NOTE: This disposition is nonprecedential.

United States Court of Appeals for the Federal Circuit

CENTRIPETAL NETWORKS, INC.,
Appellant

v.

CISCO SYSTEMS, INC.,
Appellee

2020-2057

Appeal from the United States Patent and Trademark Office, Patent Trial and Appeal Board in No. IPR2018-01760.

Decided: March 10, 2021

PAUL J. ANDRE, Kramer Levin Naftalis & Frankel LLP, Menlo Park, CA, for appellant. Also represented by JAMES R. HANNAH; CRISTINA MARTINEZ, JEFFREY PRICE, New York, NY.

PATRICK D. MCPHERSON, Duane Morris LLP, Washington, DC, for appellee. Also represented by PATRICK C. MULDOON, CHRISTOPHER JOSEPH TYSON; MATTHEW CHRISTOPHER GAUDET, Atlanta, GA; JOSEPH POWERS, Philadelphia, PA.

Before MOORE, SCHALL, and TARANTO, *Circuit Judges*.

TARANTO, *Circuit Judge*.

Centripetal Networks, Inc. owns U.S. Patent No. 9,413,722, which addresses "rule-based network-threat detection." '722 patent, col. 1, lines 45–46. In September 2018, Cisco Systems, Inc. petitioned for an inter partes review of all claims of the '722 patent, alleging that the claimed inventions in all claims (1–25) would have been obvious to a relevant artisan under 35 U.S.C. § 103 in view of a User Guide for the Sourcefire 3D System—a manual the parties have called "Sourcefire." That reference is also before us in *Centripetal Networks, Inc. v. Cisco Systems, Inc.*, Fed. Cir. Nos. 20-1635, -1636, which involves other Centripetal patents and which we decide today (*20-1635 Decision*). A common issue in this matter and in our *20-1635 Decision* is whether Sourcefire was a "printed publication[]" under 35 U.S.C. § 311(b). A distinct issue here is whether Sourcefire teaches identifying "network-threat indicators" as required by the '722 patent's claims.

The Patent Trial and Appeal Board instituted an inter partes review, and in May 2020, it ruled that Sourcefire was a printed publication and that the claimed inventions in claims 1–7, 10–12, 14–21, 24, and 25 in the '722 patent would have been obvious to a relevant artisan in view of Sourcefire. *Cisco Systems, Inc. v. Centripetal Networks, Inc.*, IPR2018-01760, 2020 WL 2549613 (P.T.A.B. May 18, 2020) (*Board Decision*). Centripetal appeals. We have jurisdiction under 28 U.S.C. § 1295(a)(4). We affirm.

I

A

Unauthorized requests for data and large volumes of network traffic are two examples of what the '722 patent calls "network threats" to the Internet. *See* '722 patent, col.

1, lines 16–19. Information about such threats, the patent says, was traditionally compiled by an organization's network devices into "logs," which were then reviewed for "data corresponding to the network-threat indicators provided by [network-threat] services." *Id.*, col. 1, lines 24–29. The patent asserts that because these logs were "generated based on the traffic processed by the network devices without regard to the network-threat indicators," reviewing them was "time consuming" and "exacerbated by the continuously evolving nature of potential threats." *Id.*, col. 1, lines 29–34.

The '722 patent proposes an improvement in the form of a "rule-based network-threat detection" system using a "packet-filtering device" that receives data packets traveling through the Internet and determines whether each packet "corresponds to criteria specified by a packet-filtering rule." *Id.*, col. 1, lines 45–52. The criteria in each rule may "correspond to one or more of the network-threat indicators." *Id.*, col. 1, lines 52–53. Network-threat indicators may include "network addresses, ports, fully qualified domain names (FQDNs), uniform resource locators (URLs), [and] uniform resource identifiers (URIs)" that are "associated with . . . network threats," such as phishing malware. *Id.*, col. 3, lines 18–33.

Packet-filtering rules also specify an "operator," which is "configured to cause packet-filtering device 144 to either prevent packets corresponding to the criteria from continuing toward their respective destinations (e.g., a BLOCK operator) or allow packets corresponding to the criteria to continue toward their respective destinations (e.g., an ALLOW operator)." *Id.*, col. 5, lines 13–24. In addition to allowing and blocking packets, the packet-filtering device "generate[s] a log entry comprising information from the packet-filtering rule," including information about (1) whether the packets corresponded to "one or more network-threat indicators" and (2) whether the packet-filtering device allowed the packet to continue or blocked it from

reaching its destination. *Id.*, col. 16, lines 8–19. The packet-filtering device communicates such information to a "user device," *id.*, col. 16, lines 22–24, which permits a user to alter the rules based on the log information by "instruct[ing] the packet-filtering device to reconfigure the operator" so that, for example, the operator "prevent[s] future packets corresponding to the criteria from continuing toward their respective destinations," *id.*, col. 2, lines 1–10. *See also id.*, Fig. 7 (depicting an example of the rules-based network-threat detection system).

