NOTE: This disposition is nonprecedential.

United States Court of Appeals for the Federal Circuit

CENTRIPETAL NETWORKS, LLC,
Appellant

v.

KEYSIGHT TECHNOLOGIES, INC.,
Cross-Appellant

2024-1406, 2024-1473

Appeals from the United States Patent and Trademark Office, Patent Trial and Appeal Board in No. IPR2022-01097.

Decided: April 23, 2026

JEFFREY B. WALL, Sullivan & Cromwell LLP, Washington, DC, argued for appellant. Also represented by DANIEL J. RICHARDSON; ANDREI IANCU, Los Angeles, CA; LAURIE STEMPLER, New York, NY; JAMES R. HANNAH, Herbert Smith Freehills Kramer (US) LLP, Redwood Shores, CA.

GERARD M. DONOVAN, Reed Smith LLP, Washington, DC, argued for cross-appellant. Also represented by JAMES CHRISTOPHER MARTIN, Pittsburgh, PA; JONAH D. MITCHELL, San Francisco, CA.

Before PROST, WALLACH, and STARK, *Circuit Judges*.

WALLACH, *Circuit Judge*.

Based on a petition filed by Keysight Technologies, Inc. ("Keysight"), the United States Patent and Trademark Office's Patent Trial and Appeal Board ("the Board") instituted inter partes review of claims 1–20 of U.S. Patent No. 10,193,917 ("the '917 Patent"). The Board found claims 1–3, 5–13, and 15–20 unpatentable for obviousness. J.A. 50. The Board found claims 4 and 14 not unpatentable for obviousness. J.A. 50. Centripetal Networks, LLC ("Centripetal"), appeals the Board's obviousness determinations as to claims 1–3, 5–13, and 15–20, and Keysight cross-appeals the Board's non-obviousness determination as to claims 4 and 14. We have jurisdiction under 28 U.S.C. § 1295(a)(4)(A). We affirm as to claims 1–3, 5–13, and 15–20 and we reverse as to claims 4 and 14.

BACKGROUND

I. The '917 Patent

Titled "Rule-Based Network-Threat Detection," the '917 Patent discloses a "packet-filtering device" that receives network packets and determines whether they correspond to criteria specified by a "packet-filtering rule." '917 Patent (Abstract). The packet-filtering rule criteria may correspond to one or more "network threat indicators." *Id.* The packet-filtering device applies an operator, specified by the packet-filtering rule, that allows it to either prevent or permit the packet to continue forward to its destination. *Id.* "The packet-filtering device may generate a log entry comprising information from the packet-filtering rule that identifies the one or more network-threat indicators and indicating whether the packet-filtering device prevented the packet from continuing toward its destination or allowed the packet to

continue toward its destination." *Id.* The packet-filtering device generates two types of log data—"packet log" data and "flow log" data. *Id.* at col. 6, ll. 29–32.

Figure 3F of the '917 Patent "depict[s] an illustrative event sequence for rule-based network-threat detection in accordance with one or more aspects of the disclosure." *Id.* at col. 2, ll. 28–29.

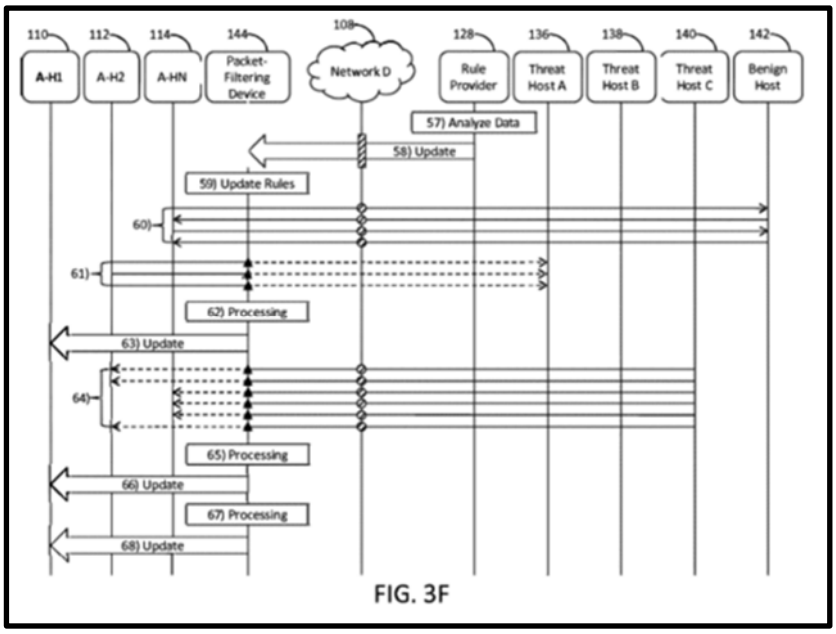


FIG. 3F

Id. at FIG. 3F. As the '917 Patent explains:

> At step 64, three packets destined for host 112 and three packets destined for host 114 are communicated by threat host 140, and packet-filtering device 144 may receive each of the six packets, apply one or more of packet-filtering rules 218 to the [six] packets, determine that each of the [six] packets corresponds to criteria specified by a packet-filtering rule of packet-filtering rules 404 (e.g., Rule: TI001), apply an operator specified by the packet-filtering rule (e.g., the BLOCK operator) to each of the six packets, prevent each of the six packets from continuing toward its respective

destination, and generate log data for each of the six packets.

Id. at col. 15 ll. 19–29.

