NOTE: This disposition is nonprecedential.

United States Court of Appeals for the Federal Circuit

CENTRIPETAL NETWORKS, LLC,
Plaintiff-Appellant

v.

CISCO SYSTEMS, INC.,
Defendant-Appellee

2024-2097

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

Decided: April 29, 2026

MATTHEW ROWEN, Clement & Murphy, PLLC, Alexandria, VA, argued for plaintiff-appellant. Also represented by PAUL D. CLEMENT, JOSEPH DEMOTT.

MARK CHRISTOPHER FLEMING, Wilmer Cutler Pickering Hale and Dorr LLP, Boston, MA, argued for defendant-appellee. Also represented by WILLIAM F. LEE; HEATH BROOKS, NORA N. XU, Washington, DC; MATTHEW CHRISTOPHER GAUDET, L. NORWOOD JAMESON, Duane Morris LLP, Atlanta, GA.

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

DYK, *Circuit Judge*.

Centripetal Networks, LLC ("Centripetal") appeals the district court's judgment of noninfringement in favor of Cisco Systems, Inc. ("Cisco") as to the asserted claims of three of its patents—U.S. Patent Nos. 9,686,193 ("'193 patent"), 9,203,806 ("'806 patent"), and 9,560,176 ("'176 patent"). These patents relate to filtering packets of data for security threats when they are transferred between computer networks.

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

BACKGROUND

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

moved for the judge's recusal under 28 U.S.C. § 455. *Id.* at 1029. In an attempt to comply with the statutory requirements, the judge placed his wife's stock in a blind trust and denied Cisco's motion. *Id.* On appeal, we held that placing stock in a blind trust did not satisfy the requirements of § 455(f) and accordingly vacated the district court's judgment; ordered that the case "be assigned to a new judge . . . pursuant to Rule 63;" and remanded "for further proceedings before [the] newly appointed judge, who shall decide the case without regard for the vacated opinions and orders." *Id.* at 1040. On remand, the new judge concluded Cisco did not infringe the three asserted patents.

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

I. THE ASSERTED PATENTS AND CISCO'S ACCUSED PRODUCTS

The case involves three separate patents. The '193 patent relates to filtering network data transfers to prevent "[a] category of cyber attack known as exfiltrations," '193 patent, col. 1 ll. 24–27, which "involve[] a circumstance where an attacker gains access to a computer inside of a network and sends protected information outside of that network," J.A. 34 n.5.[1] Claim 18, which is representative of the asserted claims, recites, in relevant part:

A system comprising:

at least one processor; and

---

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

> a memory storing instructions that when executed by the at least one processor cause the system to:
>
> > receive, from a computing device located in a first network, a plurality of packets wherein the plurality of packets comprises a first portion of packets and a second portion of packets;
> >
> > responsive to a determination that the first portion of packets comprises data corresponding to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network, wherein the data indicates that the first portion of packets is destined for the second network:
> >
> > > apply, to each packet in the first portion of packets, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and
> > >
> > > drop each packet in the first portion of packets. . . .

'193 patent, claim 18 (emphases added).

The specification of the '193 patent explains that "[t]he filtering process described herein may be viewed as having two (2) stages" where "the first stage may deter-

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

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

> A system comprising:
>
> > a plurality of processors; and
> >
> > a memory comprising instructions that when executed by at least one processor of the plurality of processors cause the system to: . . .
> >
> > > configure at least two processors of the plurality of processors to process packets in accordance with the first rule set . . .

---

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

> 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 recon figuration to process packets in accordance with the second rule set, process, in accordance with the second rule set, the one or more packets.

'806 patent, claim 9 (emphases added).

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

> A system comprising:
>
> > at least one processor; and
> >
> > a memory storing instructions that when executed by the at least one processor cause the system to:

identify a plurality of packets received by a network device from a host located in a first network;

generate a plurality of log entries corresponding to the plurality of packets received by the network device;

identify a plurality of packets transmitted by the network device to a host located in a second network;

generate a plurality of log entries corresponding to the plurality of packets transmitted by the network device;

correlate, based on the plurality of log entries corresponding to the plurality of packets received by the network device and the plurality of log entries corresponding to the plurality of packets transmitted by the network device, the plurality of packets transmitted by the network device with the plurality of packets received by the network device; and

responsive to correlating the plurality of packets transmitted by the network device with the plurality of packets received by the network device:

generate, based on the correlating, one or more rules configured to identify packets

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

'176 patent, claim 11 (emphases added).

