

No. 2021-1888

**UNITED STATES COURT OF APPEALS
FOR THE FEDERAL CIRCUIT**

CENTRIPETAL NETWORKS, INC.,

Plaintiff-Appellee,

v.

CISCO SYSTEMS, INC.,

Defendant-Appellant.

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

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

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

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

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

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

August 27, 2021

Attorneys for Defendant-Appellant Cisco Systems, Inc.

REPRESENTATIVE PATENT CLAIMS

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

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

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

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

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

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

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

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

U.S. Patent No. 9,686,193 (“Forward or Drop”)

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

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

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

CERTIFICATE OF INTEREST

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

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

Cisco Systems, Inc.

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

Not applicable.

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

None.

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

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

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

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

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

ORRICK HERRINGTON & SUTCLIFFE LLP: Elizabeth Rose Moulton

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

Reexamination No. 90/014,476 (USPTO)

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

None.

Dated: August 27, 2021

/s/ William F. Lee

WILLIAM F. LEE

WILMER CUTLER PICKERING

HALE AND DORR LLP

60 State Street

Boston, MA 02109

(617) 526-6000

TABLE OF CONTENTS

	Page
REPRESENTATIVE PATENT CLAIMS	
CERTIFICATE OF INTEREST	i
TABLE OF AUTHORITIES	vi
STATEMENT OF RELATED CASES	1
INTRODUCTION	3
JURISDICTIONAL STATEMENT	4
STATEMENT OF ISSUES	5
STATEMENT OF THE CASE.....	5
A. Cisco’s Core Networking Products: Switches, Routers, And Firewalls	5
B. Cisco’s Network Security Products	6
C. Centripetal’s RuleGATE And Its Failure In The Market	9
D. District Court Proceedings	11
SUMMARY OF ARGUMENT	14
ARGUMENT	16
I. STANDARD OF REVIEW	16
II. THE JUDGMENT CANNOT STAND BECAUSE THE DISTRICT COURT FOUND NO ACTS OF DIRECT INFRINGEMENT AND DID NOT LIMIT DAMAGES TO ANY DIRECT INFRINGEMENT	16
A. The District Court Legally Erred By Finding Direct Infringement Even Though Cisco Did Not Make, Use, Sell, Or Offer To Sell Any Product Practicing The Claims.....	16

B.	At A Minimum, The Court Erred By Awarding Damages Based On Revenues From Every Sale Of The Accused Products, Rather Than Limiting The Award To The Specific Accused Combinations.....	21
III.	THE INFRINGEMENT FINDINGS SHOULD BE REVERSED OR VACATED.....	23
A.	'806 "Rule Swap" Patent.....	23
1.	Background	23
2.	The accused product combinations do not "cease processing" or "cache" packets "responsive to being signaled".....	24
B.	'856 "Packet Filtering" Patent.....	28
1.	Background	28
2.	The accused product combination does not "filter ... the determined packets".....	30
a.	The court implicitly misconstrued "packets"	30
b.	Stealthwatch does not "filter ... the determined packets"	32
C.	'176 "Correlation" Patent.....	37
1.	Background	37
2.	The accused product combination does not "correlate" transmitted packets with received packets.....	38
a.	The accused combination does not "correlate" packets based on ingress and egress NetFlow records	38
b.	The district court's sua sponte infringement theories are unsupported.....	41
D.	'193 "Forward or Drop" Patent.....	43

1.	Background	43
2.	The accused product combination does not forward or drop packets depending on whether they are “associated with [a] particular type of data transfer”	45
IV.	THE DAMAGES AWARD SHOULD BE VACATED	51
A.	The Court Erred By Adopting Centripetal’s Flawed Apportionment Analysis	51
B.	The Royalty Rate Was Wrongly Drawn From A Single Non-Comparable License Centripetal Secured As A Settlement.....	56
C.	A New Damages Trial (And Recalculation Of Other Monetary Awards) Is Required If This Court Sets Aside Any Of The Infringement Findings.....	57
V.	THE DISTRICT COURT CLEARLY ERRED IN FINDING WILLFULNESS AND ABUSED ITS DISCRETION IN ENHANCING DAMAGES	58
A.	Cisco Did Not Copy Centripetal	59
B.	The Case Was Close.....	62
VI.	THE JUDGMENT SHOULD BE VACATED BECAUSE THE DISTRICT JUDGE WAS STATUTORILY DISQUALIFIED	64
	CONCLUSION	67
	ADDENDUM	
	CERTIFICATE OF SERVICE	
	CERTIFICATE OF COMPLIANCE	

