No.

IN THE
Supreme Court of the United States Court

CENTRIPETAL NETWORKS, INC.,
Petitioner,

v.

CISCO SYSTEMS, INC.,
Respondent.

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT

PETITION FOR A WRIT OF CERTIORARI

Paul J. Andre
Counsel of Record
Lisa Kobialka
James Hannah
Kramer Levin Naftalis
& Frankel LLP
990 Marsh Road
Menlo Park, CA 94025
(650) 752-1700
pandre@kramerlevin.com
lkobialka@kramerlevin.com
jhannah@kramerlevin.com

Counsel for Petitioner

August 9, 2021

QUESTION PRESENTED

The patent statute provides that "[a] person shall be entitled to a patent unless . . . the invention was . . . described in a printed publication . . . in this country, more than one year prior to the date of the application for patent in the United States." 35 U.S.C. § 102(b) (pre-AIA). This provision has long been interpreted by the courts to require that a document that predates the patent application by over a year is deemed a printed publication only if it is readily available to interested members of the public through generally available medium.

The question presented is:

> Can a document qualify as a printed publication if it is stored on a password-protected website, not accessible to the public, and available only to customers who pay over $25,000 dollars to purchase related software?

PARTIES TO THE PROCEEDING

All parties to the proceeding are identified in the caption.

RULE 29.6 STATEMENT

Petitioner Centripetal Networks, Inc. ("Centripetal") is a privately held company that has no parent corporation. No publicly held company owns 10 percent or more of Centripetal's stock.

RELATED PROCEEDINGS

Centripetal states that the below listed proceedings are directly related to the case in this Court within the meaning of Rule 14.1(b)(iii):

- *Centripetal Networks, Inc. v. Cisco Systems, Inc.*, Nos. 2020-1635, 2020-1636, United States Court of Appeals for the Federal Circuit. Judgment entered March 10, 2021.
- *Centripetal Networks, Inc. v. Cisco Systems, Inc.*, No. 2020-2057, United States Court of Appeals for the Federal Circuit. Judgment entered March 10, 2021.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

PETITION FOR WRIT OF CERTIORARI

Centripetal respectfully petitions for a writ of certiorari to review two related judgments of the United States Court of Appeals for the Federal Circuit in this case.

INTRODUCTION

The United States does not have two separate justice systems—one for the rich and one for the poor. Yet recent Federal Circuit holdings have established a *de facto* divide between the "haves" and "have nots." Large technology Goliaths are afforded preferential patent jurisprudence based solely on their ability to reach into their large coffers to pay for it. This dynamic has arisen in this case in connection with the Federal Circuit's determination regarding when a publication is publicly accessible. Certainly a publication which is under lock and key on a password protected website and only made available if individuals pay over $25,000 is not ***publicly*** accessible under the Patent Act.

The Federal Circuit's acceptance of this secreted document as a printed publication contravenes decades of precedent requiring that such documents be publicly available, and undermines Congress' intention that the patent system promote public disclosure of inventions and new technology. The framers of the Constitution recognized the importance of incentivizing both the development and disclosure of inventions "to promote the Progress of Science and useful Arts," and the need to reward innovators for disclosing technology they might otherwise retain as

trade secrets. U.S. CONST. art. 1, § 8, cl. 8. This insight is embodied in the longstanding interpretation of the patent statute as only permitting documents that are reasonably accessible to interested members of the public to be used as a "printed publication" to potentially invalidate a patent. In contrast, documents may not be used as printed publication prior art if they are withheld from the public and do not enrich the public domain.

This Court's review is needed to resolve the Federal Circuit's inconsistent application of the printed publication requirements and restore it to its intended scope.

OPINIONS BELOW

The Final Written Decisions of the Patent Trial and Appeal Board ("PTAB") on appeal are unreported, and are reprinted in the Appendix ("App.") 44a-121a; App. 122a-159a; and App. 160a-222a.

The Federal Circuit's two decisions affirming the PTAB's Final Written Decisions (the "Decisions") are reported at 847 Fed. Appx. 869 and 847 Fed. Appx. 881, and respectively reprinted at App. 1a-25a and App. 26a-43a. The Federal Circuit's decision reported at 847 Fed. Appx. 881 relied on the discussion reported at 847 Fed. Appx. 869. *See* App. 39a.

JURISDICTION

The Federal Circuit rendered its Decisions on March 10, 2021. App. 1a-25a; App. 26a-43a. Centripetal timely filed this appeal pursuant to Rule 13.1 and this Court's July 19, 2021 Order extending

the deadline to file a petition for a writ of certiorari. This Court has jurisdiction under 28 U.S.C. § 1254(1).

PERTINENT STATUTORY PROVISION

35 U.S.C. § 102 (pre-AIA) provides in relevant part:

Conditions for patentability; novelty and loss of right to patent.

A person shall be entitled to a patent unless —

*****

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of the application for patent in the United States.

App. 223a.

STATEMENT OF THE CASE

I. Statutory Framework

The patent statute provides that "[a] person shall be entitled to a patent unless" the claimed invention is anticipated or rendered obvious by prior art. 35 U.S.C. §§ 102(b), 103 (pre-AIA). Congress identified various categories of relevant prior art. At issue in this Petition is "printed publication" prior art. *Id.*

For decades, the Federal Circuit, its predecessor court, and the other circuit courts applied a standard that a document only qualified as a printed publication if it was reasonably accessible to interested members of the public through generally available medium that allows for wide public access. *See* p. 10-12, *infra*.

In particular, the public accessibility aspect of a printed publication has been "called the touch-stone in determining whether a reference constitutes a 'printed publication.'" *Acceleration Bay, LLC v. Activision Blizzard Inc.*, 908 F.3d 765, 772 (Fed. Cir. 2018). "A reference is considered publicly accessible if it was 'disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, can locate it.'" *Id.* (citation omitted).

II. Factual and Procedural History

A. Centripetal's Patents Benefited the Public By Disclosing New and Useful Techniques to Prevent Cyber Attacks.

Petitioner Centripetal is an innovative cyber-security company that develops and sells the RuleGate and CleanINTERNET suite of products and services, which protect a network against a variety of attacks. Centripetal spent over a decade inventing and developing new techniques to protect computer networks from a variety of hostile attacks, for which it was awarded numerous patents, including United States Patent Nos. 9,124,552 (the "'552 Patent), U.S. Patent No. 9,160,713 (the "'713 Patent"), and U.S. Patent No. 9,413,722 (the "'722 Patent").

The '552 and '713 Patents disclose to the public new and useful techniques for preventing "[a] category of cyber attack known as exfiltrations" that had, prior to the '552 and '713 Patents, been "difficult for conventional cyber defense systems to prevent." J.A. 140 at 1:15-18, J.A. 154 at 1:25-28.[1] The '722 Patent discloses new and useful techniques for proactively filtering network traffic on the basis of "network threat intelligence," which refers to information about threats on the Internet. S.J.A. 159-160 at 1:20-26, 3:18-33.

---

[1] Materials from the Joint Appendix filed in U.S. Court of Appeals for the Federal Circuit (CAFC), Case No. 20-1635, Docket 33, are cited herein as "J.A." Materials from the Joint Appendix filed in CAFC, Case No. 20-2057, Docket 21, are cited herein as "S.J.A."

B. After Centripetal Sued Cisco for Patent Infringement, Cisco Challenged the Validity of Centripetal's Patents.

Centripetal sued Cisco for infringing Centripetal's patents, including the '552, '713, and '722 Patents. Cisco filed multiple petitions for *inter partes* review ("IPR") of Centripetal's patents. Cisco asserted as printed publication prior art the user guide for a Sourcefire software product (the "Sourcefire Manual"). App. 7a; App. 27a. The PTAB found the challenged claims from Centripetal's patents invalid in view of the Sourcefire Manual. *See generally*, App. 66a-77a; App. 129a-136a; App. 172a-182a.

Centripetal argued that the Sourcefire Manual is not a printed publication (and, therefore, cannot be used as prior art), because it was not available to the public as the Sourcefire Manual was only made available under lock and key on a password protected support website and only to customers willing and able to purchase the corresponding Sourcefire software that cost over $25,000. *See* SA1-SA8.

The PTAB entered the Final Written Decisions on the '552, '713, and '722 Patents, finding that the Sourcefire Manual was a printed publication and that the challenged claims of the patents were unpatentable over the Sourcefire Manual. *See generally*, App. 66a-77a; App. 129a-136a; App. 172a-182a.

C. The Federal Circuit Affirmed the PTAB's Decisions.

A Federal Circuit panel affirmed the PTAB's Final Written Decisions after Centripetal appealed. The panel acknowledged that the makers of the Sourcefire Manual kept it on a secure website that was not available to the public. App. 15a; App. 33a; App. 34a.

The panel focused on the Board's finding that customers obtained the Sourcefire Manual through the purchase of the Sourcefire software, which cost at least $25,000. App. 17a-20a; App. 39a. As a result, on March 10, 2021, the Federal Circuit affirmed the PTAB's decisions that the Sourcefire Manual was publicly accessible, and therefore qualified as printed publication prior art. *See* App. 20a; App. 39a.

REASONS FOR GRANTING THE PETITION

This Court should grant this Petition in order to resolve the Federal Circuit's inconsistent application of the requirement that printed publication prior art be generally accessible by the public. The general accessibility requirement serves the important policy objective of promoting disclosure, which is a basic tenet of the patent system. And the Federal Circuit's effective abrogation of that requirement contravenes decades of precedent and is inconsistent with the decisions of other panels within the Federal Circuit and of its predecessor courts.

I. Requiring that Documents are Reasonably Accessible to the Public to be Considered Printed Publications Serves Congress's intent.

This Court in *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470 (1974) reviewed the purposes of the patent system. 416 U.S. at 480-81. The *Kewanee Oil* Court articulated that the patent system is designed to: (1) foster and reward innovation; (2) promote disclosure of inventions such to advance further innovation for the public benefit; and (3) assure that ideas already in the public domain remain there for use of the public. *Id.*

The Federal Circuit's Decisions therefore undermines a basic policy underlying the Patent Act by qualifying a document unavailable to the public as printed publication prior art. Doing so controverts the patent system's goal of "bring[ing] new designs and technologies into the public domain through disclosure[,]" by allowing a document made available to only a select few to be used to negate patent rights granted based on inventors' enrichment of the public commons through disclosures in patent applications. *Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*, 489 U.S. 141, 151 (1989).

The philosophical underpinnings for the patent grant and the "printed publication" rule is seen in Justice Roberts' opinion in *United States v. Dubilier Condenser Corp.*, 289 U.S. 178 (1933):

> ***An inventor deprives the public of nothing which it enjoyed before his discovery, but gives something of value to the community by adding to the sum of human knowledge***. He

> may keep his invention secret and reap its fruits indefinitely. In consideration of its disclosure and the consequent benefit to the community, the patent is granted. An exclusive enjoyment is guaranteed him for seventeen years, but, upon the expiration of that period, ***the knowledge of the invention inures to the people, who are thus enabled without restriction to practice it and profit by its use.***

289 U.S. at 186-87 (emphasis added) (citations omitted).

The "printed publication" rule follows logically from the principle that the granting of a patent serves to add to the sum of public knowledge and advance innovation, not to remove existing knowledge from the public domain. *See, e.g.*, *Graham v. John Deere Co.*, 383 U.S. 1, 6 (1966); *see also, e.g.*, *Oil States Energy Servs., LLC v. Greene's Energy Grp., LLC*, 138 S. Ct. 1365, 1374 (2018) (citing *Graham*, 138 U.S. at 6)). This principle strikes a balance between the granting of a patent and existing public knowledge, as a patent confers upon the public only new and useful discoveries and innovations that the public can use as the building blocks for further advancements. Accordingly, the "printed publication" rule ensures that the public is not deprived of any existing knowledge.

Since the first appearance of the term "printed publication" in the Patent Act of 1836, it has been understood that a printed publication must be

"intended and employed for the communication of ideas to persons in general" and "actually published in such a manner that any one who chooses may avail himself of the information it contains." 1 William C. Robinson, *The Law of Patents for Useful Inventions*, §§ 326-327 (1890); *id.* at § 325; *see also I.C.E. Corp. v. Armco Steel Corp.*, 250 F. Supp 738, 740-41 (S.D.N.Y. 1966). In other words, the accessibility of knowledge is required for a document to qualify as a printed publication. 1 William C. Robinson, *The Law of Patents for Useful Inventions*, § 327 (1890).

With the enactment of the America Invents Act ("AIA") in 2011, Senator Kyl echoed the same understanding when explaining that a document is publicly accessible if "persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, ***can locate it*** and recognize and comprehend therefrom the essentials of the claimed invention . . . ." 157 Cong. Rec S 1370 (daily ed. March 8, 2011) (statement of Sen. Kyl) (emphasis added) (citations omitted). As Senator Kyl emphasized, the accessibility of a document depends on whether interested members of the relevant public ***could obtain the information if they wanted to***. *Id.* (citing *Cordis Corp. v. Boston Scientific Corp.*, 561 F.3d 1319, 1333 (Fed. Cir. 2009)).

Consistent with this policy, for decades, the courts have interpreted "printed publication" to require availability to the interested public. In the seminal case *In re Tenney*, 254 F.2d 619 (C.C.P.A. 1958), the United States Court of Customs and Patent Appeals ("CCPA") recognized the significance of the patent grant and how the "printed publication" rule is

meant to foster, not hinder, advancements in innovation. 254 F.2d at 623-24.

The *Tenney* court articulated that the foundation of "printed publication" rule rests on the contract between the public and the inventor, as the public grants a patent in exchange for the access to the knowledge offered by the inventor that otherwise did not exist within the public domain. *Id.* at 624; *see also Pickering v. Holman*, 459 F.2d 403, 407 (9th Cir. 1972) (citing *Dubilier Condenser Corp.*, 289 U.S. at 186). In other words, "in consideration for the patent grant, something must be given to the public which it did not have before . . . . [i]f the public is already possessed of that 'something,' or if it is accessible to the public, there is failure. . . ." *In re Tenney*, 254 F.2d at 624.

The CCPA's precedent is predicated upon the proposition that for "something" (e.g., knowledge within a document) to be accessible to the public, and therefore qualify as a publicly accessible printed publication under the statute, it must have been made publicly accessible through "a medium capable of providing wide public access, . . . not commercial exploitation." *Pickering*, 459 F.2d at 407 (citing *In re Tenney*, 254 F.2d at 626).

Similarly, the Seventh Circuit in *Popeil Brothers, Inc. v. Schick Electric, Inc.*, 494 F.2d 162 (7th Cir. 1974), articulated that to "constitute a printed publication for purposes of the publication bar, all that is required is that the document in question be printed and disseminated as to provide wide public access to it." 494 F.2d at 166 (citations omitted); *see also Deep Welding, Inc. v. Sciaky Bros.,*

Inc., 417 F.2d 1227, 1235 (7th Cir. 1969) ("a more widely circulated printed item is clearly to be preferred as a printed publication evidence prior art").

Other panels within the Federal Circuit have enforced the printed publication standard. For example, in *Constant*, the Federal Circuit explained that "[a]ccessibility goes to the issue of whether interested members of the relevant public ***could obtain the information*** if they wanted to." *Constant v. Advanced Micro-Devices, Inc.*, 848 F.2d 1560, 1569 (Fed. Cir. 1988) (emphasis added).

In a dissent, Judge Newman decried the Federal Circuit's erosion of the printed publication's availability requirement and highlighted its departure from the "printed publication" precedent of "reasonably accessible through generally available media that serve to disseminate information." *Bruckelmyer v. Ground Heaters, Inc.*, 453 F.3d 1352, 1355 (Fed. Cir. 2006) (Newman, J., dissenting) (citing *In re Klopfenstein*, 380 F.3d 1345, 1348 (Fed. Cir. 2004) (for a document to qualify as a printed publication it must be "sufficiently accessible to the public interested in the art"); *see also In re Cronyn,* 890 F.2d 1158, 1160-61 (Fed. Cir. 1989) (a document to qualify as a printed publication must be sufficiently available to make it reasonably accessible to the public); *In re Hall*, 781 F.2d 897, 899 (Fed. Cir. 1986) (a document must be sufficiently accessible "at least to the public interested in the art, so that such a one by examining the reference could make the claimed invention.").

II. The Federal Circuit's Erroneous Decisions Run Afoul of Decades of Precedent and the Purpose of the Patent System.

As established above, various courts and panels within the Federal Circuit have interpreted printed publication as limited to documents reasonably accessible through a medium that serves to disseminate information. The Federal Circuit's Decisions at issue affirming the Sourcefire Manual as a printed publication is a split from this precedent. The Sourcefire Manual was not publicly accessible and a member of the public researching the then-state of the art in cyber security would have no way to know what it disclosed and no basis to spend $25,000 to obtain a copy. *See* § IIB, *supra*. Thus, the Sourcefire Manual is not a printed publication in the sense that Congress intended.

Congress enacted the patent system to give effect to the Constitution's purpose to promote the progress of science the useful arts for the benefit of the public. *See* U.S. CONST. art. 1, § 8. The patent system incentivizes inventors to publicly disclose innovations that advantage the public—that is, add to the sum of public knowledge—in exchange for the granting of a patent. *See Dubilier Condenser Corp.*, 289 U.S. at 186. As it has long been recognized that the public grants a patent to an inventor for new and useful discoveries that the public did not previously have knowledge of. *See id.*; *see also Butterworth v. United States ex rel. Hoe,* 112 U.S. 50, 59 (1884).

The panel ignores the constitutional purpose of the patent system. The Decisions here allow for an entity to shield a document from interested members of the relevant public given its high price point (which, effectively keeps it as secret work), but still use the document to defeat a patent. Importantly, Congress enacted the AIA to rid the patent system of this misconduct of withholding information from the public domain, and yet using it as prior art to invalidate patents. *Cf.* 157 Cong. Rec S 1497 (daily ed. March 9, 2011) (Senator Leahy explaining that part of the intent of the AIA was to rid the patent system of "private uses or secret processes" which are purposefully withheld from the public domain and then unveiled to be used as patent defeating prior art.); *see also I.C.E. Corp.*, 250 F. Supp at 741 (explaining that the term "'public work' was replaced by or merged into the term 'printed publication'" and by this judicial construction "the word 'public' in this context has been construed to mean 'not secret.'").

The Federal Circuit's Decisions thus turn the Constitution's purpose of the patent system on its head, as they stifle the advancement of innovation and encourage companies to withhold their inventions and documents. *See Kewanee Oil Co.*, 416 U.S. at 480-81. This is the antithesis of the patent system and its "ultimate goal . . . to bring new designs and technologies into the public domain." *Bonito*, 489 U.S. at 151.

Thus, this case presents an ideal vessel for this Court to reconfirm that "printed publications" that are being asserted as prior art must be publicly accessible, and ensure that the rule is applied consistent with

decades of precedent and the purposes of the patent system.

