

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

KEYSIGHT TECHNOLOGIES, INC.,  
Petitioner

v.

CENTRIPETAL NETWORKS, INC.,  
Patent Owner.

---

IPR2022-01097  
Patent 10,193,917 B2

---

Before BRIAN J. McNAMARA, STACEY G. WHITE, and  
AARON W. MOORE, *Administrative Patent Judges*.

MOORE, *Administrative Patent Judge*.

JUDGMENT  
Final Written Decision  
Determining Some Challenged Claims Unpatentable  
*35 U.S.C. § 318(a)*

## TABLE OF CONTENTS

|                                                                                                            |    |
|------------------------------------------------------------------------------------------------------------|----|
| I. BACKGROUND .....                                                                                        | 1  |
| A. Related Matters .....                                                                                   | 1  |
| B. The '917 Patent .....                                                                                   | 3  |
| 1. Written Description .....                                                                               | 3  |
| 2. File History .....                                                                                      | 6  |
| 3. The Challenged Claims .....                                                                             | 6  |
| II. PATENTABILITY ANALYSIS .....                                                                           | 8  |
| A. Level of Ordinary Skill in The Art .....                                                                | 8  |
| B. Claim Construction .....                                                                                | 9  |
| 1. Threat Identifier and Threat Indicator .....                                                            | 9  |
| 2. Packet Flow Entry .....                                                                                 | 10 |
| C. Overview of the Prior Art .....                                                                         | 14 |
| 1. Sourcefire .....                                                                                        | 14 |
| 2. Macaulay .....                                                                                          | 16 |
| D. Independent Claim 1 .....                                                                               | 18 |
| 1. Receiving Packets, Applying Rules to Block<br>or Allow Passage, and Generating Packet Log Entries ..... | 18 |
| 2. Updating a Packet Flow Entry .....                                                                      | 20 |
| a. Packet Flow Entry .....                                                                                 | 22 |
| b. Updating by a Packet-Filtering Device .....                                                             | 23 |
| c. Sourcefire's "Refresh Interval" .....                                                                   | 25 |
| d. Updating Based on a Packet Log Entry .....                                                              | 27 |
| e. Data Corresponding to a Plurality<br>of Packet Flow Entries .....                                       | 28 |
| 3. Communicating the Packet Flow Analysis Data .....                                                       | 28 |
| 4. Causing Display of Packet Flow Analysis Data .....                                                      | 28 |
| 5. Content Of the Packet Flow Analysis Data .....                                                          | 29 |
| 6. Conclusion for Independent Claim 1 .....                                                                | 31 |

|                                                                            |    |
|----------------------------------------------------------------------------|----|
| E. Independent Claims 11 and 20.....                                       | 31 |
| F. Dependent Claims 2–5 and 12–15.....                                     | 31 |
| 1. Claims 2 and 12: Packet Filtering Rules<br>and Environmental Data ..... | 32 |
| 2. Claims 4 and 14: Updating a Packet Flow Log Entry.....                  | 33 |
| 3. Claims 3 and 13: A Time Range of the Packets.....                       | 37 |
| 4. Claims 5 and 15.....                                                    | 38 |
| G. Dependent Claims 6 and 16.....                                          | 38 |
| 1. Petitioner’s Contentions.....                                           | 39 |
| 2. Patent Owner’s Arguments and Our Analysis.....                          | 41 |
| H. Dependent Claims 8 and 18.....                                          | 44 |
| I. Dependent Claims 7, 9, 10, 17, and 19.....                              | 46 |
| III. CONCLUSION.....                                                       | 47 |
| IV. ORDER.....                                                             | 48 |

## I. BACKGROUND

Petitioner Keysight Technologies, Inc. filed a Petition for *inter partes* review of claims 1–20 of U.S. Patent No. 10,193,917 B2 (Ex. 1001, “the ’917 patent”). Paper 1 (“Pet.”). Patent Owner Centripetal Networks, Inc. filed a Preliminary Response. Paper 6. On December 19, 2022, the Board instituted an *inter partes* review of all challenged claims. *See* Paper 8, 36.

Patent Owner filed a Response on March 27, 2023 (Paper 20, “PO Resp.”), Petitioner filed a Reply on June 19, 2023 (Paper 24, “Reply”), and Patent Owner filed a Sur-reply on July 24, 2023 (Paper 26, “Sur-reply”).

Petitioner filed a Motion to Exclude on August 28, 2023, Patent Owner filed an Opposition, and Petitioner filed a Reply. *See* Paper 30 (“Mot. to Exclude”); Paper 31 (“Mot. to Exclude Opp.”); Paper 33 (reply).

An oral hearing was held on September 20, 2023, and a transcript of the hearing is included in the record, as are the demonstratives. *See* Paper 39 (“Tr.”); Ex. 1054 (Petitioner Demonstratives); Ex. 2022 (Patent Owner Demonstratives).

We issue this Final Written Decision under 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73 and, for the reasons that follow, determine that Petitioner has shown by a preponderance of the evidence that claims 1–3, 5–13, and 15–20 are unpatentable. We further determine that Petitioner has not shown that claims 4 and 14 are unpatentable. In addition, for reasons discussed below, we grant Petitioner’s Motion to Exclude.

### A. *Related Matters*

Petitioner and Patent Owner identify the following district court proceeding involving the ’917 patent: *Centripetal Networks, Inc. v. Keysight Technologies, Inc.*, No. 2:22-cv-00002 (E.D. Va., filed Jan. 1, 2022). Pet. 4; Paper 7, 1.

The parties also identify the following International Trade Commission investigation involving the '917 patent: *Certain Computer Network Security Equipment and Systems, Related Software, Components Thereof, and Products Containing Same*, Inv. No. 337-TA-1314 (ITC, filed Apr. 19, 2022). Pet. 4; Paper 7, 1. On August 8, 2023, Administrative Law Judge MaryJoan McNamara<sup>1</sup> issued an Initial Determination finding that asserted claims 11 and 20 of the '917 patent are invalid as obvious in view of the Sourcefire reference that is presented in the Petition. *See* Ex. 1055. The finding of no violation was affirmed by the full commission on December 5, 2023. *See* Paper 38; 88 Fed. Reg. 85,913.

The '917 patent is a member of a large family, with a parent that issued as U.S. Patent No. 9,866,576, a sibling that issued as U.S. Patent No. 9,413,722, multiple continuations that have issued as nine patents, and a pending application, U.S. Patent App. No. 18/244,133, which was filed on September 8, 2023.

The sibling '722 patent was the subject of IPR2018-01760, in which its claims 1–25 were determined to be unpatentable in view of the Sourcefire reference. *See* Ex. 1030, 55. That decision was affirmed on appeal. *See Centripetal Networks, Inc. v. Cisco Sys.*, 847 Fed. Appx. 881 (Fed. Cir. 2021) (Ex. 1031).

U.S. Patent No. 10,567,413, a child of the '917 patent, was the subject of IPR2021-01149; U.S. Patent No. 10,542,028, a grandchild of the '917 patent, was the subject of IPR2021-01147; and U.S. Patent No. 10,757,126, a great, great grandchild of the '917 patent, was the subject of IPR2021-01148. Final Written Decisions issued in each of those cases earlier this year, finding all claims unpatentable in view of Sourcefire and/or Sourcefire in combination with other

---

<sup>1</sup> Administrative Patent Judge Brian J. McNamara and Administrative Law Judge Mary Joan McNamara are not related.

references. *See* IPR2021-01149, Paper 46; IPR2021-01147, Paper 40; IPR2021-01148, Paper 40.

*B. The '917 Patent*

*1. Written Description*

The '917 patent relates to “rule-based network-threat detection.” Ex. 1001, 1:44–45. The patent describes a process in which a packet-filtering device receives data packets and determines whether each packet corresponds to criteria specified by a packet-filtering rule. *Id.* at 1:49–51. The packet-filtering rule criteria may correspond to one or more “network threat indicators.” *Id.* at 1:51–53. Examples of network-threat indicators include “network addresses, ports, fully qualified domain names (FQDNs), uniform resource locators (URLs), uniform resource identifiers (URIs), or the like” that are associated with network threats. *Id.* at 3:23–34. A packet-filtering rule may specify an “operator” to be applied by the packet-filtering device when the rule is triggered, where the operator causes the device either to prevent the packet from continuing toward its destination or allow the packet to continue. *Id.* at 1:53–57.

The packet-filtering device described in the '917 patent generates two types of log data—“packet log” data and “flow log” data. *Id.* at 6:30–35. These are shown in Figure 5B, which is reproduced below:

The diagram shows a log interface with a rounded rectangular border. At the top center is the label "Log(s)". Below it are two main sections: "Packet Log" on the left and "Flow Log" on the right. The "Packet Log" section contains a table with 5 columns: Time, Packet Info, Env. Vars., Threat ID, and Disp. The "Flow Log" section contains a table with 4 columns: Time Range, Consolidated Info., Threat ID, and Counts. Reference numerals 220, 502, and 504 point to the top, left, and right edges of the log interface respectively.

| Packet Log |             |            |           |       | Flow Log   |                    |           |           |
|------------|-------------|------------|-----------|-------|------------|--------------------|-----------|-----------|
| Time       | Packet Info | Env. Vars. | Threat ID | Disp. | Time Range | Consolidated Info. | Threat ID | Counts    |
| 01         | <info.>     | <vars.>    | Threat_3  | A     | [01, 03]   | <info. vars.>      | Threat_3  | A=03 B=00 |
| 02         | <info.>     | <vars.>    | Threat_3  | A     |            |                    |           |           |
| 03         | <info.>     | <vars.>    | Threat_3  | A     |            |                    |           |           |
| 08         | <info.>     | <vars.>    | Threat_5  | A     |            |                    |           |           |
| 10         | <info.>     | <vars.>    | Threat_5  | A     |            |                    |           |           |
| 12         | <info.>     | <vars.>    | Threat_5  | A     |            |                    |           |           |
| 14         | <info.>     | <vars.>    | Threat_5  | A     |            |                    |           |           |

FIG. 5B

*Fig. 5B “depict[s] illustrative logs for rule-based network-threat detection.” Ex. 1001, 2:43–35.*

The above figure shows packet log data (on the left) and flow log data (on the right) generated by a packet-filtering device. *Id.* at 6:30–35, 7:27–34. Each packet log entry includes data for an individual packet that has been filtered by the packet-filtering device, including a time when the packet-filtering device received the packet, data derived from the packet (e.g., source address, destination address, port number, protocol type, domain name, URL, URI, or the like), environmental variables, a Threat ID, and an indication of whether the device blocked the packet or allowed it to continue toward its destination. *See id.* at 6:35–59, 7:27–30.

Each flow log entry consolidates, compresses, or summarizes entries of the packet log. *See id.* at 7:34–35. For example, a flow log entry may include a time range indicating the earliest and latest hit times indicated by the packet log entries, consolidated information from the packet log entries, information that the associated packets have in common, such as a Threat ID, a count of the associated packets allowed to continue toward their respective destination (indicated by “A”),

and a count of the associated packets prevented from continuing toward their respective destinations (indicated by “B”). *Id.* at 7:36–47.