CONFIDENTIAL MATERIAL OMITTED

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

TABLE OF AUTHORITIES

CASES

	Page(s)
<i>01 Communique Laboratory, Inc. v. Citrix Systems, Inc.</i> , 889 F.3d 735 (Fed. Cir. 2018)	63
<i>Amazon.com, Inc. v. Barnesandnoble.com, Inc.</i> , 239 F.3d 1343 (Fed. Cir. 2001)	51, 59
<i>Amgen Inc. v. Sandoz Inc.</i> , 923 F.3d 1023 (Fed. Cir. 2019)	16
<i>Aro Manufacturing Co. v. Convertible Top Replacement Co.</i> , 365 U.S. 336 (1961).....	17
<i>AstraZeneca AB v. Apotex Corp.</i> , 782 F.3d 1324 (Fed. Cir. 2015)	21
<i>Aylus Networks, Inc. v. Apple Inc.</i> , 856 F.3d 1353 (Fed. Cir. 2017)	50
<i>Cardiac Pacemakers, Inc. v. St. Jude Medical, Inc.</i> , 576 F.3d 1348 (Fed. Cir. 2009)	22
<i>Centripetal Networks, Inc. v. Cisco Systems, Inc.</i> , __ F. Supp. 3d __, 2021 WL 1030286 (E.D. Va. Mar. 17, 2021)	13
<i>Centripetal Networks, Inc. v. Cisco Systems, Inc.</i> , 492 F. Supp. 3d 495 (E.D. Va. Oct. 5, 2020)	13
<i>Centripetal Networks, Inc. v. Cisco Systems, Inc.</i> , 847 F. App'x 869 (Fed. Cir. 2021) (nonprecedential).....	43
<i>Chase Manhattan Bank v. Affiliated FM Insurance Co.</i> , 343 F.3d 120 (2d Cir. 2003)	66
<i>Commonwealth Scientific & Industrial Research Organisation v.</i> <i>Cisco Systems, Inc.</i> , 809 F.3d 1295 (Fed. Cir. 2015)	51

<i>Corning v. Fast Felt Corp.</i> , 873 F.3d 896 (Fed. Cir. 2017)	31
<i>DDR Holdings, LLC v. Hotels.com, L.P.</i> , 773 F.3d 1245 (Fed. Cir. 2014)	57
<i>Deepsouth Packing Co. v. Laitram Corp.</i> , 406 U.S. 518 (1972).....	17
<i>E.I. du Pont de Nemours & Co. v. Unifrax I LLC</i> , 921 F.3d 1060 (Fed. Cir. 2019)	24
<i>Enplas Display Device Corp. v. Seoul Semiconductor Co.</i> , 909 F.3d 398 (Fed. Cir. 2018)	21
<i>Ericsson, Inc. v. D-Link Systems, Inc.</i> , 773 F.3d 1201 (Fed. Cir. 2014)	55
<i>Exmark Manufacturing Co. v. Briggs & Stratton Power Products Group, LLC</i> , 879 F.3d 1332 (Fed. Cir. 2018)	51
<i>Finjan Inc. v. Blue Coat Systems, Inc.</i> , 879 F.3d 1299 (Fed. Cir. 2018)	54, 55
<i>Finjan, Inc. v. SonicWall Inc.</i> , No. 5:17-cv-04467 (N.D. Cal. May 21, 2021), ECF No. 477	2, 55
<i>Garretson v. Clark</i> , 111 U.S. 120 (1884).....	51
<i>Halo Electronics, Inc. v. Pulse Electronics, Inc.</i> , 136 S. Ct. 1923 (2016).....	58
<i>IGT v. Bally Gaming International Inc.</i> , 610 F. Supp. 2d 288 (D. Del. 2009), <i>aff'd</i> , 659 F.3d 1109 (Fed. Cir. 2011)	26
<i>Immunex Corp. v. Sandoz Inc.</i> , 964 F.3d 1049 (Fed. Cir. 2020)	16
<i>In re Cement Antitrust Litigation</i> , 688 F.2d 1297 (9th Cir. 1982)	66