CONCLUSION

For all the foregoing reasons, the Court should grant the petition for writ of certiorari.

August 9, 2021

Respectfully submitted,

Paul J. Andre
Counsel of Record
Lisa Kobialka
James Hannah
Kramer Levin Naftalis
& Frankel LLP
990 Marsh Road
Menlo Park, CA 94025
(650) 752-1700
pandre@kramerlevin.com
lkobialka@kramerlevin.com
jhannah@kramerlevin.com

Attorneys for Petitioner
Centripetal Networks, Inc.

APPENDIX

APPENDIX A — OPINION OF THE UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT, CASE NOS. 2020-1635, 2020-1636, FILED MARCH 10, 2021

UNITED STATES COURT OF APPEALS
FOR THE FEDERAL CIRCUIT

2020-1635, 2020-1636

CENTRIPETAL NETWORKS, INC.,

Appellant,

v.

CISCO SYSTEMS, INC.,

Appellee.

Appeals from the United States Patent and Trademark Office, Patent Trial and Appeal Board in Nos. IPR2018-01436, IPR2018-01437.

March 10, 2021, Decided

JAMES R. HANNAH, Kramer Levin Naftalis & Frankel LLP, Menlo Park, CA, for appellant. Also represented by PAUL J. ANDRE; JEFFREY PRICE, New York, NY.

PATRICK D. MCPHERSON, Duane Morris LLP, Washington, DC, for appellee. Also represented by CHRISTOPHER JOSEPH TYSON; MATTHEW CHRISTOPHER GAUDET, Atlanta, GA; JOSEPH POWERS, Philadelphia, PA.

Appendix A

Before MOORE, SCHALL, and TARANTO, *Circuit Judges*.

TARANTO, *Circuit Judge*.

Centripetal Networks, Inc. owns U.S. Patent Nos. 9,124,552 and 9,160,713, which address cybersecurity techniques for filtering encrypted packets passing between a secured and an unsecured network. In July 2018, Cisco Systems, Inc. filed petitions for inter partes reviews of the '552 and '713 patents. For all claims of both patents, Cisco asserted unpatentability under 35 U.S.C. § 103 for obviousness based on a user manual for an earlier security system—a manual that Cisco asserted was a prior-art "printed publication." 35 U.S.C. § 311(b). The Patent Trial and Appeal Board instituted both requested inter partes reviews and, in its final written decisions, agreed with Cisco about the printed-publication status of the user manual and about unpatentability of all claims. *Cisco Systems, Inc. v. Centripetal Networks, Inc.*, IPR2018-01436, 2020 WL 402817 (P.T.A.B. Jan. 23, 2020) (*'552 Decision*); *Cisco Systems, Inc. v. Centripetal Networks, Inc.*, IPR2018-01437, 2020 WL 402317 (P.T.A.B. Jan. 23, 2020) (*'713 Decision*). We affirm.

I

A

The patents address aspects of the now-common process of sending messages across networks, specifically across the Internet, using protocols that split up a

message's content into packets for transmission. J.A. 6682 ¶ 47; J.A. 6823. When packets arrive at their destination, they are assembled to recreate the original message. *See* J.A. 2064. Two common preexisting protocols, which allow encryption of the transmitted data, are relevant here: Hypertext Transfer Protocol Secure (HTTPS) and Transport Layer Security (TLS). *See* '552 patent, col. 7, lines 53-60.

Because the '713 patent issued from a continuation of the application that issued as the '552 patent, the patents share a specification, and when citing that specification, we will generally cite only the '552 patent. The patents are concerned with "filtering network data transfers" and the passage of information between a secured network (*e.g.*, a private company's network) and an unsecured network (*e.g.*, the larger Internet). '552 patent, Abstract; '713 patent, Abstract; *see also* '552 patent, col. 1, lines 62-64. The specification focuses, in particular, on preventing a type of cyberattack known as an "exfiltration," which involves stealing information (extracting it without authorization) as it exits a secure network, using "popular network data transfer protocols" to disguise the theft "as normal network behavior." *Id.*, col. 1, lines 15-23. Previous cybersecurity systems, the patents say, inadequately protected against such attacks because they tended to interpret the exfiltration as ordinary network behavior and did not account for vulnerabilities in the conventional version of TLS, *i.e.*, TLS version 1.0. *Id.*, col. 1, lines 23-25; *id.*, col. 6, lines 40-47.

Appendix A

The patents describe a solution in which packets entering or exiting a secure network are first received at a packet secure gateway, which may include "one or more computing devices configured to receive packets." *Id.*, col. 3, lines 42-44. The gateway also receives a "dynamic security policy" from a "security policy management server," *id.*, col. 4, lines 53-55, which provides the "packet filter" in the gateway with "one or more rules" to determine where (to which "operators") packets "having specified information" should be sent, *id.*, col. 5, lines 6-16. The specified information gathered from a packet may include a "five-tuple," which may comprise "one or more values selected from": the protocol type of the packet, the Internet Protocol (IP) address of the source of the packet, "one or more source port values," the IP address(es) of the destination(s) of the packet, and "one or more destination ports." *Id.*, col. 5, lines 34-42. Based on the information collected from the packet, the gateway system "determines" which operator to direct the packet to, *id.*, col. 5, lines 9-16, and the operator then applies one or more filtering rules to the packet to "allow" or "block" the packet, *see*, *e.g.*, *id.* col. 5, lines 62-67; *id.* col. 6, lines 11-16. For example, a rule may require that a packet use "version 1.1 or 1.2 of the Transport Layer Security (TLS) protocol" in order to be allowed to continue, because "the popular TLS version 1.0 protocol has a known security vulnerability that attackers may exploit to decrypt HTTPS sessions." *Id.*, col. 6, lines 27-47.

Independent claim 1 of the '552 patent recites:

1. A method, comprising:

at a computing device comprising at least one processor, a memory, and a communication interface:

receiving, via the communication interface, a plurality of hypertext transfer protocol secure (HTTPS) packets;

responsive to a determination by the at least one processor that at least a portion of the plurality of HTTPS packets have packet-header-field values corresponding to a packet filtering rule stored in the memory, applying, by the at least one processor, an operator specified by the packetfiltering rule to the at least a portion of the plurality of HTTPS packets, wherein the operator specifies one or more application-header-field-value criteria identifying one or more transport layer security (TLS)-version values for which packets should be blocked from continuing toward their respective destinations;

and

responsive to a determination by the at least one processor that one or more packets, of the at least a portion of

> the plurality of HTTPS packets, have one or more application-header-field values corresponding to one or more TLS-version values of the one or more TLS-version values for which packets should be blocked from continuing toward their respective destinations, applying, by the at least one processor, at least one packet-transformation function specified by the operator to the one or more packets to block each packet of the one or more packets from continuing toward its respective destination.

Id., col. 11, lines 5-35. Claims 8 and 15 are the only other independent claims in the '552 patent. Claim 8 claims an "apparatus" that performs the claim 1 method and claim 15 claims "non-transitory computer-readable media" containing instructions that, when executed, perform the claim 1 method. *Id.*, col. 12, line 54 through col. 13, line 15; *id.* col. 13, lines 39-67. No additional limitations in the dependent claims of the '552 patent are relevant to Centripetal's appeal.

Claim 1 of the '713 patent recites:

> 1. A method comprising:
>
> receiving, by a computing system provisioned with a plurality of packet-filtering rules, a first packet and a second packet;

> responsive to a determination by the computing system that the first packet comprises data corresponding to a transport layer security (TLS)-version value for which one or more packet-filtering rules of the plurality of packet-filtering rules indicate packets should be forwarded toward their respective destinations, forwarding, by the computing system, the first packet toward its destination; and
>
> responsive to a determination by the computing system that the second packet comprises data corresponding to a TLS-version value for which the one or more packet-filtering rules indicate packets should be blocked from continuing toward their respective destinations, dropping, by the computer system, the second packet.

'713 patent, col. 11, lines 8-25. Independent claims 8 and 15 of the '713 patent are substantially similar to claim 1; for present purposes, they are system and non-transitory computer-readable media forms of method claim 1. *See id.*, col. 12, lines 29-47; *id.*, col. 13, lines 44-61.

B

In July 2018, Cisco filed petitions for inter partes reviews of all claims (claims 1-21) of the '552 patent and all claims (claims 1-20) of the '713 patent. Cisco argued that the claimed inventions of all claims would have been obvious to a relevant artisan in view of the User Guide for the Sourcefire 3D System—a manual referred to in the matters before us as "Sourcefire."

Appendix A

Sourcefire describes a system that monitors network activity with packet-filtering devices called "3D-Sensors" that record network activity and identify (and call attention to) "intrusion events" based on an "intrusion policy applied to a detection engine on the sensor that is monitoring a specific network segment." J.A. 1460, 1683. In this system, packets traveling through the network pass through three layers that decode them, J.A. 1683, 1685, then pass through preprocessors that "normalize traffic at the application layer and detect protocol anomalies," J.A. 1685, and finally arrive at a "rules engine" that "inspects the packet headers" and "determine[s] whether they trigger any of the shared object rules or standard text rules," J.A. 1685-86. At any of these steps, a packet could cause the system "to generate an event, which is an indication that the packet or its contents" may be a security risk. J.A. 1687.

When packets arrive at Sourcefire's rules engine, the engine determines whether values in the packet header trigger one or more "intrusion rules." J.A. 1686, 1940, 2188. Intrusion rules may have two parts: (1) the rule header, which includes the five-tuple values (protocol, source and destination IP addresses, source and destination ports), the rule's action (*e.g.*, drop, alert and allow, ignore and allow), and direction indicators; and (2) the rule options part, which contains, *e.g.*, keywords and their arguments and event messages. J.A. 2189; *see also* J.A. 2188-96. Keywords in intrusion rules can be used by the preprocessor (called the Secure Sockets Layer (SSL) preprocessor) and by the rules engine to filter

packets according to their encryption protocol version (for example, their TLS version). J.A. 2252. Sourcefire permits users to write their own custom intrusion rules, J.A. 2188-96, so a user could use a keyword like "ssl_version" in an intrusion rule to cause the SSL preprocessor to match the protocol version information contained in the application headers of the packets against the protocol of the assembled packets for an encrypted session (a reassembled stream of messages known as a handshake), J.A. 2254-55; *see also* J.A. 1918, 2024-28, 2127.

In its petitions for inter partes reviews, Cisco argued that the claims of the '552 and '713 patents recite subject matter that would have been obvious in view of Sourcefire because Sourcefire describes a cybersecurity system that can be configured to meet every limitation in the claims. *'552 Decision*, 2020 WL 402817, at *8; *'713 Decision*, 2020 WL 402317, at *6-7. Specifically, Cisco relied on Sourcefire as disclosing, to a relevant artisan, the idea of writing custom intrusion rules that would permit the Sourcefire system to determine the TLS-version values of the packets it received based on keywords and to use the rules engine as an operator to apply packet-filtering rules based on those determinations. *'552 Decision*, 2020 WL 402817, at *15-16; *'713 Decision*, 2020 WL 402317, at *6-7.

After the Board instituted the requested inter partes reviews, Centripetal argued that Sourcefire was not a "printed publication" at the priority date for the patents at issue, *see* 35 U.S.C. § 102(a)(1); 35 U.S.C. § 102(b) (2006), as required for non-patent prior art in IPRs under 35 U.S.C. § 311(b). J.A. 434-38; *see also '713 Decision*, 2020

WL 402317, at *3.[1] Centripetal contended that Sourcefire (the document) was costly and was distributed only to those who bought certain products from Sourcefire (the company) and, therefore, the document was not publicly accessible because a relevant artisan could not have obtained it with reasonable diligence. J.A. 434-38.

In IPR-1436 (addressing the '552 patent), Centripetal did not dispute that Sourcefire teaches a processor, memory, and communication interface; nor did it dispute that Sourcefire teaches "receiving, via the communication interface a plurality of [HTTPS] packets." *'552 Decision*, 2020 WL 402817, at *14-15. Centripetal argued, however, that Sourcefire does not teach the "determination" limitations of the claims, specifically the requirements of (1) a "determination" that a plurality of HTTPS packets "have packet-header-field values corresponding to a packet-filtering rule" and (2) a "determination" that some of those packets "have one or more application-header-field values corresponding to one or more TLS-version values." *See* J.A. 456, 458. According to Centripetal, Sourcefire teaches extracting version information from a reassembled stream of packets ("handshake and key exchange messages," J.A. 2025), whereas the claims require a determination of version information to be made for individual packets. J.A. 461-62.

---

1. The version of 35 U.S.C. § 102 pre-dating the amendments made in 2011 (effective March 16, 2013) applies in both of these matters, given that the application that issued as the '552 patent was filed March 12, 2013, and the '713 patent is the child of the '552 patent. *See '552 Decision*, 2020 WL 402817, at *4 n.1. The current version of § 102 continues to use the phrase "printed publication."

Centripetal alleged an additional deficiency in Sourcefire's teaching of the claim limitations. It contended that Sourcefire does not teach the claimed "operator," because the claims require that the operator specify both "application-header-field-value criteria" and "a packet transformation function," and the Sourcefire system is "not capable of designing a packet-filtering rule specifying an operator that applies different packet transformation functions based on different application-layer-packet-header criteria." J.A. 471-73. Centripetal further argued that Cisco had not shown that a relevant artisan would have been motivated to modify the teachings of Sourcefire to arrive at the claims. J.A. 481. And Centripetal advanced what it urged were objective indicia of nonobviousness, including praise for its product addressing TLS vulnerabilities. J.A. 494-95.

In IPR-1437 (addressing the '713 patent), Centripetal made similar arguments. *See* J.A. 7394-99, 7403-06.

C

In IPR-1436, the Board first determined that Cisco had met its burden to show that Sourcefire was a printed publication. *'552 Decision*, 2020 WL 402817, at *8-12. Specifically, the Board found that Sourcefire, a user guide, was publicly accessible in that it was available to purchasers of Sourcefire 3D Systems and was, in fact, distributed on CD-ROM to 586 system purchasers between April 2011 and March 2013, *id.* at *9-10; no confidentiality restrictions prevented purchasers from reproducing and distributing

the document "for non-commercial use," *id.* at *10 (citing J.A. 1429); and Sourcefire advertised its products and their accompaniment by extensive documentation, *id.* at *11; J.A. 4695-99. The Board rejected Centripetal's argument that the cost of obtaining Sourcefire (the document) was prohibitive; the Board found that it could be acquired by purchasing products that cost between $1,385 and £25,000, that 586 customers actually acquired it, and that Centripetal had not shown that an interested relevant artisan was not reasonably able to obtain the material. *Id.* at *12 & n.9.

After determining that Sourcefire qualified as prior art, the Board addressed the disputed limitations in claim 1 (and claims 8 and 15). *Id.* at *14-22. Regarding the determination limitations, the Board explained that nothing in the claims requires that each individual packet be inspected or that TLS (or SSL) version information be extracted from application-header-values of individual packets, rather than a reassembled stream (handshake message). *Id.* at *17. Reassembled streams of messages, the Board continued, themselves consist of individual packets, and a relevant artisan would have known that the TLS-version information is always contained in the packet header of the first packet in the message, as Centripetal acknowledged. *Id.* at *18. Accordingly, the Board found that a relevant artisan would have understood Sourcefire, even in describing the extraction of version information from the reassembled message, as teaching the claim requirement of extraction from the first packet. *Id.* at *18-19.

Regarding the claimed "operator," the Board adopted Centripetal's claim construction, construing the term to refer to "a function specified by a packet-filtering rule that specifies one or more application-header-field criteria and a packet transformation to apply to the packet for each of the application-header-field criteria." *Id.* at *5-6. Applying that construction, the Board found that Sourcefire's keyword and argument functions (in particular, ssl_version keywords) permitted the system to (1) indicate application-header-field-value criteria (*e.g.*, the version of TLS) and (2) apply a "packet transformation function," *e.g.*, blocking the packets, as specified by the claims. *Id.* at *19. The Board also rejected Centripetal's argument that Sourcefire could not teach an operator because the "rule action" was specified in the "rule header," so that Sourcefire could apply only "one rule action" per rule (*e.g.*, could only allow certain packets, rather than allow and block some). *Id.* at *20. The Board found that Centripetal had presented no evidence to support this argument and that Cisco had shown support in Sourcefire for using different ssl_version keywords to "allow," "pass," or "drop" packets. *Id.*

Finally, the Board found that Cisco had met its burden to show that a relevant artisan would have been motivated to modify Sourcefire to meet the '552 patent's claim limitations. *Id.* at *21-22. Citing the declaration from Cisco's expert (Dr. Staniford), the Board found that the known vulnerabilities of early versions of protocols like TLS, along with the ordinary creativity of a relevant artisan, would be sufficient to motivate that artisan to use Sourcefire to write rules blocking packets with a vulnerability like that of TLS 1.0. *Id.* The Board also found

that Centripetal's objective indicia of nonobviousness—particularly the praise for its RuleGATE product—were not entitled to much weight, noting the lack of a persuasive basis for finding the nexus of cited objective indicia to the claims of the '552 patent. *Id.* at *22-24. The Board then addressed the additional limitations in the remaining dependent claims and found obviousness as to those claims as well. *Id.* at *24-26.

In IPR-1437, the Board's finding and reasoning were similar to those in IPR-1436. *See '713 Decision*, 2020 WL 402317, at *3-13.

The Board issued its final written decisions as to both IPR-1436 and IPR-1437 on January 23, 2020. Centripetal timely appealed both decisions. We have jurisdiction under 28 U.S.C. § 1295(a)(4)(A) and 35 U.S.C. §§ 141(c), 319.

II

We review the Board's final written decisions under the Administrative Procedure Act, "hold[ing] unlawful and set[ting] aside agency action, findings, and conclusions found to be . . . arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law . . . [or] unsupported by substantial evidence." 5 U.S.C. § 706; *Dickinson v. Zurko*, 527 U.S. 150, 164-65, 119 S. Ct. 1816, 144 L. Ed. 2d 143 (1999). We review the Board's legal conclusions de novo and factual findings for substantial evidence. *Nobel Biocare Services AG v. Instradent USA, Inc.*, 903 F.3d 1365, 1374 (Fed. Cir. 2018). Whether a reference qualifies as a "printed publication" is a legal conclusion based on factual findings. *Jazz Pharms., Inc.*

v. Amneal Pharms., LLC, 895 F.3d 1347, 1356 (Fed. Cir. 2018). "The underlying factual findings [in a printed-publication analysis] include whether a reference was publicly accessible." *Nobel*, 903 F.3d at 1375. Similarly, the ultimate determination of whether a claimed invention would have been obvious is a legal one reviewed de novo, but underlying factual determinations are reviewed for substantial-evidence support. *PersonalWeb Techs., LLC v. Apple, Inc.*, 917 F.3d 1376, 1381 (Fed. Cir. 2019).