At step 65, the packet-filtering device generates packet log entries (92 to 97) in packet log 502 for each of the six packets received in step 64. *Id.* at col. 15, ll. 33–35. This can be seen below in Figure 5F.

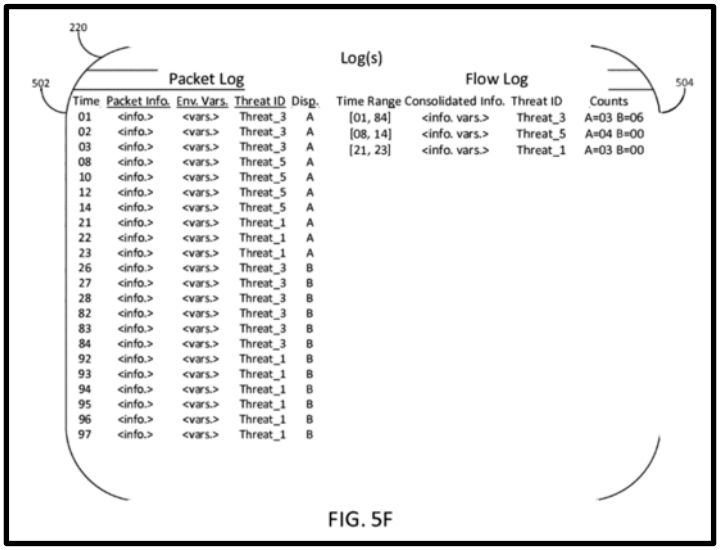


FIG. 5F

Id. at FIG. 5F. At step 67, the packet-filtering device continues to process the log data generated in step 64. *Id.* at col. 15, ll. 53–54. Referring to Figure 5G below, the packet-filtering device modifies an entry in flow log 504 for the packets received in step 64 based on the entries generated in the packet log (e.g., step 65), *id.* at col. 15, ll. 55–58, specifically, the "entry corresponding to Threat ID: Threat_1 (e.g., the time range and the count of associated packets prevented by packet-filtering device 144 from continuing toward their respective destinations)." *Id.* at col. 15, ll. 59–62.

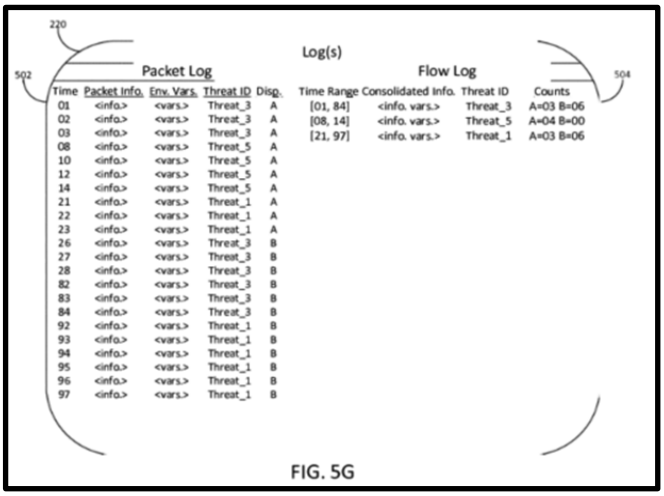


FIG. 5G

Id. at FIG. 5G.

Finally, at step 68, the packet-filtering device utilizes flow log 504 to generate data comprising an update for interface 600 and communicates the data to host 110. *Id.* at col. 15, ll. 63–65. Referring to Figure 6G below, the update causes interface 600 to update the entry in listing 606 associated with Threat ID: Threat_1 to reflect the six packets received in step 64 and a new score (e.g., 6). *Id.* at col. 15, l. 65–col. 16, l. 2.

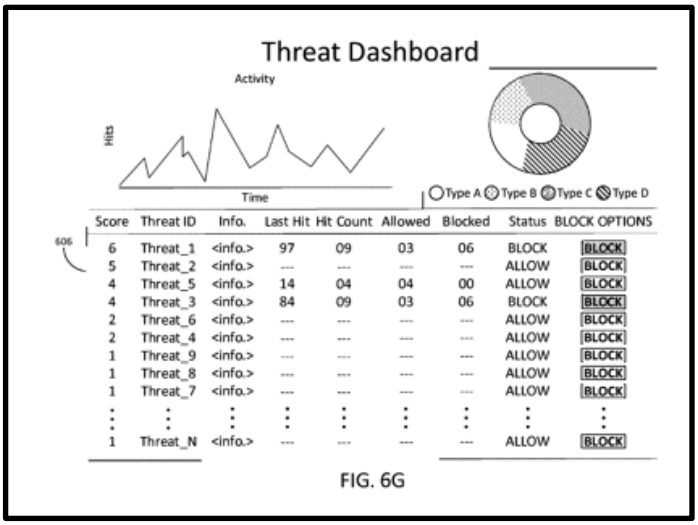


FIG. 6G

Id. at FIG. 6G.

Claim 1 is representative of the '917 Patent claims at issue[1] and recites:

> 1. A method comprising:
>
> receiving, by a packet-filtering device, a plurality of packets;
>
> responsive to a determination by the packet-filtering device that a first packet of the plurality of packets corresponds to one or more packet-filtering rules:
>
> applying, by the packet-filtering device and to the first packet, an operator specified by a corresponding packet-filtering rule and configured to cause the packet-filtering device to either prevent the first packet from continuing toward a destination of the first packet or allow the first packet to continue toward the destination of the first packet; and
>
> generating, by the packet-filtering device, a packet log entry comprising at least one threat identifier corresponding to the first packet and data indicating whether the packet-filtering device prevented the first packet from continuing toward the destination of the first packet or allowed the packet to continue toward the destination of the first packet;
>
> updating, by the packet-filtering device and based on the packet log entry, a packet flow entry, corresponding to the generated packet log entry, of packet flow analysis

---

[1] *See* Appellant Br. at Cover, Cross-Appellant Br. at Cover.

