

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KEYSIGHT TECHNOLOGIES, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, LLC,
Patent Owner.

IPR2022-01535
Patent 10,609,062 B1

Before KEVIN F. TURNER, BRIAN J. McNAMARA, and
NORMAN H. BEAMER, *Administrative Patent Judges*.

McNAMARA, *Administrative Patent Judge*.

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

I. BACKGROUND

In response to a Petition (“Pet.”), on April 18, 2023, we instituted an *inter partes* review of claims 1–20 of U. S. Patent No. 10,609,062 B1 (“the ’062 patent”). Paper 9 (“Dec. to Inst.”). Patent Owner filed a Patent Owner Response (Paper 13, “PO Resp.”), Petitioner filed a Petitioner Reply (Paper 16, “Pet. Reply”), Patent Owner filed a Patent Owner Sur-reply (Paper 19, “PO Sur-reply”), and a transcript of an oral hearing held on January 19, 2024 (Paper 25, “Hr’g Tr.”) has been entered into the record.

We have jurisdiction under 35 U.S.C. § 6. This Final Written Decision is issued pursuant to 35 U.S.C. § 318(a). We base our decision on the preponderance of the evidence. 35 U.S.C. § 316(e); 37 C.F.R. § 42.1(d).

Having reviewed the arguments of the parties and the supporting evidence, we conclude that Petitioner has demonstrated by a preponderance of the evidence that the challenged claims are unpatentable.

II. THE ’062 PATENT

The ’062 Patent relates to “rule-based network-threat detection.” Ex. 1001, 1:45–46. The Specification 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 1:49–52. The packet-filtering rule criteria may correspond to one or more “network-threat indicators.” *Id.* at 1:52–53. A network-threat indicator may be, for example, “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 (e.g., malware). *Id.* at 3:18–33. The packet-filtering rule also specifies an “operator” to be applied by the packet-filtering device when the rule is triggered, the operator being configured to cause the device to either prevent or allow the packet to

continue toward its destination. *Id.* at 1:61–67. The device also generates a log entry comprising information from the packet-filtering rule identifying the network-threat indicator(s) and whether the packet was prevented or allowed to continue. *Id.* at 1:58–63. In addition, the Specification describes that the packet-filtering device communicates this information as well to a user device, which presents the information in an interface through which the user can cause the packet-filtering device to reconfigure the operator specified by the packet-filtering rule such that future packets would be prevented from continuing. *Id.* at 1:64–2:10. Figure 7 is a flow chart illustrating an embodiment of the disclosed method, and is reproduced below.

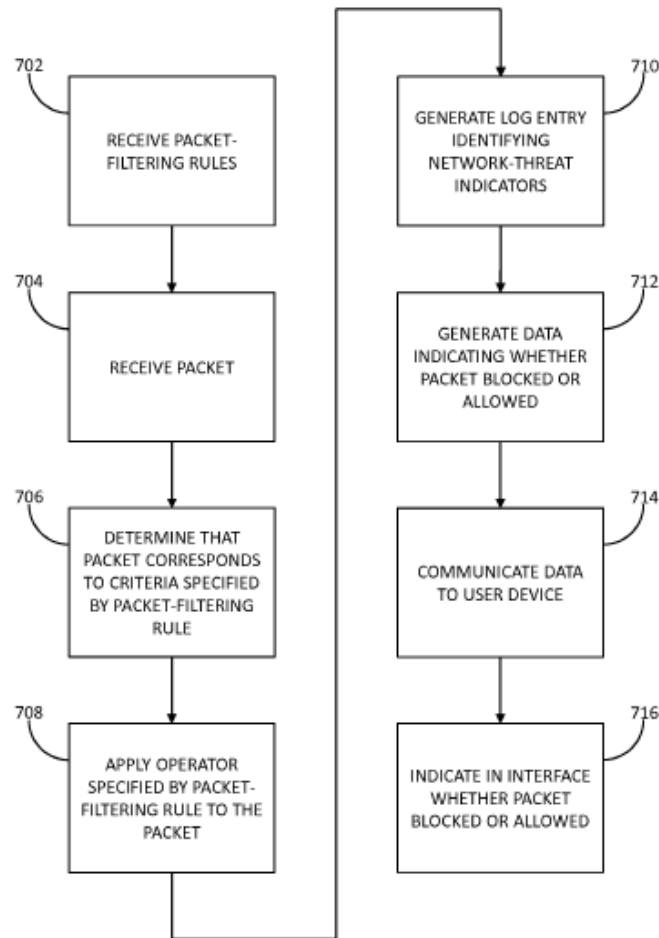


FIG. 7

Id. at Fig. 7. The above figure depicts an illustrative method for rule-based network-threat detection. *Id.* at 16:13–15; *see id.* at 15:54–16:34 (describing in detail each step depicted in Figure 7).

III. ILLUSTRATIVE CLAIM

Claim 1, shown below with paragraph designations used in the Petition in *italics*, is illustrative of the subject matter claimed in the '062 patent.

1.pre A method comprising:

1.a receiving, by a packet filtering device, a plurality of packet filtering rules configured to cause the packet

filtering device to identify packets corresponding to at least one of a plurality of network-threat indicators;

- 1.b* receiving, by the packet filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;
- 1.c* responsive to a determination by the packet filtering device that the first packet satisfies a first packet filtering rule, of the plurality of packet filtering rules, based on one or more network-threat indicators, of the plurality of network-threat indicators, specified by the first packet filtering rule:
- 1.d* applying, by the packet filtering device and to the first packet, an operator specified by the first packet filtering rule and configured to cause the packet filtering device to allow the first packet to continue toward a destination of the first packet; and
- 1.e* communicating, by the packet filtering device, information that identifies the one or more network-threat indicators, and data indicative that the first packet was allowed to continue toward the destination of the first packet;
- 1.f* causing, by the packet filtering device and in an interface, display of the communicated information in at least one portion of the interface corresponding to the first packet filtering rule and the one or more network-threat indicators;
- 1.g* receiving, by the packet filtering device and based on user selection of the at least one portion of the interface, an update to the first packet filtering rule and the one or more network-threat indicators;
- 1.h* modifying, by the packet filtering device and responsive to the received update to the first packet filtering rule, at least one operator specified by the first packet filtering rule to reconfigure the packet filtering device to prevent packets corresponding to the one or more network-threat indicators from continuing toward their respective destinations; and
- 1.i* responsive to a determination by the packet filtering device that the second packet satisfies the first packet filtering rule:

- l.j* preventing, by the packet filtering device and based on the modified at least one operator specified by the first packet filtering rule, the second packet from continuing toward a destination of the second packet;
- l.k* communicating, by the packet filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and
- l.l* causing, by the packet filtering device and in the interface, display of the data indicative that the second packet was prevented from continuing toward the destination of the second packet.

