

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*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

Keysight Technologies, Inc. (“Petitioner”) filed a petition, Paper 1 (“Petition” or “Pet.”), to institute an *inter partes* review (“IPR”) of claims 1–20 (the “challenged claims”) of U.S. Patent No. 10,609,062 B1 (“the ’062 patent”). 35 U.S.C. § 311. Centripetal Networks, Inc., known known as Centripetal Networks LLC¹ (“Patent Owner”) filed a Preliminary Response, Paper 8 (“Prelim. Resp.”), contending that the Petition should be denied as to all challenged claims. We have jurisdiction under 35 U.S.C. § 314, which provides that an *inter partes* review may not be instituted unless the information presented in the Petition “shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.”

A decision to institute under § 314 may not institute on fewer than all claims challenged in the petition. *SAS Inst., Inc. v. Iancu*, 138 S. Ct. 1348, 1359–60 (2018). In addition, per Board practice, if the Board institutes trial, it will institute “on all of the challenged claims and on all grounds of unpatentability asserted for each claim.” *See* 37 C.F.R. § 42.108(a).

Having considered the arguments and the associated evidence presented in the Petition and the Preliminary Response, for the reasons described below, we institute *inter partes* review.

II. REAL PARTIES IN INTEREST

The Petition identifies Petitioner, Keysight Technologies, Inc. as its real party-in-interest. Pet. 3. Patent Owner identifies itself, Centripetal Networks, Inc., as its sole real party-in-interest. Paper 3, 1.

¹ *See* Paper 6.

III. RELATED MATTERS

The Petition states that the '062 patent is asserted against it in *Centripetal Networks, Inc. v. Keysight Technologies, Inc.*, Civ. No. 2-22-cv-00002 (E.D. Va. January 1, 2022) (“Parallel Litigation”). Pet. 4. Patent Owner identifies the following International Trade Commission investigation as related: *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). Paper 3, 1.

Petitioner also identifies *Centripetal Networks, Inc. v. Palo Alto Networks, Inc.*, Case No. 2:21-cv-00137 (E.D. Va., filed Mar. 12, 2021) as litigation concerning three related patents. Pet. 4. Petitioner states that the three related patents are subject to pending IPRs as follows: IPR2021-01147 (10,542,028), IPR2021-01148 (10,757,126), and IPR2021-01149 (10,567,413). *Id.*

IV. EXERCISE OF DISCRETION

A. Discretion Under 35 U.S.C. § 325(d)

Under § 325(d) the Board uses the following two-part framework to determine whether to exercise its discretion to deny institution:

(1) whether the same or substantially the same art previously was presented to the Office or whether the same of substantially the same arguments previously were presented to the Office; and

(2) if either condition of the first part of the framework is satisfied, whether the petitioner has demonstrated that the Office erred in a manner material to the patentability of the challenged claims.

Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH, IPR2019-01469, Paper 6 at 8 (PTAB Feb. 13, 2020) (Decision Denying Institution) (Precedential).

In assessing whether we exercise discretion under 325(d), we consider the following factors articulated in *Becton Dickinson & Co. v. B. Braun Melsungen*, IPR2017-01586 (Paper 8, 17–18) (PTAB Dec. 15, 2017),

1. the similarities and material differences between the asserted art and the prior art involved during examination;
2. the cumulative nature of the asserted art and the prior art evaluated during examination;
3. the extent to which the asserted art was evaluated during examination;
4. the extent of the overlap between the arguments made during examination and the manner in which a petitioner relies on the prior art or a patent owner distinguishes the prior art;
5. whether a petitioner has pointed out sufficiently how the Office erred in evaluating the asserted prior art; and
6. the extent to which additional evidence and facts presented in the petition warrant reconsideration of the prior art or arguments.

