NOTE: This disposition is nonprecedential.

United States Court of Appeals for the Federal Circuit

CENTRIPETAL NETWORKS, LLC,
Appellant

v.

PALO ALTO NETWORKS, INC.,
Appellee

2023-1654, 2023-1655

Appeals from the United States Patent and Trademark Office, Patent Trial and Appeal Board in Nos. IPR2021-01147, IPR2021-01148.

Decided: October 31, 2024

JAMES R. HANNAH, Kramer Levin Naftalis & Frankel LLP, Redwood Shores, CA, argued for appellant. Also represented by PAUL J. ANDRE; JEFFREY PRICE, New York, NY; JOHN R. HUTCHINS, SCOTT M. KELLY, BRADLEY CHARLES WRIGHT, Banner & Witcoff, Ltd., Washington, DC.

DOUGLAS HALLWARD-DRIEMEIER, Ropes & Gray LLP, Washington, DC, argued for appellee. Also represented by RYAN C. BRUNNER; JAMES RICHARD BATCHELDER, ANDREW T. RADSCH, East Palo Alto, CA.

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

TARANTO, *Circuit Judge*.

Centripetal Networks, LLC owns U.S. Patent Nos. 10,542,028 and 10,757,126, both titled "Rule-Based Network-Threat Detection." Palo Alto Networks, Inc. (PAN) petitioned the Patent and Trademark Office (PTO) to institute inter partes reviews of all the claims of the '028 and '126 patents, alleging unpatentability for obviousness under 35 U.S.C. § 103 in view of a reference called the Sourcefire 3D System User Guide (Sourcefire), alone or in combination with another reference not at issue on appeal. The PTO's Patent Trial and Appeal Board, acting for the PTO Director, instituted the requested reviews, and after conducting the reviews, the Board concluded that all the challenged claims were unpatentable under § 103. J.A. 1–48, 49–92; *see Palo Alto Networks, Inc. v. Centripetal Networks, LLC*, No. IPR2021-01147, 2023 WL 1861774 (P.T.A.B. Feb. 9, 2023) (*'028 Decision*).[1]

Centripetal timely appealed in both matters, and we consolidated the appeals. We have jurisdiction under 28 U.S.C. § 1295(a)(4)(A). We affirm.

I

A

The common specification of the two patents at issue proposes an improved way of detecting "[n]etwork threats,"

---

[1] The decision in IPR2021-01148, concerning the '126 patent, does not appear in Westlaw. It is materially the same as the decision in IPR2021-01147 with respect to the issues presented on appeal. The patents also share a specification. We therefore generally limit our citations to the '028 patent and the decision about that patent.

such as "viruses, malware, [and] large volumes of network traffic designed to overwhelm network resources," and compiling "logs" of information about such threats. '028 patent, col. 1, lines 19–37. The patents disclose the use of a "packet-filtering device" that receives data packets and determines whether each packet satisfies "criteria specified by a packet-filtering rule." *Id.*, col. 1, lines 53–55. The criteria may correspond to one or more "network-threat indicators," *id.*, col. 1, lines 55–57; *id.*, col. 3, line 27, "e.g., network addresses, ports, fully qualified domain names (FQDNs), uniform resource locators (URLs), uniform resource identifiers (URIs), or the like," *id.*, col. 3, lines 27–30.

If a packet-filtering rule is triggered, further actions follow. The device may apply an "operator" (specified by that rule) that either allows or prevents the packet's continued progress to its destination. *Id.*, col. 1, lines 57–61. The device may also generate a log entry with information about the network-threat indicator(s) associated with the packet and the action that was taken regarding the packet. *Id.*, col. 1, lines 61–67.

Representative claim 1 of the '028 patent states in relevant part:

> 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, wherein the plurality of network-threat indicators are associated with network-threat-intelligence reports supplied by one or more independent network-threat-intelligence providers;

> receiving, by the packet filtering device, a plurality of packets that comprises a first packet and a second packet;
>
> *responsive to a determination by the packet filtering device that the first packet satisfies a first packet filtering rule, of the plurality of packet filtering rules, based on one or more network-threat indicators, of the plurality of network-threat indicators, specified by the first packet filtering rule*:
>
> > applying, by the packet filtering device and to the first packet, an operator specified by the first 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; and
> >
> > communicating, by the packet filtering device, information 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;
>
> . . . .