> data for a plurality of packet flow entries, and wherein each packet flow entry consolidates a plurality of packet log entries corresponding to a common threat identifier;
>
> communicating, by the packet-filtering device and to a computing device, the packet flow analysis data; and
>
> causing, based on the communicated packet flow analysis data, display of at least a portion of the packet flow analysis data,
>
> wherein the packet flow analysis data comprises at least one threat identifier corresponding to each of the plurality of logged packets, packet time data for packets corresponding to the packet flow entry, and data indicating whether the packet-filtering device prevented packets from continuing toward a respective destination or allowed packets to continue toward the respective destination.

Id. at Claim 1.

II. The Board Decision

The Board determined that Keysight met its burden of showing claims 1–3, 5, 11–13, 15, and 20 would have been obvious over Sourcefire alone and claims 6–10 and 16–19 would have been obvious over a combination of Sourcefire and Macaulay. J.A. 50. The Board also determined that Keysight did not meet its burden of showing claims 4 and 14 would have been obvious. J.A. 50.

A. Sourcefire

"Sourcefire is a user guide for the Sourcefire 3D system, a system that provides 'real-time network

intelligence for real-time network defense.'" J.A. 17 (citing J.A. 704). "The system operates via '3D Sensors' that can each run the Sourcefire 'Intrusion Prevention System' (IPS), which allows monitoring of networks for attacks by examining packets for malicious activity." J.A. 17 (citing J.A. 705–06). The "3D Sensors use 'detection engines' that 'analyze network traffic for evidence of attacks on network resources.'" J.A. 17 (citing J.A. 926). "When a packet travels over a segment monitored by a detection engine, the 3D Sensor analyzes it using a series of decoders and preprocessors and a rules engine." J.A. 17 (citing J.A. 926).

"Sourcefire users can create custom 'intrusion rules' to examine packets for attacks and manage the rules across all the 3D Sensors in the system through a centralized 'Defense Center.'" J.A. 17 (citing J.A. 706, 926). "An intrusion rule is a specified set of keywords and arguments on a 3D Sensor with the IPS component that detects attempts to exploit vulnerabilities on [a] network by analyzing network traffic to check if it matches the criteria in the rule." J.A. 1433; *see also* J.A. 17–18. "If a 'pass rule' is met, the network traffic in question is ignored (and allowed to continue)." J.A. 18 (citing 1433). "[I]f a 'drop rule' is met, the packet is dropped and an 'event' is generated." J.A. 18 (citing 1433).

"When a detection engine identifies a possible intrusion, it generates an intrusion event, which is a record indicating the date, time, the type of exploit, and contextual information about the source of the attack and its target." J.A. 926 (emphasis omitted); *see also* J.A. 18. "Intrusion events are added to a database, and reports of intrusion events can be displayed on a user interface." J.A. 18 (citation omitted). Referencing "Figure B, an annotated version of a screenshot of Sourcefire's 'table view of intrusion events,'" *see* J.A. 18, the Board explained:

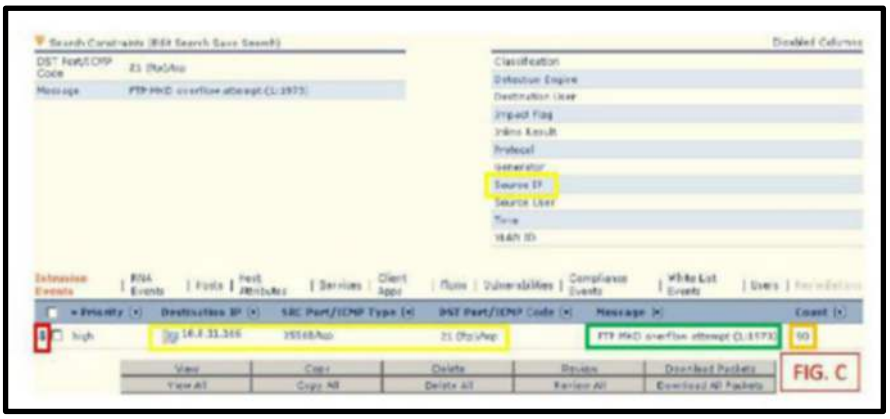
> This figure shows detailed information for packets that have triggered one or more intrusion rules,

> including (i) date and time of the event (in the blue box), (ii) an indication whether the packet was allowed or dropped (in the red box), (iii) source and destination IP addresses and ports (in the yellow box), and (iv) a message or rule-specific explanatory text for the event (in the green box).

J.A. 19 (citations omitted).

J.A. 19.

Regarding Sourcefire, the Board made four findings that are relevant to the present appeal. First, the Board found that Sourcefire discloses a "packet flow entry." J.A. 25. Relying on another annotated screenshot of Sourcefire, which is reproduced below, the Board explained that "the packet flow entry is the 'entry' shown in, for example, . . . Figure C." J.A. 25.



J.A. 24. Second, the Board found that Sourcefire discloses "packet flow analysis data." *See* J.A. 25. As the Board explained:

> [The packet flow entry] corresponds to one or more packet log entries (e.g., the 90 packet log entries) and is of "packet flow analysis data" including "data corresponding to a plurality of packet flow entries." Sourcefire's packet flow entries consolidate multiple packet log entries that all correspond to a common threat identifier, such as the "FTP MKD overflow attempt (1:1973)" event shown in Petitioner's Figure C.