See, Ex. 1006, 1–2.

IV. GROUNDS OF INSTITUTION

Trial was instituted on the following grounds:

Claim(s) Challenged	35 U.S.C. §	Reference/Basis
1–20	103 ¹	Sourcefire ²

The parties also discuss the Board’s earlier decision concerning U.S. Patent U.S. Patent 9,143,722 B1 (the ’722 patent) in *Cisco Systems Inc. v. Centripetal Networks, Inc.*, IPR2018-01760, Paper 41 Final Written Decision (PTAB May 18, 2020), (“the ’722 patent IPR”), *aff’d. Centripetal Systems, Inc. v. Cisco Sys.*, 847 Fed. Appx. 881 (Fed. Cir. 2021). See Exs. 1026, 1031.

V. CLAIM CONSTRUCTION

In the Decision to Institute, we applied the following claim constructions:

¹ As the application for the ’062 patent was filed after March 16, 2013, we apply the provisions of The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 287–88 (2011).

² Sourcefire 3D System User Guide Version 4.10 (“Sourcefire”), *available* at <https://www.scribd.com/document/96860221/Sourcefire-3DSystem-User-Guide-v4-10>

A. Network-threat indicator:

We construed this term to mean an “indicator that represents the identity of a resource associated with a network threat.” Dec. to Inst. 16. Neither party disputes this claim construction and we apply it for purposes of this Decision.

B. Network-threat intelligence providers:

We construed this term to mean “entities associated with services that disseminate network-threat-intelligence reports.” *Id.* at 17. Neither party disputes this claim constructions and we apply it for purposes of this Decision

C. “Responsive to” and “Based on”

Subsequent to institution, each party proposed additional claim constructions that we address below.

1. Responsive to

Patent Owner proposed that, applying the plain and ordinary meaning, we construe “responsive to” to require that the claimed applying and communicating steps “must be performed based on a packet satisfying a packet-filtering rule based on network-threat indicators.” PO Resp. 6. According to Patent Owner:

the “responsive to language” of the claims establishes a relationship between (i) a packet satisfying a packet filtering rule based on one or more network-threat indicators and (ii) the subsequent application of an operator that allows the packet to continue and communication of information indicating the packet was allowed to continue.

Id. at 7.

“Petitioner agrees that ‘responsive to’ in the claims requires that the applying and communicating steps must occur responsive to a determination

that the packet satisfies the rule, not merely after.” Pet. Reply 3. To this extent, we do not perceive a dispute between the parties concerning the construction of “responsive to” and we apply the term’s plain and ordinary meaning, i.e., that steps recited in the claim as being performed “responsive to” a determination, e.g., “applying an operator,” are performed after the relevant determination is made.

2. *Based on*

Claim 1 recites that the “determination by the packet filtering device that the first packet satisfies a filtering rule” is “based on one or more network-threat indicators.” Ex. 1001 17:55–60. Neither Petitioner nor Patent Owner explicitly proposes a construction of “based on.”

Petitioner characterizes arguments advanced in the Patent Owner Response as contending that “if a rule tests anything *in addition to* network-threat indicators, then the actions performed ‘responsive to’ satisfying the rule are not ‘based on’ the network-threat indicator.” Pet. Reply 4. Petitioner’s Reply contends that a person of ordinary skill would have understood that “a determination or rule being *based on* one or more network-threat indicators does not preclude the determination or rule *also* being based on other information.” Pet. Reply 4 (citing Ex. 1068, Declaration of Dr. Staniford in Support of Petitioner Reply (“Staniford Reply Decl.”) ¶¶ 16–17); *see also id.* at 5–6 (citing *Masimo Corp. v. Sotera Wireless, Inc.*, 2023 U.S. App. LEXIS 25626*5 (Fed. Cir. Sept. 28, 2023), affirming the Board’s construction of “based on” as not excluding other conditions to trigger an alarm)). According to Petitioner, in the context of claim 1, a person of ordinary skill would understand that a network-threat indicator is an essential element of a rule, but the rule could have additional elements. Pet. Reply 4–6 (citing *Masimo Corp. v. Sotera Wireless, Inc.*,

2023 U.S. App. LEXIS 25626 *5 (Fed. Cir. Sept. 28, 2023 as affirming the Board’s analysis that “based on” is a broad term that does not exclude other conditions to trigger an alarm)).

Patent Owner argues that Petitioner “contests the proper construction of the ‘responsive to limitation’ in a way that severs the ‘based on’ language from the claim element it modifies, which is the ‘determination by the packet filtering device that the first packet satisfies a first packet filtering rule.’” PO Sur-reply 1 (citing Pet. Reply 2–8). According to Patent Owner, Petitioner’s “approach unhelpfully obfuscates whether the rule is *satisfied* based on network-threat indicators or whether the rule is *constructed* based on network-threat indicators.” *Id.* Patent Owner contends that satisfaction of the rule by the presence of the network-threat indicator is faithful to the claim language, but creation of the rule based on network-threat indicators is not. *Id.* at 1–2.

Patent Owner’s argument conflates how a user interacts with Sourcefire and Sourcefire’s definition and description of a rule. During the oral hearing, Patent Owner argued

What are the key issues that we’re talking about there? There’s the claim construction issue, which . . . boils down to . . . Can the rule have additional criteria that must be met before a rule is satisfied, or does the claim as plainly written require that the rule be satisfied based on one or more network threat-indicators? We submit that the additional unclaimed, undisclosed criteria is not part of this claim.

Hr’g Tr. 23:13–18. Patent Owner returned to this theme during its oral argument in the context of Petitioner’s contention that Patent Owner is collaterally estopped from arguing the patentability of the ’062 patent claims, based on the Board’s earlier decision in the ’722 patent IPR, as affirmed by the Federal Circuit. Patent Owner stated

Here in the ‘062 Patent we specifically have a requirement that the first packet filtering rule is satisfied based on the network threat-indicator, one network threat-indicator of a plurality. That, unlike the ‘722, does not leave room for additional criteria. It’s not there in claims. It’s not there in the pending claims. What the ‘062 requires is that the rule itself, the first packet filtering rule is satisfied based on one or more network threat-indicators.

