data in entry **326** to correlate **PS'** with **PS,** and packet correlator **128** may compare data in entry **322** with data in entry **328** to correlate **P6'** with **P6.**

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

> Q. And then you said this had to be a single network device, correct?

> A. Not quite. It says a network device here, and then later it's the network device. So it's the same network device across the limitations.
>
> Q. But you do understand that in a patent, when it says A, it can mean one or more; is that correct?
>
> A. That's my understanding.
>
> Q. So this could be more than one network device, correct?
>
> A. It could be.

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

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

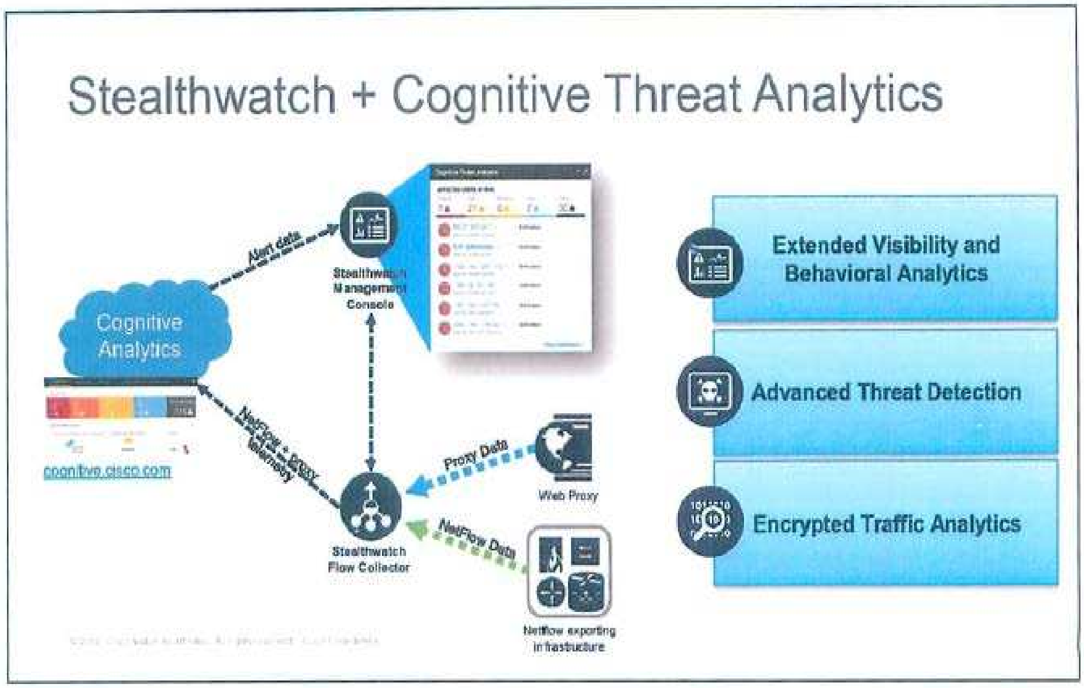
> Q. Can you explain what's going on here, Dr. Almeroth?
>
> A. Yes. What's being shown here, if you start in the bottom, it shows two different sources of information that ultimately get correlated. There's proxy data and there's NetFlow data. And when Dr. Cole testified, he represented that that NetFlow data included ingress and egress records from the same device, which was actually not the case, as the evidence and the correct operation of the devices show. And then from there, his analysis principally turned on the fact that these documents describe correlation. They absolutely use the word correlation, but it's not the correlation of the type required by the claims. And the example that's shown in this particular figure and what's described in the text below is that you're correlating NetFlow data, which is not the NetFlow data required by the claim for the reasons I've given, with other data. In this case, proxy data. And so even though these documents use the word correlate, what they're correlating is not the kind of correlation that's required by the claims.
>
> Q. Okay. And if we look, Mr. Simons, at the text below?

> BY MR. JAMESON:
>
> Q. And I don’t want to go through all of this, but is the same point made in the text below with respect to the comments you made, about the diagram?
>
> A. Yes. It’s absolutely the case that Stealthwatch correlates I think what we’ve referred to as threat intelligence with NetFlow records. But what it is not comparing, what it is not correlating is it’s not correlating the NetFlow records to themselves as required by the elements of the claims, because it tries to block or double count those NetFlow records. And so all of this evidence that Dr. Cole relied on that uses the word correlate, over and over again it describes correlation of threat intelligence with NetFlow data, which is not what the claim requires and also is not what the ‘176 patent is about.

Tr. 2256:3-2257:10.

PTX-1065

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



Stealthwatch + Cognitive Threat Analytics

Extended Visibility and Behavioral Analytics

Advanced Threat Detection

Encrypted Traffic Analytics

Cognitive Analytics
cognitive.cisco.com
Alert data
Stealthwatch Management Console
NetFlow + proxy telemetry
Proxy Data
Web Proxy
NetFlow Data
Stealthwatch Flow Collector
Netflow exporting infrastructure

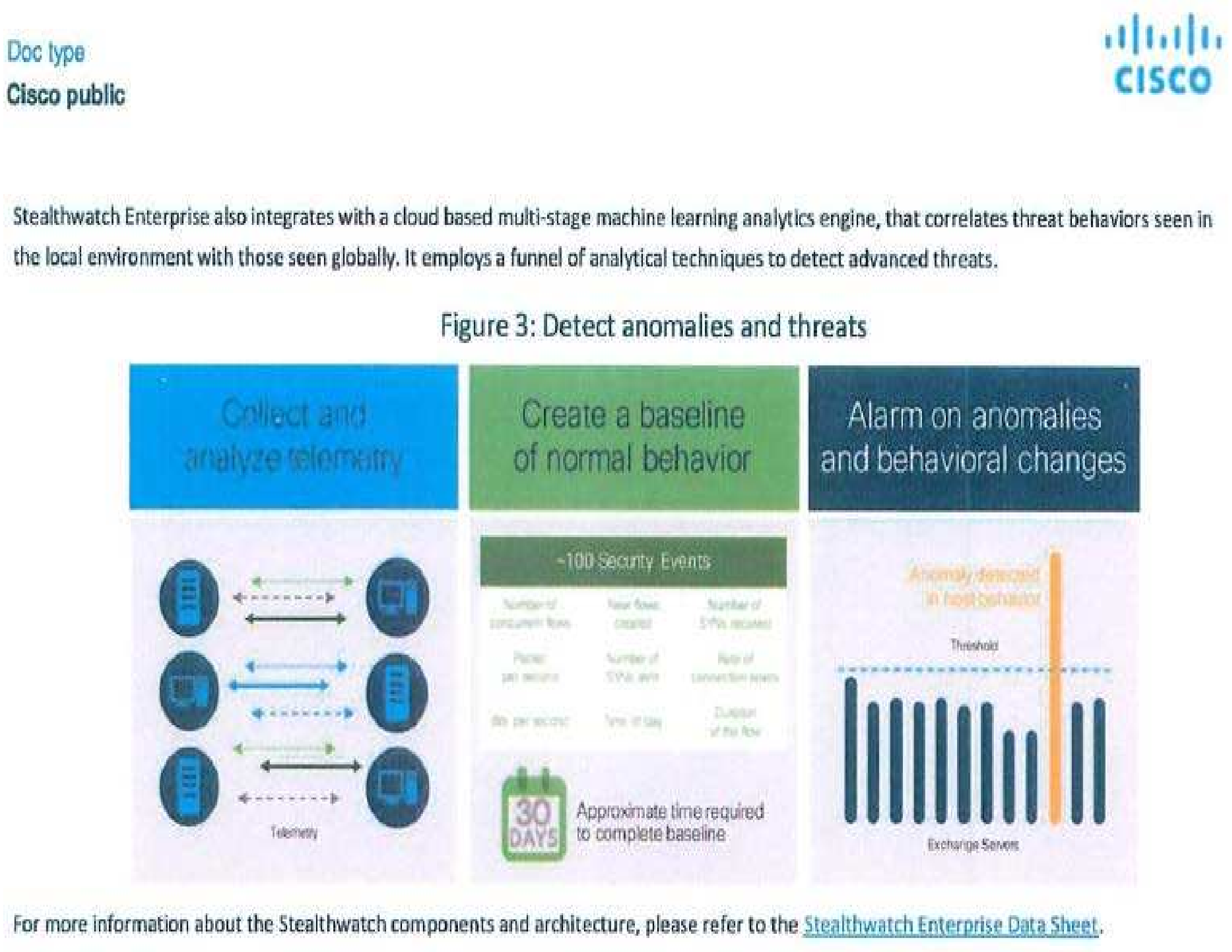
Stealthwatch integrates with Cognitive Analytics ("CA" - aka Cognitive Threat Analytics). This involves the addition of a new information panel on the SMC's WebUI, and enhances Stealthwatch further by leveraging CA's cloud based analytics engine, that correlates threat behaviors seen in the enterprise 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

Collect and analyze telemetry
Telemetry
Create a baseline of normal behavior
~100 Security Events
Number of concurrent flows
New flows created
Number of SYNs received
Packet per second
Number of SYNs sent
Rate of connection resets
Bits per second
Time of day
Duration of the flow
30 DAYS
Approximate time required to complete baseline
Alarm on anomalies and behavioral changes
Anomaly detected in host behavior
Threshold
Exchange Servers

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

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

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

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

Stealthwatch performs the exact type of correlation and provisioning of rules in response to correlations required by the '176 Patent.

iii. Findings of Fact Regarding Validity

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

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

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

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

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

24. Cisco Stealthwatch incorporated Cognitive Threat Analytics in Stealthwatch in 2017. Tr. 2342:6-7. In version 7.0.0 of Stealthwatch released in 2019, CTA was improved with

the ability to leverage threat detection from the analysis of WebFlow, produced by Syslogs, and NetFlow telemetry by correlating the data. PTX-1893 at 011.

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

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

iv. Conclusions of Law Regarding Validity

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

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

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

Tr. 3152:13-22. The technical documents, from 2014, confirm Dr. Jaegar's opinion highlighting that [t]he Stealthwatch system by Lancope is a leading solution for network visibility and security intelligence . . . ." PTX-343 at 001. Stealthwatch operates by providing "in-depth visibility and security context needed to thwart evolving threats . . . [and] quickly zooms in on any unusual behavior, immediately sending an alarm to the SMC . . . ." PTX-343.

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

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

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

Tr. 3154:6-25; see DTX-463 at 014. The post-2017 documents illustrate that the generation of rules responsive to correlations was an added functionality with the addition of CTA into Stealthwatch. The release notes for Version 7.0.0 of Stealthwatch, PTX-1893, contain a section titled "What's New" which shows the additions made to Stealthwatch in this version. PTX-1893 at 011. In this section, the technical document indicates that "CTA can now leverage detections from the analysis of WebFlow telemetry to improve the efficacy of analyzing NetFlow telemetry from Stealthwatch. This is accomplished by the system through correlation of both telemetry types." PTX-1893 at 011 (a technical document from 2019 showing this type of correlation is an enhancement to the Cognitive engine). Cisco identifies that this technology increases the number of both confirmed and detected threats in the network. Id. Cisco's presentation on the incorporation of CTA into Stealthwatch shows that the technology "uses the Proxy ingestion feature to consume Syslog information sent from proxy sources . . . [and] then correlate the received syslog and relates it to the flows collected from network devices before and after the proxy . . . ." PTX-1065 at 005 (November 2017 document). This same document highlights that "[b]ringing CTA and Stealthwatch detection together gives us unique ability to combine our local and global detection capabilities." Id. In response to the local correlations of WebFlow and NetFlow, new Stealthwatch can provision Adaptative Network Control policies based on the identification of behavioral anomalies. See PTX-569 at 272; PTX-595 at 179 (a technical document from 2019 showing how "ANC policies have replaced the previous quarantine and unquarantine feature"). Accordingly, Cisco has failed to present clear and convincing evidence that the "correlate" and "responsive to" functionality was in the Cisco prior art system. Therefore, the prior art does not render the asserted claims anticipated or obvious.

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

Dr. Jaegar opined that a person skilled in the art would be able to look at column 8, lines 46 through 63 of the '176 Patent specification and determine that the invention "utilize[s] logs to correlate packets transmitted by one or more network devices with packets received by one or more network devices." Tr. 3155:16-18; see JTX-3 at col. 8 ln. 46-63. Additionally, for the "responsive to" element, Dr. Jaegar points to column 12, line 55 through column 13, line 13. This section of the specification clearly shows that the invention identifies hosts associated with malicious entities and communicates messages identifying that host. JTX-3 at col. 12 ln. 55 – col. 13 ln. 13. Further, the specification notes that this process occurs in response to the correlation of data, as described in column 8, lines 46 through 63 of the specification. Tr. 3156:9-3157:14. Based on these sections of the specification, the Court finds that a person skilled in the art would have been in possession of the invention at issue.

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

C. THE ‘193 PATENT

i. Findings of Fact Regarding Infringement

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

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

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

4. Claim 18 is laid out below:

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

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

JTX-4.

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

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

7. Centripetal's expert, Dr. Mitzenmacher, defined the asserted claims of the '193 Patent as being related to the process of forwarding and dropping packets related to preventing exfiltrations. Tr. 465:18-21. Additionally, Dr. Mitzenmacher opined that the '193 Patent applies to the prevention of many different types of data exfiltration. Tr. 467:14-468:17.

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

companies that certain departments have access to confidential materials, while for others that access is restricted.

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

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

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

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

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

14. In their operation, the processors work within the accused Cisco switches and routers to receive and transmit packets across a network. PTX-1276 at 216 (2011 Cisco

document); Tr. 488:1-489:3. During the transmission of packets, the operating system ("IOS XE"), working in conjunction with UADP ASICs, apply a variety of different rules to packets to determine if the packet should be permitted or dropped. PTX-1276 at 215-16.[5]

15. Access Control Lists ("ACL") are often applied to packets on ingress into the device and egress out of the device. PTX-1276 at 215-16. To simplify the process of applying rules, Cisco's IOS XE utilizes a specific method where labels are applied to packets based on their source or destination. These labels are known as Secure Group Tag / Scalable Group Tag ("SGT").[6] Tr. 494:12-24; see PTX-1276 at 211.

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

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

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

[5] The technical document for the switch and router operating system shows that the switches and routers support the application of multiple different ACL rule sets including: Port ACL ("PACL"); Vlan ACL ("VACL"); Router ACL ("RACL"); Client Group ACL ("CGACL"); Security Group ACL or Role Based ACL ("SGACL or RBACL"). PTX-1276 at 215.

[6] Cisco's non-infringement expert, Dr. Crovella, confirmed that Secure Group Tag and Scalable Group Tag are in fact the same. Different names are being used at different times because of a marketing change. Tr. 2420:17.

example of a GACL that blocks or permits packets specifically based on SGTs. Tr. 2389:1-3. PTX-1276 at 215-16; see Tr. 2423:9-15.

19. On a packet's ingress into the device, the switch and/or router applies an input SGACL based upon the SGT associated with the source of where the packet was transmitted from. Tr. 2389:1-8; see PTX-1288 at 012 (showing input GACL applied based on ingress client); see also PTX-1276 at 216; PTX-1390 at 86 (2019 document).