J.A. 25–26; *see also* J.A. 33 ("The 'packet flow analysis data' is the set of packet log entries that are reflected in the flow log entry (i.e., that data underlying the entry).").

Third, the Board found that Sourcefire discloses a packet-filtering device that updates a packet flow entry based on a packet log entry. *See* J.A. 26–30. As the Board first explained:

> [T]he "packet-filtering device" is Sourcefire's "3D Sensor with IPS," which communicates "packet flow analysis data," i.e., the packet log data associated with each packet flow entry, when the user clicks on a packet flow entry, and the "computing device" to which the data is

> "communicated" is the one displaying the web interface.

J.A. 27. Next, the Board found that "Sourcefire describes applying a refresh interval to 'event views,' which is a category that includes the workflows that display the packet flow entries." J.A. 29 (citing J.A. 746; J.A. 636–37). Ultimately, the Board found that Sourcefire's "refresh will update the flow log entry to reflect additional packets that have been received and, thus, the update will be 'based on' those new packets." J.A. 30. Fourth, the Board found that Sourcefire discloses packet time data for packets corresponding to the packet flow entry. J.A. 33. As the Board explained, "[t]he 'packet flow analysis data' is the set of packet log entries that are reflected in the flow log entry (i.e., that data underlying the entry), and the packet log entries include 'time data.'" J.A. 33 (citing J.A. 953).

B. Macaulay

Published U.S. patent application No. 2015/0207809 ("Macaulay"), titled "System and Method for Generating and Refining Cyber Threat Intelligence Data," "relates generally to communication networks and, more particularly, to the generation and refinement of cyber threat intelligence data in order to identify potentially threatened assets." J.A. 4045. Macaulay "discloses an intelligence headquarters ('IHQ') in a carrier network that 'produces refined cyber threat intelligence data pertaining to particular instances of particular traffic attributes that are indicative of a threat.'" J.A. 19 (citing J.A. 4047). "The traffic attributes can include source and destination IP addresses, autonomous system numbers, domain names, source and destination ports, protocols, traffic flow rates and volumes, and time-of-day patterns." J.A. 19–20 (citing J.A. 4047).

"Based on collected raw threat intelligence, the IHQ produces comprehensive threat report 308, which is a table of records." J.A. 20 (citing J.A. 4051). "The records have

fields that could include a particular instance of a traffic attribute, an aggregation of all logged events pertaining to the particular instance of the particular traffic attribute, and a 'reputation score' indicative of the extent to which the IHQ considers traffic characterized by that traffic attribute to be compromised." J.A. 20 (citing J.A. 4051). "Macaulay discloses that the reputation score of a traffic attribute can be impacted by several factors, such as 'the number of cyber threat intelligence sources that have revealed the particular instance of the particular traffic attribute as a potential threat,' the origin of the threat intelligence, 'the number of logged events pertaining to the particular instance of the particular traffic attribute,' and 'the amount of time elapsed since the particular instance of the particular traffic attribute last appeared among the raw cyber threat intelligence.'" J.A. 20–21 (citing J.A. 4052).

STANDARD OF REVIEW

"Claim construction is ultimately a question of law, decided de novo on review, as are the intrinsic-evidence aspects of a claim-construction analysis." *Intel Corp. v. Qualcomm Inc.*, 21 F.4th 801, 808 (Fed. Cir. 2021) (citation omitted). However, "we review any underlying fact findings about extrinsic evidence . . . for substantial-evidence support when the appeal comes from the Board." *Id.*

"The ultimate question of obviousness is a legal question that we review de novo with underlying factual findings that we review for substantial evidence." *Roku, Inc. v. Universal Elecs., Inc.*, 63 F.4th 1319, 1324 (Fed. Cir. 2023) (citation omitted). Those underlying factual findings include "[w]hether a person of ordinary skill in the art would have been motivated to modify or combine teachings in the prior art, and whether he would have had a reasonable expectation of success." *AliveCor, Inc. v. Apple*

Inc., 130 F.4th 1006, 1014 (Fed. Cir. 2025) (alteration in original and citation omitted).

"Substantial evidence is something less than the weight of the evidence but more than a mere scintilla of evidence." *In re Nuvasive, Inc.*, 842 F.3d 1376, 1379 (Fed. Cir. 2016) (quoting *In re Kotzab*, 217 F.3d 1365, 1369 (Fed. Cir. 2000)). The substantial evidence standard "involves examination of the record as a whole, taking into account evidence that both justifies and detracts from an agency's decision." *TQ Delta, LLC v. Cisco Sys., Inc.*, 942 F.3d 1352, 1358 (Fed. Cir. 2019) (citation omitted). However, "the possibility of drawing two inconsistent conclusions from the evidence does not prevent an administrative agency's finding from being supported by substantial evidence." *Consolo v. Fed. Mar. Comm'n*, 383 U.S. 607, 620 (1966).

DISCUSSION

Centripetal raises two issues on appeal: first, whether the Board erred in construing the term "packet flow" because it misconstrued the term "packet flow entry"; and second, whether the Board erred in determining that claims of the '917 Patent were obvious in light of Sourcefire and Macaulay. On cross-appeal, Keysight also raises two issues: first, whether the Board erred by construing "responsive to" in claims 4 and 14 to require continuous updating; and second, whether the Board erred in finding claims 4 and 14 non-obvious.