Hr’g Tr. 19:8–14.

The claim language reciting that action be taken “responsive to a determination . . . that the first packet satisfies a first packet filtering rule . . . based on one or more network-threat indicators” does not recite how the determination is made and explicitly encompasses a determination based on one network-threat indicator or on multiple network-threat indicators. The claim also does not preclude a network-threat indicator (construed to mean an indicator that represents the identity of a resource associated with a network threat) from being determined based on the combination of several elements. For example, an IP source address may or may not be a network-threat indicator, depending on other parameters, such as the content of the message.

The term “based on” is used numerous times³ in the ’062 patent Specification without a description of its meaning. The Specification does not indicate any special meaning to the term “based on.” In one example, the ’062 patent describes assigning a score to a threat associated with a Threat ID “based on a determination that the network-threat indicators corresponding to the threat” were received from different numbers of

³ We estimate “based on” appears in the Specification between 25 and 30 times.

network-threat intelligence providers. Ex. 1001, 8:37–9:13. The Specification does not describe how that determination is made.

Patent Owner urges that we decline to extract the “based on” phrase from the “responsive to” claim limitation and interpret the entire claim in context. PO Sur-reply 4–5. Claim 1 of the ’062 patent broadly recites that “responsive to a determination . . . based on one or more network-threat indicators . . . specified by the first packet filtering rule,” certain actions are taken (e.g., applying an operator and communicating information that identifies the network-threat identifiers and indicates the packet was allowed to pass). Ex. 1001, 17:55–18:3. The claim’s recitation of an action being responsive to a determination *based on* one or more network-threat indicators does not preclude a rule that applies other considerations or tests additional criteria, provided that the rule considers at least one network-threat indicator. The broad “based on” claim language does not require that the rule perform or be structured in any particular way. Thus, we determine a rule that is responsive to one network-threat indicator is “based on” that network-threat indicator, regardless of how the rule weighs that network-threat indicator or evaluates other criteria.

Although Petitioner contends that Patent Owner’s collateral estoppel and obviousness arguments should be rejected based on an improper construction, Petitioner further contends that the term “based on” does not require construction because Sourcefire would render the claims obvious even if construed to require the determination and the rule be based solely on a network-threat indicator, as Patent Owner asserts. Pet. Reply 4–8. We address these contentions further in our analysis below. *See* Section VI.C. herein.

VI. ANALYSIS OF PRIOR ART CHALLENGES

A. Legal Standards

Petitioner contends that the challenged claims are obvious over Sourcefire. The question of obviousness is resolved on the basis of underlying factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) objective evidence of nonobviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

Additionally, the obviousness inquiry typically requires an analysis of “whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006) (requiring “articulated reasoning with some rational underpinning to support the legal conclusion of obviousness”)); see *In re Warsaw Orthopedic, Inc.*, 832 F.3d 1327, 1333 (Fed. Cir. 2016) (citing *DyStar Textilfarben GmbH & Co. Deutschland KG v. C.H. Patrick Co.*, 464 F.3d 1356, 1360 (Fed. Cir. 2006)).

An obviousness analysis “need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ.” *KSR*, 550 U.S. at 418; accord *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1259 (Fed. Cir. 2007). Petitioner cannot satisfy its burden of proving obviousness by employing “mere conclusory statements.” *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016). Instead, Petitioner must articulate a reason why a person of ordinary skill in the art would have combined the prior art references. *In re NuVasive*, 842 F.3d 1376, 1382 (Fed. Cir. 2016).

A reason to combine or modify the prior art may be found explicitly or implicitly in market forces; design incentives; the “interrelated teachings of multiple patents”; “any need or problem known in the field of endeavor at the time of invention and addressed by the patent”; and the background knowledge, creativity, and common sense of the person of ordinary skill. *Perfect Web Techs., Inc. v. InfoUSA, Inc.*, 587 F.3d 1324, 1328–29 (Fed. Cir. 2009) (quoting *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418–21 (2007)).

In determining whether a claim would have been obvious in light of the prior art, when in evidence, we consider any relevant objective evidence of non-obviousness. *See Graham*, 383 U.S. at 17. Notwithstanding what the teachings of the prior art would have suggested to one of ordinary skill in the art at the time of the invention, the totality of the evidence submitted, including objective evidence of non-obviousness, may lead to a conclusion that the challenged claims would not have been obvious to one of ordinary skill. *In re Piasecki*, 745 F.2d 1468, 1471–72 (Fed. Cir. 1984). Patent Owner does not present evidence of such objective considerations.⁴

We analyze the asserted grounds of unpatentability in accordance with these principles to determine whether Petitioner has met its burden to establish unpatentability of the challenged claims by a preponderance of the evidence.

B. 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.

⁴ In the ’722 patent IPR, the Federal Circuit affirmed the Board’s decision that Patent Owner failed to establish the required nexus between the claims and the objective indicia.

1004, 32.⁵ The Sourcefire 3D System discovers “changing assets and vulnerabilities” on a network, “determine[s] types of attacks against [a] network” and “defend[s] [a] network in real time.” *Id.* Sourcefire’s 3D Sensors aggregate network and user intelligence against internal and external threats and are capable of running the following components; the Sourcefire Intrusion Prevention System (IPS™), Real Time Network Awareness (RNA®), and Real Time User Awareness (RUA®). Ex. 1004, 34, 2074.

IPS uses the Snort® rules-based detection engine to perform real time traffic analysis and packet logging on IP networks. *Id.* at 33, 2094. Snort is “[a]n open-source detection system that performs real time traffic analysis and packet logging on IP networks.” *Id.* at 2094. IPS detection engines (mechanisms that analyze traffic on the network segment where a sensor is connected) use Snort to test packets against decoders, preprocessors and intrusion rules. *Id.* at 2078, 2094.

RNA, installed on each 3D Sensor, uses detectors to identify new and changed hosts on a network and correlate the operating system and services detected on each host with a database of known vulnerabilities to determine whether a particular host increases the risk of network compromise. *Id.* at 33, 2090, 2097. Additional detectors can be implemented via vulnerability database updates. *Id.* at 2090. RNA also uses information from detected packets to build and transmit to a Defense Center a map of devices on the network, event and flow data and sensor statistics that provide a consolidated view of events. *Id.* at 36.