On appeal, Centripetal argues that: (1) the Board erred by concluding that Sourcefire is a printed publication, *see* Centripetal Opening Br. 15-21; (2) Sourcefire does not teach a "determination" that a packet includes a specified TLS-version value, *id.* at 21-24; (3) Cisco did not show a motivation to modify Sourcefire and the Board overlooked important objective indicia of nonobviousness, *id.* at 24-31; and (4) Sourcefire does not disclose the operator described in the '552 patent, *id.* at 31-34.[2] We reject these challenges.

A

Centripetal first contends that Sourcefire was not a printed publication because it was available only to those willing to pay $25,000 for the accompanying product and was kept password-protected on Sourcefire's website, preventing access to the relevant public. Centripetal Opening Br. 15-16. We reject this argument.

2. In making their respective arguments on appeal, the parties do not distinguish between the Board's decisions in IPR-1436 and IPR-1437, except where relevant. Centripetal Opening Br. 3; Cisco Response Br. 6 n.1. We consider the decisions together unless otherwise noted.

Whether a reference is a printed publication "involves a case-by-case inquiry into the facts and circumstances surrounding the reference's disclosure to members of the public." *In re Klopfenstein*, 380 F.3d 1345, 1350 (Fed. Cir. 2004). "Because there are many ways in which a reference may be disseminated to the interested public, public accessibility has been called the touchstone in determining whether a reference constitutes a printed publication." *Blue Calypso, LLC v. Groupon, Inc.*, 815 F.3d 1331, 1348 (Fed. Cir. 2016) (cleaned up). For a reference to be publicly accessible, it must be "'disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, can locate it.'" *Acceleration Bay, LLC v. Activision Blizzard Inc.*, 908 F.3d 765, 772 (Fed. Cir. 2018) (quoting *Jazz Pharms.*, 895 F.3d at 1355-56); *see also Kyocera Wireless Corp. v. Int'l Trade Comm'n*, 545 F.3d 1340, 1350 (Fed. Cir. 2008). A reference need not be catalogued or indexed to be a printed publication; "a printed publication need not be easily searchable after publication if it was sufficiently disseminated at the time of its publication." *Suffolk Techs., LLC v. AOL Inc.*, 752 F.3d 1358, 1365 (Fed. Cir. 2014); *see also In re Lister*, 583 F.3d 1307, 1312 (Fed. Cir. 2009); *Klopfenstein*, 380 F.3d at 1348. Limited distributions of a reference may suffice. *Samsung Elecs. Co. v. Infobridge Pte. Ltd.*, 929 F.3d 1363, 1374 (Fed. Cir. 2019). In determining whether interested persons could have accessed the publication, we consider factors such as the expertise of the target audience, the avenues of distribution (*e.g.*, at a trade show), the duration of dissemination, and expectations of confidentiality or restrictions on recipients' sharing of the information.

GoPro, Inc. v. Contour IP Holding LLC, 908 F.3d 690, 694-95 (Fed. Cir. 2018).[3]

Here, the Board found, based on testimony from a Sourcefire company employee, that each of the 586 customers who purchased a range of Sourcefire products over a relevant two-year period received a CD-ROM containing the user guide, which explicitly stated that users were permitted to "use, print out, save on a retrieval system, and otherwise copy and distribute" the reference for noncommercial use. *'552 Decision*; 2020 WL 402817,

3. *See*, *e.g.*, *GoPro*, 908 F.3d at 694-95 (catalog distributed at a trade show that was only open to "dealers" of action sports vehicles and related accessories was a printed publication because there were no restrictions on the catalog's distribution, there were over 1,000 attendees, and there was no evidence that one interested in the art of digital cameras could not have obtained the catalog with reasonable diligence); *Jazz Pharms.*, 895 F.3d at 1357-59 (Affordable Care Act materials available on the FDA's website and published via constructive notice in the Federal Register were printed publications because the materials were "widely disseminated to persons of ordinary skill for a substantial time with no reasonable expectation of confidentiality"); *Klopfenstein*, 380 F.3d at 1350 (slideshow displayed at a conference for three days was a printed publication because the slide was displayed for a matter of days, the attendees included interested persons of skill in the art, there was no reasonable expectation that the slide would not be copied, and the slide could be copied with relative simplicity); *Massachusetts Inst. of Tech. v. AB Fortia (MIT)*, 774 F.2d 1104, 1108-09 (Fed. Cir. 1985) (paper orally presented at a conference and distributed to only six persons who requested the paper was a printed publication, because "between 50 and 500 persons interested and of ordinary skill in the subject matter were told of the existence of the paper . . . and the document itself was actually disseminated without restriction to at least six persons").

at *9-10 (citing J.A. 1429); *'713 Decision*, 2020 WL 402317, at *4 (same). Further, Centripetal presented no evidence to the Board showing that—despite the CD-ROM distribution—an interested person using reasonable diligence would not have been able to access Sourcefire either by purchasing the product or by receiving a copy of the user guide from another customer. *See '552 Decision*, 2020 WL 402817, at *10. Substantial evidence, including advertisements, reviews, and testimony from a Sourcefire company employee, supports the Board's finding that those interested and of skill in the art *actually* purchased Sourcefire. *Id.* at *11; *see also* J.A. 822. In sum, the large number of Sourcefire product customers, the number of years the product was available, the advertisements targeting those interested and of skill in the art, and the lack of confidentiality restrictions on copying or distributing Sourcefire support a finding of public accessibility. *See GoPro*, 908 F.3d at 694.

The Board properly rejected Centripetal's argument that *In re Bayer*, 568 F.2d 1357 (CCPA 1978), and *Medtronic, Inc. v. Barry*, 891 F.3d 1368 (Fed. Cir. 2018), require a different result. *'552 Decision*, 2020 WL 402817, at *11-12. In *Bayer*, we held that actual dissemination of a student's thesis to members of a graduate committee did not render the thesis publicly accessible. 568 F.2d at 1361-62. We recently explained in *Samsung* that the student's thesis in *Bayer* was not publicly accessible because "the only people who kn[e]w how to find it [were] the ones who created it," and thus it could not be obtained with reasonable diligence by those interested and of skill in the art. *Samsung*, 929 F.3d at 1371-72. Here, in contrast,

Sourcefire was publicly advertised and obtained by at least 586 customers.

In *Medtronic*, a video relating to spinal surgery was distributed at three separate meetings (two for surgeons, one for a private organization), and slides were distributed at two of the meetings. 891 F.3d at 1379. After the Board found lack of public accessibility of either the video or the slides, without distinguishing between the open and the closed meetings, or whether there was an expectation of confidentiality, we vacated and remanded. *Id.* at 1382-83. We instructed the Board to consider the "size and nature of the meetings," as well as whether an "expectation of confidentiality" existed, noting that these are "important considerations" in assessing public accessibility. *Id.* at 1382. In this case, the Board did exactly that. Far from finding Sourcefire to be a printed publication merely because the CD-ROMs were actually distributed to customers, the Board considered the size and nature of the group receiving the CD-ROMs and the absence of confidentiality restrictions. *'552 Decision*, 2020 WL 402817, at *10-12.

Contrary to Centripetal's contention, the Board's conclusion regarding public accessibility is not undermined by the fact that, unlike some of the cases, this case does not involve "free distribution of academic documents to conference and meeting attendees whose express purpose for attending the conference was to hear lectures regarding those same documents." Centripetal Opening Br. 18-19 (cleaned up). Public accessibility is not limited to circumstances of free or academic distributions;

"commercial distribution" can qualify. *Garrett Corp. v. United States*, 422 F.2d 874, 877-78, 190 Ct. Cl. 858 (Ct. Cl. 1970) (distribution of 80 copies of a government report, including 6 to commercial companies, constituted a printed publication because the report was "unclassified and unrestricted in its use"). The Board also reasonably found that Centripetal had not shown the cost of Sourcefire—which it found ranged from $1,385 to £25,000, *'552 Decision*, 2020 WL 402817, at *12 n.9; *see also* J.A. 4695, 4700—to be prohibitive to those interested and of skill in the art, given, *e.g.*, the evidence that at least 586 customers, at least some of them relevant artisans, purchased the product, *'552 Decision*, 2020 WL 402817, at *12; *'713 Decision*, 2020 WL 402317, at *5.

On this record, we agree with the Board that Sourcefire was publicly accessible and therefore qualifies as a printed publication.

B

We reject Centripetal's challenges to the Board's obviousness determination.

1

The Board found that Sourcefire teaches what is required by the determination claims. Centripetal argues otherwise by pointing to language in Sourcefire stating that the preprocessor "collects and reassembles all the packets" and inspects the stream as a "single, reassembled entity" rather than as "individual packets." J.A. 2064-65;

see also Centripetal Opening Br. 22. This argument does not undermine the Board's finding.

As the Board reasoned, *how* Sourcefire obtains TLS-version values is irrelevant to the claims' scope. *'552 Decision*, 2020 WL 402817, at *17-18, *'713 Decision*, 2020 WL 402317, at *8. The claims in the '552 and '713 patents do not require that each individual packet is inspected for the TLS-version value, but only that a determination is made as to what that value is. *See* '552 patent, col. 11, lines 5-35 (claims require "a determination . . . that one or more packets, of the at least a portion of the plurality of HTTPS packets, have one or more application-header-field-values corresponding to one or more TLS-version values"); '713 patent, col. 11, lines 8-25 (claims require "a determination . . . that [a packet received first or a packet received second] comprises data corresponding to a transport layer security TLS-version value").

Further, Centripetal's expert, Dr. Orso, acknowledged that the TLS-version value in a reassembled handshake is virtually always identical to the value for the individual packets associated with that handshake. J.A. 4647-48 (171:6-174:16). And substantial evidence established that relevant artisans would have understood that the TLS-version value is found in the first packet of a message. J.A. 809-10; J.A. 4653. Thus, the Board reasonably found that Sourcefire teaches determining this exact value because the information it obtains from the handshake will be identical to the first packet's header. *See* J.A. 2252 ("The SSL preprocessor extracts state and version information from specific handshake fields. Two fields within the

handshake indicate the version of SSL or TLS used to encrypt the session and the stage of the handshake."). Substantial evidence thus supports the Board's finding that Sourcefire teaches the "determination" limitations of the patent claims.

2

Centripetal argues that the Board erred by finding a motivation to modify Sourcefire based on "common sense," Centripetal Opening Br. 24-27, and by not properly considering objective indicia of nonobviousness that negate any motivation a relevant artisan would have had to modify Sourcefire, *id.* at 27-31.

Centripetal's motivation argument substantially overlaps with its arguments that Sourcefire does not teach the "determination" limitations required by the claims. Specifically, Centripetal argues that the Board found that a relevant artisan would have been motivated to modify Sourcefire to include the "missing" claim limitations—the "determination" limitations—and that such a finding was error because Sourcefire makes determinations from a reassembled packet stream, and a relevant artisan would not be motivated to modify that system to inspect individual packets. Centripetal Opening Br. 24-27. But the Board did not find that these limitations were "missing"; it found that Sourcefire taught the "determination" limitations because such limitations were not limited to systems that inspect individual packets. *See '552 Decision*, 2020 WL 402817, at *17-19; *'713 Decision*, 2020 WL 402317, at *8. And, as discussed above, nothing in either patent's

claims requires individual packets to be inspected in order to determine their TLS-version value.

We also reject Centripetal's argument that the Board failed to properly weigh objective indicia of nonobviousness (specifically, long-felt but unmet need, industry praise, and commercial success/licensing). "In order to accord substantial weight to secondary considerations in an obviousness analysis, 'the evidence of secondary considerations must have a "nexus" to the claims, *i.e.*, there must be "a legally and factually sufficient connection" between the evidence and the patented invention.'" *Fox Factory, Inc. v. SRAM, LLC*, 944 F.3d 1366, 1373 (Fed. Cir. 2019) (quoting *Henny Penny Corp. v. Frymaster LLC*, 938 F.3d 1324, 1332 (Fed. Cir. 2019) (citing *Demaco Corp. v. F. Von Langsdorff Licensing Ltd.*, 851 F.2d 1387, 1392 (Fed. Cir. 1988)).

Here, Centripetal presented several articles praising its RuleGATE product as evidence of industry praise and long-felt but unmet need, including a paper (the ESG paper), J.A. 6900-08, and a Gartner article, J.A. 6909-18. But the RuleGATE product contains far more than what is claimed in the patent claims at issue here. And as the Board found, nothing in those articles ties the praise of RuleGATE, its alleged filling of an unmet need, or its success to the limitations in the claims. *See '552 Decision*, 2020 WL 402817, at *22-24; *'713 Decision*, 2020 WL 402317, at *10-12; *see also Polaris*, 882 F.3d at 1072. Indeed, Centripetal's expert did not even create a claim-construction chart to map the products to each limitation. J.A. 4615-16. On this record, we agree with the

Board that the objective indicia of nonobviousness were not entitled to substantial weight.

3

Finally, Centripetal challenges the Board's finding that Sourcefire teaches the operator required by the '552 patent. Centripetal argues that Sourcefire relies on "Snort rules" that include a "Rule Header" with a single specified "rule action" that can be taken only "'if the packet data matches all the conditions specified in a rule.'" Centripetal Opening Br. 32-33 (quoting J.A. 2188). For that reason, Centripetal urges, Sourcefire cannot disclose the required operator because its rules cannot "apply different packet transformation functions for different TLS-version values." *Id.*

But the '552 patent's claims do not require that a rule provide for more than one action. *See*, *e.g.*, '552 patent, col. 11, lines 5-35. Moreover, even under Centripetal's construction of "operator," the Board found, Sourcefire teaches an operator that meets both criteria required by that construction—that is, Sourcefire (1) determines "application-header-field-value criteria" through its keyword function (*e.g.*, identifies the packets' TLS-version value) and (2) applies a "packet transformation function" by using its Rule Action function to either block, alert, or allow packets matching the application-header-field-value criteria corresponding to the rule. *'552 Decision*, 2020 WL 402817, at *19-21; J.A. 2189-92, 2196. The language of the claims and of Sourcefire provide substantial evidence for the Board's finding that Sourcefire teaches the operator in the '552 patent's claims.

III

We have considered the remainder of Centripetal's arguments and find them to be unpersuasive.

For the foregoing reasons, the decisions of the Patent Trial and Appeal Board in IPR-1436 and IPR-1437 are affirmed.

AFFIRMED

APPENDIX B — OPINION OF THE UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT, CASE NO. 2020-2057, DATED MARCH 10, 2021

UNITED STATES COURT OF APPEALS
FOR THE FEDERAL CIRCUIT

2020-2057

CENTRIPETAL NETWORKS, INC.,

Appellant,

v.

CISCO SYSTEMS, INC.,

Appellee.

Appeal from the United States Patent and Trademark Office, Patent Trial and Appeal Board in No. IPR2018-01760.

March 10, 2021, Decided

PAUL J. ANDRE, Kramer Levin Naftalis & Frankel LLP, Menlo Park, CA, for appellant. Also represented by JAMES R. HANNAH; CRISTINA MARTINEZ, JEFFREY PRICE, New York, NY.

PATRICK D. MCPHERSON, Duane Morris LLP, Washington, DC, for appellee. Also represented by PATRICK C. MULDOON, CHRISTOPHER JOSEPH

Appendix B

TYSON; MATTHEW CHRISTOPHER GAUDET, Atlanta, GA; JOSEPH POWERS, Philadelphia, PA.

Before MOORE, SCHALL, and TARANTO, Circuit Judges.

Centripetal Networks, Inc. owns U.S. Patent No. 9,413,722, which addresses "rule-based network-threat detection." '722 patent, col. 1, lines 45-46. In September 2018, Cisco Systems, Inc. petitioned for an inter partes review of all claims of the '722 patent, alleging that the claimed inventions in all claims (1-25) would have been obvious to a relevant artisan under 35 U.S.C. § 103 in view of a User Guide for the Sourcefire 3D System—a manual the parties have called "Sourcefire." That reference is also before us in *Centripetal Networks, Inc. v. Cisco Systems, Inc.*, Fed. Cir. Nos. 20-1635, -1636, which involves other Centripetal patents and which we decide today (*20-1635 Decision*). A common issue in this matter and in our *20-1635 Decision* is whether Sourcefire was a "printed publication[]" under 35 U.S.C. § 311(b). A distinct issue here is whether Sourcefire teaches identifying "network-threat indicators" as required by the '722 patent's claims.

The Patent Trial and Appeal Board instituted an inter partes review, and in May 2020, it ruled that Sourcefire was a printed publication and that the claimed inventions in claims 1-7, 10-12, 14-21, 24, and 25 in the '722 patent would have been obvious to a relevant artisan in view of Sourcefire. *Cisco Systems, Inc. v. Centripetal Networks, Inc.*, IPR2018-01760, 2020 WL 2549613 (P.T.A.B. May 18, 2020) (*Board Decision*). Centripetal appeals. We have jurisdiction under 28 U.S.C. § 1295(a)(4). We affirm.

Appendix B

I

A

Unauthorized requests for data and large volumes of network traffic are two examples of what the '722 patent calls "network threats" to the Internet. *See* '722 patent, col. 1, lines 16-19. Information about such threats, the patent says, was traditionally compiled by an organization's network devices into "logs," which were then reviewed for "data corresponding to the network-threat indicators provided by [network-threat] services." *Id.*, col. 1, lines 24-29. The patent asserts that because these logs were "generated based on the traffic processed by the network devices without regard to the network-threat indicators," reviewing them was "time consuming" and "exacerbated by the continuously evolving nature of potential threats." *Id.*, col. 1, lines 29-34.

The '722 patent proposes an improvement in the form of a "rule-based network-threat detection" system using a "packet-filtering device" that receives data packets traveling through the Internet and determines whether each packet "corresponds to criteria specified by a packet-filtering rule." *Id.*, col. 1, lines 45-52. The criteria in each rule may "correspond to one or more of the network-threat indicators." *Id.*, col. 1, lines 52-53. Network-threat indicators may include "network addresses, ports, fully qualified domain names (FQDNs), uniform resource locators (URLs), [and] uniform resource identifiers (URIs)" that are "associated with . . . network threats," such as phishing malware. *Id.*, col. 3, lines 18-33.