The packet-filtering device “may utilize flow log 504 to generate data comprising an update for an interface associated with packet-filtering device 144 and displayed by host 110, and may communicate the data comprising the update to host 110.” Ex. 1001, 7:48–52. The interface may include graphical depictions, such as a line chart or a pie chart to illustrate activity associated with packet-filtering device. *See id.* at 7:55–8:67. The interface “may also include listing 606, which may comprise entries corresponding to network threats and, for each threat, associated information derived by packet-filtering device 144 from flow log 504.” *Id.* at 8:1–4. An exemplary interface is shown in Figure 6A:

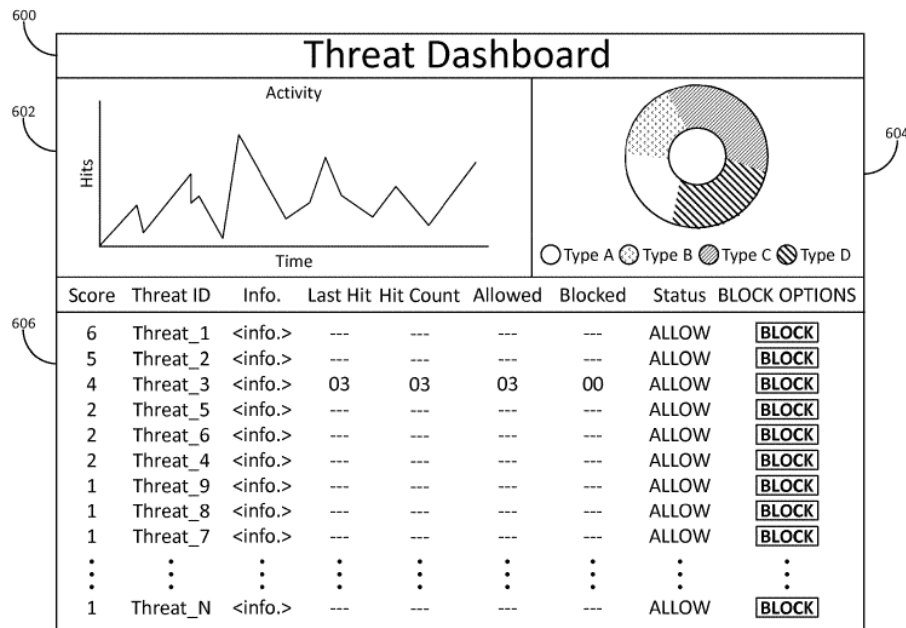


FIG. 6A

*FIG. 6A “depicts [an] illustrative interface[] for rule-based network-threat detection.” Ex. 1001, 2:37–38.*

The packet-filtering device may be configured to determine a score for each of the Threat IDs, and the display of information in Figure 6A may be ordered

based on the score. *Id.* at 8:14–20. Scores may be based on, for example, a number of associated packet hits or times associated with the packet hits corresponding to a packet flow entry. *Id.* at 8:20–23.

We note that the ’917 patent uses the term “entry” in two ways, both as an “entry” in a “log” (essentially a record in a dataset, such as a packet or flow log) and as an “entry” in the visual interface (e.g., a line corresponding to a Threat ID), as shown above.

## 2. *File History*

The application that resulted in the ’917 Patent was filed on November 30, 2017, and the patent issued on January 29, 2019, after a first action allowance with an Examiner’s Amendment. *See* Ex. 1002, 7–21. The amendment made the following changes to original independent claim 2 and corresponding changes to the other independent claims:

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 ~~the 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;

*See id.* at 13.

## 3. *The Challenged Claims*

Petitioner challenges claims 1–20. *See* Pet. 13. Claims 1, 11, and 20 are independent, claims 2–10 depend directly or indirectly from claim 1, and claims 12–19 depend directly or indirectly from claim 11. Claim 1 is illustrative of the claimed subject matter and is reproduced below (formatted for clarity and annotated to include Petitioner’s identification of limitations):

1. A method comprising:
  - [1a] receiving, by a packet-filtering device, a plurality of packets;
  - [1b] 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:
    - [1b1] 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
    - [1b2] 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;
  - [1c] 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;
  - [1d] communicating, by the packet-filtering device and to a computing device, the packet flow analysis data; and
  - [1e] causing, based on the communicated packet flow analysis data, display of at least a portion of the packet flow analysis data,
  - [1f] 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.

## II. PATENTABILITY ANALYSIS

The Petition asserts that claims 1–5, 11–15, and 20 would have been obvious in view of Sourcefire.<sup>2</sup> The Petition also asserts that claims 6–10 and 16–19 would have been obvious in view of Sourcefire and Macaulay.<sup>3</sup>

### A. *Level of Ordinary Skill in The Art*

The level of skill in the art is a factual determination that provides a primary guarantee of objectivity in an obviousness analysis. *See Al-Site Corp. v. VSI Int’l Inc.*, 174 F.3d 1308, 1323 (Fed. Cir. 1999) (citing *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966)). The level of skill in the art also informs the claim construction analysis. *See Teva Pharms. USA, Inc. v. Sandoz, Inc.*, 574 U.S. 318, 332 (2015) (explaining that claim construction seeks the meaning “a skilled artisan would ascribe” to the claim term “in the context of the specific patent claim”).

Petitioner asserts that a person of ordinary skill in the art would have had “a bachelor’s degree in computer science, computer engineering, or an equivalent, and four years of industry experience” and “a working knowledge of packet-switched networking, firewalls, security policies, communication protocols and layers, user interfaces, and the use of customized rules to address cyber-attacks.” Pet. 12–13 (citing Ex. 1003 ¶¶ 21–25). Petitioner further asserts that “[a]dditional graduate education could substitute for professional experience, and vice versa.” *Id.* at 13.

Patent Owner does not address this issue, and neither side argues that it might affect the patentability analysis or otherwise change the outcome. Thus, as

---

<sup>2</sup> Sourcefire 3D System User Guide, Ver. 4.10, Mar. 16, 2011 (Ex. 1004).

<sup>3</sup> U.S. Patent App. Pub. No. 2015/0207809 A1 (Ex. 1029).

we did at institution, we apply Petitioner’s description of an ordinarily skilled artisan, as we find it consistent with the ’917 patent and the asserted prior art.

*B. Claim Construction*

In this *inter partes* review, we apply the same claim construction standard that would be used in a civil action under 35 U.S.C. § 282(b). 37 C.F.R. § 42.100(b) (2019). We generally give claim terms their ordinary and customary meaning as would be understood by a person of ordinary skill in the art at the time of the invention and in the context of the entire patent disclosure. *See id.*; *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–14 (Fed. Cir. 2005) (en banc). We look “principally to the intrinsic evidence of record, examining the claim language itself, the written description, and the prosecution history, if in evidence.” *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 469 F.3d 1005, 1014 (Fed. Cir. 2006) (citing *Phillips*, 415 F.3d at 1312–17).

*1. Threat Identifier and Threat Indicator*

Patent Owner identifies two terms that were construed in the ITC investigation involving the ’917 patent based on constructions agreed upon by the parties. PO Resp. 9. First, the parties in the ITC investigation agreed that “threat identifier” means “information that identifies one or more network threats.” *Id.* at 11 (citing Ex. 2004, 3). Second, the parties further agreed that “threat indicator” means “information that indicates a resource associated with a network threat,” “[f]or example, network addresses, ports, FQDNs, URLs, URIs, the type of threat, geographic information, anonymous proxies, actors, or the like.” *Id.* at 11–12 (citing Ex. 2004, 3). Patent Owner asserts that these constructions should be used

in this proceeding. *Id.* at 12. Petitioner does not dispute these constructions, and we adopt them.<sup>4</sup>

2. *Packet Flow Entry*

Patent Owner argues that “packet flow” should be construed as “a connection level state where packets are identified as being part of the same connection between two endpoints.” PO Resp. 10. Patent Owner asserts that “[t]his is the exact position that Petitioner took during the recently concluded ITC trial” and that it “reflects the plain and ordinary meaning of the term to a person of ordinary skill in the art.” *Id.* (citing Ex. 2013 ¶¶ 43–44; Ex. 2014).

Petitioner responds that “packet flow” “requires no construction because the prior art renders the claims obvious even under PO’s requested construction.” Reply 2. Petitioner also argues that Patent Owner’s construction “lacks support in the intrinsic evidence” and “would contort the claims to improperly exclude the embodiment disclosed throughout the ’917 patent’s specification, which shows that packet flow log entries may consolidate packets that are part of separate connections between more than two endpoints.” *Id.* at 2–8 (describing the ’917 patent’s Figures 3A–3F and 5A–5G, and the associated description). Petitioner argues that Patent Owner’s “attempt to construe ‘packet flow’ to be limited to packets that were identified as being part of the same connection between two endpoints should be rejected because it would improperly . . . exclude the

---

<sup>4</sup> Petitioner identifies two claim terms that were construed in Board and in district court proceedings involving a related patent, but asserts that those terms do not require express construction for this proceeding. *See* Pet. 15. We do not address these terms because neither party is seeking their construction and their interpretation is not necessary for the purposes of this Decision.

embodiment disclosed in the '917 patent.” *Id.* at 8. Although Petitioner argues that Patent Owner’s proposal is incorrect, it does not offer an alternative.

In the Sur-reply, Patent Owner again argues that its proposed construction is “precisely the position Petitioner took earlier this year at the ITC hearing,” this time citing specific testimony of Petitioner’s expert in the ITC investigation regarding non-infringement, which it filed with the Sur-reply as Exhibit 2018. *See* Sur-reply 3–4; Ex. 2108, 986:18–21. Petitioner has moved to exclude Ex. 2018. *See* Mot. to Exclude 1.

Before we get to claim construction, we exclude Ex. 2018 as untimely because Patent Owner had the testimony before it filed the Response and was plainly aware of it, as it was alluded to in the Response. *See* PO Resp. 10; Mot. to Exclude Opp. 2 (admitting that the trial finished before the Response was filed and that Patent Owner filed other testimony excerpts with the Response). However, the exclusion is of little consequence because we find that the testimony would be devoid of probative value. Dr. Rubin is not a fact witness and has not been offered as an expert in this case. Patent Owner cites the testimony in an effort to show that Petitioner is taking inconsistent positions, but we fail to see how Petitioner’s conduct bears on the meaning of “flow” in the '917 patent.

We start the claim construction analysis with the language of the claims themselves. Claim 1 recites applying filtering rules to packets to block or allow them, and generating an entry in a packet log reflecting the treatment of the packet. It further recites updating a “packet flow entry” with “packet flow analysis data” for the logged packets, where the packet flow analysis data includes “data corresponding to a plurality of packet flow entries,” and “each packet flow entry consolidates a plurality of packet log entries corresponding to a common threat identifier.” The packet flow analysis data includes (1) a threat identifier, (2) packet

time data for packets corresponding to the packet flow entry, and (3) data indicating whether the packets were blocked or not. We do not find anything in the claim language as a whole that would tend to either favor or disfavor Patent Owner’s argument that the flow must be part of the same connection between two endpoints, although we note that the claim recites that the “packet flow entries” consolidate packet log entries “corresponding to a common threat identifier.” We also note that the claims recite “packet *log* entry” and “packet flow entry”—with no “log.” As will be discussed below, this claim language mirrors the specification’s distinction between an entry in a log and an entry in the interface.