<i>Intel Corp. v. Broadcom Corp.</i> , No. Civ.A. 00-796-SLR, 2003 WL 360256 (D. Del. Feb. 13, 2003)	26-27
<i>LaserDynamics, Inc. v. Quanta Computer</i> , 694 F.3d 51 (Fed. Cir. 2012)	56, 57
<i>Liljeberg v. Health Services Acquisition Corp.</i> , 486 U.S. 847 (1988)	66
<i>Lucent Technologies, Inc. v. Gateway, Inc.</i> , 580 F.3d 1301 (Fed. Cir. 2009)	22, 51
<i>MAG Aerospace Industries v. B/E Aerospace, Inc.</i> , 816 F.3d 1374 (Fed. Cir. 2016)	36
<i>MLC Intellectual Property, LLC v. Micron Technology, Inc.</i> , No. 2020-1413, __ F.4th __, 2021 WL 3778405 (Fed. Cir. Aug. 26, 2021)	55, 57
<i>Nease v. Ford Motor Co.</i> , 848 F.3d 219 (4th Cir. 2017)	16
<i>Newport News Holdings Corp. v. Virtual City Vision, Inc.</i> , 650 F.3d 423 (4th Cir. 2011)	16
<i>Omega Patents, LLC v. CalAmp Corp.</i> , 920 F.3d 1337 (Fed. Cir. 2019)	23, 57
<i>Paice LLC v. Toyota Motor Corp.</i> , 504 F.3d 1293 (Fed. Cir. 2007)	58
<i>Polara Engineering Inc. v. Campbell Co.</i> , 894 F.3d 1339 (Fed. Cir. 2018)	62, 63
<i>Regents of University of Minnesota v. AGA Medical Corp.</i> , 717 F.3d 929 (Fed. Cir. 2013)	36
<i>Rite-Hite Corp. v. Kelley Co.</i> , 56 F.3d 1538 (Fed. Cir. 1995)	58
<i>Rotec Industries, Inc. v. Mitsubishi Corp.</i> , 215 F.3d 1246 (Fed. Cir. 2000)	17

<i>Rude v. Westcott</i> , 130 U.S. 152 (1889).....	56
<i>Shell Oil Co. v. United States</i> , 672 F.3d 1283 (Fed. Cir. 2012)	64, 65, 66
<i>TrafFix Devices, Inc. v. Marketing Displays, Inc.</i> , 532 U.S. 23 (2001).....	59
<i>Twigg v. Norton Co.</i> , 894 F.2d 672 (4th Cir. 1990)	42, 43
<i>Verizon Services Corp. v. Vonage Holdings Corp.</i> , 503 F.3d 1295 (Fed. Cir. 2007)	57
<i>VirnetX, Inc. v. Cisco Systems, Inc.</i> , 767 F.3d 1308 (Fed. Cir. 2014)	51, 56
<i>Whitserve, LLC v. Computer Packages, Inc.</i> , 694 F.3d 10 (Fed. Cir. 2012)	57
<i>Wi-Lan, Inc. v. Apple, Inc.</i> , 811 F.3d 455 (Fed. Cir. 2016)	34
<i>Wordtech Systems, Inc. v. Integrated Networks Solutions, Inc.</i> , 609 F.3d 1308 (Fed. Cir. 2010)	57

STATUTES AND REGULATIONS

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

35 U.S.C.	
§ 271(a)	3, 17, 20
§ 271(b)	19
§ 271(c)	19
§ 283	58
§ 284	21
5 C.F.R. § 2634.403(a)(2)	66

LEGISLATIVE MATERIAL

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

OTHER AUTHORITIES

Judicial Conference of the United States, Committee on Codes of	
Conduct, Advisory Opinion No. 110	65
McKeown, Hon. M. Margaret, <i>To Judge or Not to Judge:</i>	
<i>Transparency and Recusal in the Federal System</i> , 30 Rev. Litig.	
653 (2011)	65-66

STATEMENT OF RELATED CASES

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

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

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

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

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

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

INTRODUCTION

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

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

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

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

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

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

JURISDICTIONAL STATEMENT

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

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

STATEMENT OF ISSUES

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

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

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

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

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

STATEMENT OF THE CASE

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

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

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

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

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

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

B. Cisco's Network Security Products

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

D. District Court Proceedings

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

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

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

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

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

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

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

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

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

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

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

SUMMARY OF ARGUMENT

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

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

packets depending on the “type of data transfer”; the court nowhere found that Cisco’s products do that.