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

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

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

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

24. The switch and/or router determines whether the packet should be permitted or blocked based on the SGT assigned to that particular source. Tr. 535:10-17; PTX-1280 at 21; see PTX-1262 at 999. This process is completed by the switch and/or router by applying operators,

such as permit or deny, to incoming and exiting packets based upon their assigned SGT. Tr. 531:18-21; PTX-1280 at 021. 22.

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

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

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

ii. Conclusions of Law Regarding Infringement

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

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

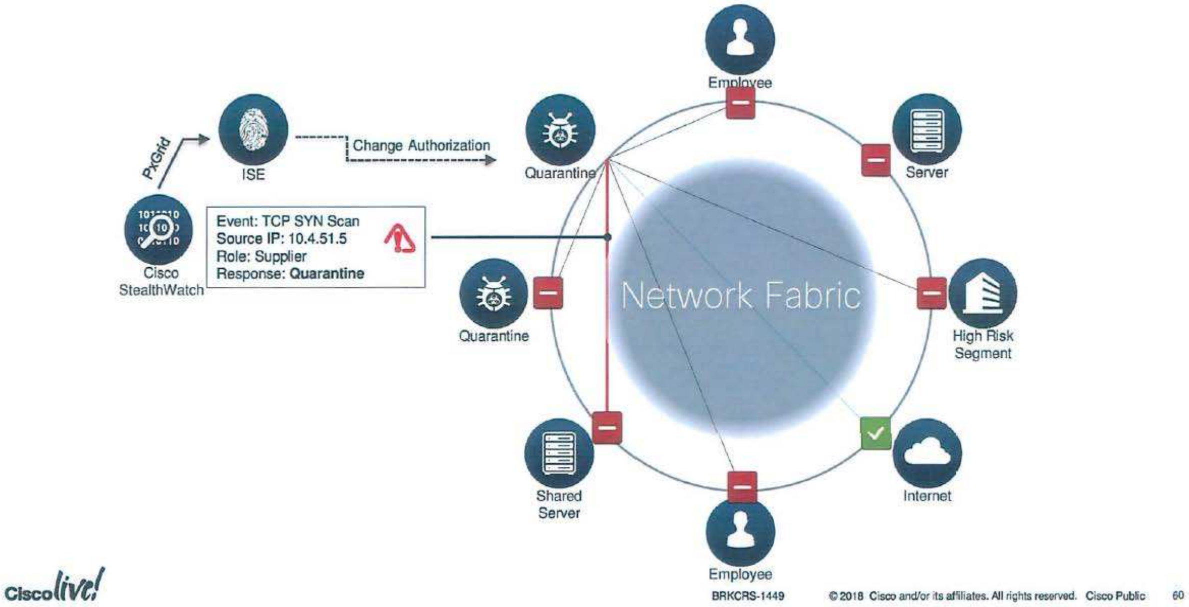
Tr. 2349:18-24. Dr. Crovella advanced two theories in his non-infringement opinion. First, that the function which is referred to as a "quarantine" blocks all traffic from a source computer and does not block a "particular data transfer," as required by the language in the claim. Second, he averred that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

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

The Cisco packet-filtering system operates by using the Identity Services Engine to assign certain endpoint devices "roles" that determine what type of packets may be sent and/or received by that specific endpoint computer. PTX-1326. Therefore, the Identity Services Engine has the ability to monitor levels of vulnerabilities based on the packets that are being transmitted by switches and routers in the network, and to adjust the permissions based on real-time network operations. As a general example, the Cisco system operates by limiting a computer located in a first network from accessing sensitive data in a protected network, while simultaneously allowing unsensitive data to be accessed. In this manner, packets from the computer in the first network may be allowed to access unprotected resources on the larger internet, but would be restricted from transmitting packets containing secure information. This is shown by Cisco's technical demonstration, PTX-563:

PTX-563

Cisco Technical Presentation on Rapid Threat Containment from 2018



Event: TCP SYN Scan
Source IP: 10.4.51.5
Role: Supplier
Response: **Quarantine**

BRKCRS-1449 ©2018 Cisco and/or its affiliates. All rights reserved. Cisco Public 60

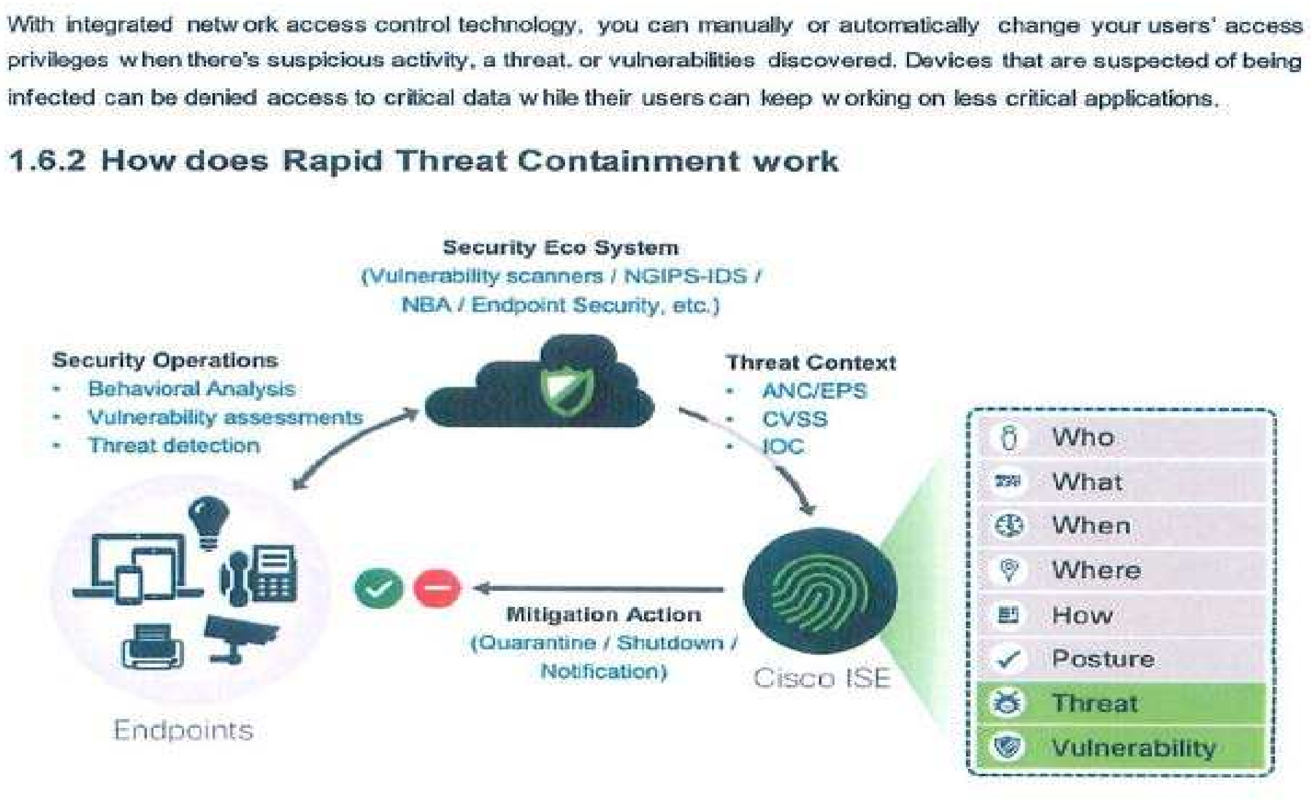
The accused switches and routers are the specific network devices used to institute this packet filtering system. In their operation, the accused products receive different portions of packets from a first computing network. PTX-1276 at 216. Upon entry into an accused device, each packet is assigned a Scalable/Security Group Tag ("SGT"). The SGT that is attached to each packet is based on the role and/or privileges that is assigned to that specific endpoint computer. Therefore, SGTs, at their most basic level, are assigned to packets based on where the packet is being transmitted from and/or the destination of the transmitted packet. In this manner, the 5-tuple information in the header of the packet, such as the source of the packet's origin and/or the destination to which it is being transmitted, is the operative data being used to determine the packet's SGT. This assignment of SGT to packets as they enter the switch or router is the first step in the operation of the quarantine process.

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

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

PTX-1326

Cisco Identity Services Engine Technical Ordering Guide from August 2019



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

1.6.2 How does Rapid Threat Containment work

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

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

> Q. . . .So we have multiple steps. First, the SGT tag is checked to see if it's present, right?
>
> A. That's right.
>
> Q. Then, if the SGT tag is present and it says, "quarantine," then a quarantine policy is applied, correct?
>
> A. That's right.
>
> Q. If the quarantine policy is applied, you check the destination, and if the destination is a protected resource in which it says, do not allow this packet to go there, it will prevent the data transfer from going to that destination, correct?
>
> A. That is, in fact, the quarantine policy. In other words, there's not two steps there. A quarantine policy is, in fact, checking the destination.
>
> Q. Okay. And if it says, block the packet, it will be prevented from the data transfer going there, right?
>
> A. That's right.
>
> Q. If it's not in there, and if there is a – it's able to go through to a permitted network or permitted resource, then the packet would be allowed to go through by the switch or the router. Isn't that right?
>
> A. That's right.

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

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

iii. Findings of Fact Regarding Validity

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

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

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

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

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

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

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

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

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

iv. Conclusions of Law Regarding Validity

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

Turning to obviousness, the prior art references advanced by Cisco do not show that a skilled artisan would have been able to combine the teachings in these technical documents and produce the patented invention. Cisco argues that the '193 Patent must be invalid because the previous system, that includes older versions of similar switches, routers, ISE and Stealthwatch, has had some method of quarantining and blocking functionality. However, the Court rejects Cisco's contention that these products have operated in the same manner and functionality just because the system had preexisting baseline functionality and consistent nomenclature. The prior art makes no mention of the infringing packet filtering process. Dr. Crovella relies on PTX-588, DTX-711, DTX-311, and PTX-1193 to contend that a person skilled in the art would have combined these references in order to teach the functionality outlined in the claims of the '193 Patent. A review of the asserted prior art shows no mention of the Identity Services Engine packet filtering system that utilizes switches and routers to attach Secure Group Tags, apply operators and then allow certain packets to be transmitted while other packets are subsequently blocked.[7] It is that system which contains the functionality taught by the claims of the '193 Patent. Cisco's own technical documents that were used to show infringing functionality are all from post-2013. See PTX-1288 at 012; PTX-1276 at 216; PTX-1280 at 21; PTX-1294; PTX-1326. Not one selection of asserted prior art shows the infringing switch and router functionality was embedded in any of the Cisco products before the '193 Patent's priority date. These conclusions allow the Court to infer that the infringing functionality was added as a result of newly designed versions of the accused products that occurred after March of 2013.

[7] The Patent and Trademark Office denied Inter Partes Review on the '193 Patent citing similar concerns regarding the operator limitation. Tr. 3013:20-3014:9; DTX-370.

Accordingly, the Court **FINDS** that Cisco has failed to present clear and convincing evidence that the prior art would allow a person skilled in the art to combine the prior art to produce a packet filtering system with the functionality taught by Claims 18 and 19 of the '193 Patent.

D. THE '806 PATENT

i. Findings of Fact Regarding Infringement

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

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

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

4. Claim 9 is laid out below:

> A system comprising:
>
> a plurality of processors; and
>
> a memory comprising instructions that when executed by
>
>> at least one processor of the plurality of processors cause the system to: receive a first rule set and a second rule set; preprocess the first rule set and the second rule set to optimize performance of the system for processing packets in accordance with at least one of the first rule set or the second rule set;
>>
>> configure at least two processors of the plurality of processors to process packets in accordance with the first rule set; after preprocessing the first rule set and the second rule set and configuring the at least two processors to process packets in accordance with the first rule set, receive a plurality of packets;
>>
>> process, in accordance with the first rule set, a portion of the plurality of packets; signal, each processor of the at least two processors, to process packets in accordance with the second rule set; and

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

JTX-2.

5. Claim 9 is identical to Claim 17 in every respect except that Claim 17 is a computer readable media claim. JTX-2. Claim 17 substitutes the introductory language of Claim 9, replacing "[a] system comprising: a plurality of processors; and a memory comprising instructions that when executed by at least one processor of the plurality of processors cause the system to:" with "[o]ne or more non-transitory computer-readable media comprising instructions that when executed by a computing system cause the computing system to:" JTX-2. For purposes of infringement, the parties treated Claims 9 and 17 the same.

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

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

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

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

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

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

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

13. Similar to the DNA Center, Firepower Management Center's Threat Intelligence Director receives rule sets from various sources and preprocesses the rule sets to create optimized policies which are distributed to firewalls. Tr. 655:10-656:20, 673:21-675:5, 680:11-681:10; see Tr. 2537:3-7, 2539:11-17.

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

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

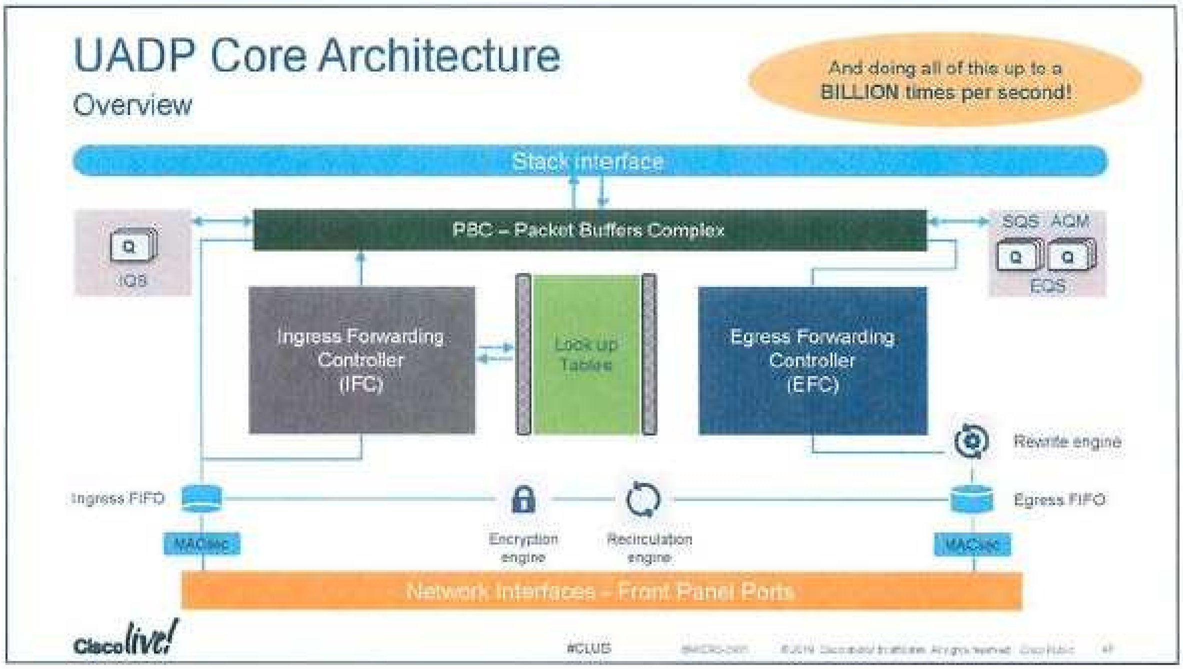
16. Mr. Peter Jones[8], a distinguished Cisco engineer responsible for building the switching, routing and enterprise network, explained in detail how the accused products process packets and swap rules. Tr. 2543:9-11, 2561:25-2562:1.