Appendix B

Packet-filtering rules also specify an "operator," which is "configured to cause packet-filtering device 144 to either prevent packets corresponding to the criteria from continuing toward their respective destinations (e.g., a BLOCK operator) or allow packets corresponding to the criteria to continue toward their respective destinations (e.g., an ALLOW operator)." *Id.*, col. 5, lines 13-24. In addition to allowing and blocking packets, the packet-filtering device "generate[s] a log entry comprising information from the packet-filtering rule," including information about (1) whether the packets corresponded to "one or more network-threat indicators" and (2) whether the packet-filtering device allowed the packet to continue or blocked it from reaching its destination. *Id.*, col. 16, lines 8-19. The packet-filtering device communicates such information to a "user device," *id.*, col. 16, lines 22-24, which permits a user to alter the rules based on the log information by "instruct[ing] the packet-filtering device to reconfigure the operator" so that, for example, the operator "prevent[s] future packets corresponding to the criteria from continuing toward their respective destinations," *id.*, col. 2, lines 1-10. *See also id.*, Fig. 7 (depicting an example of the rules-based network-threat detection system).

Claim 1 is representative and recites:

> 1. A method comprising:
>
> *receiving, by a packet-filtering device, a plurality of packet-filtering rules configured to cause the packet-filtering device to identify*

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

receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;

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:

> 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;
>
> 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;

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 packet-filtering rule and the one or more network-threat indicators;

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; and

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

responsive to a determination by the packet-filtering device that the second packet corresponds to the one or more criteria:

> preventing, by the packet-filtering device, the second packet from continuing toward a destination of the second packet;
>
> communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and
>
> 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.

Id., col. 17, line 16 through col. 18, line 2 (emphasis added). Centripetal raises no arguments on appeal with respect to limitations in the dependent claims. The only claim limitation at issue on appeal is the "network-threat indicator" limitation emphasized above. *See* Centripetal Opening Br. 12-13; *see also* Cisco Response Br. 32 & n. 7.

Appendix B

B

Cisco's petition for an inter partes review relied on Sourcefire, which is the user guide for the Sourcefire company's network security system. It was distributed on a CD-ROM to all customers who purchased certain Sourcefire products. Sourcefire customers, with a password, could also access and download the User Guide on the Sourcefire company's website. J.A. 3161 ¶ 11.

According to Sourcefire (the document), the Sourcefire system provides users with "real-time network intelligence for real-time network defense" through the use of packet-filtering devices called "3D Sensors." J.A. 1064-65. Each sensor can run Sourcefire's "Intrusion Prevention System" (IPS) to detect and prevent potential threats using a "rules-based detection engine" that permits a user to develop custom "intrusion rules" in order to "detect the attacks [the user] think[s] most likely to occur." J.A. 1065-66. Users can select, customize, and manage intrusion rules across all the Sourcefire system's sensors via a centralized "Defense Center." J.A. 1066; *see also* J.A. 1297-98.

An intrusion rule includes a rule header that consists of parameters and their associated "arguments," including 5-tuple rule criteria values (protocol, source and destination Internet Protocol (IP) addresses, and source and destination ports). J.A. 1796. The 5-tuple values, Sourcefire explains, are useful for detecting "intrusion event[s]" (potential security concerns generating a response by the system), such as multiple failed log-in

attempts to the network's server from an unknown IP address. J.A. 1471; *see also* J.A. 1793. Rule headers also include "rule actions," *e.g.*, "drop," "pass," and "alert," which is the action taken by the rules engine if it encounters packets that meet the criteria specified in the rule header. J.A. 1797. "Drop" actions block packets from continuing to their destinations, "pass" actions permit the packets to continue without interruption, and "alert" actions generate reports of "intrusion event[s]" while typically allowing packets to continue. J.A. 1793, 1797. Intrusion rules may also include a "rule options" part, containing "keywords" and their associated "arguments." J.A. 1794-95, 1801. Users may add arguments that, for example, apply the intrusion rule only to certain uniform resource identifiers (URIs). J.A. 1795.

After the Board instituted the requested inter partes review, Centripetal argued that Sourcefire was not qualifying prior art under 35 U.S.C. § 311(b) because it was not a "printed publication." J.A. 387-94. In particular, Centripetal contended that Sourcefire would not have been publicly accessible to interested persons of skill in the art because (1) the user manual is kept on a password-protected website and only available to Sourcefire purchasers, J.A. 387-89, and (2) the Sourcefire product was costly, with a purchase price of up to $25,000, J.A. 392-94.[1]

1. The priority date for the '722 patent is in April 2015, so that the "printed publication" language of 35 U.S.C. § 102(a)(2) applies in this matter. *See Board Decision*, 2020 WL 2549613, at *1 n.1. The parties accept that the standards governing that phrase are the same, at least for present purposes, as the standards governing the same phrase in 35 U.S.C. § 102(b) (2006), applicable in our *20-1635 Decision*.

As to what Sourcefire teaches, Centripetal disputed Cisco's contention that Sourcefire teaches the "network-threat indicators" recited in the claims. *See* J.A. 416-30. Specifically, Centripetal argued that rule headers do not identify *specific* threats coming from, *e.g.*, a certain IP address "associated with a network threat." J.A. 416-17, 424-26. Rather, Centripetal argued, the IP address in the Sourcefire rule header is merely a "source IP address" that permits packets associated with trusted networks to pass without inspection, J.A. 416-17, and Sourcefire's rule header functions only to "restrict packet inspection" and "reduce false positives" by identifying the packets that are safe and allowing them to pass, rather than identifying IP addresses associated with specific network threats, J.A. 416-17, 424-26. Further, Centripetal argued, the "rule options" function of Sourcefire does not teach identifying network-threat indicators, because keywords and their associated arguments identify suspicious *content* associated with data packets, rather than data packets with suspicious *identifiers*. J.A. 428-30.

Finally, Centripetal presented objective indicia of non-obviousness. J.A. 442-48. Specifically, Centripetal argued that the '722 patent "satisfied a long-felt need in the industry," which was "how to operationalize threat intelligence to proactively identify network threats." J.A. 443. It pointed to a paper entitled "Centripetal Networks Threat Intelligence Gateway: Designed to Enable Continuous Prevention Through Intelligence-led Enforcement" (the ESG paper), which praised Centripetal's products, including its Threat Intelligence Gateway (RuleGATE) for "converting indicators to rules

that drive actions," and thereby "deliver[ing] more than [was] possible with firewalls and IPS systems." J.A. 444-48 (citing J.A. 6688). Centripetal also presented a 2017 Gartner article that praised Centripetal as being "'unique in its ability to instantly detect and prevent malicious network connections based on millions of threat indicators at 10-gigabit speeds.'" J.A. 448 (quoting J.A. 6695).

C

In its final written decision, the Board held claims 1-7, 10-12, 14-21, 24, and 25 of the '722 patent to be unpatentable for obviousness in view of Sourcefire. *See Board Decision*, 2020 WL 2549613, at *23.[2] The Board concluded that Cisco had shown Sourcefire to be a printed publication at the relevant time. *See id.*, 2020 WL 2549613, at *5-8. The reasons are materially identical to those the Board relied on in the separate final written decisions we affirm in today's *20-1635 Decision*.

Next, the Board considered whether Sourcefire teaches the claim limitation requiring "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." *Board Decision*, 2020 WL 2549613, at *8-12. It found that Sourcefire teaches a "packet-filtering device" (the 3D Sensor with IPS), which receives "packet-filtering rules" (intrusion rules)

2. The Board ruled that Cisco did not show unpatentability as to claims 8, 9, 13, 22, and 23. *Board Decision*, 2020 WL 2549613, at *23. Cisco has not appealed that ruling.

that can specify "source and destination IP addresses," "source and destination ports," and "keywords and their parameters and arguments" to allow users to, *e.g.*, "restrict packet inspection to the packets originating from specific IP addresses." *Id.* at *9 (internal quotation marks omitted); *see also* J.A. 1794, 1798-99. Thus, the Board determined that Sourcefire teaches packet-filtering rules "'configured to cause the packet-filtering device to identify packets corresponding to,' for example, specific source IP addresses." *Board Decision*, 2020 WL 2549613, at *9.

The Board then rejected Centripetal's argument that Sourcefire does not teach the "network-threat indicators" recited in the claims. *Id.* It construed "network-threat indicator" to mean an "indicator that represents the identity of a resource associated with a network threat." *Id.* at *3-4, *9. Noting that Sourcefire teaches using intrusion rules to identify "exploits" and malicious activity by examining packets, *see* J.A. 1793-94, the Board found that a relevant artisan would have understood that intrusion rules could be written to identify specific network threats on the basis of the source IP address being a suspicious one. *Board Decision*, 2020 WL 2549613, at *9 (citing J.A. 980-81 ¶¶ 114-16). The Board "note[d] that the Specification of the '722 Patent itself identifies 'network addresses' associated with network threats as examples of 'network-threat indicators.'" *Id.* (citing '722 patent, col. 3, lines 23-24).

Finally, the Board considered Centripetal's objective indicia of non-obviousness and found that the evidence was not entitled to substantial weight. *Id.* at *17-19. The

Board found that Centripetal had presented no evidence to show that its RuleGATE product was coextensive with the '722 patent's claims. *Id.* at *18 (citing *Fox Factory, Inc. v. SRAM, LLC*, 944 F.3d 1366, 1373 (Fed. Cir. 2019)). It also found that Centripetal had not shown how the cited praise for its products related to the claim limitations, rejecting conclusory expert statements as unpersuasive. *Id.* at *18-19. For those reasons, the Board concluded that the objective-indicia evidence was not entitled to substantial weight. *Id.* at *20.

II

We review the Board's legal conclusions de novo and factual findings for substantial evidence. *Nobel Biocare Services AG v. Instradent USA, Inc.*, 903 F.3d 1365, 1374 (Fed. Cir. 2018). Whether a reference qualifies as a "printed publication" is a legal conclusion based on factual findings. *Jazz Pharms., Inc. v. Amneal Pharms., LLC*, 895 F.3d 1347, 1356 (Fed. Cir. 2018). "The underlying factual findings [in a printed-publication analysis] include whether a reference was publicly accessible." *Nobel*, 903 F.3d at 1375. Similarly, the ultimate determination of whether a claimed invention would have been obvious is a legal one reviewed de novo, but underlying factual determinations are reviewed for substantial-evidence support. *PersonalWeb Techs., LLC v. Apple, Inc.*, 917 F.3d 1376, 1381 (Fed. Cir. 2019).

Centripetal argues that the Board (1) erred in concluding that Sourcefire was a printed publication, *see* Centripetal Opening Br. 19-26; (2) misapplied the claim

construction it adopted for "network-threat indicator" in analyzing whether Sourcefire teaches this limitation, *id.* at 27-35; and (3) failed to give due weight to the objective indicia of non-obviousness, *id.* at 35-42. We reject these challenges to the Board's obviousness determination.

A

Centripetal first argues that Sourcefire was not a printed publication. Centripetal's arguments and the Board's analysis are materially the same as those in *20-1635 Decision*, where we upheld the Board's determination that Sourcefire was a printed publication. Centripetal has made no argument here that warrants separate discussion. We rely on our discussion in *20-1635 Decision* to affirm the Board's ruling as to Sourcefire's qualification as a printed publication here.[3]

B

Centripetal argues that the Board's finding that Sourcefire teaches filtering packets based on the "network-threat indicators" required by the claims was unsupported by substantial evidence. In advancing this argument, Centripetal essentially contends that Sourcefire does not teach using a source-identifier (like

3. In our *20-1635 Decision*, we affirmed the Board's determination that Sourcefire was publicly accessible, and therefore a printed publication, as of the March 2013 priority date of the patents at issue there. Here, the priority date is two years later. Centripetal has not denied that public accessibility before March 2013 entails public accessibility before April 2015.

an IP address) to identify threats, but only to "restrict inspection" of packets with benign IP addresses (*i.e.*, to generate "whitelists"). Centripetal Opening Br. 27.

The Board reasonably found otherwise. *Board Decision*, 2020 WL 2549613, at *9-10. Sourcefire teaches users how to write custom intrusion rules that "detect specific exploits" and "target traffic that may attempt to exploit known vulnerabilities," J.A. 1794, by using rule headers and keywords to filter packets based on 5-tuple values, which include source identifiers, *see* J.A. 1796-1801. Although Sourcefire expressly identifies creating whitelists as one potential intrusion rule, *see* J.A. 1798, the Board had a sufficient basis for finding that Sourcefire's teaching was not limited to use of the source identifier for that purpose. "Sourcefire indicates intrusion rules are used to identify 'exploits' from attackers such that 3D Sensors employing those rules examine packets for 'malicious activity.'" *Board Decision*, 2020 WL 2549613, at *9 (quoting J.A. 1066, 1793). Sourcefire teaches rules that "alert," "pass," or "drop." J.A. 1793; *see Board Decision*, 2020 WL 2549613, at *8-9 (citing J.A. 1793; agreeing with Cisco's description of Sourcefire as teaching, among other things, "passing or dropping," with Cisco citing J.A. 1794-801). And Cisco's expert explained that Sourcefire teaches the use of source IP addresses (among other information in the rule header) as a network-threat indicator for triggering of a rule to allow, drop, or alert. J.A. 980-81 ¶¶ 114-16, cited in *Board Decision*, 2020 WL 2549613, at *9.

Nor did the Board "raise, address, and decide unpatentability theories never presented by [Cisco]

and not supported by record evidence," as Centripetal contends. *In re Magnum Oil Tools Int'l Ltd.*, 829 F.3d 1364, 1381 (Fed. Cir. 2016). In its petition, Cisco argued that Sourcefire teaches using its system to write packet-filtering rules that "identify packets including data (*e.g.*, 5-tuple, application layer data) corresponding to characteristics associated with malicious activities," J.A. 213, and that those rules can be triggered by "source or destination IP addresses," causing the system to "allow, drop, [or] alert," J.A. 214. We see no significant disparity between Cisco's argument in its petition and the relevant part of the Board's rationale.

Accordingly, 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.

C

Finally, Centripetal argues that the Board failed to give due weight to evidence of a long-felt but unmet need for proactively identifying network threats, Centripetal Opening Br. 35-39, as well as industry praise for its product, *id.* at 40-42. We disagree.

"In order to accord substantial weight to secondary considerations in an obviousness analysis, 'the evidence of secondary considerations must have a "nexus" to the claims, *i.e.*, there must be "a legally and factually sufficient connection" between the evidence and the patented

invention.'" *Fox Factory*, 944 F.3d at 1373 (quoting *Henny Penny Corp. v. Frymaster LLC*, 938 F.3d 1324, 1332 (Fed. Cir. 2019) (citing *Demaco Corp. v. F. Von Langsdorff Licensing Ltd.*, 851 F.2d 1387, 1392 (Fed. Cir. 1988)). With respect to long-felt but unmet need, Centripetal focuses on the fact that the ESG paper discusses the need for "cyber threat intelligence" and systems that can use such intelligence on a large scale when detecting network threats. J.A. 6684. Centripetal contends that these issues are identified in the Background of the '722 patent, *see* '722 patent, col. 1, lines 24-33, and that the ESG paper is thus evidence that the '722 patent solved longstanding problems in cybersecurity. It also points to language in the ESG paper stating that Centripetal achieved "customized threat intelligence" on a large scale by "converting indicators to rules that drive actions across a risk spectrum." J.A. 6688.

The Board reasonably found the evidence not to establish a nexus between the claimed features in the challenged claims of the '722 patent and the ESG Paper's description of the benefits provided by the RuleGATE product. Here, Centripetal presented no non-conclusory evidence tying the statements in the ESG Paper about "driv[ing] actions across a risk spectrum" specifically to the limitations in the claims. *Board Decision*, 2020 WL 2549613, at *18.

Centripetal also did not supply the needed nexus for its cited industry praise. The Gartner article praises Centripetal's product as being "unique in its ability to instantly detect and prevent malicious network

connections based on millions of threat indicators in 10-gigabit speeds." J.A. 6695. Centripetal also identifies a designation by American Bankers as a "Top Ten FinTech Compan[y] to Watch" praising RuleGATE for its scale and for its ability to "compare[] incoming traffic against millions of rules and policies informed by analytics on known 'bad guys.'" J.A. 6732, 6745-47. Centripetal's expert added a sentence, following his description of those passages, stating that, "[a]s discussed directly above, the salutary benefits of Centripetal's [RuleGATE] product discussed in the ESG Paper and the [Gartner] article are made possible in large part by the '722 Patent's packet-filtering rules, which transform network-threat indicators into actionable rules." J.A. 6563 ¶ 123.

The Board reasonably found this evidence insufficient to establish the required nexus. The documents themselves do not meaningfully tie the benefits to the claim limitations. And the assertion by Centripetal's expert is an unelaborated conclusion, which the Board could and did reject as insufficient for that reason. *Board Decision*, 2020 WL 2549613, at *19.

III

We have considered the remainder of Centripetal's arguments and find them unpersuasive. For the foregoing reasons, the decision of the Patent Trial and Appeal Board is affirmed.

AFFIRMED

APPENDIX C — JUDGMENT OF THE UNITED STATES PATENT AND TRADEMARK OFFICE, PATENT TRIAL AND APPEAL BOARD, IPR2018-01436, DATED JANUARY 23, 2020

UNITED STATES PATENT
AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL
AND APPEAL BOARD

IPR2018-01436
Patent 9,124,552 B2

CISCO SYSTEMS, INC.,

Petitioner,

v.

CENTRIPETAL NETWORKS, INC.,

Patent Owner.

Before BRIAN J. McNAMARA, STACEY G. WHITE, and JOHN P. PINKERTON, *Administrative Patent Judges.*

PINKERTON, *Administrative Patent Judge.*

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
Denying Petitioner's Motion to Exclude
Denying Patent Owner's Motion to Exclude
35 U.S.C. § 318(a)

Appendix C

I. INTRODUCTION

Petitioner, Cisco Systems, Inc., filed a Petition for *inter partes* review of claims 1–21 of U.S. Patent No. 9,124,552 B2 (Ex. 1001, "the '552 patent"). Paper 1 ("Pet."). We instituted trial on claims 1–21 of the '552 patent on the asserted ground of unpatentability. (Paper 7, "Dec. on Inst."). After institution of trial, Patent Owner, Centripetal Networks, Inc., filed a Patent Owner Response (Paper 18, "PO Resp."), Petitioner filed a Reply (Paper 25, "Reply"), and Patent Owner filed a Sur-Reply (Paper 27, "Sur-Reply"). Patent Owner also filed Objections to Evidence in Petitioner's Reply. Paper 26.

Petitioner filed a Motion to Exclude Patent Owner's Evidence (Paper 29), to which Patent Owner filed an Opposition (Paper 33), and in support of which Petitioner filed a Reply (Paper 34). In addition, Patent Owner filed a Motion to Exclude (Paper 30), to which Petitioner filed an Opposition (Paper 31), and in support of which Patent Owner filed a Reply (Paper 35).

An oral hearing was held on December 2, 2019, and a transcript of the hearing is included in the record. Paper 39 ("Tr.").