⁵ All citations to Sourcefire refer to the document’s original pagination.

RUA correlates threat, endpoint, and network intelligence with user identity to allow creation of policies and response rules specific to users, such as individuals, or departments. *Id.* at 36.

Sourcefire also provides a Defense Center, i.e., a central management point that aggregates events the sensors generate and can be used to manage sensors by pushing to the 3D sensors software updates and policies created by the Defense Center. *Id.* at 2078. Managing 3D Sensors with IPS and RNA allows using the Defense Center to correlate intrusion events with host vulnerabilities and assign impact flags to prioritize intrusion events. *Id.* A user running RNA can set up compliance policies, compliance white lists, and traffic profiles to protect infrastructure by monitoring network traffic for unusual patterns or behavior and automatically responding as needed. *Id.* at 35–36.

Placing 3D Sensors with IPS on key network segments permits examination of packets traversing the network for malicious activity by using rules, decoders, and preprocessors to look for exploits that attackers have developed. *Id.* at 34. A rule is a construct that provides criteria against which network traffic is examined to detect intrusions, attacks, and suspicious traffic. *Id.* at 2091. “IPS compares packets against the conditions specified in each rule and, if the packet data matches all the conditions in a rule, the rule triggers.” *Id.* at 761. Sourcefire includes at least the following rules: compliance rule (*id.* at 2076), intrusion rule (*id.* at 2084), alert rule (*id.* at 2075), pass rule (*id.* at 2087), drop rule (*id.* at 2079) and preprocessor rule (*id.* at 2089). *See also id.* at 2019. Intrusion rules include rules developed by the Sourcefire Vulnerability Research Team (VRT) and custom intrusion rules developed by users. *Id.* at 34, 761. 3D Sensors with IPS can also run

preprocessors against detected network traffic to detect malicious packets.
Id. at 34.

Sourcefire rules contain a header and an options section. *Id.* at 762. The header section includes: the rule's action or type (e.g., alert), the protocol (e.g., TCP), the source (e.g., traffic on any host not on an internal network) and destination IP addresses (e.g., traffic to be delivered to a host on an internal network) and netmasks, direction indicators showing the flow of traffic from source to destination, and the source and destination ports (e.g., traffic delivered to an HTTP on an internal network). *Id.* at 762–769. The options section of a rule includes: event messages, keywords and their parameters and arguments, patterns that a packet's payload must match to trigger the rule, and specifications of which parts of the packet the rules engine should inspect. *Id.* at 762. Keywords allow performance of inspection functions, such as content matching, protocol-specific pattern matching, and state specific matching. *Id.* at 769–770. As part of defining an intrusion event in a rule, a user can “include external references to vulnerability databases.” *Id.* at 771, 776 (“[a]dding a reference provides analysts with an immediately available resource to help them identify why the packet triggered a rule”); *see also id.* at 861–864 (writing a rule). Sourcefire instructs a user

[t]o specify a reference using the rule editor, select a **reference** from the **Detection Options** list, and enter a value in the corresponding address field as follows:

id_system, id

where *id_system* is the system being used as a prefix and the *id* is the Bugtraq ID, CVE number, Arachnids ID or URL (without http://)

For example, to specify the authentication bypass vulnerability on Microsoft Commerce Server 2002 servers documented in Bugtraq ID 17134, enter the following in the **reference** field:

bugtraq, 17314.

Id. at 776.

C. Claims 1–20 As Obvious Over Sourcefire

1. Claim 1

a) Petitioner’s Contentions

The preamble of claim 1 merely recites “[a] method comprising.” Claim limitation 1[a] recites “receiving, by a packet filtering device, a plurality of packet filtering rules configured to cause the packet filtering device to identify packets corresponding to at least one of a plurality of network-threat indicators.” Ex. 1001, 17:48–51. Petitioner states that by placing 3D Sensors with IPS on key network segments, one can examine packets that traverse a network for malicious activity and use rules to look for a broad range of exploits that attackers have developed. Pet. 35 (citing Ex. 1003, Declaration of Dr. Stuart Staniford in Support of Petition, (“Staniford Decl.”) ¶¶ 141–147; Ex. 1030, 22). Petitioner identifies claim limitation 1[a] as a counterpart to claim limitation 1[a] of the ’722 patent and cites our determination in the ’722 patent IPR that Sourcefire discloses this limitation. Pet. 35–36 (citing Ex. 1006; Ex. 1030, 22). Noting that claim limitation 1[b] recites receiving a first packet and a second packet, Petitioner cites Sourcefire and the determination in the ’722 patent IPR that Sourcefire discloses a plurality of packets received at the 3D Sensors. Pet. 37 (citing Ex. 1003, Staniford Decl. ¶¶ 157–159; Ex. 1004, 255).

Petitioner argues that limitation 1[c] (the “responsive to” limitation), is a counterpart to limitation 1[c] of the ’722 patent that the Board found to be disclosed by Sourcefire in the ’722 patent IPR. Pet. 37–38. Petitioner

further argues that Sourcefire discloses generating an intrusion event upon recognizing a potentially malicious packet based on the application of the rules. *Id.* (citing Ex. 1003, Staniford Decl. ¶ 160, Ex. 1004, 274).

According to Petitioner, information in a 5-tuple could trigger a rule, e.g., a destination and source address specified by a packet filtering rule as associated with a threat are network-threat indicators. *Id.* (citing Ex. 1003, Staniford Decl. ¶¶ 161–162; Ex. 1004, 258–260, 761–769). Petitioner argues that a person of ordinary skill would have understood that a packet-filtering rule that was triggered and allowed a packet to continue would be deemed a “first” packet filtering rule, as claimed. *Id.* (citing Ex. 1003, Staniford Decl. ¶¶ 162–163).