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

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

DTX-562

Cisco Technical Presentation on UADP Core Architecture in 2019



UADP Core Architecture

Overview

And doing all of this up to a BILLION times per second!

Stack interface
PBC – Packet Buffers Complex
Q
IQS
SQS AQM
Q
Q
EQS
Ingress Forwarding Controller (IFC)
Look up Tables
Egress Forwarding Controller (EFC)
Rewrite engine
Ingress FIFO
Encryption engine
Recirculation engine
Egress FIFO
MACsec
MACsec
Network Interfaces – Front Panel Ports

Cisco live!

#CLUS ©2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

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

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

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

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

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

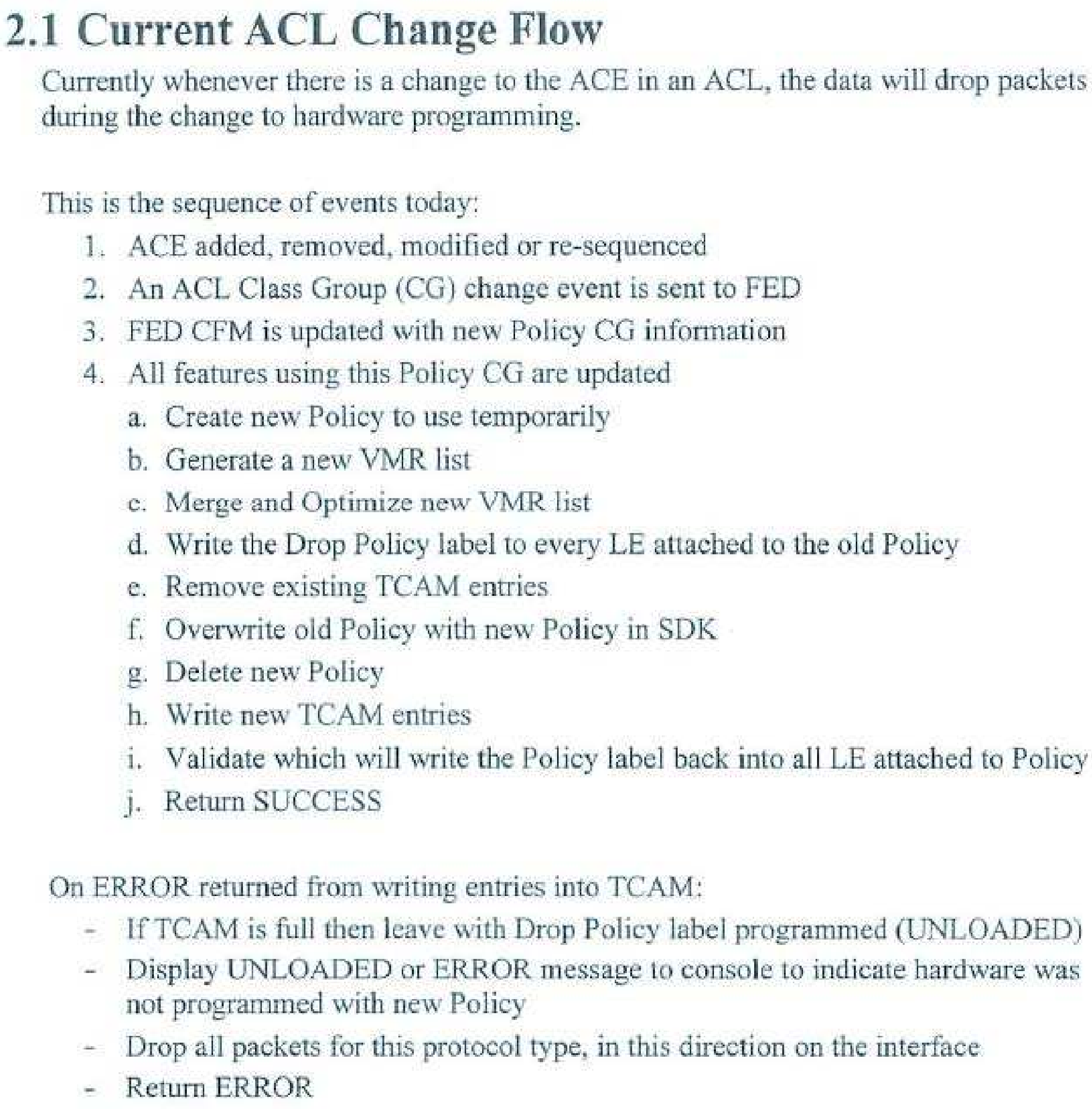
24. If the packet is transmitted, it goes through an Egress FIFO, an Egress MACSec, and then out a port on the device. Tr. 2569:1-4.

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

26. The accused products contain a new FED 2.0 Hitless ACL update. Tr. 3550:18-25. Mr. Jones testified that before the 2.0 Atomic Hitless feature was added to the accused products, performing rule swaps often resulted in a discard of a number of packets. Tr. 2552:20-23. Therefore, the new 2.0 Hitless version updated the products so that new ACLs can be placed into the device and be activated without displacing packet processing. Tr. 2551:2-5; PTX-1303 at 073. Compare the older ACL Process:

PTX-1195 at 003

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



2.1 Current ACL Change Flow

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

This is the sequence of events today:

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

On ERROR returned from writing entries into TCAM:

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

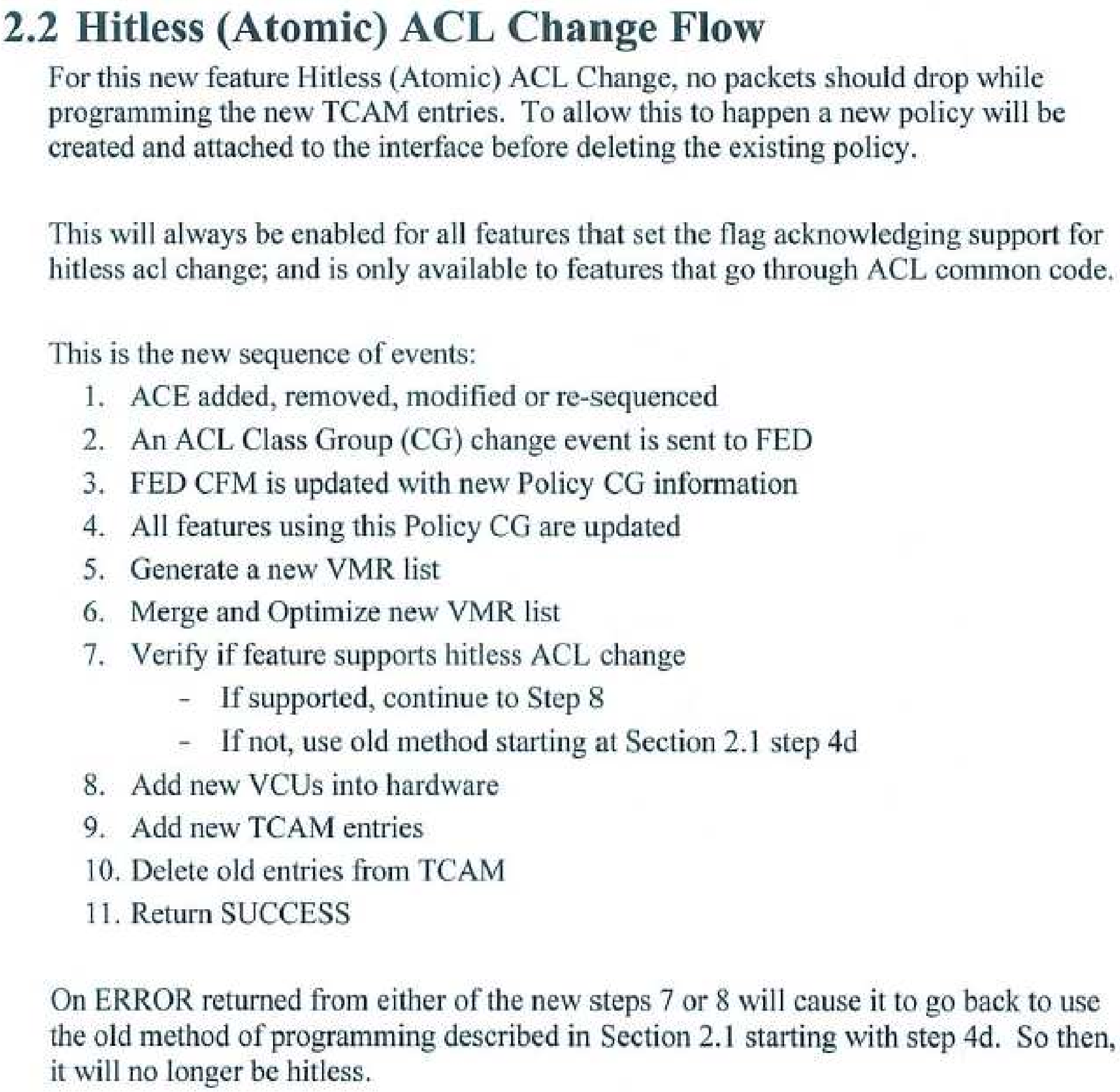
PTX-1195 at 003.

[9] The 2.1 in front of Current ACL Change Flow within Exhibit PTX-1195 does not refer to a version number, but this is a numerical heading within the document.

With the new 2.0 Hitless ACL Update:

PTX-1195 at 003

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



2.2 Hitless (Atomic) ACL Change Flow

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

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

This is the new sequence of events:

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

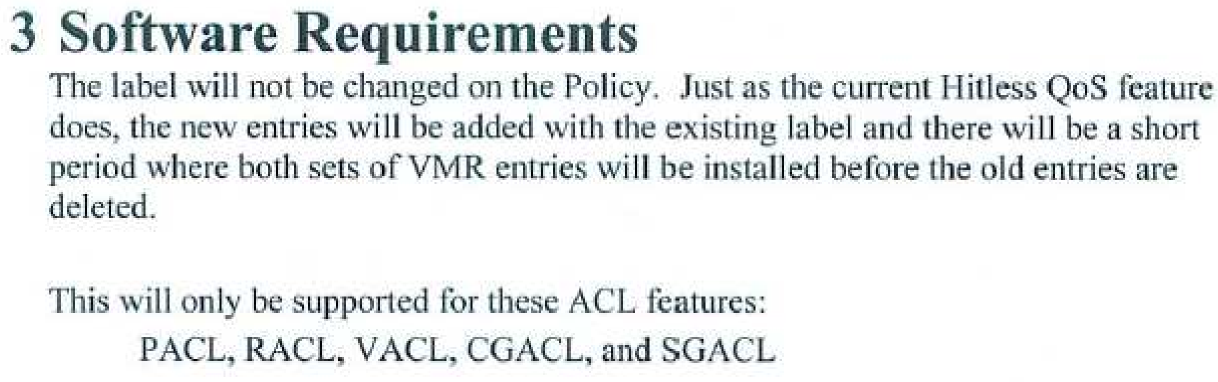
On ERROR returned from either of the new steps 7 or 8 will cause it to go back to use the old method of programming described in Section 2.1 starting with step 4d. So then, it will no longer be hitless.

[10] The 2.2 in front of Hitless (Atomic) ACL Change Flow within Exhibit PTX-1195 does not refer to a version number, but this is a numerical heading within the document.

In the same Cisco software technical specification, the requirements of the software dictate that "there will be a short period where both sets of VMR ("Virtual Media Recorder") rule entries will be installed before the old entries are deleted." See PTX-1195 at 003. Here is a copy of those Software Requirements:

PTX-1195 at 003

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



3 Software Requirements

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

This will only be supported for these ACL features:
PACL, RACL, VACL, CGACL, and SGACL

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

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

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

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

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

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

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

ii. Conclusions of Law Regarding Infringement

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

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

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

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

Turning to the first theory, Cisco employee, Peter Jones, testified that in the operation of packet processing, Cisco’s switches and routers will store packets in a part of the UADP ASIC processor known as the Packet Buffer Complex (“PBC”). The PBC operates as a holding spot for the data in the payload of the packet while the header information is forwarded to another part of the processor for the application of rules. This operation in the Cisco switches and routers is designed to maximize the speed and efficiency of packet processing through software. Tr. 622:16-18. Dr. Mitzenmacher highlights that computer scientists use the term buffer and cache interchangeably as a word denoting the use of memory to hold packets for a short period of time. Tr. 628:7-25. Dr. Mitzenmacher referenced that a buffer is a “memory that holds something . . . [o]ften for future use.” In reference to the Court’s question about defining a cache, Dr. Mitzenmacher gave a similar definition of cache in the following exchange:

> Q. What’s a cache?

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

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

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

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

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

With regard to both of these theories, Cisco argues that because this process is the normal processing functionality of the accused products, Cisco cannot in theory infringe the claims of the '806 Patent. The Court disagrees with Cisco's argument. It is true that the Cisco products do cache and cease processing packets during their normal packet processing operation. However, Cisco has implemented the rule swap functionality outlined in the ‘806 Patent to greatly improve the security functionality of its products without dropping packets. The devices, in response to an initial signal, operate to stop processing packets during an idle period, and during the idle period, unprocessed packets are cached within the Packet Buffer Complex. This process is the exact functionality as described by the cease and cache elements of the ‘806 Patent.

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

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

iii. Findings of Fact Regarding Validity

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

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

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

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

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

39. The older version of Hitless operated by completely stopping the system, eliminating ACLs, merging and replacing those ACLs, then reactivating the processing system. Tr. 3034:23-3035:2. This system resulted in overlap between the old rules and the new rules within the TCAM. This caused packets to be dropped because old ACLs were being applied alongside the new ACLs, causing conflict and disruption. Tr. 3035:3-15, 3040:2-12; see PTX-1195 at 003.

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

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

iv. Conclusions of Law Regarding Validity

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

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

Second, the Cisco Prime technical documents do not contain any functionality of the asserted claims for the ‘806 Patent. The only document presented by Dr. Reddy identifies that Prime provided monitoring and troubleshooting support for Cisco’s switches. There is no clear and convincing evidence from Dr. Reddy’s testimony, or this one document offered by Cisco, that Prime served a similar function as Cisco’s Digital Network Architecture. Accordingly, there is not clear and convincing evidence for the Court to find that Prime caused the Cisco devices to receive first and second rule sets as required by the claims. Therefore, both asserted prior art references fail to teach the invention as described by Claims 9 and 17 of the ‘806 Patent. Accordingly, the Court **FINDS** that Cisco has not proven by clear and convincing evidence that the ‘806 Patent was anticipated or obvious.