Claim 1 is representative and recites:

> 1. A method comprising:
>
> *receiving, by a packet-filtering device, a plurality of packet-filtering rules configured to cause the packet-filtering device to identify packets corresponding to at least one of a plurality of network-threat indicators*;
>
> receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;
>
> responsive to a determination by the packet-filtering device that the first packet satisfies one or more criteria, specified by a packet-filtering rule of the plurality of packet-filtering rules, that correspond to one or more network-threat indicators of the plurality of network-threat indicators:
>
> > applying, by the packet-filtering device and to the first packet, an operator specified by the packet-filtering rule and configured to cause the packet-filtering device to allow the first packet to continue toward a destination of the first packet;
> >
> > communicating, by the packet-filtering device, information from the packet-filtering

rule that identifies the one or more network-threat indicators, and data indicative that the first packet was allowed to continue toward the destination of the first packet;

causing, by the packet-filtering device, and in an interface, display of the information in at least one portion of the interface corresponding to the packet-filtering rule and the one or more network-threat indicators;

receiving, by the packet-filtering device, an instruction generated in response to a user invoking an element in the at least one portion of the interface corresponding to the packet-filtering rule and the one or more network-threat indicators; and

responsive to receiving the instruction:

modifying, by the packet-filtering device, at least one operator specified by the packet-filtering rule to reconfigure the packet-filtering device to prevent packets corresponding to the one or more criteria from continuing toward their respective destinations; and

responsive to a determination by the packet-filtering device that the second packet corresponds to the one or more criteria:

preventing, by the packet-filtering device, the second packet from continuing toward a destination of the second packet;

> communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and
>
> causing, by the packet-filtering device and in the interface, display of the data indicative that the second packet was prevented from continuing toward the destination of the second packet.

Id., col. 17, line 16 through col. 18, line 2 (emphasis added). Centripetal raises no arguments on appeal with respect to limitations in the dependent claims. The only claim limitation at issue on appeal is the "network-threat indicator" limitation emphasized above. *See* Centripetal Opening Br. 12–13; *see also* Cisco Response Br. 32 & n. 7.

B

Cisco's petition for an inter partes review relied on Sourcefire, which is the user guide for the Sourcefire company's network security system. It was distributed on a CD-ROM to all customers who purchased certain Sourcefire products. Sourcefire customers, with a password, could also access and download the User Guide on the Sourcefire company's website. J.A. 3161 ¶ 11.

According to Sourcefire (the document), the Sourcefire system provides users with "real-time network intelligence for real-time network defense" through the use of packet-filtering devices called "3D Sensors." J.A. 1064–65. Each sensor can run Sourcefire's "Intrusion Prevention System" (IPS) to detect and prevent potential threats using a "rules-based detection engine" that permits a user to develop custom "intrusion rules" in order to "detect the attacks [the

user] think[s] most likely to occur." J.A. 1065–66. Users can select, customize, and manage intrusion rules across all the Sourcefire system's sensors via a centralized "Defense Center." J.A. 1066; *see also* J.A. 1297–98.

An intrusion rule includes a rule header that consists of parameters and their associated "arguments," including 5-tuple rule criteria values (protocol, source and destination Internet Protocol (IP) addresses, and source and destination ports). J.A. 1796. The 5-tuple values, Sourcefire explains, are useful for detecting "intrusion event[s]" (potential security concerns generating a response by the system), such as multiple failed log-in attempts to the network's server from an unknown IP address. J.A. 1471; *see also* J.A. 1793. Rule headers also include "rule actions," *e.g.*, "drop," "pass," and "alert," which is the action taken by the rules engine if it encounters packets that meet the criteria specified in the rule header. J.A. 1797. "Drop" actions block packets from continuing to their destinations, "pass" actions permit the packets to continue without interruption, and "alert" actions generate reports of "intrusion event[s]" while typically allowing packets to continue. J.A. 1793, 1797. Intrusion rules may also include a "rule options" part, containing "keywords" and their associated "arguments." J.A. 1794–95, 1801. Users may add arguments that, for example, apply the intrusion rule only to certain uniform resource identifiers (URIs). J.A. 1795.