Patent Owner argues “[t]he Board should deny institution under 35 U.S.C. § 325(d) because the Petition re-uses the same art (*Sourcefire*) and arguments that were previously presented to the Patent Office.” PO Resp. 8. According to Patent Owner “*Sourcefire* was front and center during the ’062’s Patent Examination . . . The fact that *Sourcefire* was not applied in a rejection only supports the fact that the Examiner considered the claims of the ’062 Patent and found them to be patentable over *Sourcefire*.” *Id.* at 13 (citing PO Resp. Section III.B.1 Remarks in the Notice of Allowance).

Petitioner acknowledges that the Examiner considered *Sourcefire* during prosecution (*Advanced Bionics*, step 1), but emphasizes “the Examiner did not consider whether the Challenged Claims were rendered obvious over *Sourcefire* in view of the Board’s binding findings for the ’722

IPR.² Pet. 16 (citing *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); Ex. 1030. Petitioner further argues error in a manner material to patentability of the challenged claims (*Advanced Bionics*, step 2) under at least three *Becton Dickinson* factors. *Id.* at 18–20 (factors 3, 5, and 7, referred in the Petition as factors c, e, and f). As to the extent the art was evaluated by the Examiner, Petitioner argues that Examiner’s assertion in an Interview Summary that he carefully considered Sourcefire is inconsistent with the prosecution history that only reflects a conclusory analysis in the Notice of Allowance. *Id.* at 18–19; *see*, Ex. 1002, 195–201.

Petitioner further argues error material to the patentability of the claims is found in the Examiner’s reference to an “explicit progression” of steps. *Id.* at 19 (citing Ex. 1002, 200). Petitioner contends that the Examiner merely parrots the language of the claim with no substantive analysis and that the ’722 FWD found claims in the ’722 patent with the same order and arrangement to be obvious. *Id.* (citing Ex. 1006, 1–3, Ex. 1030, 20–34). Petitioner notes other findings in the ’722 FWD that are inconsistent with the Notice of Allowance. *Id.* at 19–20 (citing Ex. 1022, 199 and Ex. 1030, 32 as evidence the Examiner’s conclusion that Sourcefire does not disclose “allowing” packets to continue (Notice of Allowability page 6) is opposite

² *See* Ex. 1030, *Cisco Systems, Inc. v. Centripetal Networks, Inc.*, IPR2018-01760, Paper 41 (PTAB May 18, 2020) (Final Written Decision) (finding all challenged claims of U.S. Patent 9,413,722 B1 unpatentable); *aff’d*. *Centripetal Networks, Inc. v. Ciscosys.*, 847 Fed. Appx 881 (Fed. Cir. 2021) (Ex. 1031).

the findings of the Board and is an error material to patentability of the claims).

The '062 patent issued on March 31, 2020 following a series of Examiner initiated interviews with Patent Owner's representative. Ex. 1002, 203–204 (Examiner Interview Summary dated Jan. 30, 2020, memorializing a series of interviews between the Examiner and Applicant's Representative); *see also, id.* at 192–202 (Notice of Allowability). The '722 FWD was entered on May 18, 2020 and was affirmed by the Federal Circuit on March 10, 2021, Case 2020-2057. *See* Exhibits 1030, 1031. As the '062 patent issued earlier than the '722 FWD and the Federal Circuit's affirmance, the Examiner did not have the benefit of those decisions. Both the Board's FWD and the Federal Circuit's affirmance address Sourcefire and are consistent with the conclusion that the Office erred in a manner material to patentability under *Advanced Bionics*. Therefore, we decline to exercise discretion to deny institution under Section 325(d).