Petitioner contends that, because limitations 1[d]–1[k] of the ’062 patent are counterparts of limitations 1[d]–1[k] of the ’722 patent, these limitations were already been addressed and found to be disclosed by Sourcefire in the ’722 patent IPR. Pet. 38–47.

b) Patent Owner’s Contentions

Patent Owner contends that Sourcefire’s intrusion rules do not apply operators or communication information responsive to a determination that a packet satisfies the rule-based network-threat indicators. PO Resp. 10, 14–18. Patent Owner advances two major arguments in support of its contentions: (1) collateral estoppel does not apply to the issue of whether Sourcefire satisfies the “responsive to” limitation, and (2) Sourcefire’s rules are satisfied based on the contents of the packets, not IP addresses (the alleged network-threat indicators). *Id.* at 16–18. In support of its second argument, Patent Owner asserts that (a) Sourcefire’s Intrusion rules trigger an action responsive to satisfying a Snort rule’s keyword and arguments, not a network-threat indicator (*id.* at 14–16) and (b) Sourcefire contradicts

Petitioner's arguments that Sourcefire triggers a rule's action responsive to matching an IP address (*id* at 16–18).

Patent Owner does not explicitly dispute Petitioner's contentions concerning limitations 1[d]–1[k].

c) Analysis of Claim 1

(1) Collateral Estoppel

“Issue preclusion [i.e., collateral estoppel] is appropriate only if: (1) the issue is identical to one decided in the first action; (2) the issue was actually litigated in the first action; (3) resolution of the issue was essential to a final judgment in the first action; and (4) [the party being estopped] had a full and fair opportunity to litigate the issue in the first action.” *In re Freeman*, 30 F.3d 1459, 1465 (Fed. Cir. 1994); *see also MaxLinear, Inc. v. CF CRESPE LLC*, 880 F.3d 1373, 1376 (Fed. Cir. 2018) (holding that issue preclusion applies in the administrative context).

Petitioner contends that the challenged claims overlap with claims of the '722 patent that were found unpatentable in the '722 patent IPR. Pet. 4 (citing Ex. 1030). Petitioner emphasizes that the Court of Appeals for the Federal Circuit affirmed the Board's finding in the '722 patent IPR. *Id.* (citing Ex. 1031). *See Alphatec Holdings, Inc. et al. v. NuVasive, Inc.*, 2020 Pat. App. LEXIS 12487, *25 (PTAB July 8, 2020) (findings in prior IPR, having been affirmed by the Federal Circuit, are binding on a later IPR as a matter of collateral estoppel).

In the Decision to Institute, we determined that the requirements for collateral estoppel had been met to the extent the constructions we applied in this proceeding are the same as those applied in the '722 patent IPR. Dec. to Inst. 26 (noting that applying the *Phillips* standard, we arrive at the same construction of “network-threat indicator” as the construction the Board

applied in the '722 patent IPR under the broadest reasonable construction standard). We also noted that the remaining limitations of claim 1 are similar to those considered in the '722 patent. *Id.* at 30; *see also* PO Resp. 10–11. As the Patent Owner Response does not dispute our claim construction of network-threat indicator, collateral estoppel applies to the extent matters in this proceeding turn on the construction of “network-threat indicator.”

The Patent Owner Response contends that issue preclusion does not apply to the “responsive to” limitations because of differences in the text of “responsive to” limitation 1[c] in the '062 patent claims and the “responsive to” limitation 1[c] of the '722 patent IPR. PO Resp. 11–12. Patent Owner argues that we should reject Petitioner’s allegation that collateral estoppel applies to any single claim element of the Challenged Claims, but does not identify any other issue impacting the application of collateral estoppel. *Id.* at 13.

Patent claims need not be identical for collateral estoppel to apply. *Soverain Software LLC v. Victoria’s Secret Direct Brand Mgmt., LLC*, 778 F.3d 1311, 1319 (Fed. Cir. 2015). Rather, collateral estoppel requires that the issues of patentability be identical. *Ohio Willow Wood Co. v. Alps S., LLC*, 735 F.3d 1333, 1342 (Fed. Cir. 2013). Thus, we consider the scope of the claimed subject matter in the '062 and '722 patents.

At the oral hearing, Patent Owner argued the '062 patent specifically requires that the first packet filtering rule is satisfied based on one network threat-indicator or a plurality of them. *See* Hr’g Tr. 19:8–11. According to Patent Owner, “unlike the '722, [the '062] does not leave room for additional criteria. It’s not there in [the] claims What the '062 requires

is that the rule itself, the first packet filtering rule is satisfied based on one or more network threat-indicators.” *Id.* at 19:11–14.

The Patent Owner Response highlights differences in the language of the ’062 and ’077 patent claims. PO Resp. 11. Claim 1 of the ’062 patent is not limited to criteria that “correspond to” a network-threat indicator, as recited in the claims of the related ’722 patent that was the subject of the ’722 patent IPR. According to Patent Owner, the ’062 patent requires a determination that a packet satisfies the entire rule, not just one or more criteria, and the threat indicators be specified by the packet filtering rule, not just correspond to one or more threat indicators. *Id.* at 11–12.

Patent Owner’s argument is unavailing. The language of claim 1 does not recite that the entire rule, i.e., each and every factor of a rule, be satisfied to trigger an action in response. As the text highlighted by Patent Owner indicates, to satisfy the requirements of a rule, limitation 1[c] of the ’062 patent requires a determination that the rule is satisfied “based on” one or more network-threat indicators specified by the rule. *Id.* For purposes of collateral estoppel, we compare limitation 1[c] of the ’722 patent with limitation 1[c] of the ’062 patent. Limitation 1[c] of the ’722 patent requires a determination that one or more criteria that correspond to one or more network-threat indicators specified by the rule is satisfied. Failure to satisfy the requirement for one or more network-threat indicators criteria specified by the rule means the conditions of the rule are not satisfied, i.e., the entire rule is not satisfied based on one or more network-threat indicators, as recited in limitation 1[c] of the ’062 patent. Therefore, we determine that the scope of the “responsive to” limitation (limitation 1[c]) of the ’062 patent overlaps the “responsive to” limitation (limitation 1[c]) of the ’722 patent.