The written description repeatedly uses the term “packet flow log,” but does not define “flow,” “packet flow,” or “packet flow entry.” Petitioner argues that the description is contrary to Patent Owner’s proposed construction because it describes entries in the “Flow Log” that may reflect packet log entries with different endpoints. *See* Reply 2–8. For example, Figure 5G shows entries that are based on a common Threat ID, where the entry for Threat 1 reflects packet log entries for different times and, in some cases, for logged packets that were sent between different endpoints. That Flow Log entry would include the six packets shown in Step 64, three of which were sent from Threat Host C to Host A–H2 and three of which were sent from the Threat Host C to *different* Host A–HN. *See* Ex. 1001, 15:19–62.

Petitioner’s argument shows that a flow log entry may reflect logged packets that were sent between different endpoints,<sup>5</sup> but it falls a step short because the

---

<sup>5</sup> In the Sur-reply, Patent Owner argues that “Petitioner mistakes the [third flow log entry in Fig. 5G] as the packet flow entry as opposed to a further consolidation of packet flow entries.” Sur-reply 5. We disagree. That third entry is a consolidation of packet log entries, not a consolidation of entries from some other source that has

independent claims do not recite a “flow log.” However, the patent further explains that the packet filtering device “may utilize flow log 504 to generate data comprising an update for interface 600 and may communicate the data to host 110” and that “[f]or example, referring to FIG. 6G, the update may cause interface 600 to update *the entry in listing 606 associated with Threat ID: Threat\_1 to reflect the packets received in step 64.*” Ex. 1001, 15:65–16:5 (emphasis added).<sup>6</sup> Thus, the patent describes how the packet flow “entry” in the user interface may reflect logged packets that were sent between different endpoints (e.g., those at step 64). This description is sufficient to confirm that Patent Owner’s proposed construction of “packet flow” is too narrow. We find nothing in the patent that would limit “packet flow” to packets that are identified as part of the same connection between two endpoints.<sup>7</sup>

We agree with Patent Owner that “flow” may, in general, be used to refer to a stream of packets in a given connection between two endpoints. *See, e.g.*, Ex. 2014, 3. We nevertheless conclude that the ’917 patent describes “packet flow entries” in a way that does not limit them in the manner urged by Patent Owner. For example, the patent uses that term to refer to entries in the interface that correspond to groups of packets with a common Threat ID. That is reflected in the claim language reciting that the “packet flow entries” consolidate packet log entries “corresponding to a common threat identifier.”

---

collected packets as a “flow entry.” *See, e.g.*, Ex. 1001, 15:53–62 (describing how the entry for Threat\_1 is modified to include the packets received in step 64).

<sup>6</sup> We focus on the description for Figure 6G because it describes an update to a packet flow entry, and the claims recite “updating, by the packet-filtering device and based on the packet log entry, a packet flow entry.”

<sup>7</sup> We see nothing in the brief prosecution history of the ’917 patent that bears on the meaning of “flow,” “packet flow,” or “packet flow entry.”

For these reasons, we reject Patent Owner’s effort to narrow “flow,” as it appears in the claim term “packet flow entry,” to packets that are part of the same connection between two endpoints. We conclude that, consistent with its ordinary meaning in the context of the claims, “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.<sup>8</sup>

*C. Overview of the Prior Art*

*1. Sourcefire*

Sourcefire is a user guide for the Sourcefire 3D System, a system that provides “real-time network intelligence for real-time network defense.” Ex. 1004, 32.<sup>9</sup> 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. *Id.* at 33–34. 3D Sensors use “detection engines” that “analyze network traffic for evidence of attacks on network resources.” *Id.* at 254. 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. *Id.*

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.” *Id.* at 34, 254. An “intrusion rule” is “[a] set of keywords and arguments that, when applied to captured network traffic, identify

---

<sup>8</sup> At the hearing, Patent Owner argued that “[i]n [only] two instances do you change what [a] common[ly] understood term means: if there’s lexicography in the patent specification or there’s a clear disavow[al]” and that “[n]one of those occurred.” Tr. 34. We find this argument unpersuasive because “packet flow entry” does not have a common meaning.

<sup>9</sup> All citations to Sourcefire refer to the document’s original pagination.

potential intrusions, policy violations, and security breaches.” *Id.* at 2084. If a “pass rule” is met, the network traffic in question is ignored (and allowed to continue). *Id.* at 761. Conversely, if a “drop rule” is met, the packet is dropped and an “event” is generated. *Id.*

A Sourcefire rule may contain a “rule header” and optional “[r]ule [k]eywords and [a]rguments.” *Id.* at 762–63. The “rule header” includes the rule’s action or type (e.g., alert), the protocol (e.g., tcp), the source and destination IP addresses and netmasks, direction indicators showing the flow of traffic from source to destination, and the source and destination ports. *Id.* at 762, 764–769. “Keywords and their associated values (called arguments) dictate how the system evaluates packets and packet-related values that the rules engine tests.” *Id.* at 769. Any number of keywords can be combined to create specific tasks to perform inspection functions, “such as content matching, protocol-specific pattern matching, and state-specific matching.” *Id.*

When a detection engine identifies a possible intrusion (i.e., a security breach, attack, or exploit that occurs on the network), 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.” *Id.* at 254, 2084. Intrusion events are added to a database, and reports of intrusion events can be displayed on a user interface. *Id.* at 274–84. For example, Petitioner’s Figure B, an annotated version of a screenshot of Sourcefire’s “table view of intrusion events” (Ex. 1004, 281), is reproduced below:

Drill Down of Destination Port | Drill Down of Events | **Table View of Events** | Alerts

2006-11-11 00:00:00 - 2006-11-11 23:59:59 State

Search Constraints (Edit Search Save Search)

Disabled Columns

|                                                      |                                           |                                                |                                                 |                                                     |                                                     |                                                                    |                 |                   |                   |       |                    |
|------------------------------------------------------|-------------------------------------------|------------------------------------------------|-------------------------------------------------|-----------------------------------------------------|-----------------------------------------------------|--------------------------------------------------------------------|-----------------|-------------------|-------------------|-------|--------------------|
| Intrusion Events                                     | NSA Events                                | Hosts                                          | Host Attributes                                 | Services                                            | Client Apps                                         | Flows                                                              | Vulnerabilities | Compliance Events | White List Events | Users | Remediation Alerts |
| <div><div></div><div>Time</div></div>                | <div><div></div><div>Priority</div></div> | <div><div></div><div>Source IP</div></div>     | <div><div></div><div>Destination IP</div></div> | <div><div></div><div>SRC Port/ICMP Type</div></div> | <div><div></div><div>DST Port/ICMP Code</div></div> | <div><div></div><div>Message</div></div>                           |                 |                   |                   |       |                    |
| <div><div></div><div>2006-11-11 20:20:44</div></div> | <div><div></div><div>high</div></div>     | <div><div></div><div>10.8.12.23</div></div>    | <div><div></div><div>19.8.11.166</div></div>    | <div><div></div><div>35568/tcp</div></div>          | <div><div></div><div>21 (ftp)/tcp</div></div>       | <div><div></div><div>FTP Mkd overflow attempt (1:1973)</div></div> |                 |                   |                   |       |                    |
| <div><div></div><div>2006-11-11 20:20:62</div></div> | <div><div></div><div>high</div></div>     | <div><div></div><div>172.16.18.290</div></div> | <div><div></div><div>1054/tcp</div></div>       | <div><div></div><div>21 (ftp)/tcp</div></div>       | <div><div></div><div>21 (ftp)/tcp</div></div>       | <div><div></div><div>FTP Mkd overflow attempt (1:1973)</div></div> |                 |                   |                   |       |                    |
| <div><div></div><div>2006-11-11 20:19:59</div></div> | <div><div></div><div>high</div></div>     | <div><div></div><div>192.168.8.112</div></div> | <div><div></div><div>2859/tcp</div></div>       | <div><div></div><div>21 (ftp)/tcp</div></div>       | <div><div></div><div>21 (ftp)/tcp</div></div>       | <div><div></div><div>FTP Mkd overflow attempt (1:1973)</div></div> |                 |                   |                   |       |                    |
| <div><div></div><div>2006-11-11 20:19:11</div></div> | <div><div></div><div>high</div></div>     | <div><div></div><div>10.8.12.23</div></div>    | <div><div></div><div>19.8.11.166</div></div>    | <div><div></div><div>35568/tcp</div></div>          | <div><div></div><div>21 (ftp)/tcp</div></div>       | <div><div></div><div>FTP Mkd overflow attempt (1:1973)</div></div> |                 |                   |                   |       |                    |
| <div><div></div><div>2006-11-11 20:18:29</div></div> | <div><div></div><div>high</div></div>     | <div><div></div><div>172.16.18.290</div></div> | <div><div></div><div>1054/tcp</div></div>       | <div><div></div><div>21 (ftp)/tcp</div></div>       | <div><div></div><div>21 (ftp)/tcp</div></div>       | <div><div></div><div>FTP Mkd overflow attempt (1:1973)</div></div> |                 |                   |                   |       |                    |
| <div><div></div><div>2006-11-11 20:18:26</div></div> | <div><div></div><div>high</div></div>     | <div><div></div><div>192.168.8.112</div></div> | <div><div></div><div>2859/tcp</div></div>       | <div><div></div><div>21 (ftp)/tcp</div></div>       | <div><div></div><div>21 (ftp)/tcp</div></div>       | <div><div></div><div>FTP Mkd overflow attempt (1:1973)</div></div> |                 |                   |                   |       |                    |
| <div><div></div><div>2006-11-11 20:17:38</div></div> | <div><div></div><div>high</div></div>     | <div><div></div><div>10.8.12.23</div></div>    | <div><div></div><div>19.8.11.166</div></div>    | <div><div></div><div>35568/tcp</div></div>          | <div><div></div><div>21 (ftp)/tcp</div></div>       | <div><div></div><div>FTP Mkd overflow attempt (1:1973)</div></div> |                 |                   |                   |       |                    |
| <div><div></div><div>2006-11-11 20:16:56</div></div> | <div><div></div><div>high</div></div>     | <div><div></div><div>172.16.18.290</div></div> | <div><div></div><div>1054/tcp</div></div>       | <div><div></div><div>21 (ftp)/tcp</div></div>       | <div><div></div><div>21 (ftp)/tcp</div></div>       | <div><div></div><div>FTP Mkd overflow attempt (1:1973)</div></div> |                 |                   |                   |       |                    |
| <div><div></div><div>2006-11-11 20:16:53</div></div> | <div><div></div><div>high</div></div>     | <div><div></div><div>192.168.8.112</div></div> | <div><div></div><div>2859/tcp</div></div>       | <div><div></div><div>21 (ftp)/tcp</div></div>       | <div><div></div><div>21 (ftp)/tcp</div></div>       | <div><div></div><div>FTP Mkd overflow attempt (1:1973)</div></div> |                 |                   |                   |       |                    |
| <div><div></div><div>2006-11-11 20:16:05</div></div> | <div><div></div><div>high</div></div>     | <div><div></div><div>10.8.12.23</div></div>    | <div><div></div><div>19.8.11.166</div></div>    | <div><div></div><div>35568/tcp</div></div>          | <div><div></div><div>21 (ftp)/tcp</div></div>       | <div><div></div><div>FTP Mkd overflow attempt (1:1973)</div></div> |                 |                   |                   |       |                    |
| <div><div></div><div>2006-11-11 20:15:28</div></div> | <div><div></div><div>high</div></div>     | <div><div></div><div>172.16.18.290</div></div> | <div><div></div><div>1054/tcp</div></div>       | <div><div></div><div>21 (ftp)/tcp</div></div>       | <div><div></div><div>21 (ftp)/tcp</div></div>       | <div><div></div><div>FTP Mkd overflow attempt (1:1973)</div></div> |                 |                   |                   |       |                    |

|          |          |            |            |                      |
|----------|----------|------------|------------|----------------------|
| View     | Copy     | Delete     | Review     | Download Packets     |
| View All | Copy All | Delete All | Review All | Download All Packets |

Next

12345678910+<

(Showing 1 - 11 of 624)

FIG. B

FIG. B

“Figure B” from Page 26 of the Petition

Pet. 26 (citing Ex. 1003 ¶ 127). 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). *Id.* (citing Ex. 1003 ¶ 127; Ex. 1004, 274–282, 314–315, 1573–1575, 2077).