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

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

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

ARGUMENT

I. STANDARD OF REVIEW

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

III. THE INFRINGEMENT FINDINGS SHOULD BE REVERSED OR VACATED

A. ’806 “Rule Swap” Patent

1. Background

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

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

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

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

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

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

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

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

⁶ Emphases are added unless otherwise noted.

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

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

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

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

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

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

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

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

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

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

B. ’856 “Packet Filtering” Patent

1. Background

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

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

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

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

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

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

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

2. The accused product combination does not “filter ... the determined packets”

a. The court implicitly misconstrued “packets”

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

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

information” from packets that previously passed through a router or switch.

Appx113(¶13); Appx1134-1135(134:10-11, 134:22-135:12); Appx2818-2819(1815:5-7, 1816:4-5); Appx5219. The court called NetFlow “*representations of information*” from the *unencrypted portion* of encrypted packets.”

Appx77(¶15); *see also* Appx78(¶20); Appx99. Thus, the court implicitly construed “packets” to include not the packets themselves, but mere “representations of information” from “the unencrypted portion” of packets.

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

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

b. Stealthwatch does not “filter ... the determined packets”

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

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

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

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

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

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

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

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

filtering based on “Server Name Indication,” which is also part of NetFlow. *Id.*

But again, the document at most shows analyzing NetFlow, not filtering the packets themselves.

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

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

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

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

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

The asserted claims are narrowly drawn to a specific sequence of steps: “*determin[ing]* ... *packets*” with encrypted data corresponding to a threat indicator; “filter[ing] ... *the determined packets*”; and “rout[ing] ... *filtered packets*.” Nothing in the court’s cited marketing documents, or the testimony the court quotes at length, suggests that Stealthwatch “filter[s]” packets previously “determine[d]” to be threats or “route[s]” them to a proxy system. Appx84-94.¹⁰

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

C. '176 “Correlation” Patent

1. Background

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

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

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

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

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

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

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

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

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

Centripetal’s expert and the court relied on documents that speak only of correlating threats within a Cisco-protected system with information about threats outside the system—*not* of correlating transmitted and received packets based on egress/ingress NetFlow records. For instance, Centripetal and the court relied on an internal Cisco presentation that mentions “the cloud-based analytics engine that correlates threat behaviors seen in the enterprise *with those seen globally.*”

Appx119 (reproducing Appx5222); Appx1995(995:13-18). The court (at Appx120-121) relied on two additional documents (though Centripetal did not) that similarly speak of correlation to global threat behavior. *See* Appx5063 (PTX-202: “Cisco Stealthwatch with Cognitive Analytics ... correlates local traffic models with global threat behaviors”); Appx5150 (PTX-569: “Stealthwatch ...

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

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

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

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

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

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

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

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

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

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

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

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

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

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

D. ’193 “Forward or Drop” Patent

1. Background

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The court also stated—without citation—that Cisco’s products “limit[] a computer located in a first network from accessing sensitive data in a protected network, while simultaneously allowing unsensitive data to be accessed.”

Appx133. If the court meant, consistent with its findings elsewhere, that Cisco’s products block a computer from accessing sensitive data in a protected network, but allow that computer to access unsensitive data in a *different* network, then the statement is accurate but does not prove infringement. Infringement would require a finding that Cisco’s products block a computer from accessing “sensitive data” from a “protected” destination while allowing that same computer access to other data from the *same* destination. The court made no such finding, and no evidence would support one. Rather, as the court repeatedly recognized, Cisco’s rules block *all* packets, or allow *all* packets, between a given source and a given destination.

See supra pp. 47-48.