'028 patent, col. 17, line 47, through col. 18, line 7 (emphasis added). The claim limitation at issue is the "responsive to" limitation emphasized above.

B

The Sourcefire reference is a User Guide for the Sourcefire 3D System, a network security system that allows monitoring for and defending against attacks on the user's network using a "3D Sensor" with an "Intrusion Prevention System" component. J.A. 1275, 1306–09. The sensor equipped with that component ("Sourcefire 3D

Sensor") uses "intrusion rules" to analyze network traffic and to log "intrusion events." J.A. 2035. The user can customize the intrusion rules and manage them through a centralized "Defense Center." J.A. 1308.

An intrusion rule has two logical sections: a Rule Header and Rule Options. J.A. 2036. The Rule Header contains "information such as the source and destination ports and IP addresses." J.A. 2135; *see also* J.A. 2036–43. The Rule Header also "specifies the action the system takes when a packet triggers a rule." J.A. 2039. The Rule Options section allows the user to enter "[k]eywords and their associated values (called *arguments*)" to control how the system evaluates data packets. J.A. 2043; *see also* J.A. 2044–45. The relevant portions of the user guide included in the record on appeal do not state that the user must specify keywords and arguments. J.A. 2043–46, 2050–51, 2135–38.

To determine if a data packet poses a network threat, a component of the Sourcefire 3D Sensor will "check if it matches the criteria in the [intrusion] rule." J.A. 2035. All the criteria for a rule must be satisfied for that rule to trigger. J.A. 2035 ("[The Sourcefire 3D Sensor] compares packets against the conditions specified in each rule and, if the packet data matches all the conditions specified in a rule, the rule triggers."). Rules may specify different actions to occur upon their triggering. "If a rule is an *alert rule*, it generates an intrusion event. If it is a *pass rule*, it ignores the traffic. [The user] can view and evaluate intrusion events from the 3D Sensor web interface or . . . from the Defense Center web interface." J.A. 2035; *see also* J.A. 2039.

C

In March 2021, Centripetal sued PAN in the district court, alleging infringement of the '028 and '126 patents. In July 2021, PAN petitioned for institution of inter partes reviews of all the claims of the '028 and '126 patents. For

each patent, the Board instituted an inter partes review in February 2022 and issued a final written decision on February 9, 2023, determining that all claims were unpatentable for obviousness.

As relevant to this appeal, the Board addressed the proper construction of the "responsive to" phrase. It quoted Centripetal's arguments: that "the 'responsive to' language requires the applying and communicating steps to 'be performed *in reaction to* a packet satisfying a packet-filtering rule based on network-threat indicators . . .'"; and that "this language 'establishes a *clear cause-and-effect relationship* between (i) a packet satisfying a packet-filtering rule . . . and (ii) the subsequent application of an operator that allows the packet and communication of data indicating the packet was allowed.'" *'028 Decision*, at *7 (quoting J.A. 537) (emphases added). The Board then noted that "Petitioner does not otherwise challenge Patent Owner's construction of 'responsive to,' primarily disputing Patent Owner's characterization of the prior art with respect to this limitation." *Id.* "To the extent interpretation of this term is necessary," the Board stated, "we consider the meaning of the claim language in the context of determining whether the prior art teaches or suggests the limitations at issue." *Id.*

The Board determined that Sourcefire rendered Centripetal's claims obvious. *Id.* at *7–18. The Board found that Sourcefire "teaches or suggests" the "responsive to" limitation based on two subsidiary findings. *Id.* at *12. First, the Board found that "[w]hen a rule includes conditions in both its header and options section, Sourcefire teaches that a packet must match all the conditions specified in a rule to trigger the rule and perform the operator specified in the rule." *Id.* Because those conditions include "source and destination IP addresses in the rule header (and any criteria in the rule options section)," the Board found "that Sourcefire's 3D Sensor makes a 'determination' that a packet satisfies the

rule 'based on' one or more of those source and destination IP addresses (i.e., the claimed network-threat indicators), as required by [the 'responsive to'] limitation." *Id.* Second, the Board found that Sourcefire "teaches applying an operator and communicating information 'responsive to' the determination that a packet satisfies the rule based on the source and destination IP addresses." *Id.* "[W]hen a Sourcefire rule contains conditions in addition to IP addresses in the rule header, the operator is applied when the packet matches all the conditions." *Id.* The Board determined that the "'applying' step is 'responsive to' a determination that the packet satisfies the rule, thus meeting the requirements of the claim." *Id.*