Because we see no error in the Board's claim construction analysis and substantial evidence supports its factual findings, we affirm as to claims 1–3, 5–13, and 15–20. However, because the Board erred in its analysis of claims 4 and 14, we reverse.

I. Claim Construction

A. Notice

Centripetal argues the Board erred by construing a term that the Parties had not briefed—"packet flow entry." Appellant Br. at 33. According to Centripetal, the Board should have instead construed the term "packet flow," which it argues was "central to the scope of claims." Appellant Br. at 43. As Centripetal argues, because the Board relied on "portions of the '917 Patent [which] were not mentioned once in the parties' briefing on claim construction or at the hearing before the Board," it never "had [the] opportunity to address an argument raised for the first time by the Board about a term first put in issue by the Board." Appellant Br. at 44. Consequently, Centripetal argues the Board's decision to reach outside the Parties' dispute deprived it of "notice of the contested claim construction issues and an opportunity to be heard." Appellant Br. at 44. We disagree.

"The critical question for compliance with the APA and due process is whether [Centripetal] received 'adequate notice of the issues that would be considered, and ultimately resolved, at that hearing.'" *Genzyme Therapeutic Prods. Ltd. P'ship v. Biomarin Pharm. Inc.*, 825 F.3d 1360, 1367 (Fed. Cir. 2016). Although Centripetal argues it only asked the Board to construe a single term, "packet flow," Appellant Br. at 42, Centripetal's briefing clearly put another term in dispute—"packet flow entry." In Centripetal's response to the Board, it argued that the term "packet flow" should be construed as "a connection level state where packets are identified as being part of the same connection between two endpoints." J.A. 7244. Based on this proposed construction, Centripetal asserted that "the term 'packet flow entry' refers to an entry of 'packet flow analysis data' that represents 'a connection level state where packets are identified as being part of the same connection between two endpoints.'" J.A. 7245.

Consequently, Centripetal cannot plausibly argue that it lacked notice that the Board might construe "packet flow entry" when it proffered a meaning of "packet flow entry" based on its proposed construction of "packet flow." *See* J.A. 7244–45.

Moreover, the record further demonstrates that Centripetal had notice and an opportunity to be heard regarding the construction of "packet flow entry." At the hearing before the Board, Centripetal was explicitly asked about "packet flow entry" and was given the chance to respond to the Board's questions regarding this term. *See* J.A. 8488–90. Judge McNamara articulated a rationale for declining to construe "packet flow" over "packet flow entry." *See* J.A. 8489. The relevant portion of this discussion is reproduced below:

> Judge McNamara: The claim doesn't actually recite a packet flow. It recites packet flow entries. And then it says the packet flow analysis data comprises data corresponding to a plurality of packet flow entries. Why do I need to go beyond what's in the claim?
>
> [Centripetal's counsel]: Again, a packet flow entry is an entry of packet flow. And an entry is commonly understood as the act of storing or recording an item. So you need to - -
>
> Judge McNamara: No. A packet flow entry is defined in the claim as consolidating a plurality of packet log entries corresponding to a common threat identifier. It's very clear what packet flow entries are.
>
> [Centripetal's counsel]: But it doesn't change what a packet - - you're trying to change the definition of a flow. A flow is still commonly - -
>
> Judge McNamara: I'm not trying to change the definition of a flow. What I'm trying to do is apply

> the words that are in front of me. The words in front of me are packet flow analysis data and packet flow entries.

J.A. 8489. Centripetal's Opening Brief even concedes that the focus of the hearing was on the meaning of "packet flow entry." Appellant Br. at 43 ("[T]he Board focused at the hearing on the meaning of 'packet flow entry.'"). While Centripetal argues it only "asked the Board to construe a single term," Appellant Br. at 42, it was on notice that the Board might construe packet flow entry based on the hearing and the Parties' discussion of the term, and "[t]he Board may adopt a claim construction of a disputed term that neither party proposes without running afoul of the APA." *Google LLC v. EcoFactor, Inc.*, 92 F.4th 1049, 1057 (Fed. Cir. 2024).

Centripetal maintains that "the meaning of 'packet flow' was the critical issue before the Board, and the Board was required to resolve it." Appellant Reply Br. at 6. We conclude that the Board did resolve it. "The purpose of claim construction is to resolve 'disputed meanings and technical scope, to clarify and when necessary to explain what the patentee covered by the claims, for use in the determination of infringement' or invalidity." *Promptu Sys. Corp. v. Comcast Corp.*, 92 F.4th 1372, 1380 (Fed. Cir. 2024) (citation omitted). "Accordingly, 'only those terms need be construed that are in controversy, and only to the extent necessary to resolve the controversy.'" *Id.* (citation omitted). Here, the Board resolved the controversy regarding "packet flow" when it concluded that "nothing in the patent . . . would limit 'packet flow' to packets that are identified as part of the same connection between two endpoints." *See* J.A. 16. As we explain in detail below, that was correct. However, because the question of obviousness remained, the Board construed another term, packet flow entry, which undoubtedly appears in the numerous claims at issue and is material to the obviousness inquiry. Accordingly, the Board did not deprive Centripetal of notice

of the contested claim construction issues or an opportunity to be heard.

B. Substantive Construction

Centripetal argues the Board erred in its construction of packet flow entry because its "analysis hinged on the assumption that a 'packet flow entry' must contain information for only a single 'packet flow.'" Appellant Br. at 45. Centripetal contends there is no support in the '917 Patent for the Board's assumption. Appellant Br. at 45. According to Centripetal, "the Board's failure to engage with the intrinsic evidence is dispositive here because, without a clear definition of 'packet flow' in the '917 Patent, the Board had no basis to reject its evidence about the term's ordinary meaning in the field of computer network security." Appellant Br. at 46 (cleaned up). We disagree that the Board erred in construing packet flow entry.