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

II. PROCEDURAL HISTORY

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

After trial, Cisco moved for the district court judge's recusal based on his wife's stock ownership in Cisco. The district judge placed the stock in a blind trust and denied

---

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

the recusal motion, and Cisco appealed. On appeal, we concluded that the district court judge was required to recuse, vacated the judgment, and remanded the case for further proceedings with a new judge pursuant to Federal Rule of Civil Procedure 63 without regard to the vacated opinion. *Centripetal*, 38 F.4th at 1039–40.

On August 23, 2022, the case was reassigned to a new judge. Pursuant to Rule 63, the parties were given an opportunity to recall any witness whose testimony was material and disputed, but chose not to do so. Centripetal and Cisco also each filed a trial brief, presenting their claims and defenses, and filed proposed findings of fact and conclusions of law. The new judge then certified her familiarity with the record and held a hearing where each side presented a technology tutorial and presented argument on the '193, '806, and '176 patents.

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

---

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

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

As to the '176 patent, the district court concluded that Centripetal "failed to show that (1) the accused technology correlates the packets entering and exiting a network device and that (2) responsive to the correlating, the system generates rules configured to identify patents in a specific network." J.A. 75–76.

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

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

a "particular type of data transfer" as required by the claim language. *Id.* Instead, the district court clarified that the plain and ordinary meaning of "'particular type of data transfer' refers to the specific technique, or method, associated with the transmission," J.A. 94, and concluded that Cisco's products do not infringe the asserted claims because they only filter packets by source and destination (stage 1 filtering), not the specific technique or method of the transfer, as required by stage 2.

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

DISCUSSION

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

I

With respect to the '193 patent, Centripetal argues that the district court erred by improperly construing the term "particular type of data transfer" to exclude source and destination filtering pursuant to Cisco's quarantine procedure. Cisco argues that the district court's construction is supported by the specification and the prosecution history. We agree with Cisco.

Some background on Cisco's accused products is useful. Cisco's switches and routers are configured to apply packet-filtering rules, called access control lists ("ACLs"),

that drop or forward packets. Centripetal alleges that a particular ACL, called the Security Group ACL ("SGACL") or "quarantine rule," which involves SGT-tagging, infringes the '193 patent. This rule operates by directing a switch or router to drop a packet from a device tagged with a quarantine tag, if it is headed to a restricted destination.

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

The specification is "the single best guide to the meaning of a disputed term." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1315 (Fed. Cir. 2005) (en banc) (quoting *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996)). As described above, the specification of the '193 patent explains, "[t]he filtering process described herein may be viewed as having two (2) stages." '193 patent, col. 8 ll. 39–40. It goes on to clarify that "[c]onceptually, the first stage may determine if the network policy allows any communications between the resources [(network devices)] identified in the 5-tuple rule" and "the second stage may determine if the policy allows the specific method or type of communication . . . between the resources." *Id.* col. 8 ll. 45–52.

---

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

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

> the independent claims of the '193 patent recite rules for preventing the transfer of a subset of packets out of the network. These rules involve implementing a two-stage process for filtering traffic:
>
> > Conceptually, the first stage may determine if the network policy allows any communications between the resources identified in the 5-tuple rule; **if so, the second stage** may determine if the policy allows the specific method or type of communication (e.g., file read, file write, encrypted communication, etc.) between the resources.

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

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

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

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

---

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

at 7:00–7:15 (Centripetal agreeing it would lose based on this construction).

Centripetal also argues (somewhat inconsistently with the concession described above) that we should remand because the district court adopted a new claim construction in its post-judgment opinion, and Centripetal did not have the opportunity to present evidence of infringement under this construction. But Centripetal had adequate notice of Cisco's claim construction positions with respect to the '193 patent. In its post-trial proposed findings of fact and conclusions of law, Cisco argued that the asserted claims of the '193 patent require two-stage filtering and that its products, which allow or drop packets by source and destination, are only capable of filtering at the first stage. J.A. 17865–66. Cisco made the same argument in its trial brief and at the Rule 63 hearing. *See* J.A. 19450–54; 21283. Our cases make clear that, even in the PTAB context (with more stringent procedural requirements than in district court cases), any shift in the original construction does not create any unfairness where, as here, the challenger consistently put the patentee on notice of its interpretation of the asserted claims. *See Hamilton Beach Brands, Inc. v. f'real Foods, LLC*, 908 F.3d 1328, 1338–39 (Fed. Cir. 2018); *Google LLC v. EcoFactor, Inc.*, 92 F.4th 1049, 1057 (Fed. Cir. 2024).