V. 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 1:53–58. 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.

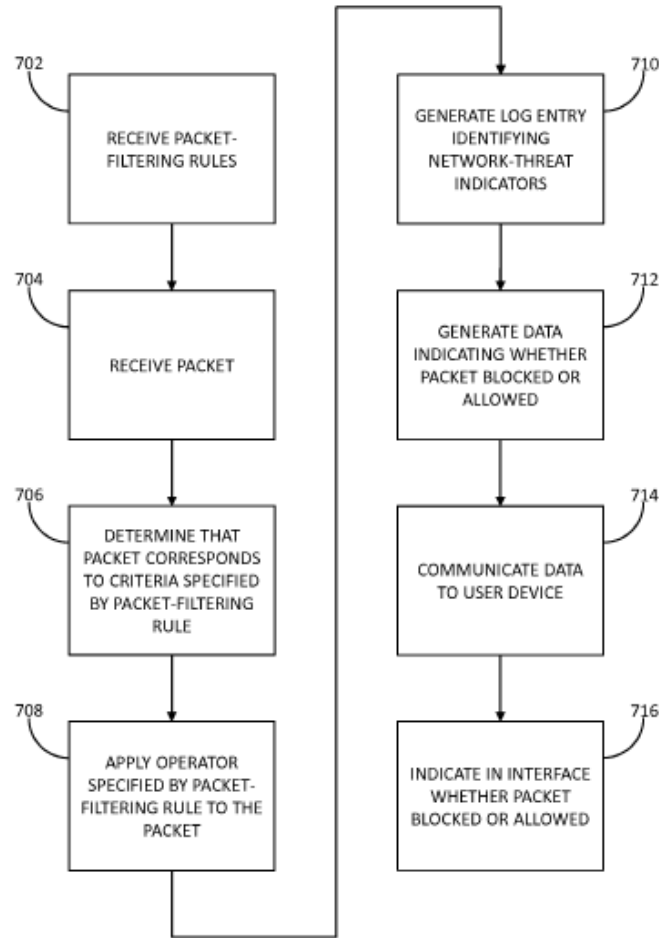


FIG. 7

Id. at Fig. 7. The above figure depicts an illustrative method for rule-based network-threat detection. *Id.* at 15:52–54; see *id.* at 15:54–16:34 (describing in detail each step depicted in Figure 7).

VI. ILLUSTRATIVE CLAIM[S]

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:

- 1.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;
- 1.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
- 1.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.

VII. ASSERTED GROUNDS

Petitioner asserts that claims [] would have been unpatentable on the following grounds:

Claim(s) Challenged	35 U.S.C. §	Reference/Basis
1–20	103	Sourcefire ³

VIII. LEVEL OF ORDINARY SKILL IN THE ART

Petitioner states that a person of ordinary skill in the art (“POSA”) would have had a bachelor’s degree in computer science, computer engineering, or an equivalent, and four years of industry experience. Pet. 12 (citing Ex. 1003, Declaration of Dr. Stuart Staniford (“Staniford Decl.”) ¶¶ 1-20, 21-25). Patent Owner does not respond to Petitioner’s description of an ordinarily skilled artisan.

The level of ordinary skill in the art usually is evidenced by the references themselves. See *Okajima v. Bourdeau*, 261 F.3d 1350, 1355

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

(Fed. Cir. 2001); *In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995); *In re Oelrich*, 579 F.2d 86, 91 (CCPA 1978). We apply Petitioner’s description of a person of ordinary skill in this proceeding, as Petitioner’s description appears commensurate with subject matter disclosed and claimed in the ’062 patent.

IX. CLAIM CONSTRUCTION

A. Introduction

For petitions filed after November 13, 2018, we interpret claim terms using “the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b).” 37 C.F.R. § 42.100(b) (2019). In this context, claim terms “are generally given their ordinary and customary meaning” as understood by a person of ordinary skill in the art in question at the time of the invention. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (citations omitted) (en banc). “In determining the meaning of the disputed claim limitation, 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). Extrinsic evidence is “less significant than the intrinsic record in determining ‘the legally operative meaning of claim language.’” *Phillips*, 415 F.3d at 1317 (citations omitted).

Any special definition for a claim term must be set forth in the specification with reasonable clarity, deliberateness, and precision. *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994). We construe only those claim terms that require analysis to determine whether to institute inter partes review. *See Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803

(Fed. Cir. 1999) (holding that “only those terms need be construed that are in controversy, and only to the extent necessary to resolve the controversy”).