## 2. Macaulay

Macaulay concerns a method of refining cyber threat intelligence data. *See* Ex. 1029 ¶ 7. It 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.” *Id.* ¶ 24. 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. *Id.*

A portion of Macaulay’s Figure 3 is reproduced below:

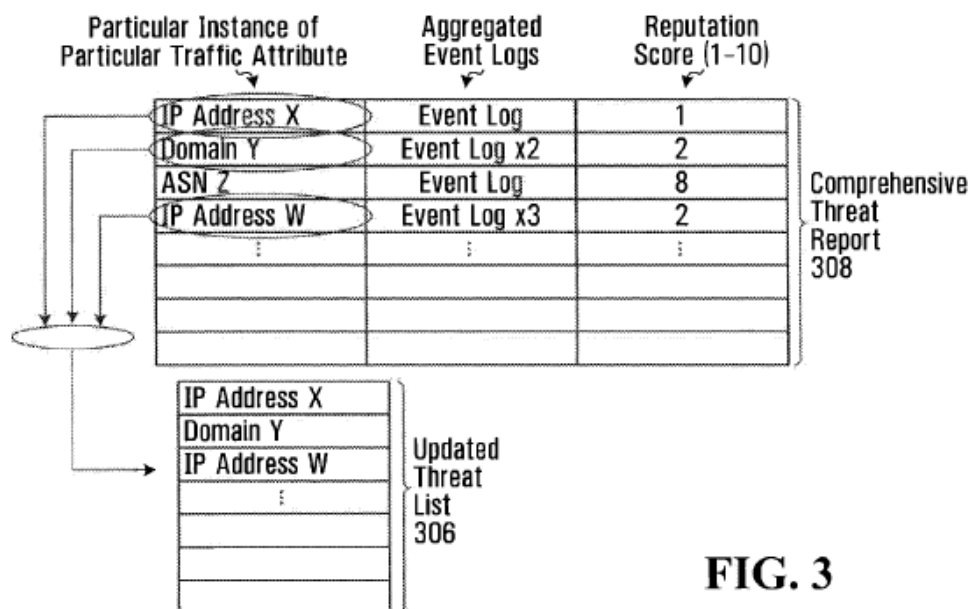


**FIG. 3**

*Macauley’s “FIG. 3 shows various forms of cyber threat intelligence data at different stages of a threat intelligence data refining process.” Ex. 1029 ¶ 16.*

Based on collected raw threat intelligence, the IHQ produces comprehensive threat report 308, which is a table of records. *See id.* ¶ 65. 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. *See id.* ¶¶ 65–70.

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.” *Id.* ¶¶ 76–82.

*D. Independent Claim 1*

We start with whether claim 1 would have been obvious in view of Sourcefire.

*1. Receiving Packets, Applying Rules to Block or Allow Passage, and Generating Packet Log Entries*

Claim 1 recites a method that begins with “receiving, by a packet-filtering device, a plurality of packets.” Then, in limitations [1b–1b2], the packet-filtering device determines whether a packet corresponds to a packet-filtering rule and, if so, applies “an operator specified by [the] packet-filtering rule” that is configured to cause the packet-filtering device to either block the packet or allow it to continue to its destination. The packet-filtering device then generates a “packet log entry” that includes a “threat identifier” corresponding to the packet and “data” indicating whether packet was blocked or allowed to continue.

Petitioner cites Sourcefire as disclosing a method in which a packet-filtering device (a 3D Sensor with IPS) receives and examines a plurality of packets traversing a network, looking for malicious activity, and reporting or taking actions based on detected malicious activity. *See* Pet. 31 (citing Ex. 1003 ¶¶ 134–137; Ex. 1004, 34–35, 254–255). Petitioner asserts that a packet may trigger a rule corresponding to a plurality of network threat indicators (e.g., a source or destination address) associated with the particular exploit the rule is designed to detect. *See id.* at 32 (citing Ex. 1004, 762–769). When a packet triggers the rule, the IPS applies the “operator” specified by the rule (e.g., allow, drop, or alert) to the triggering packet. *See id.* (citing Ex. 1004, 765–755, 290–292, 295–299). Thus, Petitioner contends that in response to a determination that a first packet

corresponds to a packet-filtering rule, the operator specified by the rule prevents the packet from continuing toward its destination (if it satisfies a drop rule) or allows the packet to continue toward its destination (if it satisfies a pass or alert rule), as required by limitations [1b] and [1b1]. *See id.* at 34 (citing Ex. 1004, 276–277, 290–292, 295–299, 358–359, 438, 761, 765).

For the packet log entry, Petitioner offers the following annotated version of Sourcefire's table view of intrusion events:

Drill Down of Destination Port > Drill Down of Events > Table View of Events > Packets

2006-11-11 00:00:00 - 2006-11-11 23:59:00  
Status

Search Constraints (Edit Search Save Search)

Disabled Column

| Intrusion Events         | RNA Events               | Hosts                    | Host Attributes          | Services                 | Client AOs               | Flows                             | Vulnerabilities          | Compliance Events        | White List Events        | Users                    | Related objects          |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|-----------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>          | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Time                     | Priority                 | Source IP                | Destination IP           | SRC Port/ICMP Type       | DST Port/ICMP Code       | Message                           |                          |                          |                          |                          |                          |
| 2006-11-11 20:08:44      | high                     | 10.0.10.20               | 10.0.11.166              | 35568/tcp                | 21 (ftp/tcp)             | FTP RFD overflow attempt (1.1973) |                          |                          |                          |                          |                          |
| 2006-11-11 20:08:02      | high                     | 172.16.10.101            | 172.16.10.200            | 1687/tcp                 | 21 (ftp/tcp)             | FTP RFD overflow attempt (1.1973) |                          |                          |                          |                          |                          |
| 2006-11-11 20:13:59      | high                     | 192.168.0.112            | 192.168.0.98             | 2659/tcp                 | 21 (ftp/tcp)             | FTP RFD overflow attempt (1.1973) |                          |                          |                          |                          |                          |
| 2006-11-11 20:13:13      | high                     | 10.0.10.20               | 10.0.11.166              | 35568/tcp                | 21 (ftp/tcp)             | FTP RFD overflow attempt (1.1973) |                          |                          |                          |                          |                          |
| 2006-11-11 20:13:00      | high                     | 172.16.10.101            | 172.16.10.200            | 1654/tcp                 | 21 (ftp/tcp)             | FTP RFD overflow attempt (1.1973) |                          |                          |                          |                          |                          |
| 2006-11-11 20:13:06      | high                     | 192.168.0.112            | 192.168.0.98             | 2659/tcp                 | 21 (ftp/tcp)             | FTP RFD overflow attempt (1.1973) |                          |                          |                          |                          |                          |
| 2006-11-11 20:13:08      | high                     | 10.0.10.20               | 10.0.11.166              | 35568/tcp                | 21 (ftp/tcp)             | FTP RFD overflow attempt (1.1973) |                          |                          |                          |                          |                          |
| 2006-11-11 20:13:56      | high                     | 172.16.10.101            | 172.16.10.200            | 1654/tcp                 | 21 (ftp/tcp)             | FTP RFD overflow attempt (1.1973) |                          |                          |                          |                          |                          |
| 2006-11-11 20:14:53      | high                     | 192.168.0.112            | 192.168.0.98             | 2659/tcp                 | 21 (ftp/tcp)             | FTP RFD overflow attempt (1.1973) |                          |                          |                          |                          |                          |
| 2006-11-11 20:14:05      | high                     | 10.0.10.20               | 10.0.11.166              | 35568/tcp                | 21 (ftp/tcp)             | FTP RFD overflow attempt (1.1973) |                          |                          |                          |                          |                          |
| 2006-11-11 20:15:22      | high                     | 172.16.10.101            | 172.16.10.200            | 1654/tcp                 | 21 (ftp/tcp)             | FTP RFD overflow attempt (1.1973) |                          |                          |                          |                          |                          |
| View                     | Copy                     | Delete                   | Review                   | Download Packets         |                          |                                   |                          |                          |                          |                          |                          |
| View All                 | Copy All                 | Delete All               | Review All               | Download All Packets     |                          |                                   |                          |                          |                          |                          |                          |

Next  
1 2 3 4 5 6 7 8 9 10 \* >|  
(Showing 1 - 11 of 634)

FIG. 8

*“Figure B” from Paragraph 150 of the Staniford Declaration*

*See* Pet. 35–37 (citing Ex. 1003 ¶ 150). Petitioner contends that each row, corresponding to an event, is a “packet log entry” that includes “a rule description (or type of exploit) and a rule ID number (SID) (green box), which is information indicating a ‘threat identifier’ and packet-filtering rule (e.g., identified in the message field as ‘FTD MKD overflow attempt (1:1973)’).” *Id.* (citing Ex. 1004, 281; Ex. 1003 ¶ 149). Petitioner also contends that each row contains an arrow (shown in the red box) indicating whether or not the packet was dropped. *See id.*

at 37 (citing Ex. 1003 ¶¶ 128, 150; Ex. 1004, 276); *id.* at 27 (explaining that options for the Inline Result (in the red box) are a black down arrow indicating a dropped packet, a gray down arrow indicating a packet would have been dropped if the user had enabled the “Drop when Inline” intrusion policy, and a blank indicating an allowed packet) (citing Ex. 1003 ¶ 128; Ex. 1004, 276, 281)). Petitioner further contends that each row includes “source and destination IP addresses and ports associated with a threat (yellow box), which are examples of network threat indicators.” *Id.* at 36 (Ex. 1003 ¶ 150).

We conclude that Petitioner has shown that Sourcefire’s event message teaches or suggests a “threat identifier.” As Petitioner points out, the event message’s text is a “rule description (or type of exploit).” Pet. 36; *see* Ex. 1004, 762 (indicating that rules may be designed to detect specific exploits). Because Sourcefire teaches that a rule itself identifies the threat, a text description of the rule, accompanied by an identification of the rule (e.g., the SID), would qualify as a “threat identifier.”