Finally, Centripetal argues that Cisco's products infringe the asserted claims of the '193 patent even under the district court's construction. Centripetal's argument appears to be based on the theory that Cisco's switches and routers could be modified to filter by a "particular type of data transfer," but this hardly suggests that Cisco's switches and routers infringe in their current configurations. The testimony Centripetal cites to support the contention that Cisco's switches and routers already have this functionality only shows that the switches and routers can identify and flag suspicious

types of data transfers which "would lead to the [implementation of] quarantine rules." J.A. 1512. Centripetal has not identified any evidence suggesting that *the quarantine rule* filters by "particular type of data transfer."

II

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

The district court found that the accused products do not infringe the asserted claims because they "cease [processing] . . . as a part of normal packet processing[,] . . . not in response to a signal to swap to a new rule set." J.A. 60–61. Centripetal argues that the district court must be reversed because "responsive to" only requires that "when the system receives a signal to perform a rule swap, it immediately proceeds to perform the entire rule-swapping sequence," Appellant's Br. 27, not that the signal be the but-for cause of each component part, such as "ceas[ing] processing." Nothing in the district court's opinion, J.A. 52–57, or anything Centripetal cites to us from its filings in the district court, indicates that Centripetal fairly presented the district court with this claim construction or argued that the plain and ordinary meaning leads to this interpretation of the claim (requiring causation of the sequence as a unit, but not of any individual component). *See* Appellee's Br. at 50 (asserting forfeiture of Centripetal's causation position at

Appellant's Br. at 27, 44); Appellant's Reply at 21–22 (not identifying where in the district court the position was presented). Under these circumstances, Centripetal forfeited this argument.

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

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

III

As to the '176 patent, Centripetal alleges Cisco's switches and routers, using a threat analysis program called Stealthwatch, infringe the asserted claims. Stealthwatch analyzes logs of packet information (called NetFlow logs) and sends alerts to a management console based on suspected malicious activity. The district court concluded that the accused products do not infringe the asserted claims because Centripetal failed to show that Cisco's technology "correlates the packets entering and exiting a network device" and "responsive to the correlating, . . . generates rules configured to identify packets in a specific network." J.A. 76. Centripetal argues the district

court's finding of noninfringement rests on erroneous factual findings. Again, we disagree.

The district court determined that Cisco's products do not infringe the '176 patent because they cannot correlate NetFlow records. Centripetal argues that the district court ignored evidence that the accused devices correlate logging records other than NetFlow records, namely Syslog and Webflow. But Centripetal conceded at the Rule 63 hearing that its infringement position was based on NetFlow records. J.A. 21464. ("I think the evidence shows that NetFlow data is what we're accusing of infringing."). And the district court cited ample evidence to support the conclusion that Cisco's products do not correlate ingress and egress NetFlow log entries. *See* J.A. 78–81. Even if we were to consider Centripetal's arguments based on Syslog and Webflow, these logging records are generated by proxy sources, not Cisco's switches and routers, *see* J.A. 75, 19969, 19979, and Centripetal's expert admitted that "we don't actually have a proxy in this case," J.A. 1978.[7]

The district court also did not err in concluding that Cisco's accused products do not satisfy the claim limitations because they require human intervention in determining whether to apply rules in particular situations. The asserted claims require that a "processor cause the system to: . . . generate . . . one or more rules" and "provision a device . . . with the one or more rules." '176 patent, claim 11. The specification further explains that the "packet correlator . . . may generate or update rule(s)" and "may provision [a] device . . . with rules." *Id.*, col. 13 ll. 14–19. The specification thus contemplates that the rules are automatically executed by the processor.

---

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

Stealthwatch does not issue rules, as the term was construed to require "a condition or set of conditions that when satisfied cause a specific function to occur." J.A. 9. Rather, as the district court found, Stealthwatch only issues *alerts* which advise individuals of potentially problematic situations. A human administrator must examine these alerts and determine whether to respond by issuing a quarantine tag. The district court did not clearly err in finding Cisco's technology does not perform these limitations of the asserted claims.

CONCLUSION

We conclude that the asserted claims of the '193 patent require filtering data at two stages, and the district court did not err in concluding that Cisco's accused products only perform filtering at the first stage. As to the '806 patent, we conclude that "responsive to" requires that the claimed signal be the but-for cause of "ceas[ing] processing" packets and, under this construction, the district court did not err in concluding that Cisco's accused products do not infringe the asserted claims. We also conclude that the district court did not err in concluding that Cisco's products do not perform every limitation of the asserted claims of the '176 patent. Accordingly, we affirm.

AFFIRMED

COSTS

Costs to Cisco.