E. THE ‘205 PATENT

i. Findings of Fact Regarding Infringement

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

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

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

4. Claim 63 is laid out below:

> A system, comprising:
>
> a security policy management server; and one or more packet security gateways associated with the
>
> > security policy management server, wherein each packet security gateway of the one or more packet security gateways comprises computer hardware and logic configure to cause the packet security gateway to:
> >
> > receive, from the security policy management server, a dynamic security policy comprising at least one rule specifying a set of network addresses and a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI);
> >
> > receive packets associated with a network protected by the packet security gateway;
> >
> > perform, on the packets, on a packet by packet basis, at least one packet transformation function of multiple packet transformation functions specified by the dynamic security policy;
> >
> > encapsulate at least one packet of the packets that falls within the set of network addresses and matches the SIP URI with a header containing a network address that is different from a destination network address specified by the at least one packet and that corresponds to a network device configured to copy information contained in the at least one packet and to forward the at least one packet to the destination network address; and
> >
> > route, based on the header, the at least one packet to the network address that is different from the destination network address.

JTX-1.

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

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

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

8. Dr. Moore specifically credits the technology in the '205 Patent as a system for operationalizing threat intelligence into policies of rules that are uploaded into network devices to block dynamic threats. Tr. 321:5-9, 320:16-25.

9. Cisco's expert on the '205 Patent, Dr. Kevin Jeffay, challenges Dr. Moore's characterization by noting that the specific claims at issue have no relation to the blocking of malicious traffic. Instead, Dr. Jeffay characterizes the claims at issue as dealing with the

encapsulation, copying and forwarding of voice traffic over the internet. Tr. 2727:11-19, 2732:2-19. More generally, Dr. Jeffay describes the claims at issue as enabling law enforcement to potentially wiretap internet calls. Tr. 2732:13-16.

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

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

12. Cisco's Digital Network Architecture Center serves as the "foundational controller . . . at the heart of Cisco's intent-based network . . . [and] provides a single dashboard for every fundamental management task." PTX-1294. Accordingly, both the DNA Center and Cisco's Firepower Management Center manage and update security policies that are employed by the accused devices. Tr. 728:21-730:9; 736:3-13; PTX-1294 at 15.

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

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

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

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

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

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

19. However, Dr. Mitzenmacher presented no technical documents that confirm that the accused firewalls have specific rules that contain both a network address and a SIP URI. Tr.

2756:18-2757:2. Furthermore, no Cisco technical document confirms that the accused switches and routers have any rules that contain both a network address and a SIP URI. Tr. 2756:18-2757:2.

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

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

ii. Conclusions of Law Regarding Infringement

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

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

> Q. And turning to slide 5, how many disputes -- on the infringement issue, how many major disputes do you intend to focus on today?
>
> A. Well, in my report I documented several disputes, but in the interest of time, we’re going to focus on two here, and these are the two that I think are the easiest to see. And the first one is really sort of a black/white issue; that Centripetal’s theory of infringement focuses on the blocking of packets. And blocking has really been the key to most of this case; that the accused products block packets. But the ‘205 [P]atent is not about blocking packets, it’s about precisely the opposite. It’s about doing things that we’ll come to see are called encapsulation and forwarding, but the point here is that we want the packets to go through to their destination. We’re going to see that the patent is really about enabling law enforcement to potentially wiretap phone calls, so we want the package to go through. And so the ‘205 claims are really about the opposite of what we’ve heard in this case; they’re about letting packets make it to their destination.

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

FIG. 6 from the '205 Patent

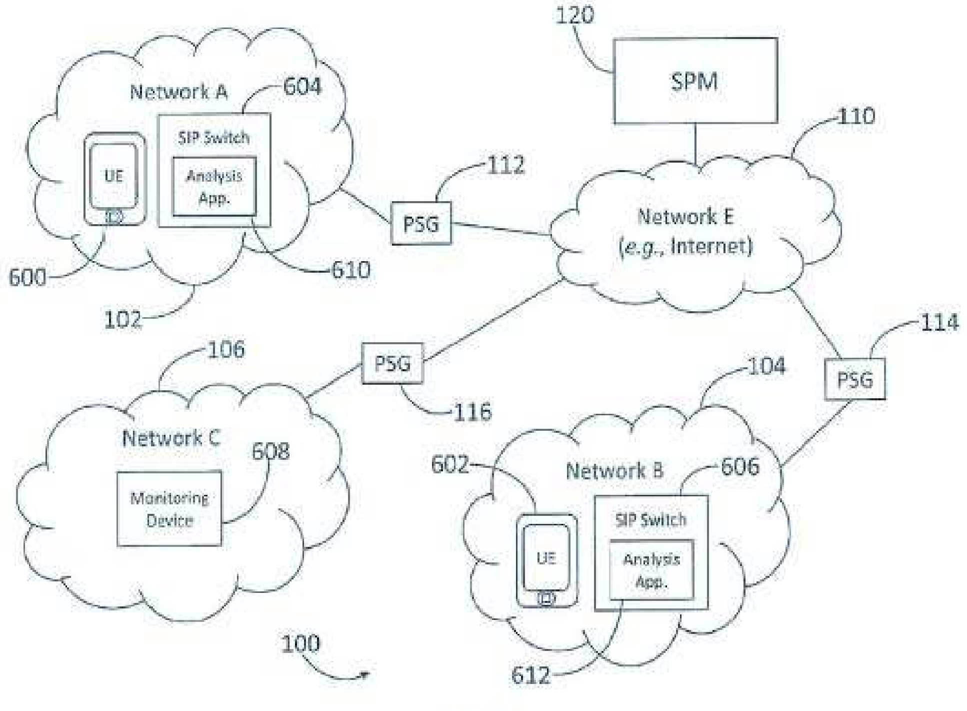


FIG. 6

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

A. Sure. So this is the world -- this a version of the world in which the claimed invention would operate. So let's focus first on network A, which is in the upper left-hand corner. And in network A there is a device, UE 600. Now, UE in the patent stands for User Equipment, but what I'd like the Court to think of it -- think of it as a phone. And you can kind of see it's drawn kind of like an iPhone. So it's a phone. And what's going to happen here is that this user in network A is going to make a phone call, a Voice over IP phone call, to a user in network B. So let's highlight network B, which is on the lower right. And we can see that also there's a UE 602, User Equipment, just basically another phone, that's in network B. So a user in network A makes a call to a user in network B, and what the patent is about is using an SPM 120 -- SPM is going to stand for Security Policy Management server; this is the entity that creates security policies. The SPM is going to send a policy that contains a rule to a packet security gateway 112. So the packet security gateway is the thing that actually looks at the packets. Now the rule -- the policy contains a rule, and the rule that's going to be sent to the packet security gateway is going to contain information to allow the packet security gateway to identify the packets corresponding to this Voice over IP phone call. And when it identifies the right kind of packets, what it's going to do is a little unusual. It's going to let the packets go through. It's not going to block the packets, but it's not going to send the packets

> to their intended destination, which is network B. It's going to send them to network C, which is shown on the lower left. And in network C you can see that there's a monitoring device, and what's going to happen is the packets are going to be routed from the packet security gateway, to network C, to this monitoring device. The monitoring device is then going to copy some information from the packets. It's going to keep that copied information, because, in theory, that's what law enforcement wants to see, but then we need the call to go through, so it's -- the network device 608 is going to unencapsulate the packet, get the original packet, and send it on its way back to network B.

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

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

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

Tr. 726:21-727:5. Dr. Mitzenmacher, in his infringement opinion, specifically focused on the use of threat intelligence being used to block malicious traffic in the network. In his testimony, Dr. Mitzenmacher confirms that the accused products can perform the encapsulation of packets. Tr. 756:8-758:21, 760:5-764:16. This is confirmed by the Cisco technical documents. PTX-1262 at 994; PTX-524 at 309; PTX-1229 at 69; PTX-1293 at 062. But the encapsulation of packets described by Dr. Mitzenmacher and the technical documents is not all that is required by the asserted claims. This element of the claim reads:

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

JTX-1 (emphasis added). Dr. Mitzenmacher presented no testimony or technical documents that confirmed that the accused products are "configured to" or have the ability to copy information, as outlined by the asserted claims. Tr. 2749:24-2750:4; see PTX-1262 at 994; PTX-524 at 309; PTX-1229 at 69; PTX-1293 at 062. Additionally, there is no evidence in the documents presented by Dr. Mitzenmacher that the encapsulated packets are those that "fall within the set of network addresses and matches the SIP URI with a header containing a network address . . . ." See PTX-1262 at 994; PTX-524 at 309; PTX-1229 at 69; PTX-1293 at 062. For these reasons, Centripetal has failed to prove by a preponderance of the evidence that the accused products embody each and every limitation of the patented claim. See V-Formation, Inc. v. Benetton Group SpA, 401 F.3d 1307, 1312 (Fed. Cir. 2005).

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

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

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

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

For both of these reasons, the Court **FINDS** that Centripetal has not met its burden to prove by a preponderance of the evidence that the accused products infringe Claims 63 and 77 of the ‘205 Patent literally or under the doctrine of equivalents.

iii. Validity

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

VI. FINDINGS OF FACT AND CONCLUSIONS OF LAW REGARDING DAMAGES

A. PAST DAMAGES

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

“Upon finding for the claimant the court shall award the claimant damages adequate to compensate for the infringement, but in no event less than a reasonable royalty for the use made of the invention by the infringer, together with interest and costs as fixed by the court.” Lucent Techs., Inc. v. Gateway, Inc., 580 F.3d 1301, 1324 (Fed. Cir. 2009) (quoting 35 U.S.C. § 284). In awarding damages under the governing statute, 35 U.S.C. §284, “a reasonable royalty is the minimum permissible measure of damages.” Deere & Co. v. Int’l Harvester Co., 710 F.2d 1551, 1558 n.9 (Fed. Cir. 1983). The Supreme Court has framed reasonable royalty damages achieved through litigation as a court’s duty to assess “the difference between [the patentee’s] pecuniary condition after the infringement, and what his condition would have been if the infringement had not occurred.” Yale Lock Mfg. Co. v. Sargent, 117 U.S. 536, 552 (1886). The burden of proving damages as a result of infringement falls on the patentee. Lucent Techs., Inc., 580 F.3d at 1324. The Federal Circuit has determined two acceptable “alternative categories of infringement compensation.” Id. The first category is based on a patentee’s lost profits. Id. To recover lost profits, “a patent owner must prove a causal relation between the infringement and its loss of profits.” Shockley v. Arcan, Inc., 248 F.3d 1349, 1362 (Fed. Cir. 2001). The patentee is required to “show a reasonable probability that ‘but for’ the infringing activity, the patentee would have made the infringer's sales." Id. The four-factor test for utilizing the lost profit model is laid out in Panduit Corp. v. Stahlin Bros. Fibre Works, Inc., 575 F.2d 1152, 1156 (6th Cir. 1978).[11] The lost profits method is not at issue in this case since Centripetal has not presented any evidence of a causal relationship between suspected lost profits and Cisco's sales of the infringing technology. The second category, which the Court adopts in this case, is based on the "the reasonable royalty . . . [the patentee] would have received through arms-length bargaining." Lucent Techs., Inc., 580 F.3d at 1324.

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

[11] "To obtain as damages the profits on sales he would have made absent the infringement, i.e., the sales made by the infringer, a patent owner must prove: (1) demand for the patented product, (2) absence of acceptable non-infringing substitutes, (3) his manufacturing and marketing capability to exploit the demand, and (4) the amount of the profit he would have made." Panduit Corp. v. Stahlin Bros. Fibre Works, Inc., 575 F.2d 1152, 1156 (6th Cir. 1978).

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

> (1) Any royalties received by the licensor for the licensing of the patent-in-suit, proving or tending to prove an established royalty.
>
> (2) The rates paid by licensee to license other patents comparable to the infringed patents.
>
> (3) The nature and scope of the license, as exclusive or non-exclusive, or as restricted or non-restricted in terms of its territory or with respect to whom the manufactured product may be sold.
>
> (4) The licensor's established policy and marketing program to maintain its right to exclude others from using the patented invention by not licensing others to use the invention, or by granting licenses under special conditions designed to preserve that exclusivity.
>
> (5) The commercial relationship between the licensor and the licensee, such as whether or not they are competitors in the same territory in the same line of business.
>
> (6) The effect of selling the patented product in promoting other sales of the licensee; the existing value of the invention to the licensor as a generator of sales of its non-patented items; and the extent of such collateral sales.
>
> (7) The duration of the infringed patents and the term of the license.
>
> (8) The established profitability of the product made under the infringed patents; its commercial success; and its popularity.

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

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

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

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

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

(14) The opinion testimony of qualified experts.

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

See Georgia-Pacific Corp. v. U.S. Plywood Corp., 318 F. Supp. 1116, 1120 (S.D.N.Y. 1970), modified sub nom. Georgia-Pacific Corp. v. U.S. Plywood-Champion Papers, Inc., 446

F.2d 295 (2d Cir. 1971). The Court will examine each of the relevant Georgia-Pacific factors that guide its determination of a proper reasonable royalty rate.[12]

Beginning with Georgia-Pacific factors one and two, the only comparable license of the patents-in-suit is the Confidential Binding Term Sheet agreed to in a previous case tried by this Court – Centripetal Networks, Inc., v. Keysight Technologies, Inc. and Ixia, Case No. 2:17-cv-383 (E.D Va.). The Court is limited to this license granted by Centripetal as the only comparable license, as neither party presented any comparable licenses for similar patented inventions or similar infringing products. Tr. 1498:2-10. Although Cisco licensed Stealthwatch for a period of years from Lancope before Cisco acquired the company in 2013, neither Centripetal nor Cisco presented evidence of this or any other license in which Cisco was involved, and the Keysight agreement is the only licensing agreement in which Centripetal has been involved. The Keysight agreement was entered into by Centripetal and Keysight/Ixia during trial to settle the patent claims at issue in that litigation. The patents asserted in the Keysight case are comparable to those in this litigation. Both the ‘205 Patent and the ‘856 Patent were asserted in the Keysight case. The ‘176 Patent, the ‘193 Patent and the ‘806 Patent are in the same patent family and covered similar fields of technology as the patents that were asserted in Keysight. Therefore, the Keysight agreement covers sufficiently similar technology to serve as a comparable technology license in this case.

The Keysight agreement granted Keysight/Ixia a three year “worldwide, non-transferable, irrevocable, non-terminable, non-exclusive license” to Centripetal’s worldwide patent portfolio in exchange for a $25 million-dollar lump-sum payment and a 10% royalty of directly competing products and a 5% royalty on non-competing products. See PTX-1125; Tr. 1487:5-1491:2. The

[12] Certain factors may be relevant regarding other factors and, therefore, the Court will often address two factors at a time. Additionally, the Court may incorporate relevant information from one factor into its analysis of another factor. For example, the Court often uses factor fourteen (i.e., the opinion testimony of qualified experts) to support its analysis of other factors.

Court agrees with Centripetal's damages expert, Lance Gunderson, that the 10% running royalty instituted in the Keysight agreement is sufficiently comparable to provide a starting point for determining a reasonable royalty based on a hypothetical negotiation. See Tr. 1486:1-24. This 10% royalty in Keysight was instituted for products that directly compete with Centripetal's RuleGate gateway product. Cisco's damages expert, Dr. Becker, contends that the Keysight license is not directly comparable because Keysight was a direct competitor in the threat intelligence gateway market, and Cisco is not. Although Centripetal does not market and sell switches and routers, Cisco has embedded the patented software functionality from the Centripetal patents into the infringing switches and routers that provides the same functionality as the RuleGate product. Centripetal does market and sell firewalls. Accordingly, the Court **FINDS** that Centripetal and Cisco are direct competitors with respect to the infringing software, as well as firewalls. This incorporation of infringing functionality persuades the Court that the infringing Cisco products are more comparable to the 10% royalty on competing products than the 5% royalty for non-competing products in Keysight. Accordingly, the 10% royalty on directly competing products in the Keysight case provides a comparable baseline license from which the Court can determine a reasonable royalty in this case.