Patent Owner does not argue these limitations, and we find that Petitioner has shown that Sourcefire teaches or suggests limitations [1a–1b2].

## 2. *Updating a Packet Flow Entry*

In limitation [1c], the packet-filtering device “updat[es], by and based on the packet log entry,” a “packet flow entry” that corresponds to the packet log entry. The packet flow entry is “of packet flow analysis data for a plurality of logged packets,” and “the packet flow analysis data comprises data corresponding to a plurality of packet flow entries.” In addition, “each packet flow entry consolidates a plurality of packet log entries corresponding to a common threat identifier.”

Petitioner contends that Sourcefire’s 3D Sensor “generates a flow-log entry that consolidates, compresses, or summarizes the entries in the event log . . . for

display on the interface as shown” in the following annotated by Petitioner and labeled “Figure C”:



*“Figure C” from Paragraph 152 of the Staniford Declaration*

See Pet. 37–38 (citing Ex. 1003 ¶ 152; Ex. 1004, 282).

According to Petitioner and Dr. Staniford, the annotated figure above shows, for a single source IP address and a single destination IP address (in the yellow box), a count (in the orange box) of the number of packets associated with a threat identifier (in the green box) and an indication of whether the packets were allowed to continue or were dropped (in the red box). *Id.* at 38–39 (citing Ex. 1004, 278, 281); Ex. 1003 ¶ 152 (citing Ex. 1004, 280–282).

Petitioner contends that the count, and therefore the packet flow entry containing the count, could be periodically updated because the “event preferences” selected by a user include a “refresh interval,” which updates event information (e.g., the count) displayed in the packet flow log at a user-selected refresh interval. Pet. 39 (citing Ex. 1003 ¶ 153; Ex. 1004, 46–47). Thus, Petitioner contends, a person of ordinary skill in the art “would have understood that updating or refreshing the count modifies or updates existing packet flow entries

that consolidate a plurality of packet log entries corresponding to a common threat identifier and rule.” *Id.* (citing Ex. 1003 ¶ 154).

Patent Owner makes five arguments concerning this limitation: (1) that there is no “packet flow entry” in view of Patent Owner’s requested construction of “packet flow”; (2) that there is no updating by a packet-filtering device; (3) that Sourcefire’s refresh interval cannot meet the claim’s “updating”; (4) that the updating in Sourcefire is not “based on [a] packet log entry”; and (5) that Petitioner has not shown a “plurality of packet flow entries.” We address the arguments in that order.

*a. Packet Flow Entry*

Patent Owner first argues that “the challenged claims are patentable because the alleged ‘packet flow entry’ is not an entry reflecting ‘a connection level state where packets are identified as being part of the same connection between two endpoints.’” PO Resp. 15. That argument is unpersuasive because it is based on Patent Owner’s proposed construction of “packet flow,” which we do not adopt.

Patent Owner argues that Sourcefire “does not maintain or store packet flow analysis data” because “[i]nstead, the 3D sensor only captures single-packet events and stores them in the event database.” PO Resp. 15. The claim, however, does not require that the packet flow analysis data be maintained or stored; instead, it simply requires “a packet flow entry” of “packet flow analysis data for a plurality of logged packets.” In Sourcefire, the packet flow entry is the “entry” shown in, for example, Petitioner’s Figure C. That 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.

Patent Owner argues that “Petitioner’s sole alleged example of a ‘packet flow entry’ does not mention a flow table (which is commonly used to track flow information of traffic), disclose any information about which connection the packet is associated with, or even contain the Source IP address which would be necessary to identify the second endpoint.” PO Resp. 15–16. None of those things, however, are required by the claims.

The ’917 patent describes the use of a flow log with entries that are updated based on the packet flow entries that match rules, whereas Sourcefire’s packet flow entries are generated on the fly as the user clicks through the different screens, but that distinction is not reflected in claim 1, which does not recite a “flow log.”

For these reasons, we find Patent Owner’s argument that Sourcefire does not disclose a “packet flow entry” unpersuasive.

*b. Updating by a Packet-Filtering Device*

Patent Owner argues that “[e]ach independent claim of the ’917 Patent requires the generation of packet flow data including a threat identifier associated with the flow” and that “[b]ecause the packet-filtering device is responsible for updating a packet flow entry of a plurality of packet flow entries before communicating the updated data to the computing device, the packet flow information must be generated and maintained by the packet-filtering device.” PO Resp. 17–18. According to Patent Owner, “[i]f the packet flow analysis data is absent, the packet filtering device could not ‘update’ one of those packet flow entries upon generating a new packet log entry,” “[n]or could the packet-filtering device communicate the updated packet flow analysis data to another computing system for display.” *Id.* at 18. Patent Owner concludes that “the packet flow

analysis data must be generated and maintained by the packet-filtering device so that it can be updated and transmitted to another computing device” and “Sourcefire’s 3D Sensor does not have any notion of packet flow data, and therefore cannot update and communicate, any packet flow analysis data.” *Id.* Patent Owner further argues that “Sourcefire’s web interface is merely a tool to view a response to a query for information from the 3D Sensor’s event log” and that the “query neither causes nor requires the packet-filtering device to update a stored packet flow entry or any other packet flow analysis data [because] it is merely a search tool for the events database.” *Id.* at 18–19.

Petitioner’s response to this argument is that the claims do not require storing packet flow analysis data and that “even if the claims also required storage of the packet flow entry of packet flow analysis data, they would be disclosed by Sourcefire.” Reply 12–13. Petitioner is correct that the claims do not require storing the data, although Petitioner does not appear to explicitly address Patent Owner’s core argument, which is that the claims require (1) that the “packet filtering device” update a packet flow entry of packet flow analysis data and, (2) that the packet flow analysis data is “communicat[ed], by the packet-filtering device and to a computing device.” We, nevertheless, agree that this subject matter is disclosed in Sourcefire. In the Petition, the “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. *See* Pet. 25–30. The claim requires that it is the “packet-filtering device” that updates the packet flow entry, but does not preclude that the packet flow entry that is being updated is the one shown in the interface. In fact, that is essentially the same as what is described

in the '917 patent, where the packet-filtering device “generate[s] data comprising an update for interface 600 and may communicate the data to host 110.” *See* Ex. 1001, 15:64–65. The examples described in '917 patent “may utilize flow log 104” to generate the update, but claim 1 is not limited to data from a flow log,<sup>10</sup> and the patent’s use of the word “may” confirms that it is not necessary.

Patent Owner asserts that “Sourcefire’s web interface is merely a tool to view a response to a query for information from the 3D Sensor’s event log” and that “[t]his query neither causes nor requires the packet-filtering device to update a stored packet flow entry or any other packet flow analysis data; it is merely a search tool for the events database.” PO Resp. 18. We find this unpersuasive because the claim does not preclude the use of a query that causes the packet filtering device to provide data to update the packet flow entry in the interface.

For these reasons, we are unpersuaded by Patent Owner’s argument that Sourcefire does not disclose a packet-filtering device updating a packet flow entry, and we thus agree with Petitioner on this issue.

*c. Sourcefire’s “Refresh Interval”*

Patent Owner argues that the claimed “updating” cannot be met by Sourcefire’s “refresh interval” because “the refresh interval refreshes the information for event views, and has nothing to do with packet flow data or the drill-down workflows.” PO Resp. 20 (citing Ex. 2013 ¶¶ 59–60; Ex. 1004, 1604 (“Refresh Interval[:] Sets the refresh interval for event views, in minutes.”)). According to Patent Owner, “[f]or drill-down workflow views, data does not refresh at the specified refresh interval” but “[i]nstead, the time window only changes when the user changes to a new workflow.” *Id.* (citing Ex. 2013 ¶¶ 59–60; Ex. 1004, 1614 (“Note that unless you have either paused the time window or

---

<sup>10</sup> Claims 4 and 14 do recite a “flow log.” *See* Section II.E.2.

have configured a static time window, the time window changes when you change workflows.”)).

Patent Owner further argues that “Sourcefire’s drill-down workflow view, which contains the alleged ‘packet flow entry,’ is generated when a user adds constraints to a table populated with information about individual events” and that “[w]hen a constraint is added, the view advances ‘to the next page in the workflow retaining the current constraints and carrying forward all events.’” PO Resp. 21 (citing Ex. 2013 ¶¶ 62, 66; quoting Ex. 1004, 281, 1606–1607). Patent Owner thus argues that “even if a refresh of the event table view would have resulted in some new events being added and some old events being removed, the drill-down workflow views contain only the events listed in the table at the time the user generated the workflow view” and “[t]he information that [is] displayed in one of these drill-down workflow views only changes when the user begins a new workflow.” *Id.* (citing Ex. 2013 ¶¶ 59–60; Ex. 1004, 1614).

Petitioner responds that “the Sourcefire manual does not say that the refresh interval only applies to event views, and not to drill-down workflows” and that “Sourcefire teaches that a user may ‘pause the time window, which allows you to examine a snapshot of the data provided by the workflow.’” Reply 13 (citing Ex. 1004, 1606).

We agree with Petitioner, because we find that Sourcefire describes applying a refresh interval to “event views,” which is a category that includes the workflows that display the packet flow entries. *See* Ex. 1004, 74 (“you can invoke event views (that is, workflows)”); Ex. 1003 ¶¶ 153–154. We thus disagree with Patent Owner’s assertion that the information in the drill-down workflow views “only changes when the user begins a new workflow.” PO Resp. 21.

For these reasons, we are not persuaded by Patent Owner’s argument that Sourcefire does not disclose the claimed updating.<sup>11</sup>

*d. Updating Based on a Packet Log Entry*

Patent Owner argues that “[e]ven granting Petitioner’s argument that drill-down workflow views would be updated with new data periodically at the ‘refresh interval,’” that technique “would not satisfy the Challenged Claims because the update would be based on the arbitrary ‘refresh interval’ rather than the claimed ‘the packet log entry.’” PO Resp. 22. Patent Owner contends that the refresh time interval is “unrelated to the traffic that Sourcefire is processing and, therefore, updates based on the ‘refresh interval’ are not based on the claimed packet log entry.” *Id.* at 23.

Petitioner responds that “because the flow log entry includes a count of packets, the only logical conclusion is that it is updated based on received packet log entries.” Reply 15. We agree with Petitioner. The 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. Patent Owner’s argument is directed to what caused the update, but claim 1 does not require that the update be caused by the receipt of new packets.

For these reasons, we are not persuaded by Patent Owner’s argument that Sourcefire does not update “based on the packet log entry.”

---

<sup>11</sup> Petitioner also argues that collateral estoppel applies because the Board found in the ’722 IPR that Sourcefire teaches “updating, by the packet-filtering device and based on a packet-log entry, a packet flow log.” *See* Pet. 38 n.9 (citing Ex. 1006, 2; Ex. 1026, cl. 6; Ex. 1030, 42–43; Ex. 1040, 58–60). This argument is moot because we resolve the issue in Petitioner’s favor, but we conclude that collateral estoppel would *not* apply, because the updating in the ’722 patent was of a “packet flow log,” which is different than the “packet flow entry” recited in the ’971 patent. This is discussed further in Section II.E.2, concerning claims 4 and 14.