We have authority under 35 U.S.C. § 6. This Final Written Decision is issued pursuant to 35 U.S.C. § 318(a). For the reasons discussed below, we determine that Petitioner has proven by a preponderance of the evidence that claims 1–21 of the '552 patent are unpatentable. *See* 35 U.S.C. § 316(e) ("In an inter partes review instituted under

this chapter, the petitioner shall have the burden of proving a proposition of unpatentability by a preponderance of the evidence.").

A. Related Matters

Patent Owner has asserted the '552 patent against Petitioner in *Centripetal Networks, Inc. v. Cisco Systems, Inc.,* No. 2:18-cv-00094-MSD-LRL (E.D. Va.). Pet. 2–3; Paper 4, 1.

B. The '552 Patent

The '552 patent, titled "Filtering Network Data Transfers," issued on September 1, 2015, from U.S. Application No. 13/795,822, filed on March 12, 2013. Ex. 1001, codes (21), (22).

The '552 patent generally discloses systems and methods for "filtering network data transfers." Ex. 1001, 1:47–48. In particular, the '552 patent is directed to filtering data packets transmitted between a secured network and an unsecured network and describes "[a] category of cyber attack known as exfiltrations (e.g., stealing sensitive data or credentials via the Internet)" [that] has proven to be especially difficult for conventional cyber defense systems to prevent." *Id.* at 1:15–16; 62–66.

Figure 1 of the '552 patent, which is reproduced below, illustrates exemplary network environment 100 in which the disclosure of the patent may be implemented. *Id.* at 3:12–14.

Appendix C

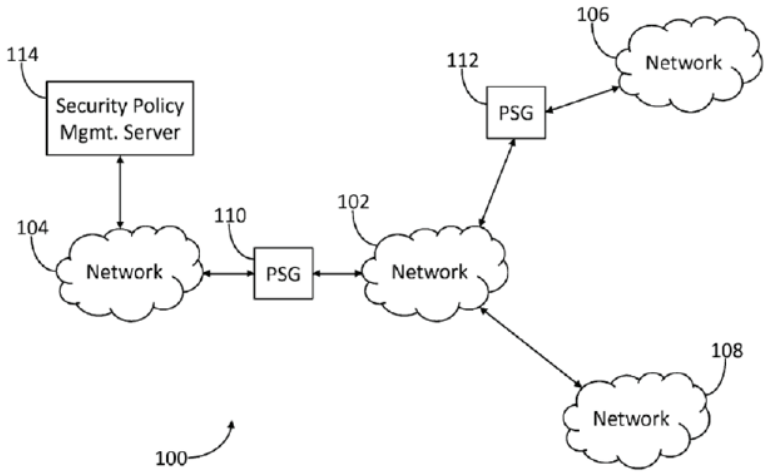


FIG. 1

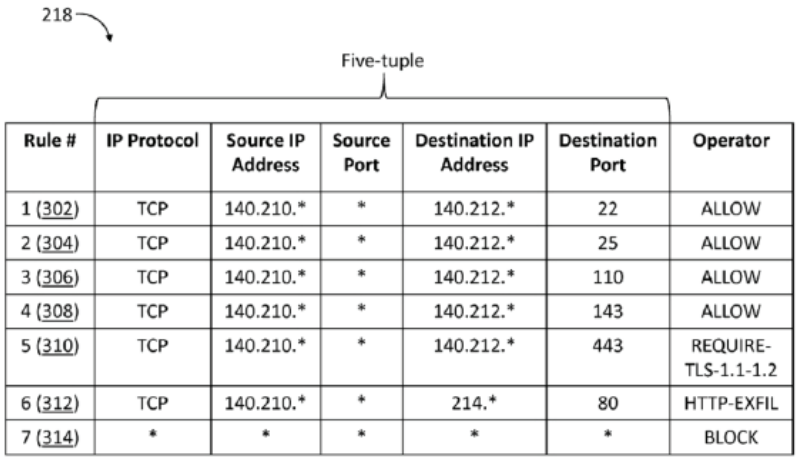
As shown in Figure 1, network environment 100 depicts four small clouds 102, 104, 106, and 108 representing networks, with cloud 102, representing the public Internet. Networks 104 and 106 are connected to network 102 through packet security gateway (PSG) 110 and 112, respectively, and network 108 is connected directly to network 102. *Id.* at 3:12–16, 63–64. The '552 patent explains that networks 104, 106, and 108 may be private networks such as Local Area Networks (LANs) and Wide-Area Networks (WANs) operated by various companies or organizations. *Id.* at 3:22–26. For example, networks 104 and 106 may be owned and operated by enterprise X and form part of a protected or secured network associated with security policy management server 114, which is shown in Figure 1 connected directly to network 104. *Id.* at 3:67–4:3. Network 108 may be owned and operated

by cyber criminal organization Z, which may attempt to steal sensitive data from enterprise X via network 102. *Id.* at 3:27–41. The '552 patent explains that to prevent exfiltrations from its networks 104 and 106, enterprise X may locate one or more Packet Security Gateways ("PSGs") at each boundary between networks 104 and 106 and network 102 (e.g., the Internet). For example, an attempt may be made to transfer data from network 104 or 106 to network 108 affiliated with organization Z. *Id.* at 4:3–14. Then, PSG 110 "may protect network 104 from one or more cyber attacks (e.g., exfiltrations) mediated by network 102 (e.g., the Internet)," and PSG 112 "may protect network 106 from one or more cyber attacks (e.g., exfiltrations) mediated by network 102." *Id.* at 4:14–19.

PSGs 110 and 112 may include one or more computing devices configured to: receive a dynamic security policy from security policy management server 114; receive packets associated with networks 104, 106, and 108; and, apply one or more rules or operators, including an identify (e.g., allow) or null (e.g., block) operator, specified by the security policy to the received packets. *Id.* at 3:42–46; 4:29–36.

Figure 3 of the '552 patent, which is reproduced below, illustrates an exemplary dynamic security policy including 7 rules. *Id.* at 5:28–30.

Appendix C



Rule #	IP Protocol	Source IP Address	Source Port	Destination IP Address	Destination Port	Operator
1 (302)	TCP	140.210.*	*	140.212.*	22	ALLOW
2 (304)	TCP	140.210.*	*	140.212.*	25	ALLOW
3 (306)	TCP	140.210.*	*	140.212.*	110	ALLOW
4 (308)	TCP	140.210.*	*	140.212.*	143	ALLOW
5 (310)	TCP	140.210.*	*	140.212.*	443	REQUIRE-TLS-1.1-1.2
6 (312)	TCP	140.210.*	*	214.*	80	HTTP-EXFIL
7 (314)	*	*	*	*	*	BLOCK

FIG. 3

Figure 3 is a table of 7 columns (with headings labeled Rule #, IP Protocol, Source IP Address, Source Port, Destination IP Address, Destination Port, and Operator) and 8 rows, with the top row containing the aforementioned headings and the other 6 rows listing rules 1–7, together with each rule's specified criteria and one or more operators under the appropriate headings. *Id.* at 5:28–42. Rule 5, for example, instructs the PSG that IP packets with one or more TCP packets, originating from a source IP address that begins with 140.210 (network 104), having any source port, destined for an IP address that begins with 140.212 (network 106), and destined for port 443 (e.g., associated with Hypertext Transfer Protocol Secure (HTTPS) protocol) should have a specified Transport Layer Security (TLS) protocol operator applied to them. *Id.* at 6:1–9. Thus, Rule 5 allows web browsers

attached to network 104 to conduct HTTPS sessions (e.g., secure web sessions) with any web servers attached to network 106, but requires the field value in the headers of application data contained in IP packets (TLS Record Protocol packet headers) to specify version 1.1 or 1.2 of the TLS protocol "because the popular TLS version 1.0 protocol has a known security vulnerability that attackers may exploit to decrypt HTTPS sessions." *Id.* at 6:37–47, 7:18–23, 7:55–60. The '552 patent explains that the application packets contained in the IP packets may be TLS Record Protocol packets in which the header fields may be unencrypted and "contain a value indicating the TLS version." *Id.* at 7:61–8:18.

The '552 patent describes what "may be viewed as" a two-stage filtering process performed at each PSG for packets exiting a trusted or secured network towards an external network to address exfiltrations. *Id.* at 8:19–31. In the first stage, "[a] determination may be made that a portion of the packets have packet header field values [e.g., the "5-tuple" of source/destination IP addresses, transport protocol, and source/destination ports] corresponding to a packet filtering rule." *Id.* at 1:49–51. In the second stage, "[a] further determination may be made that one or more of the portion of the packets have one or more application header field values corresponding to one or more application header field criteria specified by the operator." *Id.* at 1:54–58. "Conceptually, the first stage may determine if the network security policy allows any communications between the resources identified in the 5-tuple rule; if so, the second stage may determine if the policy allows the specific method or type of communication

(e.g., file read/write, encrypted communication, etc.) between the resources." *Id.* at 8:25–31.

For example, Figure 4, which is reproduced below, illustrates an exemplary method for protecting a secured network.

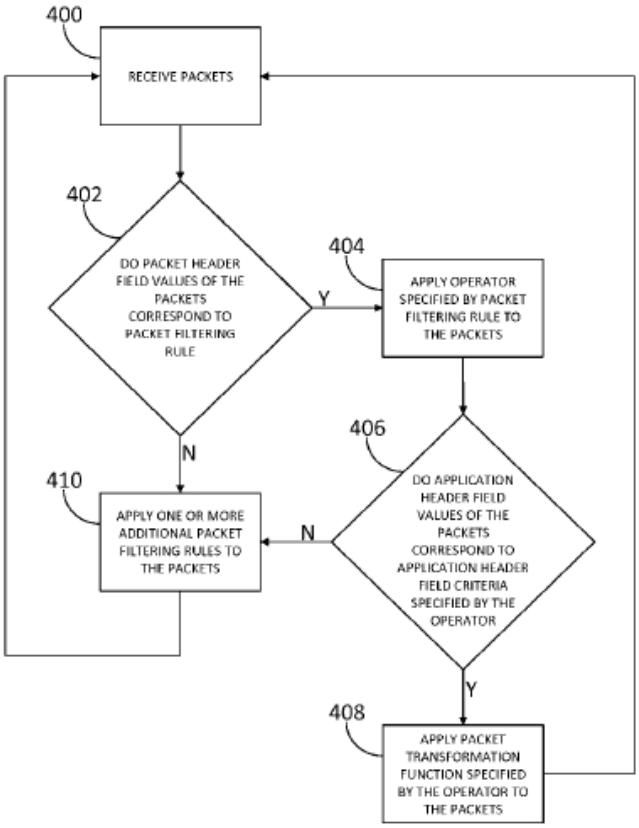


FIG. 4

Appendix C

Figure 4 is a flow diagram of an exemplary method of steps that may be performed at a PSG associated with a security policy management server. *Id.* at 8:56–60. Beginning at step 400, packets may be received from, for example, network 104 that are destined for network 106. *Id.* at 8:63–66. At step 402, a determination may be made as to whether a portion of the packets received from network 104 have packet header field values (e.g., one or more of one or more data section protocols, one or more source IP addresses, one or more source ports, one or more destination IP addresses, or one or more destination ports) corresponding to a packet filtering rule, such as rule 5. *Id.* at 9:2–8. "At step 404, responsive to determining that one or more of the portion of received packets have packet header field values corresponding to the packet filtering rule, an operator specified by the packet filtering rule may be applied to the portion of the received packets. For example, the REQUIRE TLS-1.1-1.2 operator specified by rule 5 [] may be applied to the portion of the received packets." *Id.* at 9:8–16.

Next, "[a]t step 406, a determination may be made as to whether one or more application header field values of one or more of the portion of the received packets correspond to one or more application header field criteria specified by the operator," such as "whether one or more of the portion of the received packets have application header field values corresponding to one or more application header field criteria of the REQUIRE TLS-1.1-1.2 operator specified by rule 5 [] (e.g., application header field values corresponding to TLS version 1.1 or 1.2)." *Id.* at 9:17–26.

"At step 408, responsive to determining that one or more of the portion of received packets have application header field values corresponding to one or more application header field criteria specified by the operator, a packet transformation function specified by the operator may be applied to the one or more of the portion of the received packets. For example, an ALLOW packet transformation function specified by the REQUIRE TLS-1.1-1.2 operator may be applied" to allow each of the one or more of the portion of the received packets to continue toward their respective destinations. *Id.* at 9:26–40. The method may then return to step 400 and await receipt of one or more additional packets. *Id.* at 9:40–43.

The '552 patent claims are directed to implementing the two-stage packet filtering process at the PSG. Independent claim 1 is directed to the method; independent claim 8 is a corresponding apparatus claim performing the claim 1 steps; and independent claim 15 is a corresponding claim for a computer-readable media having instructions to perform the claim 1 steps. *Id.* at 11:5–35; 12:54–13:15; 14:39–67.

C. Illustrative Claim

Among the challenged claims of the '552 patent, claims 1, 8, and 15 are independent. Claim 1, which is illustrative of the challenged claims, is reproduced below (with paragraph numbering added as in the Petition):

1. A method, comprising:

Appendix C

[i] at a computing device comprising at least one processor, a memory, and a communication interface:

[ii] receiving, via the communication interface, a plurality of hypertext transfer protocol secure (HTTPS) packets;

[iii] responsive to a determination by the at least one processor that at least a portion of the plurality of HTTPS packets have packet-header-field values corresponding to a packet filtering rule stored in the memory,

[iv] applying, by the at least one processor, an operator specified by the packet-filtering rule to the at least a portion of the plurality of HTTPS packets, wherein the operator specifies one or more application-header-field-value criteria identifying one or more transport layer security (TLS)-version values for which packets should be blocked from continuing toward their respective destinations; and

[v] responsive to a determination by the at least one processor that one or more packets, of the at least a portion of the plurality of HTTPS packets, have one or more application-header-field values corresponding to one or more TLS-version values of the one or more TLS-version values for which packets should be blocked from continuing toward their respective destinations,

> [vi] applying, by the at least one processor, at least one packet-transformation function specified by the operator to the one or more packets to block each packet of the one or more packets from continuing toward its respective destination.

Ex. 1001 at 11:5–35.

D. Evidence of Record

Petitioner relies upon the following reference:

Exhibit	Reference	Publication Date
Ex. 1004	User manual titled "Sourcefire 3D System User Guide" Version 4.10 ("Sourcefire")	April 2011

Petitioner also relies on the Declaration of Dr. Stuart Staniford (Ex. 1003). Patent Owner relies on the Declaration of Dr. Alessandro Orso (Ex. 2002).

E. Asserted Ground of Unpatentability

Petitioner challenges the patentability of claims 1–21 of the '552 patent based on the following ground under 35 U.S.C. § 103(a),[1] and we instituted trial based on this ground:

1. The Leahy-Smith America Invents Act ("AIA"), Pub. L. No. 112-29, 125 Stat. 284, 287–88 (2011), amended 35 U.S.C.

Appendix C

Claims Challenged	Basis	Reference
1–21	35 U.S.C. § 103(a)	Sourcefire in view of knowledge, skill, and creativity of a person of ordinary skill in the art ("POSA")

F. Person of Ordinary Skill in the Art

Petitioner asserts that a person of ordinary skill in the art at the time of the alleged invention of the '552 patent would have had a working knowledge of packet switched networking, firewalls, security policies, communication protocols and layers, and the use of customized rules to address cyber-attacks. Pet. 13 (citing Ex. 1003 ¶¶ 23, 60). Petitioner also asserts that a person of ordinary skill would have had a bachelor's degree in computer science, computer engineering, or an equivalent, and four years of industry experience, and that the lack of work experience can be remedied by additional education, and vice versa. *Id.* Patent Owner's declarant, Alessandro Orso, Ph.D., notes that the '552 patent claims a priority date of March 12, 2013, and opines that a person of ordinary skill in the art at the time of the invention of the '552 patent "would be someone with a bachelor's degree in computer science or related field, and either (1) two or more years of industry experience and/or (2) an advanced degree in

§ 103. Because the '552 patent was filed before the effective date of the relevant amendment, March 16, 2013, the pre-AIA version of § 103 applies.

computer science or a related field." Ex. 2002 ¶¶ 42–43. In the Institution Decision, we adopted Petitioner's proposed description of the level of ordinary skill in the art. Dec. on Inst. 16–17. We have reviewed the full record in this case and based on our analysis, for purposes of this Decision, adopt Petitioner's description of the person of ordinary skill.[2]

II. DISCUSSION

A. Claim Construction

1. Applicable Law

The Petition has been accorded a filing date of July 20, 2018. Paper 3. For petitions in an *inter partes* review accorded a filing date before November 13, 2018,[3] we interpret claim terms in an unexpired patent according to their broadest reasonable construction in light of the

2. Although Dr. Orso's description of a person of ordinary skill is slightly different than Petitioner's, we note that our decision would be unchanged if we were to apply Dr. Orso's proposal instead.

3. Although the claim construction standard applied in an *inter partes* review was recently changed to the federal court claim construction standard used in a civil action under 35 U.S.C. § 282(b), that change does not apply to this proceeding because the Petition was filed before November 13, 2018, the effective filing date of the change. See *Changes to the Claim Construction Standard for Interpreting Claims in Trial Proceedings Before the Patent Trial and Appeal Board,* 83 Fed. Reg. 51340 (Oct. 11, 2018) (to be codified at 37 C.F.R. § 42).

specification of the patent in which they appear. *See* 37 C.F.R. § 42.100(b); *Cuozzo Speed Techs. LLC v. Lee*, 136 S. Ct. 2131, 2144–46 (2016). "In claim construction, [our reviewing] court gives primacy to the language of the claims, followed by the specification. Additionally, the prosecution history, while not literally within the patent document, serves as intrinsic evidence for purposes of claim construction." *Tempo Lighting, Inc. v. Tivoli, LLC*, 742 F.3d 973, 977 (Fed. Cir. 2014). Otherwise, under the broadest reasonable construction standard, claim terms are presumed to have their ordinary and customary meaning, as would be understood by one of ordinary skill in the art in the context of the entire patent disclosure. *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007).

Only those terms in controversy need to be construed, and then only to the extent necessary to resolve the controversy. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (citing *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

2. Analysis

Patent Owner asserts that we should find the challenged claims patentable because Petitioner failed to meet its burden to construe the claims, including the term "operator," pursuant to 37 C.F.R § 42.104(b)(3). PO Resp. 18; *see also* Sur-Reply 7. Patent Owner also asserts that we should find the challenged claims patentable because Petitioner's expert, Stuart Staniford, Ph.D., "who

purported to opine on the patentability of the challenged claims, evinced little or no understanding of the role of claim construction in determining the validity of a patent claim." PO Resp. 19 (citing Ex. 2001 at 8:16–9:7). Petitioner further asserts that, at the very least, "we should give no weight to Dr. Staniford's opinions on this basis. *Id.* We are not persuaded by either of these arguments because, among other reasons, they are conclusory and unsupported.