Patent Owner also argues that collateral estoppel cannot apply because the issues in the '722 patent IPR and the current proceeding are not identical and were not decided in the '722 patent IPR. PO Resp. 12; PO-Sur-reply 8–9. Patent Owner emphasizes that the '722 patent IPR was decided applying the broadest reasonable claim construction applicable at the time, but the current procedures apply the *Phillips* claim construction standard. PO Resp. 12. As discussed above, however, claim construction is not determinative of the overlap of the subject matter of limitation 1[c]. Applying either the *Phillips* construction or the broadest reasonable interpretation, the determination “responsive to a determination. . . based on . . . network-threat indicators specified by the . . . filtering rule” recited in limitation 1[c] of the '062 patent overlaps the scope of “responsive to one or more criteria specified by a packet filtering rule . . . that correspond to network-threat indicators” recited in limitation 1[c] of the '722 patent. *See id.* at 11. We also note that the Federal Circuit affirmed the decision in the '722 patent IPR using language that mirrors the language of claim 1 of the '062 patent, stating: “we affirm the Board's finding that a relevant artisan would have understood Sourcefire to teach the claim-required filtering packets *on the basis of* network-threat identifiers as required by the challenged claims.” Ex. 1031, 6 (emphasis added). Thus, to the extent matters in this proceeding turn on the scope of the “responsive to” and “based on” language in limitation 1[c], that issue was addressed in the '722 patent IPR, and collateral estoppel applies.

Nevertheless, we need not and do not decide this case solely on the basis of collateral estoppel. We now further consider the parties' substantive arguments.

(2) *Analysis of Petitioner’s Challenge Based On Sourcefire*

Petitioner characterizes the Board’s determination in the ’722 patent IPR as finding that “Sourcefire teaches that packet-filtering rules may be triggered ‘responsive to’ matching an IP address.” Pet. Reply 17. Nevertheless, recognizing the differences in the language of the claims in the ’062 patent and the ’722 patent, we further consider Patent Owner’s arguments that (a) Sourcefire’s Intrusion rules trigger an action responsive to satisfying a Snort rule’s keyword and arguments, not a network-threat indicator (*id.* at 14–17) and (b) Sourcefire contradicts Petitioner’s arguments that Sourcefire triggers a rule’s action responsive to matching an IP address (*id.* at 17–19). As we discuss below, both of these arguments are unavailing.

Patent Owner contends that “Sourcefire’s 3D Sensors use intrusion rules to detect intrusion attempts based on the content of the packets received, not IP addresses (the alleged ‘network-threat indicator’).” PO Resp. 13 (citing Ex. 2004, Declaration of Dr. Michael T. Goodrich In Support of Patent Owner’s Response (“Goodrich Decl.”) ¶¶ 52–54). As our construction of “network-threat-indicators” in this proceeding under the *Phillips* standard is the same as the broadest reasonable interpretation construction applied in the ’722 patent IPR and is undisputed, we agree with Petitioner that collateral estoppel applies as to the construction of network-threat indicators and we turn our analysis to the network-threat indicators in the context of the language “responsive to” and “based on” in the ’062 patent.

Sourcefire discloses taking action “responsive to” a determination that a packet satisfies a packet filtering rule “based on” one or more network-threat indicators. *See* Section V.C herein. The Petition describes in detail

how a Sourcefire rule has a header section with 5-tuple criteria values useful for detecting intrusion events and an options section with keywords and arguments that aid in evaluating the packet's contents to reduce false positives and focus on intrusion information. Pet. 23–25, *see generally id.* at 21–31; *see also* Pet. Reply 14. The Petition states that

The IPS in each 3D sensor is designed such that packets would trigger a rule when data within a packet satisfied one or more specified “criteria” that corresponded to one or more network-threat indicators (e.g., source or destination IP address, source or destination port, application-layer data (e.g., protocol, URL, URI), etc.). Ex. 1003 ¶127; EX-1004 762-769. The IPS applies the “operator” specified by the rule (e.g. pass, drop, alert (and pass)) to the triggering packet upon the packet triggering the rule. EX-1003 ¶127.

Pet. 25. Petitioner notes that to meet the requirement of a determination that a packet satisfies a packet filtering rule based on a network-threat indicator, the rule would also have to be based on a network-threat indicator. Pet. Reply 7. Petitioner argues that “[t]he Petition and Dr. Staniford’s analysis showed that Sourcefire teaches using information in the 5-tuple to trigger a rule, which includes IP addresses specified by a packet-filtering rule as associated with a threat (i.e., network-threat indicators), so Sourcefire teaches both the determination and rule ‘based on’ one or more network-threat indicators.” Pet. Reply 7 (citing Pet. 38, citing Ex. 1003, Staniford Decl. ¶¶ 161–162).

Patent Owner contends that Petitioner incorrectly characterizes information in the 5-tuple as triggering a rule. PO Resp. 14. According to Patent Owner, the source and destination address in the intrusion rule header cited by Petitioner “are used only to determine whether to further evaluate a packet’s contents against the keywords specified in the instruction rules.”

PO Resp. 14 (citing Pet. 25, 34–40; Ex. 1004, 761–762; Ex. 2004, Goodrich Decl. ¶¶ 56–58). The Federal Circuit explicitly affirmed the Board’s rejection of this characterization of Sourcefire by Patent Owner in the ’722 patent IPR.⁶ Ex. 1031, 6.

In this proceeding, Patent Owner emphasizes that, in Sourcefire, “[u]nless the packet’s contents match the keywords of the intrusion rule, the 3D Sensor does not trigger the intrusions rule’s action (e.g., alert, drop) or generate an intrusion event.” PO Resp. 15 (citing Ex. 1004, 404–405, 761–762, 769–770, 776–777; Ex. 2004, Goodrich Decl. ¶ 56). According to Patent Owner, a Sourcefire packet can match the IP address in a rule header but, if packet contents do not match specified keywords and argument to generate an intrusion event, a rule is not triggered. *Id.* (citing Ex. 1004, 404–405, 761–762, 766–767, 769–770, 776–777).

At the oral hearing Patent Owner argued:

So there is no disclosure in Sourcefire that you would trigger a rule responsive to satisfying that rule based on network threat-indicators. As alluded to earlier on page 16 of the demonstratives, Sourcefire tells you what the intrusion rule is. It is a specified set of key words and arguments. It is not the rule header. The rule header is only used to determine whether or not a particular rule will be applied to network traffic. You know, neither of these issues were before the Board or decided in the earlier case.

Hrg’ Tr. 23:19–25. Patent Owner also argued:

And we haven’t argued that that first claim element is not met by Sourcefire because that’s exactly what Sourcefire’s rule header does. It tells you, should I apply this particular rule, or should I

⁶ As the Sourcefire reference in this proceeding is the same as the Sourcefire reference as in the ’722 patent IPR, the subject matter it discloses is independent of differences in the claims between the ’722 patent and the ’062 patent.

not apply this particular rule? We fully agree that, you know, if there's an IP address specified in a rule header, that Sourcefire teaches identifying packets with that network threat with that IP address. What it doesn't have is the later disclosure of a rule that is satisfied based on a network threat-indicator.