The Court recognizes that the Keysight license was obtained in the coercive environment of litigation and not the result of open negotiation. See LaserDynamics, Inc. v. Quanta Computer, Inc., 694 F.3d 51, 77 (Fed. Cir. 2012) (highlighting that "[t]he notion that license fees that are tainted by the coercive environment of patent litigation are unsuitable to prove a reasonable royalty is a logical extension of Georgia–Pacific . . ."). Generally, these types of settlement agreements "should not be considered evidence of an established royalty." Id. (citing Hanson v. Alpine Valley Ski Area, Inc., 718 F.2d 1075, 1078-79 (Fed. Cir.1983). However, the Federal Circuit has recently permitted reliance on such agreements "under certain limited circumstances." Id. In the case of ResQNet.com, Inc. v. Lansa, Inc., the Federal Circuit "permitted consideration of the settlement license on remand" because the "settlement license to the patents-in-suit in a running royalty form was 'the most reliable license in [the] record.'" Id. (discussing and quoting language from ResQNet); see ResQNet.com, Inc. v. Lansa, Inc., 594 F.3d 860, 872 (Fed. Cir. 2010).

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

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

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

Georgia-Pacific factor five has minimal impact on the royalty figure. This factor asks the Court to inquire into the commercial relationship of the parties at the hypothetical negotiation. The Court notes that Centripetal has presented evidence that Cisco's incorporation of the patented functionality into its products would result in substantial lost profits from the competing RuleGate product. Generally, this fact would weigh in favor of increasing the royalty as Centripetal, in the hypothetical negotiation, would consider the substantial loss that may be attributed to licensing the patented technology.[13] From Cisco's perspective, it would gain substantially from licensing the asserted patents as it could incorporate advanced security functionality into its products, thus improving the profitability of its networking products. See Carnegie Mellon Univ. v. Marvell Tech. Group, Ltd., 807 F.3d 1283, 1304 (Fed. Cir. 2015) (noting "a basic premise of the hypothetical negotiation is the opportunity for making substantial profits if the two sides [are] willing to join forces by arriving at a license of the technology").

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

However, the Court must consider that Cisco has incorporated the infringing technology into hardware products, such as switches and routers, that Centripetal does not produce or sell. Additionally, even if Centripetal sold versions of the infringing products, it would be difficult to meet the customer demand of these products that Cisco, as the largest provider of network infrastructure and services in the world, would be able to accomplish. See Tr. 1449:17-1451:2. Therefore, Centripetal's bargaining position in the hypothetical negotiation would be limited by the incentive of Centripetal to license the patented software technology to Cisco in order to take advantage of Cisco's substantial market share. See Tr. 1449:17-1451:2. The Court **FINDS** that all these considerations generally neutralize each other and warrant no variance to the royalty number.

Georgia-Pacific factor six does call for some upward influence. Cisco has incorporated the patented software functionality into a variety of its routers, switches and firewalls in its network security system. Therefore, the effect of the sales and the profits therefrom are promoted by Centripetal's software. The upward influence is somewhat offset by the apportionment analysis of Centripetal's experts. There was no evidence presented that the infringing products contributed to increased sales of any of Cisco's other non-infringing products.

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

Georgia-Pacific factor eight deals with the profitability of products made under the patent and the commercial success of those products. One of Centripetal's damages experts, Mr. Gunderson, presented detailed evidence of Cisco's profitability of the infringing products. The Federal Circuit has expressly noted that "anticipated incremental profits under the hypothesized conditions are conceptually central to constraining the royalty negotiation . . . [and] . . . [e]vidence of the infringer's actual profits generally is admissible as probative of his anticipated profits." Aqua Shield v. Inter Pool Cover Team, 774 F.3d 766, 772 (Fed. Cir. 2014); see Sinclair Refining Co. v. Jenkins Petroleum Process Co., 289 U.S. 689, 698 (1933) (noting "[e]xperience is then available to correct uncertain prophecy"). In the context of the hypothetical negotiation, "the core economic question is what the infringer, in a hypothetical pre-infringement negotiation under hypothetical conditions, would have anticipated the profit-making potential of use of the patented technology to be, compared to using non-infringing alternatives." Aqua Shield, 774 F.3d at 770-71 (emphasis in original) (noting that "[i]f a potential user of the patented technology would expect to earn X profits in the future without using the patented technology, and X + Y profits by using the patented technology, it would seem, as a prima facie matter, economically irrational to pay more than Y as a royalty—paying more would produce a loss compared to forgoing use of the patented technology").

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

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

Stealthwatch	81.4%
Identity Service Engine	91.5%
Digital Network Architecture	-1.9%

An examination of this data establishes that Cisco was reaping considerable profit margins on products that incorporate the infringing functionality. See Tr. 1495:16-1496:19. Moreover, a Cisco article, published on November 7, 2019, expresses the very high profitability of the new Catalyst 9000 series switches as compared to older models:

PTX-515

Cisco Article Published on Website from November 7, 2019

Cisco Blogs / Networking / Cisco Catalyst 9000 – The best keeps getting better.

November 7, 2019 5 Comments

Networking

Cisco Catalyst 9000 – The best keeps getting better.

While we recognize that we cannot predict the future, we understand that we can plan for the unknown by building flexibility into both our hardware and software. This was the design philosophy behind the Cisco Catalyst 9000 family and likely why it has been so successful. With the modular Cisco IOS XE and the programable UADP ASIC as its foundation, combined with the automation and assurance of Cisco DNA Center and SD-Access, Catalyst 9000 switches open the door for IT to shift focus from reactive analysis to predictive analytics, from using hands-on CLI-based, box-by-box interaction to network-wide automation and assurance.

Cisco More Than Doubles Its Catalyst 9000 Customer Base
Cisco winner in campus switching market

Venerable Cisco Catalyst 6000 switches ousted by new Catalyst 9600

Cisco CEO trumpets Catalyst 9K advances,
Robbins has said the Catalyst 9000 is the company's fastest-selling product ever.

Cisco's Catalyst 9K Switch
Propels the Company's Finances

Cisco drove Q1 campus switching market growth: report
Cisco's Catalyst 9000 switches helped fuel campus switching market growth in the first quarter of this year, according to a report by Dell'Oro Group.

There have been many highlights and headlines about the Catalyst 9000 product family and its meteoric rise since it was launched in June 2017:

- fastest ramping product in Cisco's history
- fastest to exceed $1B quarterly run rate
- over a million units shipped to tens of thousands of customers in every geography, vertical, and market segment.
- recognized by CRN as Product of the Year for 2017 and 2018 (when does 2019 awards come out?)

This is not by accident. And the positive headlines are not likely to stop. Key innovations like multigigabit technology, 90W UPOE+, Encrypted Traffic Analytics, and onboard app hosting help our

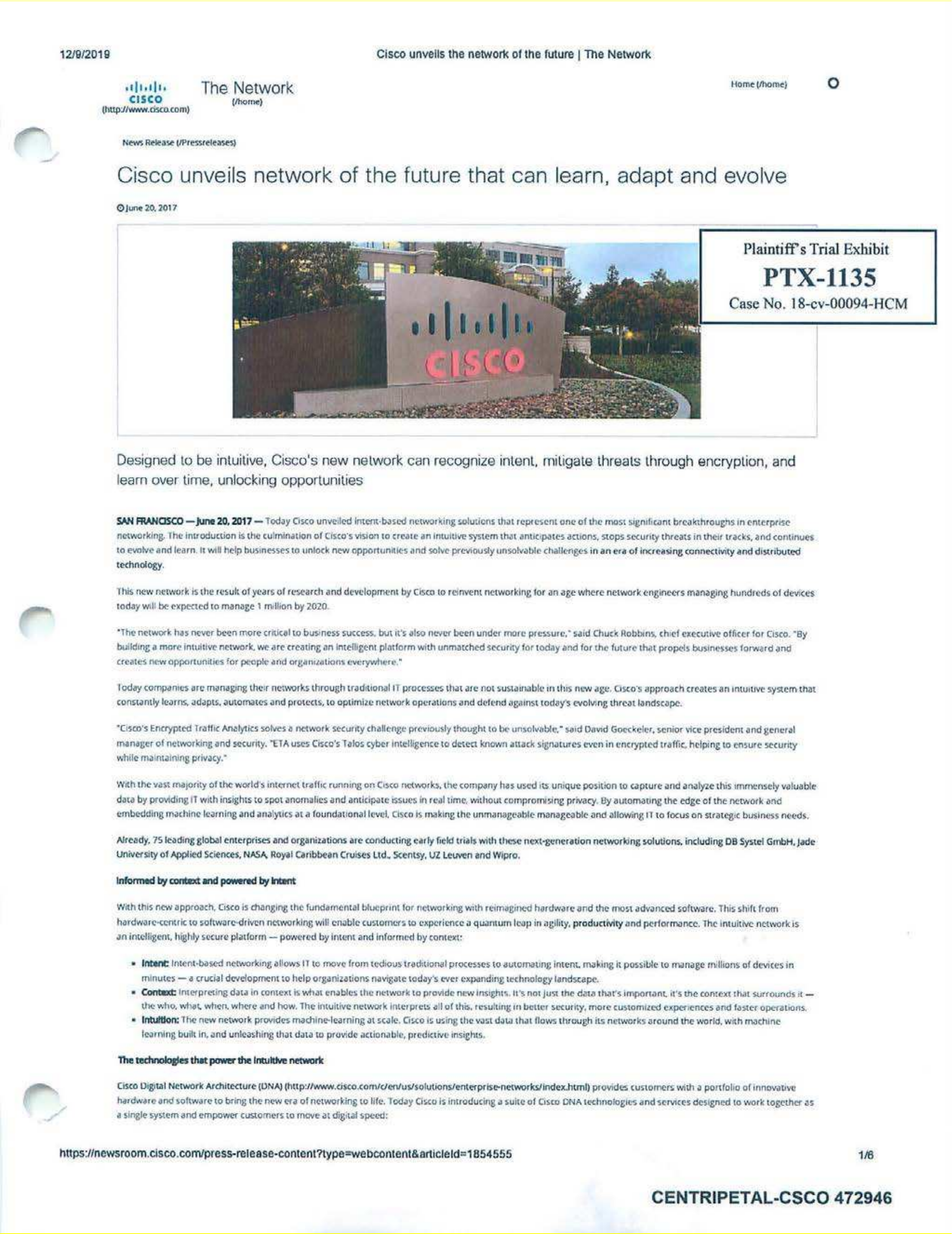
PTX-515. Additionally, Cisco presented no evidence to contest these profit margins or the cost of any non-infringing alternative that would achieve the same functionality as incorporated in the patented technology. See Tr. 1602:8-16 (Mr. Malackowski noting that "Cisco did not suggest or offer any alternatives or even what it would cost to come up with alternatives"). Therefore, at a hypothetical negotiation, Centripetal would hold a considerable advantage due to the lack of non-infringing alternatives and the ability for Cisco to make large profits from the use of the technology. This evidence of high profits and lack of alternatives supports a higher reasonable royalty rate. See Lucent Techs., Inc., 580 F.3d at 1335 (noting that approximately 70–80% profit margin of the products at issue supports a higher versus a lower reasonable royalty).

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

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

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

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



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:

Cisco repeatedly described the addition of Encrypted Traffic Analytics ("ETA") as solving the "network security challenge previously thought to be unsolvable." PTX-1135 (David Goeckeler, Cisco's Senior Vice President of Sales, representing Cisco's new technology). Additionally, these representations made by as dominant a company as Cisco would have a devastating impact upon Centripetal as the original inventor of the technology. Therefore, under factor nine, Cisco's technical and marketing documents, as well as previous business acquisitions, support a higher royalty rate, as the addition of the infringing technology greatly improved Cisco's sales and the profitability of its new infringing versions of the products over older models. See Deere & Co. v. Int'l. Harvester Co., 710 F.2d 1551, 1558 (Fed. Cir. 1983) (supporting a higher royalty rate in light of descriptions that the infringing product had a "bright future").

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

Product	Increase in Revenues %	Increase in Revenues $ (in millions)
Switches	40.9%	$3,973.4
Routers	13.2%	501.5
Adaptative Security / Firepower	29.5%	550.4
Stealthwatch	36.0%	70.2
Firepower Management Center	3.5%	1.7
Identity Services Engine	52.0%	225.3
Digital Network Architecture[14]	100%	252.9
Total Increase		5,575.4

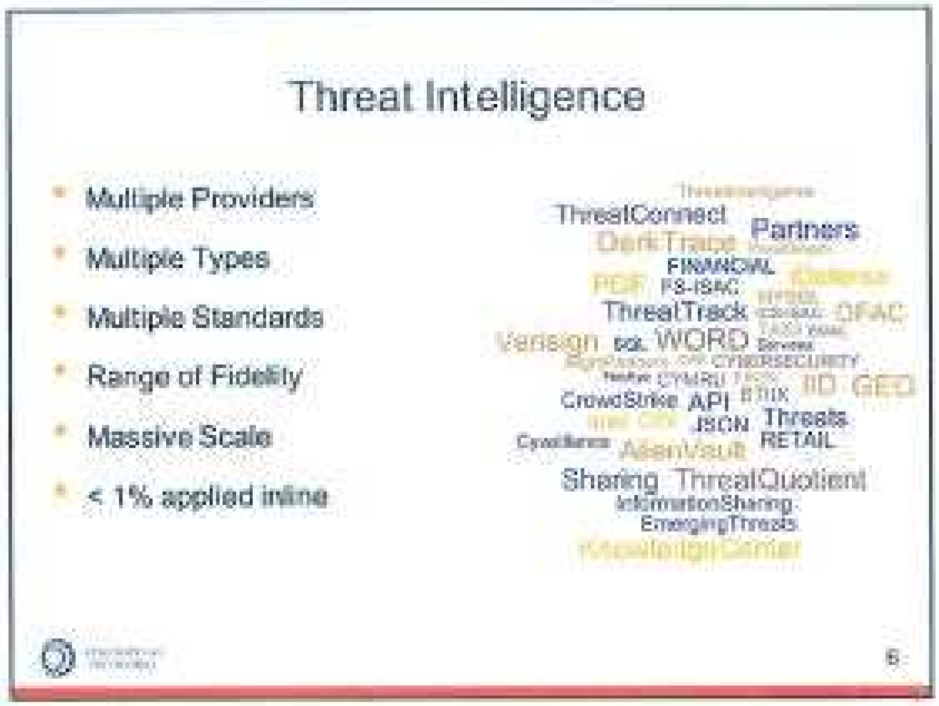
Tr. 3464:8-14 (Mr. Malackowski describing the increases in revenues for the infringing products). This data supports a finding that the addition of the infringing software functionality to older models of the infringing products support the economic reality of the enormous increase in revenues. There is no evidence that these increases in sales revenue were attributed to improvements in the hardware itself. The infringing software significantly improved existing hardware by not only adding security functionality, but speed and scalability as well. See Tr.