*e. Data Corresponding to a Plurality of Packet Flow Entries*

Finally, Patent Owner argues that “[a]ccording to Petitioner, Sourcefire’s single-entry drill-down table view ‘shows a packet flow entry that consolidates [90] packet log entries corresponding to a common threat identifier,’” but that Petitioner does not explain where Sourcefire discloses ‘a plurality of packet flow entries,’ as is its burden under 37 C.F.R. § 42.104(b)(4).” PO Resp. 26 (citing Pet. 39). We find this argument unpersuasive because, as explained above, the “packet flow analysis data” is the set of entries in the packet log that correspond to the flow log entry.

\* \* \*

Because we agree with Petitioner’s analysis and find Patent Owner’s arguments unpersuasive, we determine that Petitioner has shown that Sourcefire teaches limitation [1c].

*3. Communicating the Packet Flow Analysis Data*

Limitation [1d] recites “communicating, by the packet-filtering device and to a computing device, the packet flow analysis data.”

Petitioner contends that Sourcefire teaches that the 3D Sensor communicates packet flow analysis data to a Defense Center (i.e., a computing device) and also communicates packet flow analysis data to a computing device when providing it to a local web interface. *See* Pet. 40 (citing Ex. 1003 ¶ 156; Ex. 1004, 34–35, 254–255, 284).

Patent Owner does not separately argue this limitation, and we find that Petitioner has shown that Sourcefire teaches limitation [1d].

*4. Causing Display of Packet Flow Analysis Data*

In limitation [1e], the method “caus[es], based on the communicated packet flow analysis data, display of at least a portion of the packet flow analysis data.”

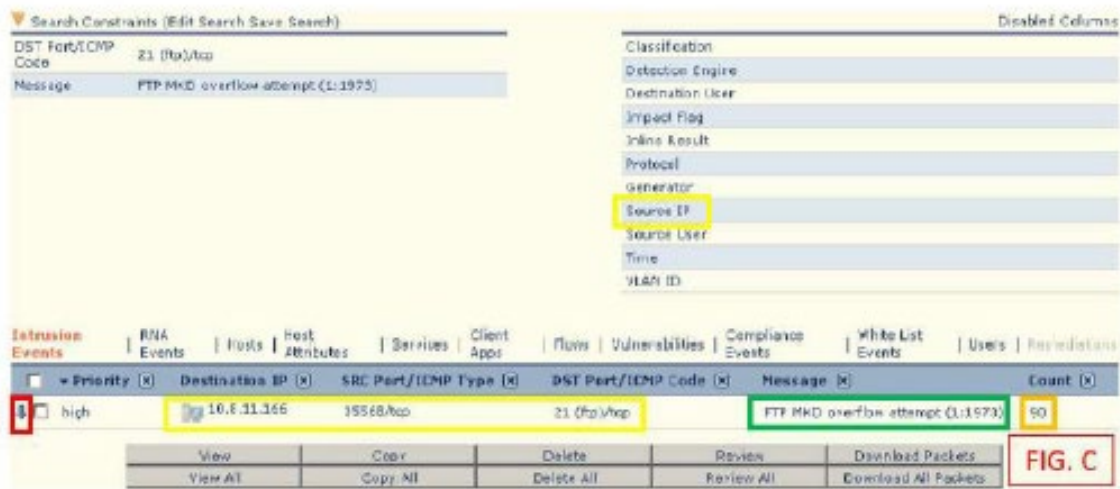
Petitioner contends that Sourcefire teaches causing at least a portion of the communicated packet flow analysis data to be displayed on the local web user interface, as shown above for limitation [1c]. *Id.* at 41 (citing Ex. 1003 ¶ 157; Ex. 1004, 34–35, 56, 280).

Patent Owner does not separately argue this limitation, and we find that Petitioner has shown that Sourcefire teaches limitation [1e].

5. *Content Of the Packet Flow Analysis Data*

Final limitation [1f] requires that the packet flow analysis data includes (1) a “threat identifier corresponding to each of the plurality of logged packets,” (2) “packet time data for packets corresponding to the packet flow entry,” and (3) data indicating whether packets were blocked or allowed to continue.

For this limitation, Petitioner refers to its annotated Figure C (reproduced again below), which shows packet flow analysis data, including a threat identifier (in the green box) and data indicating whether the 3D Sensor allowed the packets to continue or dropped them (in the red box). Pet. 42–43 (citing Ex. 1003 ¶¶ 158–159; Ex. 1004, 278, 281–282). For the time data, Petitioner points to the “disabled” columns in annotated Figure C, including “Time,” and notes that the disabled columns may be added to the view. *Id.* at 43 (citing Ex. 1003 ¶ 160; Ex. 1004, 281–282, 289). According to Petitioner, the hidden “Time” column teaches or suggests that the packet flow analysis data includes packet time data for the packets corresponding to the displayed packet flow entry. *Id.*



*Petitioner's Figure C*

Patent Owner argues that Sourcefire does not disclose “packet time data for packets corresponding to the packet flow entry.” *See* PO Resp. 23–26. Patent Owner disputes that the hidden time column could be added to the drill-down workflow view because “the time associated with each event in Sourcefire’s event database is unique,” such that “it would have been impossible to consolidate any two events into something resembling a packet flow entry while also maintaining the Time column.” PO Resp. 23. This argument is not persuasive because the claim does not require displaying the time data, as it only requires causing “display of *at least a portion* of the packet flow analysis data.” Ex. 1001, 18:1–3 (emphasis added). 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), and the packet log entries include “time data.” *See, e.g.*, Ex. 1004, 281 (“The columns in the table list information such as the time, the source IP address and port, the destination IP address and port, the event priority, the event message, and more.”).

For these reasons, we determine that Petitioner has shown that Sourcefire teaches limitation [1f].

6. *Conclusion for Independent Claim 1*

For the reasons explained above, we determine that Petitioner has shown by a preponderance of the evidence that Sourcefire teaches or suggests all the limitations of claim 1.

E. *Independent Claims 11 and 20*

Independent claims 11 and 20 are substantially similar in scope to claim 1, except that they require “a packet log entry comprising at least one threat *indicator*” rather than “a packet log entry comprising at least one threat *identifier*.” Compare Ex. 1001, 19:34–35, 21:24–25, with *id.* at 17:51–52. As noted above, Petitioner contends that each row of Sourcefire’s table of intrusion events includes “source and destination IP addresses and ports associated with a threat (in the yellow box), which are examples of network threat indicators.” See Pet. 36 (citing Ex. 1003 ¶ 150). For the remaining limitations of claims 11 and 20, Petitioner presents the same analysis as for claim 1. See Pet. 30–43.

Patent Owner does not separately argue claims 11 or 20, or dispute that Sourcefire teaches “a packet log entry comprising at least one threat indicator.”

Thus, for the same reasons as set forth above for independent claim 1, we determine that Petitioner has shown by a preponderance of the evidence that Sourcefire teaches or suggests all the limitations of claims 11 and 20.

F. *Dependent Claims 2–5 and 12–15*

Petitioner contends that dependent claims 2–5 and 12–15, each of which depends directly from independent claim 1 or independent claim 11, would have

been obvious in view of Sourcefire, and explains how Sourcefire teaches or suggests each claim limitation. *See* Pet. 44–52.

*1. Claims 2 and 12: Packet Filtering Rules  
and Environmental Data*

Claims 2 and 12 require that the packet log entry include data identifying a corresponding packet filtering rule, and claims 4 and 14 require updating a packet flow log entry to indicate a corresponding packet filtering rule. Noting that “Petitioner identifies the alleged threat identifier (i.e., the message field) as the packet filtering rule,” Patent Owner argues that “the threat identifier does not identify the rule that was applied to the packet, nor what in the packet triggered the rule.” PO Resp. 28. Petitioner responds that “the rule ID number (i.e., Snort ID or SID) included within the message field is data identifying a corresponding packet filtering rule.” Reply 23 (citing Pet. 45, 49). Patent Owner replies that “Petitioner now changes its theory to argue that it is relying on the Snort ID or SID” and that, in any event, “SID cannot meet the claim requirements” because “[a]s noted in Sourcefire, the SID is associated with vulnerability not the rule itself.” Sur-reply 16 (citing Ex. 1004, 981 (stating that the SID is “[t]he identification number associated with the vulnerability in the Snort ID (SID) database”)).

We find Patent Owner’s argument unpersuasive because Sourcefire explains that the Snort IDs identify the packet-filtering rules. *See, e.g.*, Ex. 1004, 499 (“The event’s SID indicates which specific rule triggered.”). On the page cited by Patent Owner, Sourcefire’s “Vulnerability Detail Information” table explains that “if an intrusion rule can detect network traffic that exploits a particular vulnerability, that vulnerability is associated with the intrusion rule’s SID.” *Id.* at 981. The phrase “the intrusion rule’s SID” confirms that an SID identifies a rule. That a rule may also be associated with one or more vulnerabilities does not mean that it is not a

rule. And, contrary to Patent Owner’s claims, the Petition did explain that the Snort ID identified a packet-filtering rule. *See* Pet. 45–46.

Patent Owner also argues that “environmental data,” as recited in claims 2 and 12, refers to “data that either specifically identifies the packet filtering device amongst many or to the ingress/egress interfaces of the packet filtering device.” PO Resp. 28 (citing Ex. 1001, 6:43–49). Patent Owner argues that the “Detection Engine” identified by Petitioner is not a packet filtering device or an ingress/egress interface of a packet filtering device because it “instead refers to an internal analysis system.” *Id.* at 28–29. Patent Owner also argues that the “VLAN ID” identified by Petitioner “is applied to the packets before they arrive at Sourcefire and, thus, cannot be used to identify an ingress/egress interface of the Sourcefire device.” *Id.* at 29.

Petitioner responds that Patent Owner’s argument “contradicts the specification, which does not reference “environmental data,” but gives an open list of examples of environmental variables, including an identifier associated with a packet-filtering device.” Reply 24 (citing Ex. 1001, 6:43–49).

Neither party has sought a construction of “environmental data,” so we apply the ordinary meaning of the term, which is simply data concerning the environment, and we agree with Petitioner that either the detection engine or the VLAN ID would qualify as data about the environment.

For these reasons, we determine that Petitioner has shown by a preponderance of the evidence that Sourcefire teaches or suggests the packet filtering rules and environmental variables of claims 2, 4, 12, and 14.