In regard to claim construction, Patent Owner seeks construction of the terms "operator" (*id.* at 19–21) and "HTTPS packet" (*id.* at 21–23). We consider each term below.

a. "operator"

Patent Owner contends that, in the context of the challenged claims, "operator" is "a function specified by a packet filtering rule that specifies (1) one or more application-header-field-value criteria and (2) a packet transformation function to apply to the packet for each of the one or more application-header-field-value criteria." *Id.* at 19 (citing Ex. 2002 ¶ 64; *see also* '552 patent, claims 1, 8, 15). Patent Owner also asserts that the term "operator" is used in the '552 patent, in some circumstances, to refer simply to "a packet transformation function without also specifying application-header-field-value criteria."[4] *Id.*

4. Patent Owner states that to distinguish between the two types of operators, Patent Owner will refer to "operators that do not specify application-header-field-value criteria . . . along with their particular functionality specified (*e.g.,* as a 'null operator' or an 'identity operator')." PO Resp. 21.

at 20 (citing Ex. 2002 ¶ 66; Ex. 1001, 2:7–16; Ex. 2001, 25:16–27:7). Patent Owner argues that both usages of the term "operator" are explained in the following portion of the Specification:

> Such packet filters may implement at least two operators: an **identity operator**, which may allow the packet to continue towards its destination, and a **null operator** which may prevent, or block, the packet from continuing towards its destination. In some embodiments, the network packet filter may implement one or more **additional operators** having the capability to determine if a packet contains an application-level header that specifies a particular method associated with a data transfer protocol; and, if so, whether to apply an identity operator or null operator to the packet.

Id. (quoting Ex. 1001, 2:7–16 (emphasis added by Patent Owner)).

Petitioner agrees that the two constructions asserted by Patent Owner "are the plain and ordinary meanings of the term operator as used in the specification." Reply 7. Petitioner also argues that because "Sourcefire discloses [an] operator under any reasonable interpretation . . . no construction of the term operator is necessary." *Id.*

As reflected in the above discussion of the parties' contentions, the parties agree that the term "operator" is described in the Specification of the '552 patent to

have two meanings: (1) a packet transformation function, without specifying application-header-field-value criteria; and, (2) a function specified by a packet-filtering rule that specifies one or more application-header-field criteria and a packet transformation to apply to the packet for each of the application-header-field criteria. Patent Owner argues, and we agree, that as used in the claims of the '552 patent, the term "operator" has the latter meaning, which Patent Owner and the Specification refer to as the "additional operator." PO Resp. 21. In that regard, claim 1 recites, in limitation [iv], "applying . . . an *operator* specified by the packet-filtering rule to the at least a portion of the plurality of HTTPS packets, wherein the *operator specifies one or more application-header-field-value criteria* identifying one or more transport layer security (TLS)-version values *for which packets should be blocked*" and, in limitation [vi], "applying . . . at least one *packet-transformation function specified by the operator . . . to block* each packet."[5] Ex. 1001, 11:15–21; 11:31–34. As discussed in the Institution Decision, the '552 patent discloses that allowing or blocking transmission of a packet is a "packet transformation function." *See* Dec. on Inst. 29–30 (citing Ex. 1001, 7:17–23, 8:14–17, 9:26–37). Thus, considering the express terms of each of the independent claims, they recite the "additional operator" described in the Specification, although in a different format than in Patent Owner's proposed construction of the term "operator." Accordingly, the term "operator" as used in the claims is the additional operator described in

5. Independent claims 8 and 15 recite commensurate limitations. *See* Ex. 1001, 12:64–13:2, 13:12–14 (claim 8); 14:48–54, 14:64–66 (claim 15).

the Specification that specifies one or more application-header-field-value criteria and a packet transformation function.

b. "HTTPS packet"

Patent Owner contends that "HTTPS packet" means "an IP packet in an HTTPS session." PO Resp. 21, 23. Patent Owner argues that the Specification of the '552 patent discloses the relationship between the terms HTTPS, HTTP, TLS protocol, IP packets, and TLS Record Protocol Packets:

> HTTPS may be used to encrypt HTTP sessions. HTTPS is not a protocol per se, but rather the result of layering the HTTP protocol on top of the TLS protocol. For an HTTPS session composed of IP packets, the application packets contained in the IP packets may be TLS Record Protocol packets. The header fields of TLS Record Protocol packets may not be encrypted. One of the header fields may contain a value indicating the TLS version.

Id. (quoting Ex. 1001, 7:53–60). According to Patent Owner, "in other words, the term HTTPS refers to a communications session 'composed of IP packets' in which the HTTP protocol is layered 'on top of the TLS protocol.'" *Id.* at 22 (citing Ex. 2002 ¶ 69). Patent Owner also argues that "[a]n HTTPS packet is an IP packet in such a session, while the term 'TLS Record Protocol packet' refers to an 'application packet contained in the IP packet.'" *Id.*

Patent Owner further argues that this understanding of the term HTTPS packets is confirmed because the claims recite "a determination . . . that at least a portion of the plurality of HTTPS packets have packet-header-field values," which would not be present "if HTTPS packets referred to application-layer messages rather than IP packets." *Id.* Moreover, Patent Owner argues that because claim 1 recites that the HTTPS packets are received "via the communication interface," a person of ordinary skill would understand that "only L2 (link layer) or L3 (network layer, or IP) packets could be received at the communications interface of a computing device." *Id.* at 23 (citing Ex. 2002 ¶ 72).

As Petitioner notes, the term "HTTPS packet" is not used in the Specification of the '552 patent, but is only included in the claims. Reply 7. Although Patent Owner argues that Petitioner does not rebut Patent Owner's argument concerning the meaning of "HTTPS packet" (Sur-Reply 7–8), we do not agree. Petitioner quotes essentially the same portion of the Specification of the '552 patent as quoted by Patent Owner:

> HTTPS is not a protocol per se, but rather the result of layering the HTTP protocol on top of the TLS protocol. For an HTTPS session composed of IP packets, the application packets contained in the IP packets may be TLS Record Protocol packets. The header fields of TLS Record Protocol packets may not be encrypted. One of the header fields may contain a value indicating the TLS version.

Reply 8 (quoting Ex. 1001, 7:54–60). Petitioner, however, relying on this and other portions of the Specification, as well as the deposition testimony of Dr. Orso (Ex. 1041), sets forth a different interpretation of the term "HTTPS packet" than Patent Owner.

First, Petitioner argues, and we agree, that a person of ordinary skill ("POSA") "understood that by layering the HTTP protocol on top of the TLS protocol creates what the specification refers to as an 'application packet', which a POSAunderstood is a Layer 7 packet." Reply 8 (citing Ex. 1001, 2:21–25, 6:1–6, 6:48–52, 7:17–19, 7:55–58, 8:10–12; Ex. 1041, 128:6–128:23, 138:23–139:1, 143:4–17). Second, Petitioner argues, and we agree, "[t]he specification also refers to a 'TCP packet', which a POSA understood to be a Layer 4 packet, and an 'IP packet', which a POSA understood to be a Layer 3 packet." *Id.* (citing Ex. 1001, 5:42–43, 5:49–50, 5:56–57, 5:62–63, 6:1–2, 6:48–49, 8:19–25; Ex. 1041, 132:14–133:4). Third, Petitioner argues, and we agree, "a POSA understood that, for transmission over the Internet, the application packet would be contained in a TCP packet which is contained in an IP packet." *Id.* (citing Ex. 1001, 2:21–22, 7:17–19, 7:41–42, 7:55–57, 8:9–11, 8:49–50; Ex. 1041, 133:5–17, 154:20–157:18). Thus, we agree with Petitioner that the term "HTTPS packet" should not be construed as "an IP packet in an HTTPS session," as Patent Owner proposes, because, as Petitioner argues, "the application packet (HTTPS packet) exists separate from an IP packet, and to the extent it is transmitted through the Internet, the application packet is contained in a TCP packet contained in an IP packet." *Id.* at 9.

B. Asserted Obviousness of Claims 1–21 Over Sourcefire in View of the Knowledge of a POSA

Petitioner contends that claims 1–21 of the '552 patent are unpatentable as being obvious over Sourcefire in view of the knowledge of a POSA. Pet. 23, 32–69. Relying on the testimony of Dr. Staniford, Petitioner contends that Sourcefire in view of the knowledge of a POSA teaches or suggests all of the limitations of the challenged claims and that a POSA would have been motivated to apply the teachings of Sourcefire to achieve certain of the claimed features. *Id.*; Ex. 1003 ¶¶ 99–222. Patent Owner, relying on the testimony of Dr. Orso, disputes Petitioner's contentions. PO Resp. 27–69.

Petitioner also contends that Sourcefire qualifies as a prior art printed publication under 35 U.S.C. § 102(b). Pet. 23 (citing Ex. 1005). Patent Owner contends that Petitioner has failed to establish that Sourcefire was "publically accessible" so that it qualifies as a printed publication. PO Resp. 3–8. Because the only reference cited explicitly in Petitioner's challenge to the claims is Sourcefire, the threshold issue before us is whether Petitioner has shown that Sourcefire is prior art to the '552 patent. Thus, before we consider the underlying merits of Petitioner's challenge, we first address whether Petitioner has established by a preponderance of the evidence that Sourcefire qualifies as a printed publication.

Appendix C

1. Sourcefire as a Printed Publication

a. Applicable Law[6]

Our governing statutes provide "[a] petitioner in an *inter partes* review may request to cancel as unpatentable 1 or more claims of a patent only on a ground that could be raised under section 102 or 103 and only on the basis of prior art consisting of patents or printed publications." 35 U.S.C. § 311(b). Although Patent Owner challenges whether Sourcefire is a printed publication, the burden of persuasion remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015) (*citing Tech. Licensing Corp. v. Videotek, Inc.*, 545 F.3d 1316, 1326–27 (Fed. Cir. 2008)) (discussing the burden of proof in an *inter partes* review). Petitioner must demonstrate by a preponderance of the evidence that the challenged claims are unpatentable—including showing that the references relied upon are patents or printed publications. *See* 35 U.S.C. §§ 311(b); *Nobel Biocare Servs. AG v. Instradent USA, Inc.*, 903 F.3d 1365, 1375 (Fed. Cir. 2018), *as amended* (Sept. 20, 2018).

---

6. *See also Hulu, LLC v. Sound View Innovations, LLC*, 2019 WL7000067 *3–4 (PTAB Dec. 20, 2019), in which the PTAB's Precedential Opinion Panel ("POP") summarized the principles of law regarding whether a reference qualifies as a "printed publication" under 35 U.S.C. § 102 in connection with a request for rehearing of the Board's decision denying institution of an *inter partes* review. Our statement of the applicable law is consistent with POP's summary in *Hulu*.

Appendix C

The determination of whether a reference qualifies as a "printed publication" is a legal conclusion based on underlying factual findings. *Nobel*, 903 F.3d at 1375 (citing *Jazz Pharm., Inc. v. Amneal Pharm., LLC*, 895 F.3d 1347, 1356 (Fed. Cir. 2018)). The underlying factual findings include whether the reference was publicly accessible. *Id.* (citing *In re NTP, Inc.*, 654 F.3d 1279, 1296 (Fed. Cir. 2011)).

The determination of whether a document is a "printed publication" under 35 U.S.C. § 102 "involves a case-by-case inquiry into the facts and circumstances surrounding the reference's disclosure to members of the public." *Medtronic, Inc. v. Barry*, 891 F.3d 1368, 1380 (Fed. Cir. 2018) (citing *In re Klopfenstein*, 380 F.3d 1345, 1350 (Fed. Cir. 2004)). In certain situations, particularly for manuscripts or dissertations stored in libraries, courts may inquire whether a reference was sufficiently indexed, catalogued, and shelved. *See, e.g.*, *In re Hall*, 781 F.2d 897, 898–99 (Fed. Cir. 1986); *In re Lister*, 583 F.3d 1307, 1315 (Fed. Cir. 2009) (manuscript became publicly accessible once it was placed in a searchable database). In other situations, such as for information displayed at meetings and trade shows, courts have explained that indexing is not required if it was sufficiently disseminated. *See Medtronic*, 891 F.3d at 1381 (citing *Suffolk Techs., LLC v. AOL Inc.*, 752 F.3d 1358, 1365 (Fed. Cir. 2014)). The Federal Circuit has summarized that "[w]hile cataloging and indexing have played a significant role in our cases involving library references, we have explained that neither cataloging nor indexing is a necessary condition for a reference to be publicly accessible." *Lister*, 583 F.3d at 1312 (citing *Klopfenstein*, 380 F.3d at 1348).

"Because there are many ways in which a reference may be disseminated to the interested public, 'public accessibility' has been called the touchstone in determining whether a reference constitutes a 'printed publication' bar under 35 U.S.C. § 102(b)." *Blue Calypso, LLC v. Groupon, Inc.*, 815 F.3d 1331, 1348 (Fed. Cir. 2016) (quoting *In re Hall*, 781 F.2d at 898–99). "A given reference is 'publicly accessible' upon a satisfactory showing that such document has been disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art exercising reasonable diligence, can locate it." *SRI Int'l, Inc. v. Internet Sec. Sys., Inc.*, 511 F.3d 1186, 1194 (Fed. Cir. 2008) (quoting *Bruckelmyer v. Ground Heaters, Inc.*, 445 F.3d 1374, 1378 (Fed. Cir. 2006)).

What constitutes a "printed publication" must also be determined in light of the technology employed. *Samsung Elecs. Co. v. Infobridge Pte. Ltd.*, 929 F.3d 1363, 1369 (Fed. Cir. 2019) (citing *Wyer*, 655 F.2d at 226). Public accessibility requires more than technical accessibility. *Id.* (citing *Acceleration Bay, LLC v. Activision Blizzard Inc.*, 908 F.3d 765, 773 (Fed. Cir. 2018)). "[A] work is not publicly accessible if the only people who know how to find it are the ones who created it." *Id.* at 1372. On the other hand, "a petitioner need not establish that specific persons actually accessed or received a work to show that the work was publicly accessible." *Id.* at 1374. "In fact, a limited distribution can make a work publicly accessible under certain circumstances." *Id.* (quoting *GoPro, Inc. v. Contour IP Holding LLC*, 908 F.3d 690, 694 (Fed. Cir. 2018)).

b. Analysis

Petitioner contends that Sourcefire was publicly accessible at least as early as April 2011, and qualifies as prior art under § 102(b), because (1) a copy was enclosed on documentation disks (CD-ROM/DVD) included with each Sourcefire 3D System product sold by Sourcefire, Inc., and (2) it was available "for download by persons who had received a login and password from Sourcefire, Inc. to its support website." Pet. 23; *see also* Reply 3–7. Petitioner supports these contentions with the declaration testimony of John Leone, the former Technical Writer (from September 2002 to February 2005) and Documentation Manager and Director of Technical Publications and Certifications (from February 2005 to August 2013) at Sourcefire, Inc. *See* Ex. 1005[7] ¶¶ 1–2.

Mr. Leone testified that the Sourcefire reference (i.e., version 4.10 of the Sourcefire 3D System User Guide) was released "on or around April 2011." *See id*. ¶¶ 14–17. He

7. Patent Owner asserts, in a footnote, that considering the Leone Declaration would be "improper" under 37 C.F.R. § 42.6(a)(3). PO Resp. 5, n.1. Although we agree that citing an exhibit in its entirety typically is inadequate to comply with our Rules, here the Leone Declaration is brief, and we find that a reasonable party would be able to sufficiently discern the testimony that supports the statements in the Petition. Further, we determine that the Petition did not improperly incorporate arguments from the Leone Declaration. The Petition sets forth the relevant factual assertions (i.e., distribution of Sourcefire with each product sold and website availability), and Mr. Leone's testimony provides underlying facts directly supporting those assertions. *See* Pet. 23; Ex. 1005 ¶¶ 14–19. Although the brevity of the Petition's explanation of these facts may bear on its persuasive weight, it does not warrant exclusion.

further testified that, on or about April 2011, the Sourcefire reference was "enclosed . . . on documentation disks (CD-ROM or DVD) included with each Sourcefire 3D System appliance subsequently sold," and that "approximately 586 customers purchased the Sourcefire 3D System from April 2011 through March 2013 and had access to" the Sourcefire reference. *Id.* ¶¶ 18–19. In addition, Mr. Leone testified that, on or about April 2011, the Sourcefire reference would have been posted "to [Sourcefire, Inc.'s] customer-facing support website." *Id.* ¶ 18.

Patent Owner argues that, "[e]ven if these two allegations [in the Petition] are accepted as true, this would not be enough for the Board to find that Sourcefire was 'publically accessible.'" PO Resp. 3–4 (citing *Acceleration Bay, LLC v. Activision Blizzard, Inc.*, 908 F.3d 765, 772 (Fed. Cir. 2018)). According to Patent Owner, Petitioner "effectively concedes that Sourcefire was not widely disseminated in a manner that would have enabled a POSA exercising only reasonable diligence to locate it" because "access to Sourcefire was limited by login and password" (*id.* at 4, 6–7) and "the CD-ROM version of Sourcefire was distributed only to a small subsection of the public—i.e., only the 'approximately 586 customers [that] purchased the Sourcefire 3D System' (*id.* at 5)." Patent Owner also argues that "tellingly absent from Petitioner's argument is any allegation of *why* or *how* a POSA would have or could have found Sourcefire through mere reasonable diligence." *Id.* at 6. Patent Owner further argues that Petitioner does not explain how many documentation disks were provided with the product and whether the disks were indexed in any meaningful way. *Id.* at 7. Moreover, Patent Owner argues "there is no evidence that Sourcefire was or would have been made available to non-customers

upon request" and "[t]he high cost of the corresponding Sourcefire products weighs heavily against finding that the manual was publically accessible." Sur-Reply 4 (citing Exs. 1042, 1043 (trade magazines listing price of certain Sourcefire products).

Even if we were to agree with Patent Owner that Petitioner has not proven that Sourcefire was "publicly accessible" via the Sourcefire website, we nevertheless determine that Petitioner has proven by a preponderance of the evidence that Sourcefire was "publicly accessible" through distribution on CD-ROM disks with public sales of the corresponding Sourcefire products for several reasons. First, Patent Owner does not dispute Petitioner's evidence that the Sourcefire 3D System was publicly sold, or that a copy of the Sourcefire reference was included on a CD-ROM disc with every Sourcefire 3D System product sold in the relevant timeframe. The evidence discussed above that the Sourcefire 3D System was sold to at least 586 customers over two years (Ex. 1005 ¶¶ 18–19) does not support a finding that sales of the relevant Sourcefire products were restricted or limited to only certain customers, or that the cost of acquiring a Sourcefire 3D System product was prohibitively high. Nor is there any evidence of confidentiality obligations on customers who received the Sourcefire reference with their Sourcefire products. To the contrary, Sourcefire specifically states (in the section titled "Terms of Use and Copyright and Trademark Notices") that "you may use, print out, save on a retrieval system, and otherwise copy and distribute the Documentation solely for non-commercial use." Ex. 1004, 2. Thus, the uncontested facts and circumstances here reflect that Sourcefire was regularly distributed to

each customer purchasing a Sourcefire 3D system product with no obligations of confidentiality.