Claims 1–7 recite a method in which a packet filtering device receives packet filtering rules that cause the device to filter packets based on at least one of a plurality of network-threat indicators. Claims 8–14 recite a method, claims 15–17 recite a device, and claims 18–20 recite a non-transitory computer readable medium in which a packet filtering device receives a plurality of network-threat indicators from one or more independent network-threat-intelligence providers.

Petitioner does not propose any term be construed differently from the construction we applied in the ’722 IPR under the broadest reasonable interpretation standard. Pet. 13–14. Patent Owner contends that the applicability of the *Phillips* claim construction standard to this proceeding requires that we construe “network-threat indicator” (all claims) differently from the construction we applied in the ’722 IPR and that we construe “network-threat-intelligence providers” (claims 8–20). Prelim. Resp. 19–22.

B. Network-threat indicator

In the ’722 IPR, applying the broadest reasonable construction standard, we construed *network-threat indicator* to mean an “indicator that represents the identity of a resource associated with a network threat.” ’722 FWD 8–10. Patent Owner contends that applying the *Phillips* standard “the Board should construe the term “network-threat indicators” to mean “indicators that represent the identity of a resource previously determined to be associated with a network threat.” PO Resp. 22. Patent Owner acknowledges that its construction imports into the claim a negative limitation by excluding from network-threat indicators information not previously associated with a network threat. *Id.* at 21–22 (stating that a

person of ordinary skill “would understand that the plain and ordinary meaning of ‘network-threat indicator,’ in light of the ’062 Specification, excludes mere resource-identifying information (e.g., source/destination IP addresses) that lacks any indication that the resource was previously determined to be associated with a network threat.”).

To justify its proposed construction, Patent Owner states “most of the Challenged Claims require receiving packet filtering rules that identify packets on the basis of ‘network threat-indicators’ that are associated with reports supplied by network-threat-intelligence providers.” *Id.* at 21. According to Patent Owner, “at the time packet filtering rules are received, the ‘network-threat indicators’ have already been determined to be associated with a network threat.” *Id.*

We construe claims according to the principles articulated above; we do not construe terms based on “most” of the claims. *See* Section IX.A *supra*. Although all the challenged claims recite “network-threat indicators,” only claims 8–20 recite that the network-threat indicators are “associated with network-threat intelligence reports supplied by one or more independent network-threat-intelligence providers.” *See*, Ex. 1001, 17:46–24:42.

Patent Owner also states “Sourcefire is silent with respect to filtering packets based upon the identity of a resource previously associated with a network threat.” Prelim. Resp. 20. We look to the ’062 patent claims, its disclosure, and its prosecution history to construe the terms of the ’062 patent. As Patent Owner asserts Sourcefire is silent on whether a resource is previously associated with a network threat, we do not look to Sourcefire to provide a description of how a person of ordinary skill would interpret the language of the ’062 patent claims.

The claim language itself is clear. Claims 1–7 recite a method in which a packet filtering device receives rules that are configured to cause the device to identify packets based on network-threat indicators. Such a packet filtering device can only receive rules that actually exist, i.e., those rules must be configured to cause the device to filter packets based on network threat indicators, regardless of whether those indicators were somehow “predetermined.” Claims 8–20 further limit the network-threat identifiers to those “associated with network-threat-intelligence reports supplied by one or more independent network-threat-intelligence providers.” In claims 8–20, the device receives rules that are configured to cause the device to identify packets corresponding to network-threat indicators that are associated with threat-intelligence reports. Those reports must exist, regardless of whether the network-threat indicators were somehow predetermined, i.e. whether the network-threat indicators existed before threat-intelligence provider developed or provided the reports.