After the Board instituted the requested inter partes review, Centripetal argued that Sourcefire was not qualifying prior art under 35 U.S.C. § 311(b) because it was not a "printed publication." J.A. 387–94. In particular, Centripetal contended that Sourcefire would not have been publicly accessible to interested persons of skill in the art because (1) the user manual is kept on a password-protected website and only available to Sourcefire purchasers,

J.A. 387–89, and (2) the Sourcefire product was costly, with a purchase price of up to $25,000, J.A. 392–94.[1]

As to what Sourcefire teaches, Centripetal disputed Cisco's contention that Sourcefire teaches the "network-threat indicators" recited in the claims. *See* J.A. 416–30. Specifically, Centripetal argued that rule headers do not identify *specific* threats coming from, *e.g.*, a certain IP address "associated with a network threat." J.A. 416–17, 424–26. Rather, Centripetal argued, the IP address in the Sourcefire rule header is merely a "source IP address" that permits packets associated with trusted networks to pass without inspection, J.A. 416–17, and Sourcefire's rule header functions only to "restrict packet inspection" and "reduce false positives" by identifying the packets that are safe and allowing them to pass, rather than identifying IP addresses associated with specific network threats, J.A. 416–17, 424–26. Further, Centripetal argued, the "rule options" function of Sourcefire does not teach identifying network-threat indicators, because keywords and their associated arguments identify suspicious *content* associated with data packets, rather than data packets with suspicious *identifiers*. J.A. 428–30.

Finally, Centripetal presented objective indicia of nonobviousness. J.A. 442–48. Specifically, Centripetal argued that the '722 patent "satisfied a long-felt need in the industry," which was "how to operationalize threat intelligence to proactively identify network threats." J.A. 443. It

---

[1] The priority date for the '722 patent is in April 2015, so that the "printed publication" language of 35 U.S.C. § 102(a)(2) applies in this matter. *See Board Decision*, 2020 WL 2549613, at *1 n.1. The parties accept that the standards governing that phrase are the same, at least for present purposes, as the standards governing the same phrase in 35 U.S.C. § 102(b) (2006), applicable in our *20-1635 Decision*.

pointed to a paper entitled "Centripetal Networks Threat Intelligence Gateway: Designed to Enable Continuous Prevention Through Intelligence-led Enforcement" (the ESG paper), which praised Centripetal's products, including its Threat Intelligence Gateway (RuleGATE) for "converting indicators to rules that drive actions," and thereby "deliver[ing] more than [was] possible with firewalls and IPS systems." J.A. 444–48 (citing J.A. 6688). Centripetal also presented a 2017 Gartner article that praised Centripetal as being "'unique in its ability to instantly detect and prevent malicious network connections based on millions of threat indicators at 10-gigabit speeds.'" J.A. 448 (quoting J.A. 6695).

C

In its final written decision, the Board held claims 1–7, 10–12, 14–21, 24, and 25 of the '722 patent to be unpatentable for obviousness in view of Sourcefire. *See Board Decision*, 2020 WL 2549613, at *23.[2] The Board concluded that Cisco had shown Sourcefire to be a printed publication at the relevant time. *See id.*, 2020 WL 2549613, at *5–8. The reasons are materially identical to those the Board relied on in the separate final written decisions we affirm in today's *20-1635 Decision*.

Next, the Board considered whether Sourcefire teaches the claim limitation requiring "receiving, by a packet-filtering device, a plurality of packet-filtering rules configured to cause the packet-filtering device to identify packets corresponding to at least one of a plurality of network-threat indicators." *Board Decision*, 2020 WL 2549613, at *8–12. It found that Sourcefire teaches a "packet-filtering device"

---

[2] The Board ruled that Cisco did not show unpatentability as to claims 8, 9, 13, 22, and 23. *Board Decision*, 2020 WL 2549613, at *23. Cisco has not appealed that ruling.

(the 3D Sensor with IPS), which receives "packet-filtering rules" (intrusion rules) that can specify "source and destination IP addresses," "source and destination ports," and "keywords and their parameters and arguments" to allow users to, *e.g.*, "restrict packet inspection to the packets originating from specific IP addresses." *Id.* at *9 (internal quotation marks omitted); *see also* J.A. 1794, 1798–99. Thus, the Board determined that Sourcefire teaches packet-filtering rules "'configured to cause the packet-filtering device to identify packets corresponding to,' for example, specific source IP addresses." *Board Decision*, 2020 WL 2549613, at *9.