"When construing claim terms, we first look to, and primarily rely on, the intrinsic evidence, including the claims themselves, the specification, and the prosecution history of the patent, which is usually dispositive." *Personalized Media Commc'ns, LLC v. Apple Inc.*, 952 F.3d 1336, 1340 (Fed. Cir. 2020) (citation omitted). We begin our analysis with the claim language itself.

Claim 1 recites, in relevant part:

> updating, by the packet-filtering device and based on the packet log entry, a packet flow entry, corresponding to the generated packet log entry, of packet flow analysis data for a plurality of logged packets, wherein the packet flow analysis data comprises data corresponding to a plurality of packet flow entries, and wherein each packet flow entry consolidates a plurality of packet log entries corresponding to a common threat identifier.

'917 Patent at Claim 1. While the claim language links "packet flow entry," to "packet log entries," and further

links it to a "common threat identifier," *see* '917 Patent at Claim 1, it does not entirely resolve the proper meaning of packet flow entry. Of note, while the claims of the '917 Patent use the term "packet flow" as part of larger terms (e.g., "packet flow entry," "packet flow analysis data," and "packet flow log entry"), it never appears by itself in the specification or claims, but "entry" does appear in the specification.

Turning to the specification, the '917 Patent uses the term "entry" in two ways: (1) as an "entry" in a "log" (basically a record in a dataset, such as Figure 5G's packet or flow log), *see* J.A. 76 (FIG. 5G), and (2) as an "entry" in the interface (e.g., a row corresponding to a Threat ID), as shown in Figure 6G, *see* J.A. 83 (FIG. 6G). Focusing on Figure 6G's interface, in the first "entry," which is associated with Threat_1, it shows a total of nine packets received. *See* '917 Patent at FIG. 6G. For these nine packets, the specification explains that they come from three connections: (1) three packets between threat host 140 and host 144 (step 22), *id.* at col. 9, ll. 10–11, (2) three packets between threat host 140 and host 112 (step 64), and (3) three packets between threat host 140 and host 114 (step 64), *id.* at col. 15, ll. 19–21. This shows that when the "entry in listing 606" that is "associated with Threat ID: Threat_1" is updated, at steps 29 and 68, the Threat_1 "entry" in Figure 6G represents a total of nine packets sent in different connections between different endpoints. *See id.* at col. 11, ll. 6–12; col. 15, l. 63–col. 16, l. 5.

Thus, "packet flow" itself cannot refer "to data packets that are part of the same connection between two endpoints," as Centripetal argues, *see* Appellant Br. at 33, because that construction fails to account for the six packets received at step 64. "We normally do not interpret claim terms in a way that excludes embodiments disclosed in the specification." *Oatey Co. v. IPS Corp.*, 514 F.3d 1271, 1276 (Fed. Cir. 2008) (citations omitted). As explained above, the "packet flow entry," depicted in Figure 6G,

corresponds to packets in different connections between different endpoints. As such, under de novo review, the specification directs this Court to one reasonable outcome: "packet flow entry" refers to an entry—including, in particular, an entry in a user interface—that reflects a set of packets with a common feature, such as a common threat ID. To construe the term otherwise would run afoul of the '917 Patent's specification, which we will not do.

II. Obviousness

A. The Board's Obviousness Determination as to Independent Claims 1, 11, and 20 Is Supported by Substantial Evidence[2]

Centripetal argues the Board erred, as to the independent claims, because even accepting the Board's claim construction, Sourcefire does not disclose: (1) "packet flow analysis data," (2) a device that "updates" a "packet flow entry," and (3) packet time data that corresponds to the packet flow entries. Appellant Br. at 52. We disagree. Substantial evidence supports the Board's obviousness determination as to claim 1. As explained above, the Board found, among other things, that Sourcefire discloses: (1) packet flow analysis data, (2) a device that updates a packet flow entry, and (3) packet time data that corresponds to the packet flow entries. *See supra* Background Section II.A. A review of the record, mainly Sourcefire itself, shows that a reasonable factfinder could have arrived at the same conclusion the Board did.

---

[2] Because claims 11 and 20 are substantially similar to claim 1, the Board did not independently analyze these claims. J.A. 34. Instead, it adopted, and applied, its reasoning for claim 1 to determine that Sourcefire teaches or suggests all the limitations of claims 11 and 20, *see* J.A. 34, and we do the same.

While Centripetal argues that Sourcefire does not disclose these three elements of the patented invention, Appellant Br. at 52, its reasons as to why these elements are not disclosed fail to persuade us that the Board's findings lack substantial evidence support, *see generally* Appellant Br. at 52–64. Centripetal's arguments ask this Court to look at the evidence before the Board and draw a contrary conclusion—that Sourcefire does not disclose these elements. While a different conclusion may be plausible, as noted above, "the possibility of drawing two inconsistent conclusions from the evidence does not prevent an administrative agency's finding from being supported by substantial evidence." *Consolo*, 383 U.S. at 620. Here, the Board adequately explained its rationale throughout every part of its analysis and made express findings of fact regarding claim 1, which are firmly grounded in the record. As such, we see substantial evidentiary support for the Board's findings.