Second, Petitioner argues, and we agree, that Petitioner's evidence showing 586 sales of the Sourcefire 3D system, each including a copy of Sourcefire, "far exceeds the number of disclosures recognized under the relevant dissemination law for printed publications." Reply 3–4 (citing *Mass. Inst. of Tech. v. AB Fortia*, 774 F.2d 1104, 1109 (Fed. Cir. 1985) (dissemination of a conference paper to six persons rendered it a printed publication); *In re Klopfenstein*, 380 F.3d 1345, 1349 (Fed. Cir. 2004) ("[t]he key to the [*MIT*] court's finding was that actual copies of the [reference] *were distributed*."). Patent Owner argues that these cases should be distinguished because "they involved the free distribution of academic documents to conference and meeting attendees." Sur-Reply 5. We do not agree because, as Petitioner argues, the principle of establishing public accessibility by actual distribution of a reference "is not limited to free-of-charge references; rather, it includes commercial distribution." Reply 4 (citing *Garrett Corp. v. U.S.*, 422 F.2d 874, 878 (U.S. Ct. Cl. 1970)). In *Garrett*, the court held that a government report was a "printed publication" under § 102(b) because approximately 80 copies were disseminated, including to six commercial companies. 422 F.2d at 878. The court held that "distribution to commercial companies without restriction on use clearly" establishes that the report is a printed publication. *Id.*

Third, Patent Owner's argument that Petitioner "does not even attempt to explain why a POSA would have purchased the Sourcefire 3D System and therefore discovered the corresponding user manual included

in accompanying CD-ROM documentation disks" (PO Resp. 7) is not persuasive because, as Petitioner argues, Patent Owner "ignores that POSAs *actually purchased* Sourcefire" and ignores a Sourcefire press release (Ex. 1034) that advertises the capabilities and announces the release of Sourcefire v4.10 software and related products. Reply 4. In addition, as Petitioner argues, Patent Owner's evidence also establishes that (1) Sourcefire regularly advertised its products for sale and (2) those products were accompanied by manuals. *Id.* 4–5 (citing Ex. 1043, 2) ("The appliance comes with a CD that contains documentation .... [There] is an administrator manual. But the documentation is very long, more than 900 pages, and is geared to operating the suite as a whole."). Although Patent Owner criticizes this exhibit for various reasons (*see* Sur-Reply 6–7), we determine the evidence establishes that Sourcefire was actively advertised and promoted as being included with the Sourcefire 3D system. Furthermore, it is undisputed that the customers who received Sourcefire included entities interested in network security products, including persons of ordinary skill in the art. *See* Tr. 54:5–17.

Fourth, as Petitioner argues, and we agree, Patent Owner's arguments that limit printed publications to indexed references available without any significant effort or cost misstate the law. Reply 6. For example, as discussed *supra*, for information displayed at meetings and trade shows, courts have explained that indexing is not required if it was sufficiently disseminated. *SeeMedtronic,* 891 F.3d at 1381 ("a printed publication 'need not be easily searchable after publication if it was sufficiently disseminated at the time of its publication"). As also discussed *supra*, the Federal Circuit has summarized that "[w]hile cataloging

and indexing have played a significant role in our cases involving library references, we have explained that neither cataloging nor indexing is a necessary condition for a reference to be publicly accessible." *Lister*, 583 F.3d at 1312 (citing *Klopfenstein*, 380 F.3d at 1348).

Fifth, we do not agree with Patent Owner's argument that limited distribution of the Sourcefire manual to customers of the Sourcefire product is insufficient to demonstrate "public accessibility." Sur-Reply 2–5. Patent Owner argues that courts "have held that actual dissemination is insufficient on its own to demonstrate that a document is a printed publication." *Id.* at 3 (citing *Medtronic,* 891 F.3d at 1382 ("[d]istributing materials to a group of experts, does not, without further basis, render those materials publicly accessible or inaccessible"); *In re Bayer*, 568 F.2d 1357 (C.C.P.A. 1978) (actual dissemination of a thesis to members of a graduate committee does not raise a presumption that the public concerned with the art would know about the thesis). However, the Federal Circuit has held that "a limited distribution can make a work publicly accessible under certain circumstances." *Samsung,* 929 F.3d at 1369. And, for the reasons discussed *supra*, the circumstances here reflect that Sourcefire was "publicly accessible" because it was distributed to all purchasers of the Sourcefire 3D system, with no obligations of confidentiality and with the expectation that the Sourcefire manual could be shared, *i.e.,* copied and distributed solely for non-commercial use.[8]

8. The two decisions by Board panels cited by Patent Owner (Sur-Reply 3–4) in support of its argument that "distribution of a product manual along with a product does not make the *manual* publically accessible" are not persuasive, and are factually

Moreover, *Medtronic* and *Bayer*, which are relied on by Patent Owner, are distinguishable. In *Medtronic*, the video and slides at issue were disseminated to attendees of three separate programs or meetings. 891 F.3d at 1379. The Federal Circuit distinguished *Medtronic* from past cases involving references stored in repositories, such as libraries; the court found that rather than considerations like indexing and cataloguing, the relevant inquiry was whether the *distribution* of the materials to certain groups of people was sufficient for public accessibility. *Id.* at 1379–80. Issues underlying that inquiry include, for example, "whether there is an expectation of confidentiality between the distributor and the recipients of the materials," as well as "[t]he expertise of the target audience." *Id.* at 1382. Although agreeing with the Board that "[d]istributing materials to a group of experts" is not enough for public accessibility "simply by virtue of the relative expertise of the recipients," the Federal Circuit held that the Board in that case had not considered sufficiently all of the recipients of the distributed materials, or whether the recipients were expected to hold the distributed materials in confidence. *Id.* at 1382–83. Here, as discussed, Petitioner has presented uncontested evidence that Sourcefire was distributed with no obligations of confidentiality and with

---

distinguishable, because they both involved references that were subject to restrictions prohibiting their reproduction or further dissemination. *See ASM IP Holding B.V., v. Kokusai Elec. Corp.*, IPR2019-00369, Paper 8, at 18 (PTAB June 27, 2019); *VMAC Global Techs. Inc. v. Vanair Mfg, Inc.*, IPR2018-00670, Paper 9, at 13–14 (PTAB Aug. 10, 2018). In *ASM*, the panel further noted that there was no evidence of actual dissemination to interested artisans. *See ASM*, Paper 8, at 17.

expectations that the information could be shared.

In *Bayer*, a student's thesis, was accessible to three members of a faculty review committee. *See Bayer*, 568 F.2d at 1361. Although the distribution of a reference to three people can mitigate against a finding of public accessibility, here Petitioner has shown distribution to a substantially larger group, i.e., 586 purchasers of the Sourcefire 3D system received a copy of Sourcefire. In discussing *Bayer*, and *SRI Int'l, Inc. v. Internet Sec. Sys., Inc.*, 511 F.3d 1186, 1196 (Fed. Cir. 2008), in which "only one non-SRI person" had access to a reference found not be publicly accessible, the Federal Circuit stated that "[t]aken together, these cases suggest that a work is not publicly accessible if the only people who know how to find it are the ones who created it . . . . To hold otherwise would disincentivize collaboration and depart from what it means to publish something." *Samsung*, 929 F.3d at 1372. Here, as discussed *supra*, the facts show that Sourcefire, Inc. is not the only company or person who knew how to find Sourcefire because the evidence shows that Sourcefire was advertised and promoted as being included with any purchase of the Sourcefire 3D system. *See, e.g.* Ex. 1043.

Sixth, we are not persuaded by Patent Owner's contention that "the high cost of the corresponding Sourcefire products weighs heavily against finding that the manual was publically accessible." *See* Sur-Reply 4. The cost did not prevent 586 customers from actually obtaining Sourcefire by purchasing Sourcefire 3D system products. Moreover, Patent Owner did not present any evidence as to whether an interested artisan would,

or would not, have found the cost[9] too high to acquire Sourcefire by purchasing a Sourcefire 3D system product.

Thus, we find Petitioner has proven by a preponderance of the evidence that Sourcefire was distributed commercially through sales of the Sourcefire 3D system to 586 customers with no obligations of confidentiality and with expectations that the information could be shared for non-commercial use. Therefore, we conclude that Sourcefire qualifies as a prior art printed publication under § 102(b).

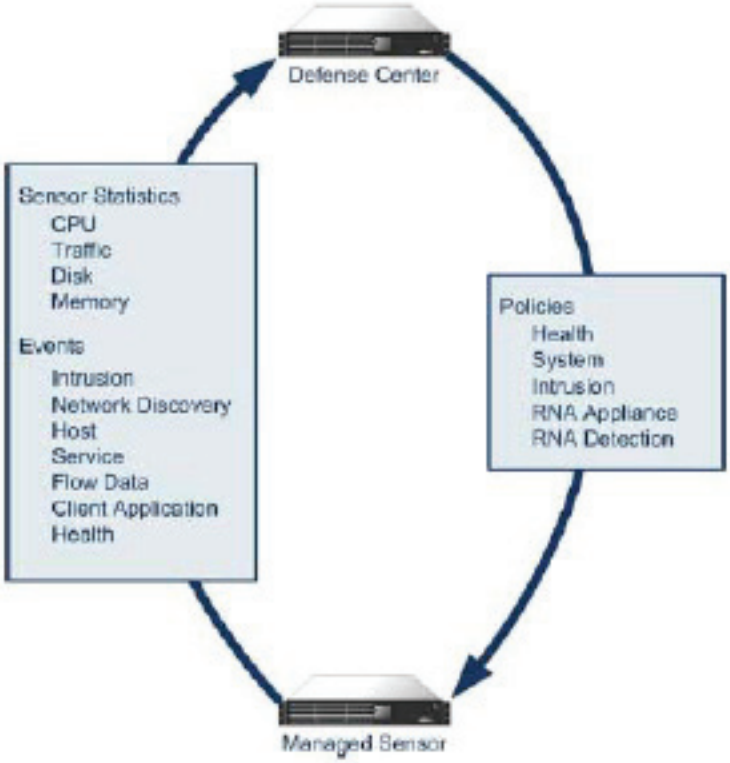
2. Overview of Sourcefire

Sourcefire is a user manual for the Sourcefire 3D System. Pet. 23; Ex. 1004. Sourcefire describes that the 3D System could identify changing assets and vulnerabilities on the network, determine the types of attacks against the network and their impact, and defend the network in real time. Ex. 1004, 32.

Sourcefire describes packet–filtering devices (3D Sensors) of the 3D System that a user may deploy in a network to passively or "inline" monitor network traffic. *Id.* at 33. Each deployed 3D Sensor is capable of running

9. The record includes evidence of a range of prices for various configurations of Sourcefire 3D system products, from $1,385 to £25,000. Ex. 1042, 1; Ex. 1043, 1. Based on Mr. Leone's testimony, Sourcefire would have been distributed with the purchase of any of these products. Ex. 1005 ¶ 11 (testifying that Sourcefire was "included with each Sourcefire 3D System appliance (*e.g.*, 3D Sensor, Defense Center) sold to a customer").

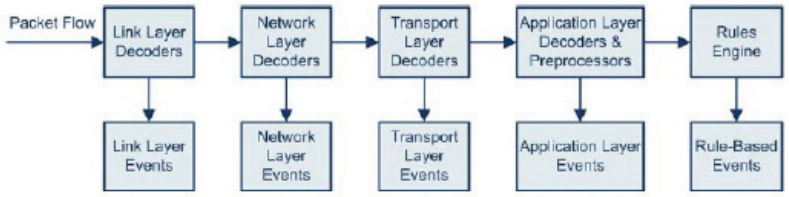
any combination of three major software components: (1) Intrusion Protection System (IPS); (2) Real-time Network Awareness (RNA); and (3) Real-time User Awareness (RUA). *Id.* at 33–34. Each 3D Sensor includes a processor (CPU), memory, and disk storage and, if managed by the centralized management service called the Defense Center, periodically sends statistics regarding such components (and events generated by applying rules to packets received via a communication interface) to the Defense Center. *Id.*; Ex. 1003 ¶ 129. The figure reproduced below depicts an exemplary 3D System. Ex. 1004, 106–107.



Appendix C

In the 3D System shown above, the Defense Center is located above, and spaced apart from, the 3D Sensor, which is designated Managed Sensor. An arrow extends upwardly at the left from the Managed Sensor to the Defense Center and includes a box listing the types of Sensor Statistics and Events transmitted from the Managed Sensor to the Defense Center. An arrow extends downwardly at the right from the Defense Center to the Managed Sensor and includes a box listing the categories of system policies that may be sent from the Defense Center.

Each deployed 3D Sensor with IPS analyzes network traffic and generates intrusion events, which are records of the traffic that violate the intrusion policy applied to a detection engine on the sensor that is monitoring a specific network segment. Ex. 1004, 256. The IPS performs these functions on packets using a series of decoders, preprocessors, and a rules engine, as illustrated in the figure below.



Id. The above figure shows two rows of 5 boxes. The boxes in the top row are labeled Link Layer Decoders, Network Layer Decoders, Transport Layer Decoders, Application Layer Decoders & Preprocessors, and Rules Engine. At the left edge of the first box in the top row is an arrow

pointing to the right labeled Packet Flow; there is also an arrow pointing to the right that extends from the right edge of each box to the left edge of the adjacent box. Each of these boxes has an arrow extending downwardly from the bottom of the box to the top of the corresponding box below it in the second row, which boxes are labeled Link Layer Events, Network Layer Events, Transport Layer Events, Application Layer Events, and Rule-Based Events.

Sourcefire explains that after the packets are decoded through the first three TCP/IP layers, they are sent to preprocessors, which normalize traffic at the application layer and detect protocol anomalies. *Id.* at 258. After the packets have passed through the preprocessors, they are sent to the rules engine, which inspects the packet headers and payloads to determine whether they trigger any of the shared object rules or standard text rules. *Id.* at 258–259. At each step of the process shown in the figure above, a packet could cause the 3D System to generate an event, which is an indication that the packet or its contents may be a risk to the security of the network. *Id.* at 260. Sourcefire describes that the rules engine implements intrusion rules to determine whether the packet headers and/or payloads of received packets triggered one or more of such rules. *Id.* at 256–259, 513, 2084, 2089.

Sourcefire explains that the IPS allows a user to write its own custom intrusion rules tuned to the user's specific network environment. *Id.* at 256–260, 428–430, 761–770. The intrusion rules had 5-tuple values associated with them: the protocol; the source and destination IP

addresses; and, the source and destination ports. *Id.* at 762–764. Sourcefire also explains that intrusion rules contain two logical parts: (1) the rule header, which contained the 5-tuple, the rule's action (e.g., alert and allow, drop, ignore and allow), and direction indicators; and, (2) the rule options part, which contained, among other things, event messages and keywords and their arguments. *Id.* at 761–770.

Sourcefire describes that keywords of intrusion rules could be used by the application-layer preprocessor, called the SSL preprocessor, and rules engine of a 3D Sensor to filter packets by encryption protocol version (e.g., TLS or SSL version). *Id.* at 825. For example, the ssl_version keyword could be used in an intrusion rule, causing the SSL preprocessor to match against such protocol version information in the application layer header (e.g., Record header) of received packets and/or unencrypted application-layer payload (e.g., Record) of received handshake packets for an encrypted session. *Id.* at 827–828, 491, 597–601, 700.

3. Analysis Regarding Claims 1–21

a. Applicable Law

A claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. *See KSR Int'l Co. v.*

Teleflex Inc., 550 U.S. 398, 406 (2007). 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 skill in the art; and (4) when in evidence, objective evidence of nonobviousness, i.e., secondary considerations. *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

We are also mindful that "obviousness concerns whether a skilled artisan not only *could have made* but *would have been motivated to make* the combinations or modifications of prior art to arrive at the claimed invention." *Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064, 1073 (Fed. Cir. 2015). 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. Info-USA, Inc.*, 587 F.3d 1324, 1329 (Fed. Cir. 2009) (quoting *KSR*, 550 U.S. at 418–21).

b. Claims 1, 8, and 15

Independent claims 1, 8, and 15 have substantially similar limitations, and Patent Owner argues these claims together. *See* PO Resp. 27–47. Accordingly, we focus our analysis below on claim 1. To begin with, we evaluate the parties' contentions regarding whether Sourcefire in view of the knowledge of a POSA teaches or suggests

the limitations of claim 1. We then evaluate whether a POSA would have been motivated to modify Sourcefire to achieve the claimed invention and Patent Owner's objective evidence of nonobviousness.

(1) Limitation 1[i]

Petitioner contends that Sourcefire teaches limitation 1[i] reciting "a computing device comprising at least one processor, a memory, and a communication interface." Pet. 32–33. In particular, Petitioner contends that each Sourcefire 3D Sensor included a processor (CPU), memory, and disk storage. *Id.* at 32 (citing Ex. 1004, 33–34, 106–107; Ex. 1003 ¶ 129). Petitioner also contends that each 3D Sensor received packets through a communication interface. *Id.* at 33 (citing Ex. 1004, 222–230; Ex. 1003 ¶ 130). As to this claim element, Patent Owner does not dispute Petitioner's contentions explicitly. For the reasons asserted by Petitioner, we determine that Petitioner has shown that Sourcefire teaches limitation 1[i].

(2) Limitation 1[ii]

Petitioner contends that Sourcefire teaches limitation 1[ii] reciting "receiving, via the communication interface, a plurality of hypertext transfer protocol secure (HTTPS) packets." Pet. 33–35. Specifically, Petitioner contends that two of the 3D Sensor's communication interfaces were "inline" interfaces in which decoder rules, preprocessor rules, and intrusion rules dropped or allowed packets received into such decoders, preprocessors, and rules engine via the inline communication interface of the 3D

Sensor. *Id.* at 33–34 (citing Ex. 1004, 222–223, 234–235, 253–254, 257, 262–264, 435–439; Ex. 1003 ¶ 133). Petitioner also contends that Sourcefire describes that the 5-tuple information specified in the rule header of an intrusion rule implemented by the network layer and transport layer decoders, SSL preprocessor, and/or rules engine could include destination port 443, which Sourcefire describes as the destination port for HTTPS. *Id.* at 34 (citing Ex. 1004, 768–769, 256, 600; Ex. 1003 ¶ 13). Petitioner further contends that Sourcefire discloses a preprocessor module specifically intended for dedicated processing of SSL/TLS traffic, the SSL preprocessor. *Id.* at 35 (citing Ex. 1004, 596–601; Ex. 1003 ¶ 135). As to this claim element, Patent Owner does not dispute Petitioner's contentions explicitly. For the reasons asserted by Petitioner, we determine that Petitioner has shown that Sourcefire teaches limitation 1[ii].