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

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

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

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

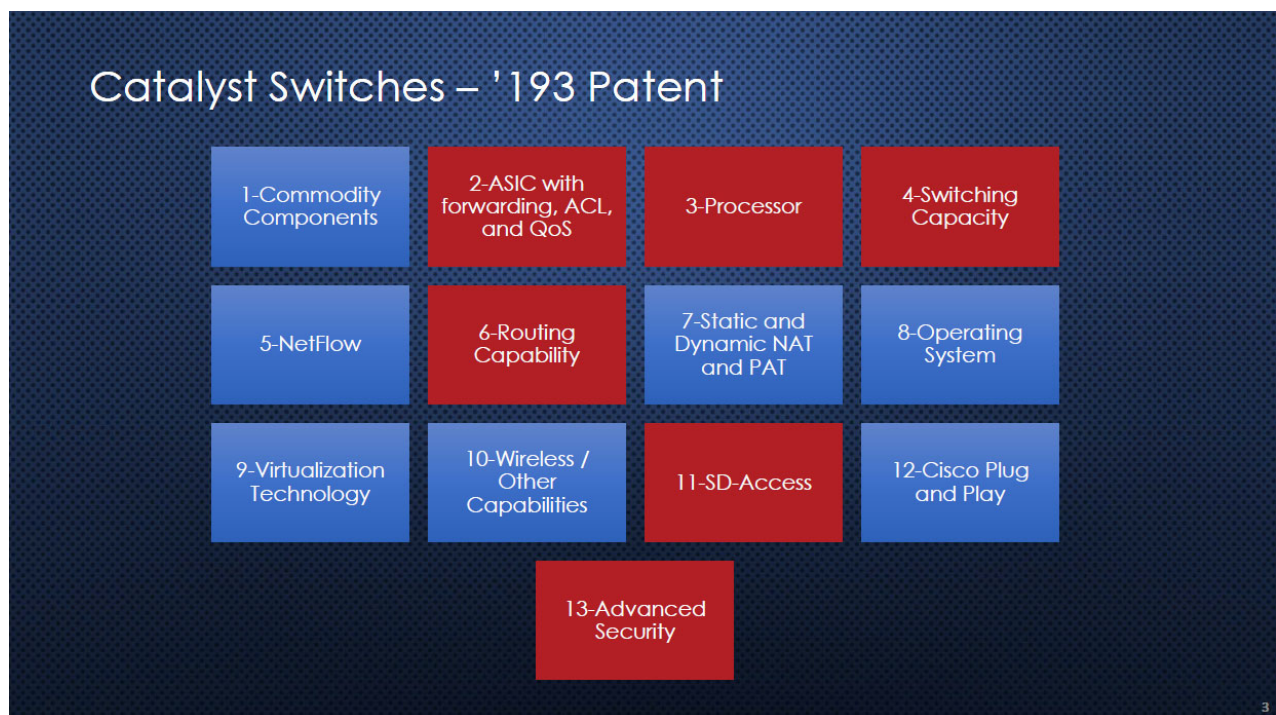
IV. THE DAMAGES AWARD SHOULD BE VACATED

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

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

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

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



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

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

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

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

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

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

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

Nothing in *Blue Coat* justifies Dr. Striegel’s approach. Indeed, *Blue Coat* elsewhere rejected a methodology similar to Dr. Striegel’s that failed to fully apportion out the accused product’s “non-infringing features.” 879 F.3d at 1310-1311 (“Because DRTR is itself a multi-component software engine that includes non-infringing features ... [f]urther apportionment was required to reflect the value of the patented technology[.]”). And the same district court that decided *Blue Coat* recently excluded Dr. Striegel’s “top-level function[.]” analysis in another case, holding that it does not satisfy the apportionment requirement. Order at 16-20, *Finjan, Inc. v. SonicWall Inc.*, No. 5:17-cv-04467 (N.D. Cal. May 21, 2021), ECF No. 477.¹³

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

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

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

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

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

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

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

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

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

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

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

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

A. Cisco Did Not Copy Centripetal

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

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

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

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

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

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

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

in Centripetal's algorithms and patents. Appx5047. Although the court asserted that Centripetal presented "detailed, highly sensitive, confidential and proprietary information about its patented technology," Appx193, attendees from *both* companies expressly contradicted that assertion: most described the information provided as "high-level," which the meeting's slide deck confirms.

Appx1393(393:4-17); Appx3818-3820(2810:24-2812:19); Appx5125-5131; Appx5873(36:13-19); Appx5876-5877(76:12-81:22); Appx5897-5898(33:4-34:25).

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

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

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

B. The Case Was Close

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CONCLUSION

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

Respectfully submitted,

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

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

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

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

*Attorneys for Defendant-Appellant
Cisco Systems, Inc.*

August 27, 2021