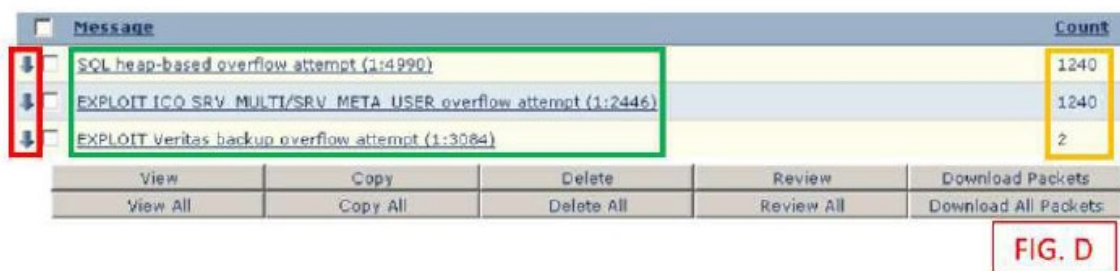
## *2. Claims 4 and 14: Updating a Packet Flow Log Entry*

Petitioner contends that Sourcefire discloses the limitations of claims 4 and 14. *See* Pet. 48–50. Patent Owner argues that “the claim language for Claims 4

and 14 require[s] that the packet flow log entry is updated in response to a determination that each packet corresponds to one or more packet-filtering rules” and that “Petitioner merely points to the refresh or update interval that will update the orange count box.” PO Resp. 29. Patent Owner contends that “the ‘Count’ is determined when the user clicks on constraints that result in multiple rows having matching data, not in response to determination that each packet corresponds to a packet filtering rule.” *Id.*

Petitioner responds that “claims 4 and 14 are directed to modifying an existing packet flow log entry, not modifying the display” and that “Sourcefire updates the packet flow entry in response to a determination that each packet triggers a packet-filtering rule.” Reply 25. Petitioner asserts that “when the display is updated, the display shows the packet flow entry that was updated in response to packets triggering rules” and that “the updating or modifying of the packet flow log entry is still in response to the determination of whether packets trigger rules and are allowed or blocked.” *Id.*

We agree with Patent Owner, because Petitioner has not shown that Sourcefire satisfies the claim language “*modifying . . . responsive to a determination that each packet corresponds to one or more packet-filtering rules, and based on the packet log entry, an existing packet flow log entry.*” Petitioner points to its Figure D, reproduced below, which it says 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.” Pet. 49.



| Message                                                       | Count |
|---------------------------------------------------------------|-------|
| SQL heap-based overflow attempt (1:4990)                      | 1240  |
| EXPLOIT ICQ.SRV.MULTI/SRV.META.USER overflow attempt (1:2446) | 1240  |
| EXPLOIT Veritas backup overflow attempt (1:3084)              | 2     |

|          |          |            |            |                      |
|----------|----------|------------|------------|----------------------|
| View     | Copy     | Delete     | Review     | Download Packets     |
| View All | Copy All | Delete All | Review All | Download All Packets |

FIG. D

*Petitioner's Figure D*

However, those entries are generated on the fly in response to the user clicking on the entry for one of the ports on the preceding screen. *See* Ex. 1004, 280–281 (showing “a drill-down page with the number of events generated for each destination port” and explaining 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”). Figure D may show an “entry” in the interface, but Petitioner has not shown how or why it could be an “existing flow log entry.”

Moreover, even assuming the Figure D entries could each be a “log entry,” Petitioner fails to show that they are updated “responsive to a determination that each packet corresponds to one or more packet-filtering rules.” Petitioner asserts that the number of packets could be updated according to the refresh interval (*see* Pet. 50), but, even if that is true, we agree with Patent Owner that it is insufficient to show that the modifying happens *in response to* a determination that a packet matches a rule. In 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. That 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. *See, e.g.*, Ex. 1001, 15:30–41 (“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.”).<sup>12</sup>

In addition, claims 4 and 14 require that the existing packet flow log entry be modified “to indicate one or more corresponding packet-filtering rules” and whether the device “prevented each packet from continuing toward each packet’s respective destination or allowed each packet to continue toward each packet’s respective destination.” The only modification Petitioner identifies concerns a change to the number of packets for each type of event. Petitioner 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.”

Petitioner asserts that we are bound on this issue by the result in the affirmed ’722 IPR, where “the Board found that Sourcefire teaches updating a packet flow log based on packet log entries.” Pet. 49 (citing Ex. 1026 cl. 6; Ex. 1030, 42–43; Ex. 1040, 58–60). We do not agree that the ’722 IPR result controls, because the Final Written Decision in the ’722 IPR found that Sourcefire disclosed updating “a packet flow log,” while claims 4 and 14 are directed to updating “an existing packet flow log *entry*.” To the extent the panel in the ’722 IPR agreed with that petitioner regarding claim 6, it agreed that Sourcefire disclosed a “packet-flow log,” not a “packet-flow log entry.”<sup>13</sup> Again, those refer to different things in the

---

<sup>12</sup> We note 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.”

<sup>13</sup> For claims 4 and 14, Petitioner largely copied the argument made in the ’722 IPR petition for claim 6, but changed “packet-flow log” to “packet-flow log entry” without explanation. Compare Pet. 49 (“*the flow log entry* includes consolidated information from the packet log entries generated by the 3D Sensor identifying packets corresponding to packet-filtering rules (green box) by updating the count

'917 patent. We conclude that the difference between “packet flow log” and “packet flow log entry” is sufficient to “materially alter the question of invalidity,” such that collateral estoppel does not apply. *See MaxLinear, Inc. v. CF CRESPE LLC*, 880 F.3d 1373, 1377 (Fed. Cir. 2018) (quoting *Ohio Willow Wood Co. v. Alps South, LLC*, 735 F.3d 1333, 1342 (Fed. Cir. 2013)).

For these reasons, we conclude that Petitioner has not shown claims 4 and 14 to be unpatentable in view of Sourcefire.

3. *Claims 3 and 13: A Time Range of the Packets*

Claim 3 depends from claim 1 and recites that “the packet flow analysis data comprises a time range of the plurality of packet log entries corresponding to the common threat identifier, and wherein the time range indicates an earliest hit time and a latest time hit.” Claim 13, which depends from Claim 11, includes similar limitations.

Petitioner contends “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.’” Pet. 47 (citing Ex. 1003 ¶ 167). Patent Owner argues that “the views that allegedly show this data do not have any possible data fields that could represent the first and last

---

(orange box) of the packets as well as an indication (red box) of whether the packets were allowed to continue toward their respective destinations or [were] dropped”), *with* Ex. 1040, 66 (“***the packet-flow log*** included consolidated information generated by the 3D Sensor identifying the same threat indicator (green) by updating the count (orange) of the packets associated with each threat indicator as well as an indication (red) of whether the packets were allowed to continue or [were] dropped”).

packet timestamps because the timestamps are specific to individual packets.” PO Resp. 30 (citing Ex. 2013 ¶¶ 68–69, 75–79).

Patent Owner’s argument is unpersuasive because although the claims require that the packet flow analysis data include a time range, they do not require that the time range is displayed, because they only recite “display of *at least a portion* of the packet flow analysis data.” As explained above, Sourcefire describes displaying a threat identifier, which is “at least a portion of the packet flow analysis data.”

For these reasons, we determine that Petitioner has shown by a preponderance of the evidence that Sourcefire teaches or suggests the time range of claims 3 and 13.

#### 4. *Claims 5 and 15*

For claims 5 and 15, which respectively depend from claims 1 and 11, Patent Owner argues that “[a]s discussed for Claims 4 and 14, Petitioner fails to identify the claimed packet flow log entry.” *Id.* This is unpersuasive because claims 5 and 15 do not recite a “packet flow log entry.” Instead, they recite “packet flow entry” and “packet log entry.”

Patent Owner does not make other arguments for these claims, and we determine that Petitioner has shown by a preponderance of the evidence that Sourcefire teaches or suggests the subject matter of claims 5 and 15.

#### G. *Dependent Claims 6 and 16*

Claim 6 depends from claim 1 and adds that the packet flow analysis data includes “one or more scores . . . associated with a corresponding packet flow entry.” Ex. 1001, 18:45–48. The scores are determined based on the number of packets associated with the packet flow entry and on times associated with the packets. The scores are “updat[ed] . . . based on each packet log entry” and

“indicat[ed]” in the packet flow analysis data. Claim 16 depends from independent claim 11 and recites substantially the same limitations as claim 6.

*1. Petitioner’s Contentions*

Petitioner refers to its annotated Figure C, which it contends shows flow analysis data for a packet flow entry, including a threat identifier corresponding to the logged packets and a priority level, which is pre-specified for the rule associated with the threat identifiers. Pet. 58 (citing Ex. 1003 ¶ 185; Ex. 1004, 278, 281); *see* Ex. 1004, 282. Petitioner contends that when a 3D Sensor (packet-filtering device) in Sourcefire generates an intrusion event, it assigns an event priority. Pet. 58 (citing Ex. 1003 ¶ 185; Ex. 1004, 276).

Petitioner then contends that Macaulay teaches aggregating or summarizing logged data into a comprehensive threat report that includes information such as a particular instance of a particular traffic attribute and a reputation score. *Id.* at 58–59 (citing Ex. 1003 ¶ 186; Ex. 1029 ¶¶ 65–70). Petitioner contends that a person of ordinary skill in the art would have been motivated to include Macaulay’s reputation score in Sourcefire’s flow analysis data to communicate the risk associated with a given threat, similar to how the reputation score is presented in the table in Macaulay’s Figure 3. *Id.* at 59. Petitioner contends it would have been obvious to do so by replacing Sourcefire’s high/medium/low priority level with a numerical score. *Id.* (citing Ex. 1003 ¶¶ 90–97, 186).

For determining the scores based on a number of packets associated with the packet flow entry and on times associated with the packets, Petitioner cites Macaulay for teaching a reputation score based on various traffic attributes including “traffic flow rate/volume” and “time-of-day patterns.” Pet. 59 (citing Ex. 1029 ¶ 24). Petitioner contends that a person of ordinary skill in the art would have understood that a traffic flow rate is a number of packets over time, and that

Macaulay therefore teaches scores based on both a number of packets associated with a threat and the time of those packets. *Id.* at 60 (citing Ex. 1003 ¶ 187).

Petitioner further cites Macaulay as teaching that “a reputation score may be impacted by, and thus based on, other factors, including ‘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 appeared among the raw cyber threat intelligence.’” *Id.* (citing Ex. 1003 ¶ 188; Ex. 1029 ¶¶ 76, 80, 82).

Petitioner contends that Macaulay teaches updating scores over time based on the number of logged events, with a greater number of logged events having a lowering (i.e., worsening) effect on the reputation score. Pet. 60 (citing Ex. 1003 ¶ 190; Ex. 1029 ¶ 80). Petitioner also cites Macaulay’s “decay factor,” which “causes a reputation score to rise if time has increased since the threat was detected, and based on other factors, such as a flow rate, time-of-day patterns, or the number of sources that have revealed a traffic attribute as a threat.” *Id.* at 60–61 (citing Ex. 1003 ¶ 190; Ex. 1029 ¶¶ 24, 76–82). According to Petitioner, a person of ordinary skill in the art would have updated Macaulay’s reputation scores based on each packet log entry. *Id.* at 61 (citing Ex. 1003 ¶ 190). For example, scores would decrease with a greater number of logged packets or greater flow rate associated with a threat. Ex. 1003 ¶ 190.

Petitioner notes that Sourcefire’s priority levels are based on a priority keyword associated with the rule that triggered the event, which is set manually when the rule is created, such that the priority is determined by the person or entity that created the rule. Pet. 55 (citing Ex. 1004, 293, 310, 772; Ex. 1003 ¶ 180). Petitioner asserts that Macaulay teaches a better approach to prioritization, including, for example, a reputation score based on the number of cyber threat

intelligence sources that revealed the threat. *Id.* (citing Ex. 1003 ¶ 180; Ex. 1029 ¶¶ 76–77). According to Petitioner, Macaulay thus provides a nimbler scoring system that captures intelligence from multiple sources, reflecting industry consensus, and updates in real time. *Id.* at 55–56.