B. The Board's Obviousness Determinations as to Dependent Claims 2–3, 5–10, 12–13, and 15–19 Are Supported by Substantial Evidence

Centripetal next argues the Board's obviousness determinations as to claims 2–3, 5–10, 12–13, and 15–19 were mistaken. Appellant Br. at 65. Again, we disagree. For claims 2, 5, 12, and 15, Centripetal's only argument is that the Board's decision should be reversed if we find the Board erred as to claims 1, 11, and 20. Appellant Br. at 65–69. Because we concluded, above, substantial evidence supports the Board's findings with respect to claims 1, 11, and 20, we decline to reverse the Board's decision as to claims 2, 5, 12, and 15. Thus, we turn our analysis to the remaining dependent claims—claims 3, 6–10, 13, and 16–19.

Starting with claims 3 and 13, Centripetal argues the Board erred because it "did not grapple with the specific limitations of these claims," which "require a 'time range'

for a 'plurality of packet log entries,' which includes both an 'earliest hit time' and a 'latest hit time' for the full set." Appellant Br. at 66. According to Centripetal, "even if the Board were correct that the disabled 'time' column in Sourcefire is sufficient to disclose 'packet time data,' it surely does not disclose the 'time range' required by these claims." Appellant Br. at 66–67. We disagree.

Substantial evidence supports the Board's finding that "Sourcefire teaches or suggests the time range of claims 3 and 13." *See* J.A. 41. In reaching this finding, the Board analyzed, and credited, Keysight's position that "Sourcefire discloses that flow data fields for drill-down pages in a custom workflow may include fields such as a 'first packet,' which is 'the date and time of the first packet of the session was seen' and a 'last packet,' which is 'the date and time the last packet of the session was seen,'" which is supported by the cited declaration of Keysight's expert, Dr. Staniford. *See* J.A. 40–41 (citing J.A. 645). Although Centripetal's arguments on appeal cite the '917 Patent for support, they fail to address Sourcefire's teachings or Keysight's credited explanation as to why Sourcefire discloses the time range of these claims. *See* Appellant Br. at 65–67. As such, substantial evidence—the declaration of Dr. Staniford and Sourcefire—supports the Board's finding. *See* J.A. 645 (citing J.A. 953–54).

For claims 6 and 16,[3] Centripetal argues the Board erred because it improperly reasoned "that a skilled artisan would combine Sourcefire's packet flow analysis data with Macaulay's reputation scores to render claims 6 and 16 obvious." *See* Appellant Br. at 67. As Centripetal

---

[3] In its Opening Brief, Centripetal asserts that because claims 7–10 and 17–19 depend from claims 6 and 16, its reasoning as to why Sourcefire and Macaulay do not render claims 6 and 16 obvious applies to those claims as well. Appellant Br. at 68 n.2.

argues, "because Sourcefire does not disclose the 'packet flow analysis data' or 'packet flow entry' required by Claims 6 and 16, Macaulay cannot supply what is missing." Appellant Br. at 68. We disagree. The record amply supports the Board's determination that claims 6 and 16 would have been obvious over the teachings of Sourcefire and Macaulay. For instance, Keysight's expert testified extensively as to what Macaulay teaches and why a person of ordinary skill in the art would have been motivated to combine the teachings of Sourcefire and Macaulay. *See* J.A. 651–63. Moreover, Centripetal's argument—that Sourcefire does not disclose packet flow analysis data or packet flow entry—fails because, as explained above, the Board's finding that Sourcefire disclosed these elements is supported by substantial evidence. *See supra* Discussion Section II.A. Accordingly, we conclude that substantial evidence supports the Board's obviousness determinations as to claims 2–3, 5–10, 12–13, and 15–19.

III. Cross-Appeal

On cross-appeal, Keysight argues the Board's non-obviousness determination, as to claims 4 and 14, should be reversed because it erred by construing "responsive to" in such a way as to conflict with the '917 Patent and "overlooked aspects of Sourcefire's teachings that render the claims obvious." Cross-Appellant Br. at 70. Keysight also argues that "the Board additionally erred by discounting this Court's prior finding that Sourcefire teaches updating a packet flow log based on packet log entries."[4] Cross-Appellant Br. at 80. We agree with Keysight.

---

[4] Because we ultimately conclude that the Board committed reversible error, we decline to reach the question of whether collateral estoppel applies to claims 4 and 14.

Substantial evidence does not support the Board's findings that Sourcefire fails to disclose: (1) an "existing flow log entry"; (2) updating flow log entries "responsive to a determination that each packet corresponds to one or more packet-filtering rules"; and (3) modifying the existing packet flow log entry "to indicate one or more corresponding packet-filtering rules" and whether the packet-filtering device "prevented each packet from continuing." *See* J.A. 38–39.

First, the Board's finding that Sourcefire fails to disclose an "existing flow log entry," J.A. 38, is not supported by substantial evidence. In making this finding, the Board rejected Keysight's argument that its annotated screenshot (Figure D) shows how Sourcefire "generates a packet-flow log entry, which consolidates, compresses, or summarizes the entries in the packet-log for display on the interface." *See* J.A. 37–38. In so doing, the Board found that the "entries [in Figure D] are generated on the fly in response to the user clicking on the entry for one of the ports on the preceding screen." J.A. 38. The Board reasoned, "Figure D may show an 'entry' in the interface, but [Keysight] has not shown how or why it could be an 'existing flow log entry.'" J.A. 38. Keysight argues the Board erred because the Sourcefire pages it cites in support of its finding do not state or otherwise disclose that the entries in Figure D are generated "on the fly." *See* Cross-Appellant Br. at 76. We agree.