There is no basis in the claim language to incorporate a further unarticulated (and possibly indefinite) “predetermined” limitation on the term network-threat indicator. Patent Owner’s argument that at the time the packet filtering rules are received, the network threat indicators have already been determined to be associated with a network threat (Prelim. Resp. 21) is unavailing. Patent Owner’s proposed construction places no such restrictions on “previously determined.” For example, Patent Owner’s proposed construction does not articulate when a resource is previously determined to be associated with a network threat or who made the relevant determination. The Specification describes network-threat-intelligence providers transmitting reports that contain the recited network-threat-indicators. Ex. 1001, 3:27–38. By importing into “network-threat indicator”

a “predetermined” requirement that is not specific as to the time the threat is identified or who identified the threat, Patent Owner excludes from the scope of the claims a system that is capable of identifying new threats, i.e. threats that have not been previously determined to be associated with a network threat. A network-threat-intelligence provider transmitting intelligence that excludes information about newly identified threats is at odds with the network protection goals of network protection systems such as those in the ’062 patent.

The Specification explicitly describes network-threat indicators and gives at least the following examples:

network-threat-intelligence reports that include network-threat indicators (e.g., network addresses, ports, fully qualified domain names (FQDNs), uniform resource locators (URLs), uniform resource identifiers (URIs), or the like) associated with the 30 network threats, as well as other information associated with the network threats, for example, the type of threat (e.g., phishing malware, botnet malware, or the like), geographic information (e.g., International Traffic in Arms Regulations (ITAR) country, Office of Foreign Assets Control (OFAC) 35 country, or the like), anonymous proxies (e.g., Tor network, or the like), actors (e.g., the Russian Business Network (RBN), or the like).

Ex. 1001, 3:27–38. *See also id.* at 1:25–27, 4:36–64 (describing network threat intelligence providers communicating to a rule provider threat intelligence reports that include threats and one or more associated network threat indications, “e.g. network addresses, ports, FQDNs, URLs, URIs, or the like” and “other information associated with network threats (e.g., e.g., the type of threat, geographic information, anonymous proxies, actors, or the like”). The ’062 patent does not describe a network threat indicator as a function of when it was identified or who identified it. Instead, the ’062

patent describes parameters that may serve as network-threat indicators that can be used in rules to filter packets that may be a threat to a network.

Having considered the arguments and evidence of record, we conclude that the proper construction of “network-threat indicator” under the under the *Philips* standard is not different from the construction we applied in the ’722 IPR. We construe the term “network-threat indicator” to mean an “indicator that represents the identity of a resource associated with a network threat.”

C. Network-threat-intelligence provider

Arguing that the ’062 Specification describes network-threat-intelligence providers as providers of network-threat indicators via network-threat-intelligence reports, Patent Owner contends that “[t]he term ‘network-threat-intelligence providers’ means ‘providers of a service that distributes network-threat indicators.’” Prelim. Resp. 23. Claims 8–20 recite that the received rules cause the packet filtering device to filter packets corresponding to network threat indicators associated with network-threat-intelligence reports supplied by independent network threat intelligence providers. *See*, Ex. 1001, 20:21–24:42.

The Specification discloses that

Network-threat-intelligence providers [. . .] may be associated with services that monitor network threats (e.g., threats associated with threat hosts [. . .] and disseminate (e.g., to subscribers) network-threat-intelligence reports that include network-threat indicators (e.g., network addresses, ports, fully qualified domain names (FQDNs), uniform resource locators (URLs), uniform resource identifiers (URIs), or the like) associated with the network threats, as well as other information associated with the network threats, for example, the type of threat (e.g., phishing malware, botnet malware, or the like), geographic information (e.g., International Traffic in Arms

Regulations (ITAR) country, Office of Foreign Assets Control (OFAC) country, or the like), anonymous proxies (e.g., Tor network, or the like), actors (e.g., the Russian Business Network (RBN), or the like).

Ex. 1001, 3:22–38. The Specification makes clear that network-threat intelligence providers “may be associated with services that monitor network threats” and “disseminate (e.g., to subscribers) network threat intelligence reports.” *Id.* Those reports include “network-threat indicators [. . .] associated with network threats” and “other information associated with network threats,” such as the type of threat, geographic information, anonymous proxies, and the like. *Id.*

Claims 8–20 recite “network-threat-intelligence reports supplied by one or more independent network threat intelligence providers.” The recitation in claims 8–20 that the network-threat indicators are associated with network-threat-intelligence reports is a limitation on the network-threat indicators, not a limitation on the providers.