The Board then rejected Centripetal's argument that Sourcefire does not teach the "network-threat indicators" recited in the claims. *Id.* It construed "network-threat indicator" to mean an "indicator that represents the identity of a resource associated with a network threat." *Id.* at *3–4, *9. Noting that Sourcefire teaches using intrusion rules to identify "exploits" and malicious activity by examining packets, *see* J.A. 1793–94, the Board found that a relevant artisan would have understood that intrusion rules could be written to identify specific network threats on the basis of the source IP address being a suspicious one. *Board Decision*, 2020 WL 2549613, at *9 (citing J.A. 980–81 ¶¶ 114–16). The Board "note[d] that the Specification of the '722 Patent itself identifies 'network addresses' associated with network threats as examples of 'network-threat indicators.'" *Id.* (citing '722 patent, col. 3, lines 23–24).

Finally, the Board considered Centripetal's objective indicia of non-obviousness and found that the evidence was not entitled to substantial weight. *Id.* at *17–19. The Board found that Centripetal had presented no evidence to show that its RuleGATE product was coextensive with the '722 patent's claims. *Id.* at *18 (citing *Fox Factory, Inc. v. SRAM, LLC*, 944 F.3d 1366, 1373 (Fed. Cir. 2019)). It also found that Centripetal had not shown how the cited praise for its products related to the claim limitations, rejecting

conclusory expert statements as unpersuasive. *Id.* at *18–19. For those reasons, the Board concluded that the objective-indicia evidence was not entitled to substantial weight. *Id.* at *20.

II

We review the Board's legal conclusions de novo and factual findings for substantial evidence. *Nobel Biocare Services AG v. Instradent USA, Inc.*, 903 F.3d 1365, 1374 (Fed. Cir. 2018). Whether a reference qualifies as a "printed publication" is a legal conclusion based on factual findings. *Jazz Pharms., Inc. v. Amneal Pharms., LLC*, 895 F.3d 1347, 1356 (Fed. Cir. 2018). "The underlying factual findings [in a printed-publication analysis] include whether a reference was publicly accessible." *Nobel*, 903 F.3d at 1375. Similarly, the ultimate determination of whether a claimed invention would have been obvious is a legal one reviewed de novo, but underlying factual determinations are reviewed for substantial-evidence support. *PersonalWeb Techs., LLC v. Apple, Inc.*, 917 F.3d 1376, 1381 (Fed. Cir. 2019).

Centripetal argues that the Board (1) erred in concluding that Sourcefire was a printed publication, *see* Centripetal Opening Br. 19–26; (2) misapplied the claim construction it adopted for "network-threat indicator" in analyzing whether Sourcefire teaches this limitation, *id.* at 27–35; and (3) failed to give due weight to the objective indicia of non-obviousness, *id.* at 35–42. We reject these challenges to the Board's obviousness determination.

A

Centripetal first argues that Sourcefire was not a printed publication. Centripetal's arguments and the Board's analysis are materially the same as those in *20-1635 Decision*, where we upheld the Board's determination that Sourcefire was a printed publication. Centripetal has made no argument here that warrants separate discussion.

We rely on our discussion in *20-1635 Decision* to affirm the Board's ruling as to Sourcefire's qualification as a printed publication here.[3]

B

Centripetal argues that the Board's finding that Sourcefire teaches filtering packets based on the "network-threat indicators" required by the claims was unsupported by substantial evidence. In advancing this argument, Centripetal essentially contends that Sourcefire does not teach using a source-identifier (like an IP address) to identify threats, but only to "restrict inspection" of packets with benign IP addresses (*i.e.*, to generate "whitelists"). Centripetal Opening Br. 27.

The Board reasonably found otherwise. *Board Decision*, 2020 WL 2549613, at *9–10. Sourcefire teaches users how to write custom intrusion rules that "detect specific exploits" and "target traffic that may attempt to exploit known vulnerabilities," J.A. 1794, by using rule headers and keywords to filter packets based on 5-tuple values, which include source identifiers, *see* J.A. 1796–1801. Although Sourcefire expressly identifies creating whitelists as one potential intrusion rule, *see* J.A. 1798, the Board had a sufficient basis for finding that Sourcefire's teaching was not limited to use of the source identifier for that purpose. "Sourcefire indicates intrusion rules are used to identify 'exploits' from attackers such that 3D Sensors employing those rules examine packets for 'malicious activity.'" *Board*

---

[3] In our *20-1635 Decision*, we affirmed the Board's determination that Sourcefire was publicly accessible, and therefore a printed publication, as of the March 2013 priority date of the patents at issue there. Here, the priority date is two years later. Centripetal has not denied that public accessibility before March 2013 entails public accessibility before April 2015.