The Board cited to two pages from Sourcefire in support of its finding, explaining that Sourcefire (1) shows "a drill-down page with the number of events generated for each destination port" and (2) explains that "[w]hen you 'drill-down' to find more information for one or more destination ports, you automatically select those events and the next page in the workflow [i.e., Figure D] appears." J.A. 38 (alterations in original). However, the record contains no "generated on the fly" language besides the Board's own statement. Further, as Keysight argues, and

we agree, Sourcefire discloses that "drill-down pages are populated with a subset of columns available in the database." Cross-Appellant Br. at 76 (citing J.A. 2246). Because of this, Keysight argues that "an existing column in the database includes the 'count,' and, therefore, the packet flow log entry that is used to update the packet flow entry in the interface." Cross-Appellant Br. at 76.

In addition, the Board's reasoning as to why Sourcefire does not disclose an "existing flow log entry" is contrary to its prior factfinding. For claim 1, the Board found that "[Sourcefire's] refresh will update the flow log entry to reflect additional packets that have been received, and thus, the update will be 'based on' those new packets." J.A. 30. Thus, it logically follows that if Sourcefire can update a flow log entry, then the flow log entry must already be in existence. Otherwise, there would be no entry in the flow log to update.

As such, we conclude that the Board's finding—that Sourcefire does not disclose an existing flow log entry—is unsupported by substantial evidence. *TQ Delta*, 942 F.3d at 1358 (explaining the substantial evidence standard "involves examination of the record as a whole, taking into account evidence that both justifies and detracts from an agency's decision" (citation omitted)).

Second, substantial evidence does not support the Board's finding that, even if the entries in Figure D constituted flow log entries, Sourcefire does not disclose they are updated "responsive to a determination that each packet corresponds to one or more packet-filtering rules." *See* J.A. 38–39. As the Board explained, "[i]n Sourcefire, updating happens in response to a user clicking on an item to create a new view or at the expiration of the refresh interval," which "is different than what is described in the '917 patent, where the packet-filtering device continuously updates the flow log to reflect how packets are being handled." J.A. 38. However, the language of claims 4 and

14 do not require continuous updates, nor do they exclude a user selection or a refresh interval. *See* '917 Patent at Claim 4, Claim 14.

Although the Board cited language from the specification as support for its finding, *see* J.A. 38–39, that verbiage does not support reading "continuously" into the claims. The cited specification language recites:

> For example, . . . packet-filtering device 144 may generate entries in packet log 502 for each of the packets received in step 64 while modifying an entry in flow log 504 for the packets received in step 61 based on the entries generated in packet log 502.

J.A. 38–39 (citing '917 Patent at col. 15, ll. 30–41). This language neither contains the restrictive language imputed by the Board, nor does it disclose that updating occurs continuously or immediately after the packet-filtering device determines that received packets trigger a rule. As Keysight argues, the specification instead "discloses intervening steps occurring between packets triggering a rule and the packet-filtering device modifying an entry in the flow log to reflect the triggering packets [(e.g., the flow log entry is not modified to account for the packets received at step 61 until step 65)]." Cross-Appellant Br. at 72. We agree.

Moreover, while the Board tried to align its analysis of claim 1 with its analysis of claims 4 and 14, an error is still present. Specifically, the Board noted "that Sourcefire's refreshing is sufficient for claim 1 because that claim's 'updating' need only be 'based on the packet log entry,' not 'responsive to a determination that each packet corresponds to one or more packet-filtering rules.'" J.A. 39 n.12. We disagree, and to the contrary: we see no meaningful distinction between "based on the packet log entry" and "responsive to a determination that each packet corresponds to one or more packet-filtering rules." It logically follows that if packets are never logged, then there

would never be a "modifying" that occurs "responsive to a determination that each packet corresponds to one or more packet-filtering rules." *See* '917 Patent at Claim 4. As such, the Board's finding is not supported by substantial evidence.

Third, the Board's finding that Sourcefire does not disclose modifying an existing packet flow log entry "to indicate one or more corresponding packet-filtering rules" and whether the device "prevented each packet from continuing," *see* J.A. 39, is also unsupported by substantial evidence. Here, the Board asserted that "[t]he only modification [Keysight] identifies concerns a change to the number of packets for each type of event," but Keysight does not explain how that shows "a modification 'to indicate one or more corresponding packet-filtering rules' or about whether 'the packet-filtering device prevented each packet from continuing.'" J.A. 39 (emphasis omitted). As Keysight argues, its petition explained how Sourcefire discloses these elements. Cross-Appellant Br. at 79 (citing J.A. 221–22). We agree with Keysight. Keysight's petition explicitly referenced Figure D and explained how the detailed portions of the interface met these elements of claims 4 and 14, and it provided evidentiary support from Sourcefire and the declaration of its expert. *See* J.A. 220–22. A review of this evidence shows that the Board's finding lacks substantial evidence support. Accordingly, we reverse as to claims 4 and 14. *See Corning v. Fast Felt Corp.*, 873 F.3d 896, 901–02 (Fed. Cir. 2017) (explaining that reversal is warranted where only one answer is supported by substantial evidence and there is neither a request nor an apparent reason to grant a second record-making opportunity).

CONCLUSION

We have considered Centripetal's remaining arguments but do not find them persuasive. For the foregoing reasons, we affirm the Board's obviousness

determinations as to claims 1–3, 5–13, and 15–20. In light of Keysight's cross-appeal, we reverse the Board's non-obviousness determination as to claims 4 and 14.

AFFIRMED IN PART, REVERSED IN PART

COSTS

No costs.