Consistent with the language of the claims and the disclosure in the Specification, we construe “network-threat-intelligence providers” to mean “entities associated with services that disseminate network-threat-intelligence reports.”

X. ANALYSIS

A. Introduction

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 is 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). At this stage of the proceeding 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 a reasonable likelihood of success at trial.

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. 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, 33, 2074.

⁴ In the ’722 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.

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

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 s 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.

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 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. *Claim 1 as obvious over Sourcefire*

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 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 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).

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). Petitioner provides the following chart comparing claim 1 of the '062 patent challenged in this proceeding with claim 1 of the '722 patent that was found unpatentable in the '722 IPR. Ex. 1006. Highlighted text indicates the differences Petitioner identified.

'062 Patent	'722 Patent
1[pre] A method comprising:	1[pre] A method comprising:
[1a] 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.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;

[1c] 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:	[1c] responsive to a determination by the packet-filtering device that the first packet satisfies one or more criteria, specified by a packet-filtering rule of the plurality of packet-filtering rules, that correspond to one or more network-threat indicators of the plurality of network-threat indicators:
[1d] 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	[1d] applying, by the packet-filtering device and to the first packet, an operator specified by the packet-filtering rule and configured to cause the packet-filtering device to allow the first packet to continue toward a destination of the first packet;
[1e] 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;	[1e] communicating, by the packet-filtering device, information from the packet-filtering rule that identifies the one or more network-threat indicators, and data indicative that the first packet was allowed to continue toward the destination of the first packet;
[1f] 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;	[1f] causing, by the packet-filtering device and in an interface, display of the information in at least one portion of the interface corresponding to the packetfiltering rule and the one or more network-threat indicators;
[1g] 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;	[1g] receiving, by the packet-filtering device, an instruction generated in response to a user invoking an element in the at least one portion of the interface corresponding to the packet-filtering rule and the one or more network-

	threat indicators;
[1h] 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	[1h] responsive to receiving the instruction : modifying, by the packet-filtering device, at least one operator specified by the packet-filtering rule to reconfigure the packet-filtering device to prevent packets corresponding to the one or more criteria from continuing toward their respective destinations; and
[1i] responsive to a determination by the packet filtering device that the second packet satisfies the first packet filtering rule :	[1i] responsive to a determination by the packet-filtering device that the second packet corresponds to the one or more criteria :
[1j] 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;	[1j] preventing, by the packet-filtering device, the second packet from continuing toward a destination of the second packet;
[1k] communicating, by the packet filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and	[1k] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and
[1l] 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.	[1l] 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.

Ex. 1006.

Patent Owner argues that, because the '722 IPR was decided using the broadest reasonable claim construction standard and the *Phillips* clam

construction standard applies to this proceeding, the issues before us are not identical to those presented in the '722 IPR and collateral estoppel cannot apply. Prelim. Resp. 27–29. According to Patent Owner, we should reject Petitioner’s allegation that collateral estoppel applies to any single element of the challenged claims and to the network-threat indicators element in particular. *Id.* at 29.

As discussed above, applying the *Phillips* standards, we arrive at the same construction of “network-threat indicator” in this proceeding as we applied in the '722 IPR. *See* Section IX herein; Ex. 1030, 8–10. In addition, in this proceeding we construe the term “network-threat-intelligence provider,” as used in claims 8–20. *See* Section IX.C. To the extent that the construction we apply in this proceeding is the same as that we applied in the '722 IPR, the requirements for collateral estoppel have been met and we need not re-visit our findings, which have been affirmed, in that proceeding. Nevertheless, as discussed below, we would reach the same result even if we applying Patent Owner’s proposed construction. Our analysis of claims 8–10 addresses the limitations that recite “network-threat-intelligence provider.”

2. *Claim 1*

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. Noting that claim limitation 1.a is a counterpart to claim limitation 1.a of the '722 patent, Petitioner cites our findings in the '722 IPR that Sourcefire discloses this limitation. Pet. 35–36 (citing Ex. 1006; Ex. 1030, 22).