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

2621:5-10, 2634:14-18 (showing how ASICs process packets at high speeds and how Centripetal's rule swap technology aids that process and is disclosed in the '806 Patent); see PTX-547.

PTX-547

Centripetal Demonstrative Presentation Presented to Cisco About Patented Technology

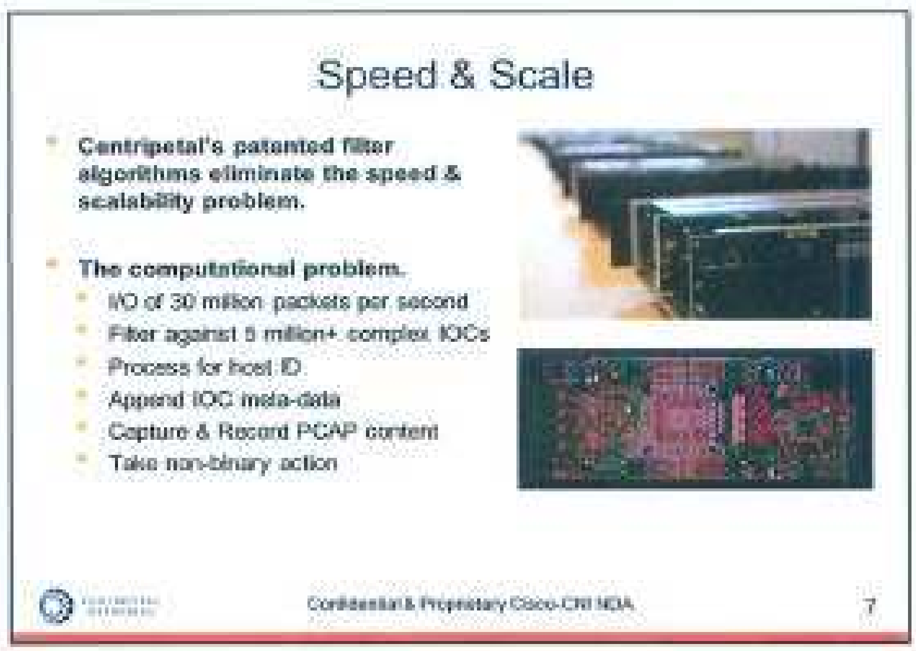


Threat Intelligence

- Multiple Providers
- Multiple Types
- Multiple Standards
- Range of Fidelity
- Massive Scale
- < 1% applied inline

ThreatConnect
Partners
DarkTrace
FINANCIAL
PDF
FS-ISAC
ThreatTrack
OFAC
Verisign
SQL
WORD
CYBERSECURITY
CYMRU
IID
GEO
CrowdStrike
API
STIX
JSON
Threats
RETAIL
AlienVault
Sharing
ThreatQuotient
InformationSharing
EmergingThreats
KnowledgeCenter

6



Speed & Scale

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

Confidential & Proprietary Cisco-CNI NDA

7

Viewing both Cisco's technical documents, marketing representations and the sales data, the Court **FINDS** that the patented functionality added very significant value to the older technology. Therefore, this factor supports a substantially increased royalty figure.

Accordingly, based upon its analysis of the Georgia-Pacific factors, the Court determines that the weight of the factors as a whole strongly favors Centripetal. As a result, the Court **FINDS** that the Keysight royalty rate of **10%** of the apportioned value of its infringed technology is a reasonable royalty rate to compensate Centripetal for Cisco's past infringement. This figure is supported both by the comparable factors in the Keysight license and 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).

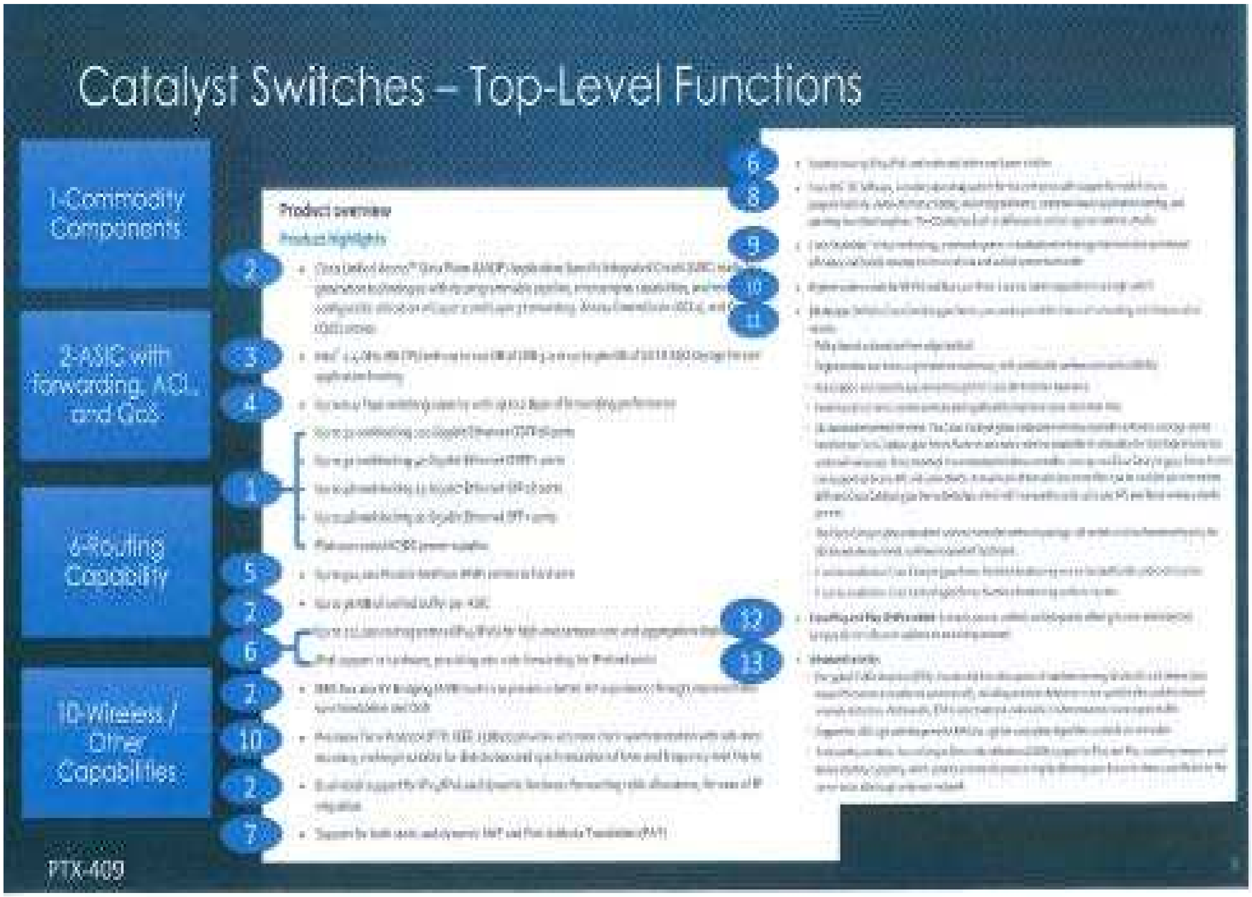
This flexibility in methodology is centered on "the difficulty that patentees may face in assigning value to a feature that may not have ever been individually sold." Virnetx, Inc. v. Cisco Sys., Inc., 767 F.3d 1308, 1328 (Fed. Cir. 2014). Therefore, the integral inquiry is "whether the data utilized 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



Catalyst Switches – Top-Level Functions

1-Commodity Components
2-ASIC with forwarding, ACL, and QoS
6-Routing Capability
10-Wireless / Other Capabilities
Product overview
Product highlights
Support for both static and dynamic NAT and Port Address Translation (PAT)
2
3
4
1
5
2
6
2
10
2
7
6
8
9
10
11
12
13
PTX-409

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

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

Tr. 1338:9-15. This is exactly the type of materials relied upon by Dr. Layne-Farrar in the Finjan case, where the Federal Circuit determined that the jury was entitled to rely upon such information as substantial evidence to support a damages award. Accordingly, the Court **FINDS** that Dr.

Striegel's analysis is admissible as "reliable and tangible" evidence of apportionment of the infringing products. See Ericsson, Inc., 773 F.3d at 1226 (highlighting that a court or jury must "apportion the defendant's profits and the patentee's damages between the patented feature and the unpatented features" using 'reliable and tangible' evidence"). Accordingly, the Court **FINDS** Dr. Striegel's apportionment evidence and analysis to be a reliable method to determine a royalty base.

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

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

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

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

After Dr. Striegel’s technical apportionment, Centripetal’s expert on patent evaluation, Mr. Gunderson, applied these apportionment percentages to total sales revenues from the infringing products since the date of first infringement, June 20, 2017, through December 31, 2019. At the final damages hearing, these figures were updated through Cisco’s sales data ending on June 20, 2020 and totaled $21,467,079,878.00 billion. See Doc. 488, Ex. 7 (updated version produced at damages hearing). The Court adopts Centripetal’s exhibits outlining the sales revenues of Cisco. Cisco presented a patent by patent damages breakdown instead of a full picture of the sales of infringing products. The Court rejected the proposed patent by patent calculation of damages by Cisco’s expert Dr. Becker, in favor of the appointment method utilized by Centripetal’s experts approved by the Federal Circuit in Finjan, Inc. v. Blue Coat Sys., Inc., 879 F.3d 1299, 1310 (Fed. Cir. 2018).

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

Here is a reproduction of the apportionment percentages applied to Cisco's gross revenues from June 20, 2017 through June 20, 2020, by using Centripetal's update to PTX-1629, Doc. 488, Ex. 7:

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

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

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

ii. Findings of Fact Regarding Willful Infringement and Enhanced Damages

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

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

3. As a result of these meetings, on January 26, 2016, Centripetal and Cisco entered into a nondisclosure agreement ("NDA"), requiring Cisco to keep Centripetal's confidential, proprietary or non-public information "strictly confidential" and "not use any Information in any manner . . . other than solely in connection with its consideration of" a possible partnership. Tr. 1213:16-20; PTX-99.

[18] The royalty base begins with the gross sales of the infringing products, whereas the chart outlining the increase in sales of the infringing products as compared to pre-June 20, 2017 sales of Cisco's predecessor products is estimated as $5,575.4 billion.

4. After Cisco executed the NDA, Centripetal, on February 4, 2016, presented in a WebEx meeting detailed, highly sensitive, confidential and proprietary information about its patented technology and products to Cisco, including details of its patented technology for the Asserted Patents. For example, Centripetal detailed how its "patented filter algorithms eliminate the speed and scalability problem," how its "patented system, live update, and correlation technologies 'automate workflow' and how its "patented" "instant host correlation" conveys "real time analytics." PTX-547 at 389-91; Tr. 258:21-25, 260:2-18; 1220:1-1222:25.

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

6. The next day, on February 5, 2016, Centripetal's Jonathan Rogers sent an e-mail to Cisco summarizing the WebEx meeting, noting that Cisco "seemed to hone in on our filter technology and algorithms. The algorithms are a significant networking technology with broad application that we've productized for security. There were also a few questions on our patents..." Tr. 1226:10-1227:18; PTX-102; PTX-1046

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

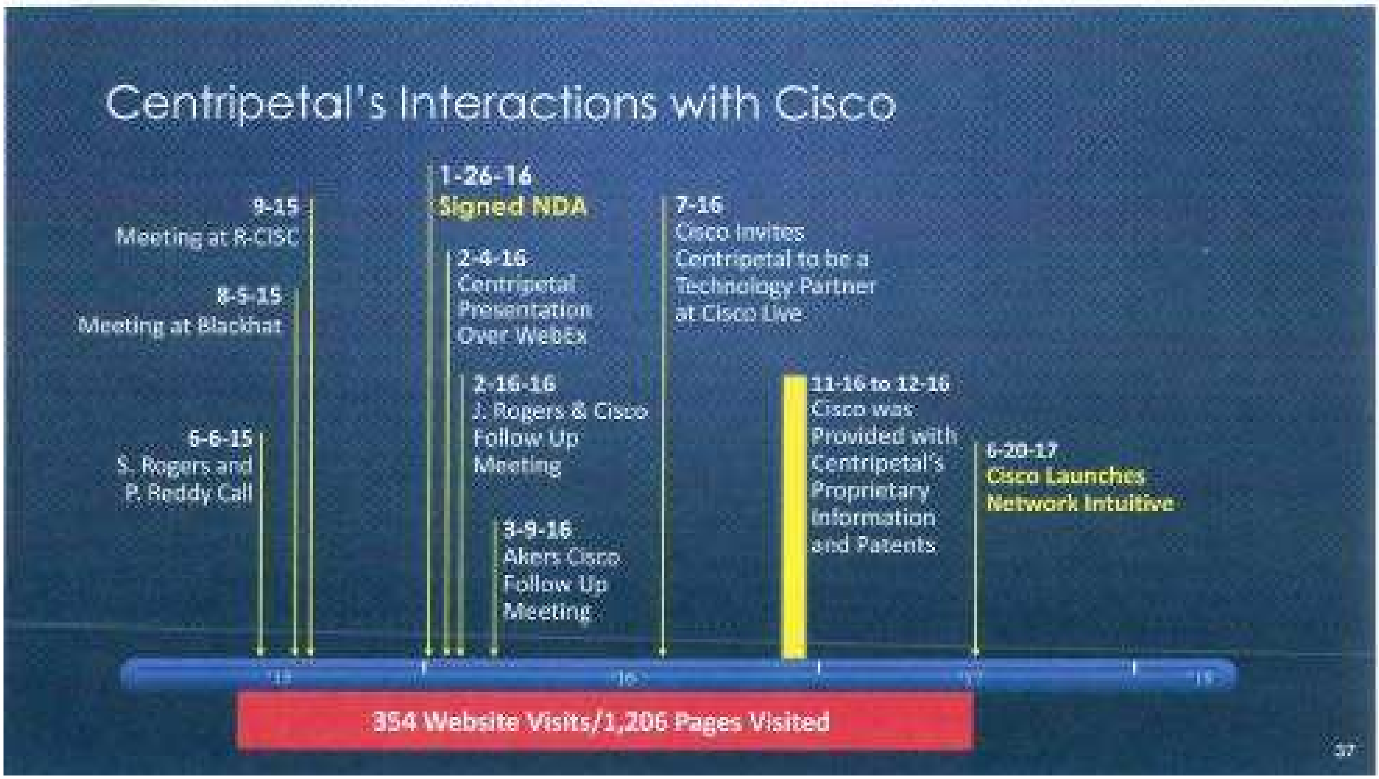
8. In November and December 2016, Cisco had several meetings with Oppenheimer

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

9. After all of these detailed meetings with Centripetal, Cisco released its "network of the future" products on June 20, 2017, which incorporated Centripetal's patented technology. See PTX-1135. Below is Centripetal's demonstrative, Slide 37, presented during opening statements which accurate reflects the evidence presented at trial surrounding the events of Centripetal and Cisco's relationship[19].