II

We decide the correctness of the Board's legal determinations *de novo*, and we review the Board's factual findings for substantial-evidence support. *See*, *e.g.*, *Nobel Biocare Services AG v. Instradent USA, Inc.*, 903 F.3d 1365, 1374 (Fed. Cir. 2018) (citation omitted). "A finding is supported by substantial evidence if a reasonable mind might accept the evidence to support the finding." *Id.* (citing *Consolidated Edison Co. v. National Labor Relations Board*, 305 U.S. 197, 229 (1938)). We review "the Board's ultimate claim constructions and any supporting determinations based on intrinsic evidence" without deference, whereas "[w]e review any subsidiary factual findings involving extrinsic evidence for substantial evidence." *Personalized Media Communications, LLC v. Apple Inc.*, 952 F.3d 1336, 1339 (Fed. Cir. 2020) (citation omitted). We review the Board's ultimate determination of obviousness without deference, and we review the underlying factual determinations for substantial evidence. *Personal Web Technologies, LLC v. Apple, Inc.*, 848 F.3d 987, 991 (Fed. Cir. 2017).

On appeal, Centripetal argues that the Board impermissibly declined to construe the "responsive to"

phrase, ignored the proper understanding of the "based on one or more network-threat indicators" language within the "responsive to" limitation, and erred in finding that Sourcefire taught the "responsive to" limitation. In addition, Centripetal argues that the Board misconstrued the claim term "comprising," an argument dependent for significance on adopting Centripetal's view of the "responsive to" limitation. PAN argues that issue preclusion (collateral estoppel) bars Centripetal from relitigating the Board's previous factual findings about the teachings of Sourcefire.

We hold that the Board did construe "responsive to" in the respect at issue and that the Board was correct in understanding the "responsive to" phrase and the "responsive to" limitation to allow the "applying" and "communicating" steps to be performed in reaction to a determination that a packet satisfies a packet-filtering rule based on network-threat indicators *as well as* other criteria. Under that construction, the Board had substantial evidence to find that Sourcefire taught the limitation, and its determination of obviousness is correct on that basis. Given those conclusions on our part, we need not reach the parties' arguments regarding the term "comprising" and issue preclusion.

A

Regarding claim construction, we follow the established principle that "[w]e may affirm an agency ruling if we may reasonably discern that it followed a proper path, even if that path is less than perfectly clear." *Ariosa Diagnostics v. Verinata Health, Inc.*, 805 F.3d 1359, 1365 (Fed. Cir. 2015) (citing *Bowman Transportation, Inc. v. Arkansas-Best Freight System, Inc.*, 419 U.S. 281, 285–86 (1974)). Discerning the path followed is made more difficult when, as occurred here, claim construction and application are not clearly separated—sometimes difficult enough to warrant a remand to avoid judicial

encroachment on agency discretion. In this case, however, the construction adopted and applied is ultimately clear, and we can assess both the construction and its application.

When the Board summarized Centripetal's proposed construction of "responsive to" as meaning "in reaction to," or having "a clear cause-and-effect relationship," which PAN did not oppose, the Board did not reject Centripetal's proposal. *'028 Decision*, at *7. Instead, it referred forward, for any necessary interpretation, to its upcoming discussion of the application of the claim limitation to Sourcefire. *Id.* We have recognized an application discussion to sometimes be the locus of what amounts to a claim construction in Board opinions. *See*, *e.g.*, *HTC Corp. v. Cellular Communications Equipment, LLC*, 877 F.3d 1361, 1367 (Fed. Cir. 2017); *Network, LLC v. Centraal Corp.*, 242 F.3d 1347, 1355–56 (Fed. Cir. 2001). And in the present matter, the Board's discussion of Sourcefire establishes an interpretation—one elaborating on (and not inconsistent with) the "in reaction to" and "cause-and-effect" language the Board earlier quoted from Centripetal without disapproval—namely, that being "responsive to" a source indicating a network threat includes deciding on an action to take based on that source information *in combination with* other possible criteria. *'028 Decision*, at *12.