Patent Owner contends that Sourcefire does not teach or suggest filtering packets based on network-threat identifiers. Prelim. Resp. 24–27. According to Patent Owner, Petitioner does not demonstrate that Sourcefire teaches or suggests network-threat-indicators that represent the identity of a resource previously identified to be associated with a network threat. *Id.* at 25. As our construction of “network threat-indicators” in this proceeding under the *Phillips* standard is the same as the broadest reasonable interpretation construction we applied in the ’722 IPR, we agree with Petitioner collateral estoppel applies. In particular, the Federal Circuit “affirm[ed] 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.

Even if we adopted Patent Owner’s construction that the network-threat indicators are somehow predetermined, Petitioner demonstrates that Sourcefire discloses rules that include network-threat identifiers or criteria previously identified as associated with a network threat.

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. The Petition further notes that

the IPS in each 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. To the extent a Sourcefire rule includes criteria that trigger the rule when detected, the network-threat indicators are predetermined.

Patent Owner further argues that Sourcefire filters traffic based on its content, rather than network-threat indicators. *Id.* at 25–27. As an initial matter, it is not clear how a network-threat indicator could be used to filter packets as claimed if the network-threat indicator is not part of the packet’s contents.

Nevertheless, according to Patent Owner, “Petitioner asserts that *Sourcefire*’s disclosure of ‘source and destination IP addresses’ specified by an intrusion rule meets the limitation of a network-threat indicator,” but “fails to identify any disclosure within *Sourcefire* disclosing that the source and destination IP addresses in *Sourcefire*’s Rule Header represent resources associated with a network threat, let alone resources previously determined to be associated with a network threat.” Prelim. Resp. 25–26 (citing Pet. 38). Patent Owner argues that

Sourcefire discloses the source and destination IP addresses are used to “restrict packet inspection,” to “reduce[] the amount of packet inspection the system must perform,” and to “also reduce[] false positives by making the rule more specific and removing the possibility of the rule triggering against packets whose source and destination IP addresses do not indicate suspicious behavior.

Id. at 26 (citing Ex. 1004, 766–767).

Patent Owner’s argument is unavailing. Patent Owner appears to acknowledge that source and destination IP addresses are network-threat indicators. *Id.* To the extent that Sourcefire uses such network-threat

indicators to restrict certain packets from further inspection, Sourcefire is simply implementing a rule that causes the 3D Sensor to allow other packets to continue toward its destination, as recited in claim 1. *See* Ex. 1004, 761. Sourcefire discloses: “IPS compares packets against the conditions specified in each rule and, if the packet data matches all the conditions specified in a rule, the rule triggers. If a rule is an *alert rule*, it generates an intrusion event. If it is a *pass rule*, it ignores the traffic.” *Id.* Sourcefire also discloses drop rules. *Id.*

Patent Owner also contends that “[r]ather than identifying packets corresponding to network ‘network-threat indicators’ *Sourcefire* instead guides the POSITA to use the Rule Options section, which contains “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.” Prelim. Resp. 26 (citing Ex. 1004, 762). Patent Owner notes that such “intrusion rules” in Sourcefire “provide broader and deeper packet inspection” and “keywords and their associated values (called arguments) dictate how the system evaluates packets and packet-related values that the rules engine tests.” *Id.* at 26–27 (citing Ex. 1004, 254, 769).

Patent Owner’s argument is unavailing. 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 the rule, or even that the rule includes the network-threat indicator. 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 to identify packets corresponding to network-threat indicators, as claimed.

Having considered the evidence and arguments of record, we find that Petitioner has demonstrated that Sourcefire teaches the features recited in claim limitation 1.a to a person of ordinary skill in the art.