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

SLIDE 37 FROM CENTRIPETAL's OPENING STATEMENT



Centripetal's Interactions with Cisco

9-15
Meeting at R-CISC

8-5-15
Meeting at Blackhat

6-6-15
S. Rogers and
P. Reddy Call

1-26-16
Signed NDA

2-4-16
Centripetal
Presentation
Over WebEx

2-16-16
J. Rogers & Cisco
Follow Up
Meeting

3-9-16
Akers Cisco
Follow Up
Meeting

7-16
Cisco Invites
Centripetal to be a
Technology Partner
at Cisco Live

11-16 to 12-16
Cisco was
Provided with
Centripetal's
Proprietary
Information
and Patents

6-20-17
Cisco Launches
Network Intuitive

354 Website Visits/1,206 Pages Visited

iii. Conclusions of Law Regarding Willful Infringement and Enhanced Damages

Under the patent damages provisions of 35 U.S.C. § 284, a court "may increase the damages up to three times the amount found or assessed." Halo Elecs., Inc. v. Pulse Elecs., Inc., 136 S. Ct. 1923, 1931 (2016) (quoting 35 U.S.C. § 284). The use of "may" in the statute indicates that enhancement under § 284 is within the discretion of the district court. Id. The Supreme Court in Halo Elecs., Inc. v. Pulse Elecs., Inc., explicitly noted that a court exercising discretion to award enhanced damages merits an analysis of "the particular circumstances of each case" unencumbered by the "inelastic constraints" of a rigid framework. Id. at 1932. Although the statute does not include a "precise rule or formula" for an enhanced damages award, the "court's discretion should be exercised in light of the considerations underlying the grant of that discretion." Id. Halo, additionally, mandated that the award of enhanced damages is governed by a preponderance of the evidence standard. Id. at 1934.

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

Additionally, the Supreme Court noted that even if these types of conduct traditionally underlie enhanced damages, there is no requirement that the court find egregious conduct to award enhanced damages. Id. at 1933. Accordingly, in deciding to award enhanced damages, a court, in its discretion, "should take into account the particular circumstances of each case," while remembering the historical underpinnings that enhanced damages should generally "be reserved for egregious cases typified by willful misconduct." Id. at 1933-34.

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

> (1) deliberate copying;
>
> (2) defendant's investigation and good faith-belief of invalidity or non-infringement;
>
> (3) litigation behavior;
>
> (4) defendant's size and financial condition;
>
> (5) closeness of the case;
>
> (6) duration of the misconduct;
>
> (7) remedial action by the defendant;
>
> (8) defendant's motivation for harm; and
>
> (9) attempted concealment of the misconduct.

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

Moreover, the Federal Circuit has outlined that "[k]nowledge of the patent alleged to be willfully infringed continues to be a prerequisite" to the court finding that enhanced damages are warranted. Id. Therefore, prior knowledge of the patents at issue appears to be "a necessary but not sufficient condition for an award of enhanced damages." Mich. Motor Techs. LLC, 2020 U.S. Dist. LEXIS 122276, at *11-13 (collecting cases noting pre-suit knowledge of the patent is not alone sufficient to uphold a finding of willfulness and requires more factual allegations to meet Halo's egregious conduct standard). Accordingly, in light of this guidance, the Court will first determine if Cisco has pre-suit knowledge of the patents at issue. Second, the Court will use the Read factors to aid its analysis of whether infringement of the patents was willful, and to what degree enhanced damages should be assessed under the circumstances. The Court **FINDS** that Cisco willfully infringed the '856 Patent, the '176 Patent, the '193 Patent, and the '806 Patent, therefore enhanced damages are warranted under the evidence.

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

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

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

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

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

Centripetal employees and provided detailed presentations of the patents and their functionality. See Georgetown Rail Equip. Co. v. Holland L.P., 6:13-CV-366, 2016 WL 3346084, at *17 (E.D. Tex. June 16, 2016), aff'd, 867 F.3d 1229 (Fed. Cir. 2017) (showing disclosure of patented systems under a non-disclosure as evidence of copying).

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

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

With respect to Read factor three, Cisco's trial attorneys' hands were tied by Centripetal's use of Cisco's own technical documents, coupled with the adverse testimony of Cisco engineers.

Cisco had to shield the engineers who authored its current technical documents and the executives who praised its new security functionality for "solving problems previously thought unsolvable" from answering to their own writings and statements.

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

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

[20] The Court leaves out the Digital Network Architecture from this range, as it represents a statistical outlier and it was stated that DNA was a new product with no defined predecessor.

689 F. Supp. 2d at 866). Therefore, based on Cisco's immense size and commercial success with the infringing products, this factor weighs strongly in favor of enhanced damages.

Read factor five deals with the closeness of the case. The Court **FINDS** that the rulings on the four patents that were found infringed and valid were clear and not a close call. In the presentation of its defense, Cisco repeatedly relied upon animations prepared ex post facto for trial, while ignoring their own technical documents. The great majority of the Cisco technical documents were introduced by Centripetal. Not only did the animations conflict with Cisco's own technical documents, but in several instances contradicted Cisco's employee witnesses. Cisco avoided calling the authors of its technical documents as well. There was no testimony that Centripetal attempted to broaden the reach of the four infringed patents, thus opening the door to additional prior art. See 01 Communique Lab., Inc. v. Citrix Sys., 889 F.3d 735, 742 (Fed. Cir. 2018). Nonetheless, Cisco, in its invalidity case, cited its old technology as prior art, while claiming its new technology did not infringe. This led to many inconsistencies in its evidence, on both issues. Of course, Cisco could not rely upon its own documents, as they proved Centripetal's case.[21] Therefore, this factor weighs heavily in favor of enhanced damages.

Read factor six addresses the duration of the misconduct and Read factor seven weighs the remedial action taken by the infringer. While Read factor nine looks at whether the infringer attempted to conceal any misconduct.[22] The infringing conduct has been continuous and unabated without any form of remedial action from June 20, 2017 to the present time. See Acantha LLC v. Depuy Synthes Sales, Inc., 406 F. Supp. 3d 742, 761 (E.D. Wis. 2019) (citing Broadcom Corp. v. Qualcomm Inc., No. SACV 05-467-JVS, 2007 U.S. Dist. LEXIS 62764, 2007 WL 2326838, at *3

[21] The ruling on the '205 Patent was equally clear in favor of Cisco, yet this was the sole patent found not to clearly infringe.

[22] Read factor eight addresses the infringer's motivation for harm. There was no evidence presented on this factor.

(C.D. Cal. Aug. 10, 2007) ("The length of [defendant's] infringement (approximately two years), coupled with the fact that infringement continued after [plaintiff] filed suit, supports an increase in damages.")); see also Crane Sec. Techs., Inc. v. Rolling Optics AB, 337 F. Supp. 3d 48, 59 (D. Mass. 2018) (no remedial action supporting treble damages). Moreover, Cisco, through its course of conduct, continually gathered information from Centripetal as if it intended to buy the technology from Centripetal. Cisco, then, appropriated the information gained in these meetings to learn about Centripetal's patented functionality and embedded it into its own products. See Liqwd, Inc. v. L'Oréal USA, Inc., No. 17-14-JFB-SRF, 2019 U.S. Dist. LEXIS 215668, at *21 (D. Del. Dec. 16, 2019) (noting how the defendants "concealed their misconduct in gathering information from the plaintiffs so as to create the infringing products" and weighing this factor in favor of enhanced damages). Therefore, all three of these factors weigh in favor of enhanced damages.

The Court **FINDS** that Cisco did not advance any objectively reasonable defenses at trial as to the four infringed and valid patents including the '856 Patent, the '176 Patent, the '193 Patent, and the '806 Patent. Its non-infringement case was grounded upon their old technology. The infringing functionality was added to their accused products post June 20, 2017, and resulted in a dramatic increase in sales which Cisco touted in both technical and marketing documents.

Cisco's invalidity evidence often contradicted its non-infringement evidence and failed to recognize the new functionality which it copied from Centripetal during and after the Nondisclosure Agreement. PTX-99. It embedded the copied software functionality from the patents in its post June 20, 2017 switches, routers and firewalls and then ignored the accused products while claiming its pre-June 20, 2017 technology as prior art. Moreover, its damages evidence was deeply flawed in attempting to base its calculations on each patent separately instead of considering its own sales of the infringing products. Again, the increase in its sales of the accused products illustrates how completely unrealistic its damages evidence was compared to the reality of the marketplace. Accordingly, in the exercise of its discretion, the Court considers the sound legal principles underlying the history of enhanced damages and **FINDS** this is an egregious case of willful misconduct beyond typical infringement. Halo Elecs., Inc., 136 S. Ct. at 1935.

However, there are other considerations. Cisco did prevail as to one of the patents. In considering the cases awarding enhanced damages, and comparing these cases to this case, the Court **FINDS** that enhancing the damages by a factor of 2.5 is appropriate. Accordingly, the Court's past damages award of $755,808,545 is properly enhanced by a multiple of 2.5 times to award lump sum past damages of $1,889,521,362.50.

iv. Pre-judgment Interest

35 U.S.C. § 284 grants the Court discretionary authority to award interest and costs. 35 U.S.C. § 284; see General Motors Corp. v. Devex Corp., 461 U.S. 648, 653 (1983). The Supreme Court has interpreted the interest provision of section 284 and has instructed courts that pre-judgment interest should ordinarily be awarded, "absent some justification for withholding such an award." Id. at 657. The Supreme Court determined that the "fixed by the court" language in section 284 leaves the court's some discretion in awarding pre-judgment interest. Id. at 656-57. In determining the rate of pre-judgment interest, "the district court has the discretion to determine whether to use the prime rate, the prime rate plus a percentage, the U.S. Treasury rate, state statutory rate, corporate bond rate, or whatever rate the court deems appropriate under the circumstances." Century Wrecker Corp. v. E.R. Buske Mfg. Co., 913 F. Supp. 1256, 1280 (N.D. Iowa 1996) (citing Allen Archery, Inc. v. Browning Manuf. Co., 898 F.2d 787, 789 (Fed. Cir. 1990)).

Here, the Court will use the statutory post-judgment rate from the date of first infringement June 20, 2017, of 1.21%. See 28 U.S.C. § 1961. The Court calculates simple interest at the 1.21% rate over the infringement period of three years from June 20, 2017 to June 20, 2020 using the award of damages (excluding enhanced damages) of $755,808,545. This calculation makes an interest determination of $27,243,850.[23] The Court divides this number by two to account for the fact that infringement occurred over this three-year period. Accordingly, the total interest number awarded by the Court is $13,717,925. This interest is added to the final damages award, including the damages enhancement, to reach a final past damages award of $1,903,239,287.50.

B. FUTURE DAMAGES

"There are several types of relief for ongoing infringement that a court can consider: (1) it can grant an injunction; (2) it can order the parties to attempt to negotiate terms for future use of the invention; (3) it can grant an ongoing royalty; or (4) it can exercise its discretion to conclude that no forward-looking relief is appropriate in the circumstances." Whitserve, LLC v. Comput Packages, Inc., 694 F.3d 10, 35 (Fed. Cir. 2012). As described herein, the Court has considered the evidence presented at trial and the arguments and proposed findings of fact and conclusions of law advanced by all parties, and **FINDS** that a permanent injunction is not appropriate relief for the infringement of the '856 Patent, the '176 Patent, the '193 Patent, or the '806 Patent, and that an ongoing, future royalty should be imposed for all four Patents.

i. Injunctive Relief

Centripetal requests injunctive relief with regard to Cisco's firewall products. In order to merit injunctive relief, Centripetal must prove: "(1) that [they have] suffered an irreparable injury; (2) that remedies available at law, such as monetary damages, are inadequate to compensate for

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

that injury; (3) that, considering the balance of hardships between the [Proponents and Opponents], a remedy in equity is warranted; and (4) that the public interest would not be disserved by a permanent injunction." eBay, Inc. v. MercExchange, LLC, 547 U.S. 388, 391 (2006). "[A]n injunction is a drastic and extraordinary remedy, which should not be granted as a matter of course." Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 165 (2010) (citing Weinberger v. Romero–Barcelo, 456 U.S. 305, 311-12 (1982)). "If a less drastic remedy . . . [is] sufficient to redress [Proponents'] injury, no recourse to the additional and extraordinary relief of an injunction [is] warranted." Id. at 165-66. If the Court were to grant an injunction, it would do so on every infringing product and not solely on Cisco's firewalls, as Centripetal originally requested.[24] Moreover, the test for injunctive relief is not met in this case. Cisco's switches, routers, and firewalls make up large portions of the global internet infrastructure. These products are components of both civilian and military networks. Therefore, granting an injunction on the infringing products will likely cause massive adverse effects on the functional capabilities of Cisco's customers and have an adverse ripple effect on national defense and the protection of the global internet.

Therefore, as to factor two, monetary damages are more appropriate to compensate Centripetal for patent infringement. The Keysight license shows that Centripetal is willing to patent its technology to direct competitors. Courts have stated that an injunction is improper where a patent owner has shown that they are willing to accept monetary damages. See EcoServices, LLC v. Certified Aviation Servs., LLC, 340 F. Supp. 3d 1004, 1023 (C.D. Cal. 2018); Cave Consulting Grp., LLC v. Optuminsight, Inc., No. 5:11-CV-00469-EJD, 2016 WL 4658979, at *21 (N.D. Cal. Sept. 7, 2016) (finding that where a patent holder is willing to "forego its patent rights for

[24] Centripetal later expanded its request for injunctive relief to additional products. While EBay factor one has been clearly proven, factor two has clearly not.

compensation," "monetary damages are rarely inadequate"); see also Advanced Cardiovascular Sys., Inc. v. Medtronic Vascular, Inc., 579 F. Supp. 2d 554, 560 (D. Del. 2008) ("The fact that [plaintiff] was selective regarding its licensing compensation—exchanging its technology only for other licenses to competing technology—does not rectify the fact that [plaintiff] was willing, ultimately, to forego its exclusive rights for some manner of compensation. Money damages are rarely inadequate in these circumstances."). As to factor three, the greater hardship would clearly impact Cisco. Factor four, the public interest, does not support injunctive relief for the same reasons outlined as to factor two. Accordingly, for these reasons, the Court **FINDS** that an injunction is not an appropriate legal remedy for Cisco's infringement.

ii. Ongoing Royalty

Rather, the Court **FINDS** that an ongoing royalty is proper in this case. An ongoing royalty is essentially a compulsory license for future use of the patented technology during the life of the patents. Indeed, pre-verdict and post-verdict royalties are "fundamental[ly] differen[t]." XY, LLC v. Trans Ova Genetics, 890 F.3d 1282, 1397 (Fed. Cir. 2018). When setting an ongoing royalty for future use, the district court should consider "the change in the parties' bargaining positions, and the resulting change in economic circumstances." See id., ("When patent claims are held to be not invalid and infringed, this amounts to a 'substantial shift in the bargaining position of the parties."') (quoting ActiveVideo Networks, Inc. v. Verizon Commc'ns, Inc., 694 F.3d 1312, 1342 (Fed. Cir. 2012)). Such differences include a Court's determination that certain of the patents at issue are valid, enforceable, and would be infringed by the accused products. See id.