For a motivation to combine, Petitioner asserts that replacing Sourcefire’s basic priority levels with Macaulay’s reputation score would more accurately identify and respond to potential threats. *See id.* at 56 (citing Ex. 1003 ¶¶ 180–181). Petitioner contends there would have been a reasonable expectation of success in doing so given the extent of art in the area and because it would have been a straightforward use of common mathematical operators. *Id.* (citing Ex. 1003 ¶¶ 90–96, 180–183). Petitioner further contends that the combination would still allow for manual setting of a reputation score, like Sourcefire’s priority keyword setting, but with a scoring system that would allow for more accurate prioritization of and response to threats. *Id.* at 56–57 (citing Ex. 1003 ¶ 180). Petitioner adds that a person of ordinary skill in the art would have been motivated to calculate scores for one or more threat identifiers disclosed by Sourcefire because Macaulay’s score represents the risk associated with a given threat. *Id.* at 57 (citing Ex. 1003 ¶ 182).

## 2. *Patent Owner’s Arguments and Our Analysis*

Patent Owner contends that “Petitioner’s argument ignores the actual language of the claim, which states that the ‘score is associated with a corresponding packet flow entry,’” and that “Petitioner fails to provide an explanation as to how a score can be associated with a packet flow entry that requires a user to select columns in a drill down system to come into existence.” PO Resp. 32 (quoting Ex. 2013 ¶¶ 83–85). This argument is not persuasive because the “packet flow entry” in the combination is the line with the colored

boxes in Petitioner’s Figure C, which includes the Message, “FTP MKD overflow attempt (1:1973)” identifying an event, which would have a priority. *See, e.g.*, Ex. 1004, 293 (listing a “high” priority for the event “BACKDOOR DoomJuice/mydoom.a.backdoor.upload/execute attempt (1:2375)”).

Patent Owner argues that “Sourcefire lacks the requisite packet flow entry,” that “[t]he view in Sourcefire simply displays the number of packets blocked, but does not contain any flow or connection information,” and that “because there is no flow information, there cannot be any information regarding the timing of packets associated with the flow entry.” PO Resp. 32–33 (citing Ex. 2013 ¶ 84). We do not agree with this argument. An example of a “packet flow entry” is shown in Petitioner’s Figure C and reflects ninety packets blocked by the rule. The packet log entries for the individual ninety packets would include the time information. *See* Ex. 1004, 281–283 (showing the packet view with times).

Noting that Petitioner “asserts that the comprehensive threat report 308 in Macaulay Figure 3 teaches the claimed packet flow analysis data because it aggregates or summarizes logged data,” Patent Owner argues that “packet flow analysis data requires . . . data corresponding to a plurality of packet flow entries, with each of the packet flow entries consolidating a plurality of packet log entries corresponding to a common threat identifier, and packet time data,” and “[t]he threat report 308 of Macaulay does not meet these requirements.” PO Resp. 33. This contention is unpersuasive because Petitioner is not arguing that Macaulay’s threat report provides all of the claimed packet flow analysis data. Instead, Petitioner argues that Sourcefire supplies the data required by claim 1 and that Macaulay would provide claim 6’s scores based on the number of packets and times associated with the packets. *See* Pet. 56–57.

Patent Owner also argues that Petitioner “incorrectly asserts that a ‘reputation score’ shown in the Macaulay threat report 308 is ‘a score associated with the corresponding packet flow entry,’” but “nothing in Macaulay indicates that any of the rows of Macaulay’s threat report 308 in Figure 3 is associated with a packet flow entry as defined by Claim 1.” PO Resp. 33. This argument also is not persuasive. In the combination, the “packet flow entry” is found in Sourcefire and is modified to include Macaulay’s scoring. We see no reason why “rows of Macaulay’s threat report 308” would otherwise need to be “associated with a packet flow entry as defined by Claim 1.”

Finally, Patent Owner argues that Petitioner “ignores differences between the Sourcefire priority levels and the Macaulay reputation score.” PO Resp. 33. Specifically, Patent Owner argues that “Sourcefire’s high, medium, or low priority levels are network specific and represent the likelihood that an event will affect a particular organization’s network,” but “Macaulay’s reputation scores, on the other hand, are network-agnostic and reflect the extent to which an ‘intelligence headquarters’ of a carrier network considers that network traffic characterized by a particular instance of a particular traffic attribute is compromised.” PO Resp. 33–34 (citing Ex. 1004, 309–310, 322, 1540; Ex. 1029 ¶ 70). Patent Owner asserts that “Petitioner’s proposed replacement would change the principle of operation of Sourcefire and would defeat the purpose of the Sourcefire priority level—providing a customizable parameter for categorizing intrusion events to tailor event analysis (via reports, workflows, and notifications) to a specific organization’s network.” *Id.* at 34.

We find this argument unpersuasive for three reasons. First, Patent Owner overstates the disclosure on page 322 of Sourcefire, which simply explains that an administrator handling incident investigation would need an “understanding how a

detected event can affect the security of [their] network assets” as, “[f]or example, an attack against hosts running Microsoft SQL Server is not a high priority for organizations that use a different database server.” This does not show that Sourcefire’s priority levels are “network specific”; instead, it suggests that the response should be based on how the specific network might be affected. Second, Petitioner asserts that it would have been obvious to either replace Sourcefire’s priority levels *or* augment the priority levels with Macaulay’s techniques, providing the benefits of both approaches. *See* Pet. 56. Third, a motivation to combine does not require showing that an asserted combination is the “preferred, or most desirable, combination.” *In re Fulton*, 391 F.3d 1195, 1200 (Fed. Cir. 2004). Rather, an obvious combination may be one that is “described as somewhat inferior to some other product for the same use.” *Id.* (quoting *In re Gurley*, 27 F.3d 551, 552–53 (Fed. Cir. 1994)). In this case, we agree that it would have been obvious to build a system like Sourcefire but implement Macaulay’s scoring for its stated advantages (*see* Pet. 55), even if that meant the loss of some alleged network specific benefits.

\* \* \*

For these reasons, we determine that Petitioner has shown it would have been obvious to modify Sourcefire as taught by Macaulay to arrive at the subject matter of claims 6 and 16. Thus, we find that Petitioner has shown by a preponderance of the evidence that claims 6 and 16 would have been obvious over the teachings of Sourcefire and Macaulay.

#### *H. Dependent Claims 8 and 18*

Claim 8 recites that the score determining is “based on an identity of one or more network-threat-intelligence providers that provided network-threat indicators associated with a corresponding threat identifier, and a number of network-threat

intelligence providers that provided network-threat indicators associated with a corresponding threat identifier.” Claim 18 is of corresponding scope.

Petitioner asserts that “Macaulay discloses that the score may be impacted by ‘the origin of the raw cyber threat intelligence (external versus internal),’ and that ‘seed information from law enforcement can be given the maximum weight.’” Pet. 64 (citing Ex. 1003 ¶ 194; Ex. 1029 ¶¶ 76–78). Petitioner further argues that “Macaulay also discloses determining a reputation score based on a ‘number of cyber threat intelligence sources that have revealed the particular instance of the particular traffic attribute as a potential threat.’” *Id.* (citing Ex. 1003 ¶ 195; Ex. 1029 ¶¶ 76–77).

Patent Owner argues that “to the extent that Petitioner relies on Sourcefire to provide the network threat indicators from a network intelligence provider, the Board has already determined that “Snort is not a threat intelligence provider—Snort is an open source intrusion detection system for real-time traffic analysis and packet logging that uses a rules language to describe network traffic that the IPS should collect or pass.” PO Resp. 35 (citing Ex. 2007, 29). This argument is not persuasive because Petitioner is not “rel[ying] on Sourcefire to provide the network threat indicators from a network intelligence provider.”

Patent Owner also argues that “Petitioner [does not] explain how the packet-filtering device would combine with Macaulay’s IHQ to make a score determination as required by Claim 18.” PO Resp. 35 (citing Ex. 2013 ¶ 88). This argument is also unpersuasive. The combination involves substituting or augmenting Sourcefire’s priority levels with a Macaulay-type scoring system, and the Petition explains how this would satisfy the language of claims 8 and 18. *See* Pet. 63–64.

For these reasons, we determine that Petitioner has shown by a preponderance of the evidence that Sourcefire teaches or suggests the subject matter of claims 8 and 18.

*I. Dependent Claims 7, 9, 10, 17, and 19*

Patent Owner does not separately argue claims 7, 9, 10, 17, or 19. Having reviewed the arguments and evidence of record, we agree with Petitioner that the subject matter of these claims is taught or suggested in Sourcefire. *See* Pet. 62–63 (claims 7 and 17), 65–66 (claims 9 and 19), 66–67 (claim 10). Thus, we find that Petitioner has shown by a preponderance of the evidence that claims 7, 9, 10, 17, and 19 would have been obvious over the teachings of Sourcefire and Macaulay.

### III. CONCLUSION

Petitioner has met its burden of showing that claims 1–3, 5–13, and 15–20 of the '917 patent are unpatentable but has not met its burden of showing that claims 4 and 14 are unpatentable.<sup>14</sup> The results are summarized below:

| Claim(s)                   | 35<br>U.S.C. § | Reference(s)         | Claim(s)<br>Shown<br>Unpatentable | Claim(s) Not<br>Shown<br>Unpatentable |
|----------------------------|----------------|----------------------|-----------------------------------|---------------------------------------|
| 1–5,<br>11–15, 20          | 103            | Sourcefire           | 1–3, 5, 11–13,<br>15, 20          | 4, 14                                 |
| 6–10,<br>16–19             | 103            | Sourcefire, Macaulay | 6–10, 16–19                       |                                       |
| <b>Overall<br/>Outcome</b> |                |                      | 1–3, 5–13,<br>15–20               | 4, 14                                 |

---

<sup>14</sup> Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner's attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. See 84 Fed. Reg. 16654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. See 37 C.F.R. § 42.8(a)(3), (b)(2).

#### IV. ORDER

For the reasons given, it is:

ORDERED that Petitioner's Motion to Exclude (Paper 30) is granted;

ORDERED that claims 1–3, 5–13, and 15–20 of U.S. Patent 10,193,917 B2 have been shown to be unpatentable and that claims 4 and 14 of U.S. Patent 10,193,917 B2 have not been shown to be unpatentable;

FURTHER ORDERED that, because this is a Final Written Decision, the parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

FOR PETITIONER:

Gerard M. Donovan  
Peter J. Chassman  
Jonathan I. Detrixhe  
Sidharth Kapoor  
REED SMITH LLP  
gdonovan@reedsmith.com  
pchassman@reedsmith.com  
jdetrixhe@reedsmith.com  
skapoor@reedsmith.com

FOR PATENT OWNER:

James Hannah  
Jeffrey H. Price  
Jenna Fuller  
KRAMER LEVIN NAFTALIS & FRANKEL LLP  
jhannah@kramerlevin.com  
jprice@kramerlevin.com  
jfuller@kramerlevin.com

Bradley C. Wright  
Scott M. Kelly  
Blair Silver  
BANNER & WITCOFF, LTD  
bwright@bannerwitcoff.com  
skelly@bannerwitcoff.com  
jhutchins@bannerwitcoff.com  
bsilver@bannerwitcoff.com