Hr'g Tr. 21:15–21.

Petitioner responds that Patent Owner is mistaken because, although Sourcefire requires its rules to have some keywords, most are optional and its mandatory keywords do not evaluate a packet's content, as they are merely informational. Pet. Reply 15 (citing Ex. 1068, Staniford Reply Decl. ¶¶ 23–24; Ex. 1067, Transcript of Deposition of Dr. Michael T. Goodrich, Sept. 28, 2023 (“Goodrich Tr.”) 49:11–20). Petitioner also notes that Sourcefire's rules are not required to include keywords and arguments that evaluate the contents of a packet, and that Sourcefire provides for custom rules that require only header information, such as source and destination IP addresses and ports. Pet. Reply 15–17 (citing Ex. 1004, 862–864).

“Sourcefire provides two types of intrusion rules: shared object rules and standard text rules.” Ex. 1004, 761. “All standard text rules contain two logical sections: the rule header and the rule options.” *Id.* at 762; *see also id.* at 764. “The rule header contains: the rule's action or type, the protocol, the source and destination IP addresses and netmasks The rule options section contains . . . keywords and their parameters and arguments.” *Id.* at 762. Rule actions include pass, alert and drop. *Id.* at 765. “Rule headers include the source and destination IP addresses of traffic that the rule inspects.” *Id.* at 766. In the options section of a rule, “keywords and their associated values (called arguments) dictates how the system evaluates packets and . . . allow you to perform inspection functions.” *Id.* at 769. To reduce the amount of packet inspection, a user can “[u]se the content

keyword to specify content that you want to detect in a packet. The rules engine searches the packet payload or stream for that string.” *Id.* at 776.

Claim 1 of the ’062 patent recites only that the packet filtering device receives rules configured to cause the device to identify packets corresponding to network-threat indicators. Claim 1 does not recite the format or structure of the rule, e.g., claim 1 does not recite where the network-threat indicator appears in any particular part of a rule. A network-threat indicator is no less a network-threat indicator simply because it appears in the Rule Options section of Sourcefire rule. Sourcefire’s ability to provide broader and deeper packet inspection does not change the fact that Sourcefire’s 3D Sensors receive packet filtering rules that are configured act on packets in response to a determination that a rule is satisfied based on network-threat indicators, as claimed.

Even under Patent Owner’s construction that precludes the use of parameters in addition to network-threat indicators, Sourcefire’s ability to use optional keywords in a rule does not mean that the action taken by a rule is not responsive “based on” a network-threat indicator. Sourcefire discloses that in the options section of a rule “keywords and their associated values (called *arguments*) dictate how the system evaluates packet and packet-related values that the rules engine tests.” *Id.* at 769 (describing how keywords can be used to perform inspection function) (emphasis added). Not all Sourcefire rules test keywords. Sourcefire discloses that a user “can restrict packet inspection to packets originating from specific IP address or those destined to a specific IP address.” *Id.* at 766. Thus, as in limitation 1[c], responsive to a specific network-threat indicator, e.g., an IP address, Sourcefire discloses rules that will not further inspect the packet. Instead, the packet filtering device acts according to the action specified in the rule,

i.e., causing the packet filtering device to ignore the traffic, allowing it to proceed to its destination (pass rule), or dropping the packet, preventing it from continuing to its destination (drop rule). *Id.*; *see also id.* at 761, 861–862 (“you can use the rule header settings to focus the rule to only match traffic using a specific protocol and travelling to or from a specific IP addresses or ports.”). Sourcefire discloses standard text rules that specify an action (e.g., pass or alert) when the Source IP or destination IP address “triggers the rule.” *Id.* at 862–863; *see also* Ex. 1031, 6 (Federal Circuit finding “reasonable” the Board’s conclusion in the ’722 patent IPR that Sourcefire teaches the use of source IP addresses as a network-threat indicator for triggering a rule to allow, drop, or alert).

In summary, Sourcefire discloses rules with a header section that includes source and destination IP addresses. It is undisputed that IP addresses can be network-threat indicators. Pet. 6, PO Resp. 2. Packet inspection can be restricted to packets originating from or destined to a specific IP address. *Id.* at 766. Thus, Sourcefire discloses rules that, responsive to a determination that the packet’s source and destination IP address satisfy a filtering rule, i.e., contain a network-threat indicator, cause Sourcefire to inspect or not inspect the packet further and take an appropriate action (pass, drop, or alert). Should the rule indicate further inspection of a packet is warranted, Sourcefire’s rule engine inspects the packet payload for strings or other information in the options section of the rule that, together with the IP address, indicates the presence of a network-threat and determines a responsive action. Thus, under any construction of the terms “responsive to” and “based on,” Sourcefire discloses taking action “responsive to a determination by the packet filtering rule device that the first packet satisfies a first packet filtering rule . . . based on one or more

network-threat indicators,” i.e., limitation 1[c]. For the reasons discussed above, we determine that Petitioner has demonstrated Sourcefire would have taught the limitations of claim 1 to an ordinarily skilled artisan

2. *Claims 2–7*

Claims 2–7 depend directly or indirectly from claim 1. Noting that some of the limitations in dependent claims 2–7 are counterparts to limitations the Board considered in the ’722 patent IPR, Petitioner nonetheless provides an analysis of each of the limitations recited in these claims. Pet. 47–62. Claim 2 depends from claim 1 and recites determining the rule allows a packet to continue to its destination. Ex. 1001, 18:35–40. Claim 3 depends from claim 2 and recites that the packet filtering device is located at a boundary between a first and second network, the first and second packets are received from a common host in the first network, and determining that the first packet is allowed to proceed to a common host in the second network while the second packet is prevented from proceeding to the common host in the second network. *Id.* at 18:41–62. Claims 4 and 5 depend from claim 2 and recite other routing decisions. *Id.* at 18:63–19:43. Claim 6 depends from claim 1 and recites updating a packet flow log to indicate a determination of whether the packet filtering device prevented or allowed a packet from proceeding to its destination. *Id.* at 19:44–52. Claim 7 depends from claim 6 and recites further details concerning the generation and modification of entries in packet flow logs. *Id.* at 19:54–20:20

Patent Owner does not respond to Petitioner’s contentions concerning claims 2–7. We have considered the evidence and arguments in the Petition and find that Petitioner has demonstrated Sourcefire would have disclosed or suggested the limitations of claim 2–7 to a person of ordinary skill. *See* Pet. 47–62.