The Court should analyze future royalties in the context of the Georgia-Pacific factors. Indeed, this is the approach adopted by other district courts, after modifying the Georgia-Pacific analysis to resolve any uncertainty as to whether the accused product will infringe the patent claims, whether the asserted patents are enforceable, and whether the asserted patent claims are valid. See Creative Internet Advert. Corp. v. Yahoo! Inc., 674 F. Supp. 2d 847, 860 (E.D. Tex. 2009); Paice LLC v. Toyota Motor Corp., 609 F. Supp. 2d 620, 623-24 (E.D. Tex. 2009); Boston Sci. Corp. v. Johnson & Johnson, No. C 02-00790 SI, 2009 WL 975424 (N.D. Cal. Apr. 9, 2009). As discussed supra, this Court has analyzed the Georgia-Pacific factors in the context of past damages. The Court, here, incorporates its analysis of the previous Keysight license but takes into consideration the distinct differences in determining a past damages award as opposed to an ongoing royalty. Therefore, as it did before, the Court **FINDS** the Keysight license as a comparable license for use in determining ongoing royalties. In light of that, the Court **FINDS** an appropriate future royalty is **10% on the APPORTIONED REVENUES OF THE INFRINGING PRODUCTS FOR THREE (3) YEARS**, beginning June 21, 2020 and payable annually beginning June 20, 2021, without interest. The revenues shall be apportioned in the same manner as the pre-judgment damages, and shall apply to the infringing technology as described in the Court's Findings of Fact and Conclusions of Law. Successor products to the infringing product shall pay the same percentage royalty on sales revenue as applied to the current infringing products, so long as the successor products contain any technology found to infringe in this Opinion and Order. As to the four patents infringed, assigning different nomenclature to infringing products, or to Cisco's software technology found to infringe, shall not relieve Cisco of its obligation to pay its royalty. After this three-year term, the Court **FINDS** the royalty should be decreased to **5% FOR ANOTHER THREE (3) YEAR TERM**. Due to Cisco's dominant position in the cyber security software and firewall markets and the resulting damage to Centripetal as the first inventor the Court **FINDS** a six year term is called for in lieu of the three year term agreed upon in Keysight. Similar to the Keysight license, the Court imposes a minimum and maximum on the imposed ongoing royalty. For the **first three-year term at 10%,** such annual royalty **shall not be less than $167,711,374.10** and **shall not be more than $300,076,834.** For the **second three-year term at 5%,** such annual royalty **shall not be less than $83,855,867.00** and **shall not be more than $150,038,417**. The maximum and minimum of each year is based upon the highest and lowest years of apportioned revenues per a full year of infringement from the 2017-2020 time frame. See Doc. 411 Ex. 7. Similarly, the maximum and minimum is reduced by one-half during the second three year term to reflect the reduced royalty rate. See id. At the conclusion of this second term of three years, there shall be no further monetary payments or other relief for the sale or use of the infringing products or their successors[25].

VII. CONCLUSION

For the reasons stated within, the Court **FINDS** the ‘856 Patent, the ‘176 Patent, the ‘193 Patent, and the ‘806 Patent claims valid and literally **INFRINGED** and the ‘205 Patent **NOT INFRINGED**. The Court **FINDS** the actual damages suffered by Centripetal as a result of infringement total $755,808,545; that the infringement was willful and egregious and shall be enhanced by a factor of 2.5x to equal $1,889,521,362.50. The Court awards pre-judgment interest of $13,717,925 applied to the actual damages before enhancement plus its costs. This, accordingly, equals a total award of $1,903,239,287.50 payable in a lump sum due on the judgment date. The Court, additionally, imposes a running royalty of 10% on the apportioned sales of the accused products and their successors for a period of three years followed by a second three year term with a running royalty of 5% on said sales upon the terms described supra. It **DENIES** any further relief to Centripetal at the termination of the second three year term.

[25] The minimums and maximums are based upon the minimum apportioned annual revenue of $167,711,374.10 for the period of June 20, 2017 to June 20, 2018 and the maximum apportioned annual revenue of $300,076,834.00 for the period of June 20, 2018 to June 20, 2019.

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

It is **SO ORDERED**.

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

October 5, 2020
Norfolk, Virginia

APPENDIX A
EXPLANATION OF ABBREVIATIONS

Computer engineers use abbreviations to describe basic functionality as well as to describe the specific functionality of individual patented technology. To assist with interpreting their testimony and documents, the Court has compiled a list of the abbreviations used in the testimony and documents cited in this opinion.

ACL	Access Control List
ACE	Access Control Entry
ANC	Adaptive Network Control
ASA	Adaptive Security Appliance
ASDM	Adaptive Security Device Manager
ASR	Aggregation Services Router
ASIC	Application-Specific Integrated Circuit
CLI	Command Line Interface
CPU	Central Processing Unit
CRM	Computer-Readable Media
CSIRT	Computer Security Incident Response Team
CTA	Cognitive Threat Analytics
CTI	Cyber Threat Intelligence
DNA	Digital Network Architecture

DNS	Domain Name Server
DOE	doctrine of equivalents
ETA	Encrypted Traffic Analytics
FC	Flow Collector
FMC	Firepower Management Center
GACL	Group Access Control List
HTTP/HTTPS	HyperText Transfer Protocol (Secure)
ISE	Identity Services Engine
IDP	Initial Data Packet
IDS	Intrusion Detection System
IOS-XE	Internetwork Operating System – XE
IT Manager	Information Technology Manager
ISR	Integrated Services Router
IP	Internet Protocol
IPR	*inter partes* review
IPS	intrusion prevention system
IDS	intrusion detection system

ML	Machine Learning
NAT	network address translation
NSEL	NetFlow Secure Event Logging
PBC	Packet Buffer Complex
PTAB	Patent Trial and Appeals Board
SD-Access	Software Defined Access
SGACL	Security Group Access Control List
SGT	Security Group Tag
SPLT	Sequence of Packet Lengths and Times
SIO	Security Intelligence Operations
SIP	Session Initiation Protocol
Stealthwatch	Stealthwatch Enterprise
SLIC	Stealthwatch Labs Intelligence Center
SMC	Stealthwatch Management Console
SMTP	Simple Mail Transfer Protocol
SNI	Server Name Indication
SSL	Secure Sockets Layer

TID	Threat Intelligence Director
TCAM	Ternary Content-Addressable Memory
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
UADP	Unified Access Data Plane
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VoIP	Voice over Internet Protocol
VMR	Virtual Media Recorder
VPN	Virtual Private Network

APPENDIX B
OUTLINE OF COURT'S PROTOCOLS FOR TRIAL

B. Exhibits

1. Exhibit Lists

The parties have segregated the documents, summaries and other exhibits that may be offered into evidence at trial into exhibit lists. A joint Exhibit List, including documents identified by both parties and not objected to, is attached as Exhibit A; Centripetal's Exhibit List and Defendants' objections thereto are attached as Exhibit B; Defendants' Exhibit List and Centripetal's objections thereto are attached as Exhibit C. The parties reserve the right to object to any additional documents sought to be added to the Exhibit Lists and further reserve the right to object to any additional documents added to the Exhibit Lists under the Federal Rules of Evidence, the Federal Rules of Civil Procedure, or any other appropriate basis.

2. Efforts to Resolve Objections

The parties have been working diligently to resolve or narrow all objections lodged as to their respective exhibits. The parties have successfully resolved many objections and will continue their effo1is to resolve the objections to each other's proposed exhibits.

3. Exhibits to Which No Objections Have Been Made

The parties agree that the documents, summaries and other exhibits listed on their Exhibit Lists to which no objection has been specified may be introduced into evidence, without the necessity of further proof of admissibility through a witness, subject to foundational requirements, provided that a witness offers testimony about the exhibit at trial, either live or by deposition. This is without prejudice to motions in Limine and Daubert motions concerning certain of these documents and related testimony.

4. Cross Examination and Impeachment Exhibits

The Exhibit Lists set forth the parties' exhibits for their respective cases-in-chief; the lists do not include potential cross examination or impeachment exhibits that may or may not be introduced into evidence. The Exhibits Lists also include documents relied upon by experts in rendering opinions which may or may not be introduced into evidence. The parties reserve the right to offer exhibits for purposes of impeachment that are not included in the Exhibit Lists.

5. Authenticity Stipulations For Exhibits

The Parties stipulate to the authenticity of each document that on its face appears to be generated by a party (plaintiff or defendant), including documents generated by its employees during the course of their employment for a party, and produced in this case by that party. Notwithstanding this stipulation, each party preserves its right to object to the document on any ground other than authenticity.

C. Procedures Regarding Witnesses and Exhibits

The parties are required to disclose the expected order in which the witnesses will be called, and use good faith in identifying non-demonstrative exhibits that are intended to be used in the direct testimony of each witness or as part of opening statements. Each party must identify to opposing counsel the identity of any live witnesses to be called at trial (and the order in which they will be called) by no later than 6:30 p.m.[26]three (3) calendar days before the trial day on which that witness is expected to testify (e.g., witnesses to be called on Tuesday must be disclosed by 6:30 p.m. the preceding Saturday).

Except for when a fact witness is testifying during trial, fact witnesses are not permitted to witness or have access to the trial proceedings in any manner until after that fact witness has

[26] All times identified herein are Eastern Time.

completed all testimony that witness will provide at trial. The only exception is the parties' client representative, who will be allowed to witness and have access to the trial proceedings, even if testifying in the case. Expert witnesses may have access to the trial proceedings while other witnesses are testifying.

Any exhibits to be used on direct examination with any live witness must be identified by no later than 7 p.m. two (2) calendar days before the start of the trial day on which that exhibit will be offered (e.g., the exhibit(s) for witnesses to be called on Tuesday must be disclosed by 7 p.m. the preceding Sunday). Objections to exhibits disclosed by a party must be provided by 8 p.m. two (2) calendar days before the start of the trial day on which that exhibit will be offered (e.g., objections to exhibits for witnesses to be called on Tuesday must be provided by 8 p.m. the preceding Sunday). The parties will each designate one or more counsel who shall meet and confer regarding any such objections by 8:30 p.m. on the day when the objections are provided. The notice provisions above shall not apply to illustrative exhibits created in the virtual courtroom during testimony or to the enlargement, highlighting, ballooning, or excerpting of trial exhibits, demonstratives, or testimony, so long as the underlying exhibit is pre-admitted or the party has identified the exhibit or deposition testimony according to the agreed schedule.

The parties will cooperate in seeking to have the Court resolve any objections they are unable to resolve among themselves prior to the proposed testimony. Each party will deliver exhibits to the Court that it anticipates using on direct examination by 9 a.m. ET the day of the direct examination in the form of a witness binder. Each party will deliver exhibits to the Court that it anticipates using on cross-examination by 9 a.m. ET the day of the cross-examination, and to opposing counsel by e-mail prior to commencing cross-examination.

Any document that on its face appears to have been authored or prepared by an employee, officer, or agent of a party, or was produced from the files of a party, shall be deemed primafacie authentic under F.R.E.901 and 902, subject to the right of the party against whom such a document is offered to introduce evidence to the contrary. The parties reserve the right to add additional deposition designations to establish the foundation and authenticity of an exhibit to the extent the admissibility of a particular document is challenged.

Legible or better quality copies may be offered and received in evidence in lieu of originals thereof, subject to all foundational requirements and other objections which might be made to the admissibility of such originals, and subject to the right of the party against whom they are offered to inspect an original upon request. The parties may use electronic, native versions of exhibits that are spreadsheets or slide presentations to the extent such documents were produced during discovery or otherwise agreed to by both parties.

D. Procedures Regarding Deposition Testimony and Discovery Response Designations

The parties are required to provide opposing counsel the identity of any deposition designations or designations of discovery responses and a list of any exhibits to be introduced along with those designations according to the schedule set forth above for disclosure of witnesses/exhibits. Objections and counter-designations to any such designations disclosed by a party will be provided according to the schedule set forth above for objections to exhibits. For deposition testimony, the party introducing the deposition testimony shall be responsible for editing the deposition testimony to include the testimony and any counter-designation testimony, and remove any attorney objections, and provide a final version of the deposition testimony excerpts (testimony clip report) to the other party by 6:30 p.m. the day before the testimony is to be submitted, read or played to the Court. The parties will each designate one or more counsel who will meet and confer regarding any objections, including objections to any applicable counter-designations[27], by 8:30 p.m. the same day that such objections are disclosed.

The parties will cooperate in seeking to have the Court resolve any objections they are unable to resolve among themselves prior to the proposed testimony or presentation of a discovery response. Each side is to provide the discovery response or deposition testimony excerpts of the specific portions of the deposition video(s) to be played or read, to opposing counsel and to the Court at the time each such designation is presented to Court.

The parties agree that any counter-designations, to which the other party did not object or to which the Court overruled the objection, will be included in the designation of discovery responses or testimony clip report of deposition designations, and that passages of testimony from a deposition will be presented chronologically. The parties further agree to withdraw any objections or attorney colloquy contained with the deposition designations by both sides to the extent possible. For allocating time between the parties for witnesses presented by deposition, witnesses presented by video or read testimony will be divided by the actual time for designations and counter-designations by each party. For witnesses presented by read testimony, the allocation

[27] The parties agreed not to serve objections to counter-designations as part of this pretrial order, and to raise necessary objections to such counter designations at the time of trial.

of trial time will be determined by the ratio of deposition testimony lines designated by each party to the total number of lines read by that witness. No time will be allocated to the parties for deposition testimony submitted to the Court as an exhibit only, with no video or read testimony. Deposition summaries will be offered at trial as appropriate pursuant to Local Rule 30(G). All testimony clip reports for deposition testimony provided to the Court will be admitted as a trial exhibit. The parties' current deposition designations, objections, and counter-designations are attached as Exhibit D (Centripetal) and Exhibit E (Defendant). The parties' discovery responses designations, objections, and counter-designations are attached as Exhibit F (Centripetal) and Exhibit G (Defendant).

III. Witnesses

The parties agree that for current employees of a party, any such witness that such party expects to call in their case-in-chief will appear live by video. For those non-employee witnesses who will be called in a party's case-in-chief via deposition, the parties agree that any counter-designated testimony will be presented to the Court together with the designated deposition testimony, subject to the resolution of any objections to the designated or counter-designated testimony, as discussed above. The parties also agree that a party who wishes to call an employee of the other party as part of its case-in-chief can do so by deposition, regardless of the availability of that witness to testify live.

The parties agree that all fact and expert witnesses will provide any trial testimony from a location remote from their lawyers or staff working on this matter. A remote location means a home, building or office different from any home, building or office where lawyers or staff working on this matter are present. Furthermore, while providing testimony at trial, no witness shall access any form of communication other than the Zoom video or audio feed provided by the Court. Once sworn, no witness shall communicate with anyone else regarding the substance of the witness's testimony (absent express permission of the Court) until such time as the witness is excused by the Court from further participation in the trial. The agreement reflected in the foregoing sentence does not apply to fact witnesses or Dr. Medvidovic, Dr. Striegel, and Dr. Almeroth should they be called to testify on more than one occasion during the trial. For such witnesses, the parties agree that they will not communicate or speak with the witness once he begins testimony on the subject matter for which they are in the middle of testimony, as delineated by the Court. Once the witness has completed such testimony and leaves the stand, that witness can speak with counsel before taking the stand to testify at a later time during the trial.