The Petition includes a detailed analysis of the remaining limitations of claim 1. Pet. 37–47. As shown in Petitioner's table comparing claim 1 of the '062 patent with claim 1 of the '722 patent, the remaining limitations of claim 1 are similar to the limitations of claim 1 that we considered in the '722 IPR. Patent Owner does not respond to Petitioner's arguments concerning the remaining limitations of claim 1. We have considered the arguments and evidence in the Petition and find that, for purposes of institution, Petitioner has demonstrated Sourcefire would have disclosed or suggested all of the limitations of claim 1 to a person of ordinary skill in the art.

D. 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 we considered in the '722 IPR, Petitioner nonetheless provides an analysis of each of the limitations recited in these claims. Pet. 47–62. 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.

E. 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 address the corresponding individual limitations of independent claims 1, 8, 15, and 18 together. Pet. 33–47. The Petition addresses additional the additional feature recited in claim limitations 8.a, 15.a, and 18.a 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 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.

Patent Owner contends that collateral estoppel does not apply to claims 8–20 because this additional limitation was not addressed in the '722 IPR.

This additional limitation does not change the implications of collateral estoppel as to the functions and features of the claimed network-threat indicators. We now address this additional limitation, i.e., the association of network threat indicators with reports supplied by independent network-threat-intelligence providers.

According to Patent Owner, under either the *Phillips* construction standard or the broadest reasonable construction, Petitioner has not shown Sourcefire discloses network-threat identifiers associated with a network-threat-intelligence reports supplied by independent threat-intelligence providers. Prelim. Resp. 30–34 (citing Pet. 36–37). In addition to arguing that VRT is not independent of Sourcefire, Patent Owner argues that Petitioner never alleges that Sourcefire’s source and destination IP addresses are related in any way to the alleged reports from external indices, e.g., Bugtrac and CVE, or that Sourcefire uploads any alleged reports. *Id.* at 32–33.

Patent Owner’s arguments are unavailing for two reasons. First 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.

Second, as discussed above, 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, as Patent Owner seems to imply. 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 543 (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).

We have reviewed Petitioner’s arguments concerning the remaining limitations of claims 8, 15, and 18. Patent Owner does not respond to Petitioner’s arguments concerning these limitations. Having considered the evidence and arguments currently of record, we find that Petitioner has, for purposes of institution, demonstrated that Sourcefire discloses the limitations of independent claims 8, 15, and 18.

F. Claims 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, for purposes of institution, Petitioner has demonstrated that Sourcefire discloses the limitations recited in dependent claims 9, 16, and 19.

G. Claims 10, 17, 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. 67–68. Patent Owner does not respond to Petitioner’s contentions concerning these claims.

Having considered the evidence and arguments currently of record, we find that, for purposes of institution, Petitioner has demonstrated that Sourcefire discloses the limitations recited in dependent claims 10, 17, and 20.

H. Claims 12, 13, and 14

Claims 12 depends from claim 8, claim 13 depends from claim 12 and claim 14 depends from claim 13. 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, for purposes of institution, Petitioner has demonstrated that Sourcefire discloses the limitations recited in dependent claims 12, 13, and 14.

XI. CONCLUSION

For the reasons discussed above, we find that Petitioner has demonstrated a reasonable likelihood that it will succeed on its sole challenge that claims 1–20 are unpatentable over Sourcefire.

XII. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that, pursuant to 35 U.S.C. § 314(a) an *inter partes* review of the '062 Patent is hereby instituted, commencing on the entry date of this Order, and pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial.

FURTHER ORDERED that the trial is authorized on all grounds set forth in the Petition, in particular, claim 1–20 as unpatentable over Sourcefire;

FURTHER ORDERED that the trial will be conducted in accordance with a corresponding separately issued Scheduling Order.

IPR2022-01535
Patent 10,609,062 B1

FOR PETITIONER:

Gerard Donovan
Peter 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 Price
Jenna Fuller
Bradley Wright
Scott Kelly
KRAMER LEVIN LLP
jhannah@kramerlevin.com
jprice@kramerlevin.com
jfuller@kramerlevin.com
bwright@bannerwitcoff.com
skelly@bannerwitcoff.com