3. *Independent Claims 8, 15, and 18*

Independent claim 8 is a method claim, similar to claim 1. Independent claim 15 recites a packet filtering device comprising a processor and a memory comprising instructions to carry out steps similar to those recited in claim 1. Independent claim 18 is a corresponding claim drawn to non-transitory computer-readable media comprising instructions that, when executed by one or more processors of a packet filtering device, cause the packet filtering device to carry out steps similar to those recited in claim 1. The Petition addresses the corresponding individual limitations of independent claims 1, 8, 15, and 18 together. Pet. 33–47. For the same reasons as those discussed above in our analysis of claim 1, we determine that Petitioner has demonstrated the Sourcefire teaches the corresponding limitations of independent claims 8, 15, and 18.

The Petition also addresses an additional feature recited in claim limitations 8.a, 15.a, and 18.a, i.e., that the plurality of network-threat indicators is associated with network-threat intelligence reports provided by one or more independent network-threat-intelligence providers. *See id.* at 36. The Petition cites Sourcefire as disclosing default rules based on intelligence reports generated by the Sourcefire Vulnerability Research Team (VRT), receiving Snort rules in uploaded files that constitute network intelligence reports, and receiving network intelligence reports for network-threat intelligence providers other than VRT, including Bugtraq and CVE. *Id.* (citing Ex. 1004, 254, 283, 776, 873–874, 1710; Ex. 1003, Staniford Decl. ¶¶ 147–156). Petitioner explains that, although the '062 patent Specification does not describe independent network-threat-intelligence providers, a person of ordinary skill would understand that providers, e.g., Bugtraq and CVE, are independent of Sourcefire and VRT. *Id.* at 36–37.

This additional limitation does not change the implications of collateral estoppel as to the functions and features of the claimed network-threat indicators. We also note that the claims recite only that the network-threat indicators are associated with reports supplied by the network-threat intelligence providers. The claims do not recite any specific reports, the form of such reports, or that such reports must be uploaded in some way. In addition, the claims do not recite that the network-threat indicators must be in any particular part of a rule, or even be part of a rule itself. As the claims only recite that the rule is configured to cause the packet filtering device to identify packets corresponding to the network-threat indicators, there is no requirement that the network-threat indicators be in the header of the rule. Sourcefire explicitly identifies a rule as including keywords and arguments that are “detection options.” Ex. 1004, 762–763. Sourcefire also explicitly identifies several external attack identification systems and states that specifying a reference, e.g., specifying a detection option from the detection options list, can “help identify why the packet triggered a rule.” *Id.* at 776 (demonstrating how to specify a vulnerability in a rule using a Bugtraq ID number as an indicator of a threat); *see also id.* at 534 (explicitly identifying CVE as the Current Vulnerabilities and Exposures database maintained by MITRE (an independent network-threat-intelligence provider) and disclosing how a CVE ID number can be used to specify a vulnerability in a rule as an indicator of a threat).

The Patent Owner Response does not explicitly address these additional limitations. Having reviewed the evidence and arguments of record, we determine that Petitioner has demonstrated that Sourcefire would have disclosed or suggested all the limitations of claim 8, 15, and 18 to a person of ordinary skill.

4. *Claim 9, 16, and 19*

Claims 9, 16, and 19 depend from claims 8, 15, and 18, respectively and recite similar limitations, i.e., causing a user interface to display data indicative that the first packet was allowed to continue toward the destination of the first packet. Petitioner provides a detailed analysis concerning how Sourcefire discloses the subject matter recited in these limitations. Pet. 62–66. Patent Owner does not respond to Petitioner’s contentions concerning these claims. Having considered the evidence and arguments currently of record, we find that Petitioner has demonstrated that Sourcefire discloses the limitations recited in dependent claims 9, 16, and 19.

5. *Claims 10, 17, and 20*

Claims 10, 17, and 20 depend from claims 8, 15, and 18, respectively and recite similar limitations, i.e., that responsive to the determination by the packet filtering device that the first packet satisfies the first packet filtering rule, a packet log entry comprising a first threat identifier corresponding to the first packet and data indicating that the packet filtering device allowed the first packet to continue toward the destination of the first packet. Petitioner provides a detailed analysis concerning how Sourcefire discloses the subject matter recited in these limitations. Pet. 66–68. Patent Owner does not respond to Petitioner’s contentions concerning these claims. Having considered the evidence and arguments currently of record, we find that Petitioner has demonstrated that Sourcefire discloses the limitations recited in dependent claims 10, 17, and 20.

6. *Claims 12, 13, and 14*

Claims 12 depends from claim 8, claim 13 depends from claim 12 and claim 14 depends from claim 13 and concern generating and updating packet

log entries and the ordering of network threats. Petitioner provides a detailed analysis concerning how Sourcefire discloses the subject matter recited in these limitations. Pet. 68–73. Patent Owner does not respond to Petitioner’s contentions concerning these claims. Having considered the evidence and arguments currently of record, we find that Petitioner has demonstrated that Sourcefire discloses the limitations recited in dependent claims 12, 13, and 14.

VII. CONCLUSION⁷

Having reviewed all the evidence and arguments of record, we determine that Petitioner has demonstrated by a preponderance of the evidence that claims 1–20 of the ’062 patent are unpatentable.

In summary:

Claim(s)	35 U.S.C. §	Reference(s)/ Basis	Claim(s) Shown Unpatentable	Claim(s) Not shown Unpatentable
1–20	103	Sourcefire	1–20	
Overall Outcome			1–20	

⁷ 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. 16,654 (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).

VIII. ORDER

In consideration of the above it is:

ORDERED that claim 1–20 of the '062 patent are unpatentable; and

FURTHER ORDERED that that, because this is a Final Written Decision, 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.

IPR2022-01535
Patent 10,609,062 B1

FOR PETITIONER:

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

FOR PATENT OWNER:

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

Bradley Wright
Scott Kelly
BANNER & WITCOFF, LTD
bwright@bannerwitcoff.com
skelly@bannerwitcoff.com