Decision, 2020 WL 2549613, at *9 (quoting J.A. 1066, 1793). Sourcefire teaches rules that "alert," "pass," or "drop." J.A. 1793; *see Board Decision*, 2020 WL 2549613, at *8–9 (citing J.A. 1793; agreeing with Cisco's description of Sourcefire as teaching, among other things, "passing or dropping," with Cisco citing J.A. 1794–801). And Cisco's expert explained that Sourcefire teaches the use of source IP addresses (among other information in the rule header) as a network-threat indicator for triggering of a rule to allow, drop, or alert. J.A. 980–81 ¶¶ 114–16, cited in *Board Decision*, 2020 WL 2549613, at *9.

Nor did the Board "raise, address, and decide unpatentability theories never presented by [Cisco] and not supported by record evidence," as Centripetal contends. *In re Magnum Oil Tools Int'l Ltd.*, 829 F.3d 1364, 1381 (Fed. Cir. 2016). In its petition, Cisco argued that Sourcefire teaches using its system to write packet-filtering rules that "identify packets including data (*e.g.*, 5-tuple, application layer data) corresponding to characteristics associated with malicious activities," J.A. 213, and that those rules can be triggered by "source or destination IP addresses," causing the system to "allow, drop, [or] alert," J.A. 214. We see no significant disparity between Cisco's argument in its petition and the relevant part of the Board's rationale.

Accordingly, we affirm the Board's finding that a relevant artisan would have understood Sourcefire to teach the claim-required filtering packets on the basis of network-threat identifiers as required by the challenged claims.

C

Finally, Centripetal argues that the Board failed to give due weight to evidence of a long-felt but unmet need for proactively identifying network threats, Centripetal Opening Br. 35–39, as well as industry praise for its product, *id.* at 40–42. We disagree.

"In order to accord substantial weight to secondary considerations in an obviousness analysis, 'the evidence of secondary considerations must have a "nexus" to the claims, *i.e.*, there must be "a legally and factually sufficient connection" between the evidence and the patented invention.'" *Fox Factory*, 944 F.3d at 1373 (quoting *Henny Penny Corp. v. Frymaster LLC*, 938 F.3d 1324, 1332 (Fed. Cir. 2019) (citing *Demaco Corp. v. F. Von Langsdorff Licensing Ltd.*, 851 F.2d 1387, 1392 (Fed. Cir. 1988)). With respect to long-felt but unmet need, Centripetal focuses on the fact that the ESG paper discusses the need for "cyber threat intelligence" and systems that can use such intelligence on a large scale when detecting network threats. J.A. 6684. Centripetal contends that these issues are identified in the Background of the '722 patent, *see* '722 patent, col. 1, lines 24–33, and that the ESG paper is thus evidence that the '722 patent solved longstanding problems in cybersecurity. It also points to language in the ESG paper stating that Centripetal achieved "customized threat intelligence" on a large scale by "converting indicators to rules that drive actions across a risk spectrum." J.A. 6688.

The Board reasonably found the evidence not to establish a nexus between the claimed features in the challenged claims of the '722 patent and the ESG Paper's description of the benefits provided by the RuleGATE product. Here, Centripetal presented no non-conclusory evidence tying the statements in the ESG Paper about "driv[ing] actions across a risk spectrum" specifically to the limitations in the claims. *Board Decision*, 2020 WL 2549613, at *18.

Centripetal also did not supply the needed nexus for its cited industry praise. The Gartner article praises Centripetal's product as being "unique in its ability to instantly detect and prevent malicious network connections based on millions of threat indicators in 10-gigabit speeds." J.A. 6695. Centripetal also identifies a designation by American Bankers as a "Top Ten FinTech Compan[y] to Watch" praising RuleGATE for its scale and for its ability to

"compare[] incoming traffic against millions of rules and policies informed by analytics on known 'bad guys.'" J.A. 6732, 6745–47. Centripetal's expert added a sentence, following his description of those passages, stating that, "[a]s discussed directly above, the salutary benefits of Centripetal's [RuleGATE] product discussed in the ESG Paper and the [Gartner] article are made possible in large part by the '722 Patent's packet-filtering rules, which transform network-threat indicators into actionable rules." J.A. 6563 ¶ 123.

The Board reasonably found this evidence insufficient to establish the required nexus. The documents themselves do not meaningfully tie the benefits to the claim limitations. And the assertion by Centripetal's expert is an unelaborated conclusion, which the Board could and did reject as insufficient for that reason. *Board Decision*, 2020 WL 2549613, at *19.

III

We have considered the remainder of Centripetal's arguments and find them unpersuasive. For the foregoing reasons, the decision of the Patent Trial and Appeal Board is affirmed.

AFFIRMED