That interpretation, we conclude, is correct. Centripetal's contention is that this limitation requires the "applying" and "communicating" steps to be triggered by a determination that a packet-filtering rule is satisfied based on network-threat indicators *and no other criteria*, *i.e.*, on network-threat indicators alone. That contention is unpersuasive.

The words of a patent claim are generally given their ordinary and customary meaning as understood by a relevant artisan at the time of the invention and in the

context of all the intrinsic evidence. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) (en banc). As a matter of ordinary and customary meaning, if an action is taken in reaction to the satisfaction of a rule with two criteria, then the action is taken "based on" each of the two criteria. We have recognized this common English-language point in a recent opinion. *See Masimo Corp. v. Sotera Wireless, Inc.*, No. 2022-1415, 2023 WL 6307959, at *2 (Fed. Cir. Sept. 28, 2023) (non-precedential) ("We agree with the Board that the plain meaning of 'based on' . . . [is] broad, and this broad claim language does not exclude the use of . . . other conditions to trigger an alarm. . . . [I]n light of the plain meaning of the claim and the specification, the Board did not err in construing 'based on' . . . to mean a non-exclusive 'condition precedent' to the triggering of an alarm."). The asserted claims here do not include any limiting language, such as "only," as in "based *only* on one or more network-threat indicators," that would indicate that additional conditions cannot be considered. *See, e.g.*, *Strattec Security Corp. v. General Automotive Specialty Co.*, 126 F.3d 1411, 1418 (Fed. Cir. 1997) (determining that claim term "only four elements" was not literally infringed by activities involving a device with five elements). Centripetal has identified no intrinsic evidence, including the specification, that would indicate that the "responsive to" limitation should be read in a narrower way.

We therefore conclude that the Board correctly understood the "responsive to" limitation to be met when the "applying" and "communicating" steps are triggered by a determination that a packet satisfies a packet-filtering rule based on one or more network-threat indicators and additional criteria.

B

Under that construction, the Board's finding that Sourcefire teaches the "responsive to" limitation must be affirmed (and with it, the obviousness ruling). The Board

found that, in Sourcefire, a given intrusion rule is triggered when both the Rule Header—which can include IP addresses, which are undisputedly "network-threat indicators"—and any optional criteria in the Rule Options are satisfied. *'028 Decision*, at *11–12. Sourcefire supports that finding, as explained persuasively by the expert testimony from both parties. *See id.* at *12 ("As [PAN's expert] Dr. Lee explains, traffic matches a rule in Sourcefire when it 'match[es] all the conditions, in the rule header and also in the content, meaning the optional part.'"); *id.* ("Patent Owner's expert, Dr. Orso, agrees that '[i]f the rule header matches, and then the keywords and argument match, then the rule is triggered.'"). In its ruling on the '126 patent, the Board also noted Centripetal's own admission: "Patent Owner has acknowledged that Sourcefire uses a packet's IP address, i.e., a network-threat indicator, to determine whether to further evaluate a packet's contents." J.A. 77–78.

Centripetal's arguments on appeal regarding Sourcefire in large part repeat its claim-construction arguments, which we have already rejected. Centripetal contends that Sourcefire does not disclose the "responsive to" limitation, because the "IP addresses in the Rule Header are only used to determine whether to further evaluate a packet's contents against the keywords specified in those intrusion rules [by the Rule Options]," and "[a]ctions are not performed on packets in reaction to detecting any particular IP address," so "a packet can match the IP addresses in a rule header and *not* trigger a rule or generate an intrusion event (e.g., any time a packet's contents do not match all of the specified 'keywords and arguments')." Centripetal Opening Br. at 26. But that argument depends on the view that action must be triggered by particular IP addresses alone, without consideration of other criteria, which is the claim construction we have rejected. Centripetal does not argue that the Board lacked substantial evidence to find that

Sourcefire teaches instances where a rule *is* triggered when a Rule Header is satisfied (along with Sourcefire's other teachings).

III

We have considered Centripetal's remaining arguments and find them unpersuasive. The decisions of the Board are affirmed.

AFFIRMED