(3) Limitations 1[iii]—[v]

Other than Petitioner's arguments in the Petition, the parties' arguments in their briefs do not specifically address these limitations individually. Accordingly, we consider these limitations together, as appropriate. We first set forth Petitioner's arguments in the Petition and then analyze them in view of Patent Owner's arguments in the Response, as well as the arguments in the Reply and Sur-Reply.

(a) Petition

Limitation 1[iii] recites "responsive to a determination by the at least one processor that at least a portion of the

plurality of HTTPS packets have packet-header-field values corresponding to a packet filtering rule stored in the memory." Petitioner contends that Sourcefire in view of the knowledge of a POSA teaches or suggests this limitation. Pet. 35–36. In particular, Petitioner contends that the rule headers in every intrusion rule specified 5-tuple information and that a POSA would have understood the rules used by the 3D Sensor were stored in a memory accessed by the 3D Sensor. *Id.* at 35 (citing Ex. 1004, 762–769, 358–359; Ex. 1003 ¶¶ 138–139). Petitioner also contends that Sourcefire provides an example of determinations made from analyzing packet-header-field values, such as destination port 443, corresponding to the rule header of a packet-filtering rule; according to Petitioner, a POSA would have understood that the SSL processor or rules engine implementing such a rule would determine that packet-header-field values of at least a portion of the received packets identified destination port 443, if such portion of the received packets were HTTPS packets. *Id.* at 35–36 (citing Ex. 1004, 768–769, 256, 600; Ex. 1003 ¶ 140).

Limitation 1[iv] recites:

> applying, by the at least one processor, an operator specified by the packet-filtering rule to the at least a portion of the plurality of HTTPS packets, wherein the operator specifies one or more application-header-field-value criteria identifying one or more transport layer security (TLS)-version values for which packets should be blocked from continuing toward their respective destinations.

Appendix C

Petitioner contends that Sourcefire in view of the knowledge of a POSA teaches or suggests this limitation. Pet. 36–43. In particular, Petitioner contends that Sourcefire describes that a user could configure SSL preprocessor rules and intrusion rules to look only for packets traveling over standard SSL/TLS ports (*e.g.*, port 443) or could configure such rules to be "adaptive" to identify Record Protocol packets traveling over non-standard ports. Pet. 38. According to Petitioner, Sourcefire teaches that "[i]f a SSL/TLS identifier is found, the SSL preprocessor was invoked to process the now-identified Record Protocol packets using the SSL keyword(s) and arguments of the preprocessor rules and intrusion rules even if the packets came over a nonstandard SSL/TLS port." *Id.* at 37–38 (citing Ex. 1004, 598, 697–701; Ex. 1003 ¶ 146). Petitioner contends Sourcefire describes that the keyword "ssl_version" could be included in such intrusion rules and used to block harmful, or allow benign, Record Protocol packets. *Id.* at 39–40 (citing Ex. 1004, 827–828, 491, 597–601, 435–439; Ex. 1003 ¶ 147). According to Petitioner, it would have been obvious to a POSA that, for traffic in versions of SSL/TLS later than SSLv2 (SSLv3, TLS 1.0-TLS 1.2),[10] the version could be obtained from the Record Header of Record Protocol packets and that the SSL preprocessor must look at the Record headers in order to parse such packets at all. *Id.* at 40 (citing

10. Petitioner contends that Sourcefire teaches that "SSLv2 may have vulnerabilities associated with it" and that "[s]ecurity vulnerabilities with SSLv2 were also widely known." Pet. 41–42 (citing Ex. 1004, 827); *id.* at 42 n.4 (citing Ex. 1037, Ex. 1039, Ex. 1016; Ex. 1003 ¶ 152).

Ex. 1003 ¶ 149).[11] Thus, Petitioner contends that a POSA "understood that Sourcefire taught the use of ssl_version as a keyword, and thus it could be used as an application-layer header field value in a packet-filtering rule" to pass or block the associated packet whose SSL/TLS version matched the keyword. *Id.* at 40–42.

Limitation 1[v] recites:

> responsive to a determination by the at least one processor that one or more packets, of the at least a portion of the plurality of HTTPS packets, have one or more application-header-field values corresponding to one or more TLS-version values of the one or more TLS-version values for which packets should be blocked from continuing toward their respective destinations.

Petitioner contends that Sourcefire in view of the knowledge of a POSA teaches or suggests this limitation. Pet. 43–44. In particular, Petitioner contends, as discussed

11. In the Petition, Petitioner also relied on Sourcefire's "adaptive mode," which Petitioner asserted can change how SSL preprocessing works. Pet. 38–39 (citing Ex. 1004, p. 598, 697–701; Ex. 1003 ¶ 146). Petitioner argued Sourcefire discloses that when adaptive profiles are enabled, "the preprocessor engine checks each packet for service identifiers to see if the packet is SSL traffic." Ex. 1004, 598; *see also id.* at 600 ("To check each packet for SSL identifiers, enable adaptive profiles."). In its Response, Patent Owner argued that Sourcefire's adaptive mode is not applicable to the challenged claims. *See* PO Resp. 33–37. Petitioner did not attempt to rebut Patent Owner's argument and stated it "is simply not relevant to the claim limitations." Reply 17.

above, that Sourcefire discloses packet-filtering rules using the ssl_version keyword to identify packets having the specified SSL or TLS version and discloses that, if the packet data matched the specified rule conditions, the rule triggers. *Id.* at 43 (citing Ex. 1004, 761; Ex. 1003 ¶ 156). Petitioner also contends that Sourcefire discloses that when a drop rule was triggered, the IPS dropped (i.e., blocked) the packet. *Id.* at 43–44 (citing Ex. 1004, 761; Ex. 1003 ¶ 157).

Limitation 1[vi] recites "applying, by the at least one processor, at least one packet-transformation function specified by the operator to the one or more packets to block each packet of the one or more packets from continuing toward its respective destination." Petitioner contends that Sourcefire in view of the knowledge of a POSA teaches or suggests this limitation. Pet. 44. Specifically, Petitioner contends, and we agree (as discussed *supra*), the '552 patent describes that passing or blocking transmission of a packet is a "packet transformation function." *Id.* (citing Ex. 1001, 9:26–40). Petitioner also contends that a POSA understood that Sourcefire discloses that the TLS version value for a packet could be used to apply a packet transformation function (block or drop) to block the packet from continuing toward its destination. *Id.* (citing Ex. 1003 ¶ 160).

(b) Analysis

(i) "determination"

In its Response, Patent Owner contends that Sourcefire does not disclose (1) a "determination" that

some number of "HTTPS packets have packet-header-field values corresponding to a packet filtering rule"[12] and (2) a "determination" that some of those "HTTPS packets . . . [have] one or more application-header-field values corresponding to one or more TLS-version values" based on an operator specified by the packet filtering rule.[13] PO Resp. 27, 38–39. Patent Owner argues that rather than determining that "an HTTPS packet includes the application-header-field value," Sourcefire discloses "invoking the SSL preprocessor, which previously extracted the SSL version information for that **session** from a **reassembled TCP stream**" (*id.* at 27 (citing Ex. 2002 ¶ 81; Ex. 1004, 596–597 and 628)). Patent Owner states that Dr. Staniford confirmed this aspect of Sourcefire's operation during cross-examination (*id.* at 27–28 (citing Ex. 2001, 120:19–123:17)). Patent Owner also argues that the SSL version information extracted by the SSL preprocessor is not determined to be "in an HTTPS packet, as required by the challenged claims," but is extracted from "handshake and key exchange messages" that a POSA would understand are not HTTPS packets, but rather "application-layer messages reassembled from a received TCP stream." *Id.* at 30–31 (citing Ex. 2001 ¶ 86; Ex. 1004, 596). Stated differently, Patent Owner asserts that Sourcefire does not disclose these limitations because Sourcefire "does not inspect HTTPS packets," but extracts information from a reassembled TCP stream. *See id*. at 25–26, 41.

---

12. *See, e.g,* limitation 1[iii].

13. *See, e.g.,* limitation 1[iv].

Appendix C

According to Patent Owner, Petitioner incorrectly argues that "a POSA understood that Sourcefire describes the use of SSL/TLS rule keywords to invoke the application-layer SSL preprocessor and extract information about SSL or TLS version and session state from Record headers in packets for an encrypted session" (*see* Pet. 37) because Sourcefire's SSL preprocessor extracts the SSL version information from reassembled handshake messages during the SSL handshake, "well before any rule incorporating the ssl_version keyword invokes the SSL [p]reprocessor." *Id.* at 31–32 (citing Ex. 2002 ¶ 88, Ex. 1004, 596–597). Thus, Patent Owner asserts that the SSL preprocessor "maintains state information as it inspects the SSL handshake" by evaluating the reassembled handshake messages and then returns that maintained information if and when the SSL preprocessor is later invoked by the rules engine. *Id.* at 32 (citing Ex. 2002 ¶ 89, Ex. 1004, 597). Moreover, Patent Owner asserts that Petitioner incorrectly argues that "Sourcefire discloses that the SSL preprocessor implemented the SSL preprocessor rules and intrusion rules, including SSL keywords (e.g., ssl_version)" because it is Sourcefire's "rules engine" that uses the "ssl_version keyword," which, rather than specifying any application-level packet-header information, merely requests the preprocessor to return the SSL version it already extracted from other packets associated with that session. *Id.* at 37 (citing Ex. 2002 ¶ 96, Ex. 1004, 827).

Regarding the "determination" limitations of the claims (*see, e.g.,* limitations 1[iii] and 1[v]), Petitioner argues that neither the '552 patent nor the claims are

limited to any specific method of determining a TLS version of any HTTPS packet. Reply 10. Petitioner also argues that the claims do not require "inspection" of the application header fields of any packets, but rather require a "determination" that "one or more packets of . . . the plurality of HTTPS packets, have one or more application-header-field-values corresponding to one or more TLS version values," without requiring any specific method of how the determination is made. *Id.* at 12–13.

In response, Patent Owner asserts that Petitioner misrepresents the express claim language and that the '552 patent teaches how to determine that an HTTPS packet has application-header-field value corresponding to a TLS-version value for which packets should be blocked. Sur-Reply 9–11 (citing Ex. 1001, 8:8–18). Patent Owner's argument is not persuasive. The '552 patent does not teach a specific procedure or "how" to determine what an HTTPS packet contains, but merely states that a particular operator "may accept as input an IP packet."[14] Ex. 1001, 8:8–10. Patent Owner does not identify any specific claim language requiring "inspection" of the application header fields of HTTPS packets. The claims

14. Furthermore, to the extent Patent Owner contends that claim 1 should be limited by an example in the Specification of the '552 patent, which purportedly teaches "how to determine that an HTTPS packet . . . has an application-header-field value . . . for which packets should be blocked" (*see* Sur-Reply 10–11), Patent Owner has not persuasively explained why doing so is warranted, and we decline to read any such limitations into the claim. *See SuperguideCorp. v. DirecTV Enters., Inc.*, 358 F.3d 870, 875 (Fed. Cir. 2004).

require only a "determination" that "one or more packets of . . . the plurality of HTTPS packets, have one or more application-header-field-values corresponding to one or more TLS version values," rather than an "inspection" of the HTTPS packets. Thus, Patent Owner's argument is not persuasive because it is not commensurate with the scope of the claims. *See In re Self*, 671 F.2d 1344, 1348 (CCPA 1982) ("[A]ppellant's arguments fail from the outset because . . . they are not based on limitations appearing in the claims.").

Petitioner argues, and we agree, that Patent Owner admits that "'[a]s Sourcefire's SSL preprocessor encounters handshake messages, it 'extracts state and version information from specific handshake fields. Two fields within the handshake indicate the version of SSL or TLS used to encrypt the session and the stage of the handshake.'" Reply 13 (citing PO Resp. 28, citing Ex. 1004, 825). Petitioner also argues, and we agree, that Patent Owner further admits "'Sourcefire discloses using ssl_version keywords to detect SSL or TLS version being used for a particular session.'" *Id.* (citing PO Resp. 28, citing Ex. 1004, 597). Moreover, Petitioner argues, and we agree, that the "header of a post-handshake HTTPS packet will have the same TLS version value as previously identified in the handshake HTTPS packet associated with that session" because Dr. Orso "attested that all post-handshake packets for a particular HTTPS session are encrypted using the same TLS version under almost all circumstances."[15] *Id.* (citing Ex. 1041, 171:6–174:16). Thus,

15. In view of Dr. Orso's testimony, we are not persuaded by Patent Owner's argument that Petitioner "cites no evidence" to

as Petitioner asserts, and we agree, because the claims do not require that each packet in a session be inspected to determine the TLS version for the respective packet, "Sourefire's disclosure of using a handshake packet to 'determine' that one or more HTTPS packets have an application-header-field-value corresponding to one or more TLS versions satisfies the recited claim limitation."[16] *Id.*

Petitioner further argues that, during his cross-examination, Patent Owner's expert, Dr. Orso, confirmed that Sourcefire in view of the knowledge of a POSA teaches the "determination" limitations. *Id.* at 14. In that regard, Petitioner argues that Dr. Orso "confirmed that a POSA would understand that a handshake message could fit into a single application packet of a single IP packet and that such a packet would include a TLS version value. *Id.* (citing Ex. 1041, 161:15–163:7, 171:6–173:5). Petitioner asserts that Dr. Orso also confirmed that the '552 Specification teaches that a handshake packet that includes a TLS

---

support its view that "any given post-handshake HTTPS packet will have ***any*** TLS version values." Sur-Reply 14. In addition, as Patent Owner acknowledged, a person of ordinary skill would have understood that when TLS protocol is used, information about TLS version always is located in the packet header of the first packet in the message. *See* Tr. 42:10–43:1.

16. We are not persuaded by Patent Owner's argument that this is an "entirely new rationale," which should be ignored (Sur-Reply 12–13), because this argument was made by Petitioner in response to Patent Owner's arguments in its Response that Sourcefire does not teach the "determination" limitations. *See, e.g.,* PO Resp. 25–27, 30–32, 38–39.

version 1.0 value would be blocked and, by doing so, the session would terminate (Ex. 1041, 171:6–177:7), thereby effectively blocking all remaining packets in that session. Based on Dr. Orso's testimony, we agree with Petitioner's argument.

Patent Owner, however, disputes this argument for several reasons: (1) Petitioner's evidence demonstrates that "a TLS handshake message is not an HTTPS packet because the handshake occurs before any HTTPS session begins;" (2) "because the SSL preprocessor operates on reassembled handshake messages rather than HTTPS packets, the SSL preprocessor does not make any determination tha[t] an HTTPS packet includes any data regardless of whether the entire message might have fit within a single pack;" and, (3) because the SSL preprocessor does not implement intrusion rules, "the extraction of the version information from a handshake message is not a determination that any packets includes application-header-field values ***for which packets should be blocked***." Sur-Reply 14–15.

We do not agree with Patent Owner's argument. Even assuming *arguendo* that Patent Owner is correct that Sourcefire discloses only obtaining TLS version information from reassembled handshake messages, we find that Sourcefire still teaches a determination that a *packet* comprises TLS version information.[17] It is undisputed

17. As Petitioner argues, and we agree, Patent Owner's argument that the rules engine inspects the stream as a single reassembled entity, rather than inspecting only the individual packets, "is not relevant" because the claims "do not require inspecting only the individual packets." Reply 16.

that such reassembled or reconstructedmessages consist of packets. *See* Tr. 35:4–6, 39:14–16. According to Patent Owner, the technology of the claimed invention "works because the [TLS version] information we're looking for is always going to be in the first packet." *Id.* at 35:6–8. In other words, as Patent Owner acknowledged, a person of ordinary skill would have understood that when TLS protocol is used, information about TLS version always is located in the packet header of the first packet in the message. *See id.* at 42:10–43:1; Ex. 1041, 194:17–23.

The sole difference in this regard between claim 1 and the teachings of Sourcefire, according to Patent Owner, is that claim 1 recites determining that a packet (i.e., the first packet of the message) comprises TLS version data, whereas Sourcefire teaches determining that the reassembled handshake message comprises TLS version data *by extracting that data from the first packet of the message*. *See* Tr. 40:3–12. We find that a person of ordinary skill would have understood that, in both instances, the relevant data is located in the first packet of the message (e.g., a handshake message). Whether the system of Sourcefire itself recognizes that fact or deduces it is irrelevant; the relevant question is whether a *person of ordinary skill* would have been taught the recited determination (i.e., determining that a packet comprises TLS version data) based on Sourcefire and his/her own knowledge. *See In re Keller*, 642 F.2d 413, 425 (CCPA 1981) ("The test for obviousness is not . . . that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art.").

Thus, based on Dr. Orso's testimony as cited above, we agree with Petitioner's argument that, even under Patent Owner's view of the claims and Specification, the portions of Sourcefire cited by Patent Owner (*see* PO Resp. 31–37, discussed above) disclose the "determination" limitations. *Id.*

(ii) "operator"

Patent Owner argues that Petitioner has not shown that Sourcefire in view of the knowledge of a POSA discloses applying the claimed "operator" that "specifies one or more application-header-field-value criteria identifying one or more transport layer security (TLS)-version values for which packets should be blocked from continuing toward their respective destinations,"[18] as recited in claims 1, 8, and 15. PO Resp. 39–43. Patent Owner argues that the claimed "operator" specifies both "application-header-field-value criteria" and "a packet transformation function."[19] *Id.* at 41. According to Patent Owner, although Petitioner argues that "a POSA understood that Sourcefire discloses that the TLS version value for a packet could be used to apply a packet transformation function (block or drop) to block the packet from continuing toward its destination," it does not argue that the alleged "packet transformation

18. *See, e.g.*, limitation 1[iv].

19. We agree with Patent Owner's argument based on the express terms of the claims (*see* § II.A.2.a) and our discussion of the term "packet transformation function" in the Institution Decision (*see id.*).

function" is specified by an "operator," as recited in the claims. *Id.* at 41–42 (citing Pet. 44). Patent Owner argues that a packet transformation function is not specified by an "operator" in Sourcefire because Sourcefire works on the basis of Snort rules that include a "rule header" that includes "the rule's action." *Id.* at 42 (citing Ex. 2002 ¶ 104, Ex. 1004, 762–763); *see* Ex. 1029 (describing "Snort"). Patent Owner asserts that this distinction is not trivial because, as discussed in regard to claims 2, 9, and 16, "Sourcefire is not capable of designing a packet-filtering rule specifying an operator that applies different packet transformation functions based on different application-layer-packet-header criteria." *Id.* at 42–43.

Patent Owner's arguments regarding the claimed "operator" are not persuasive for several reasons. First, Petitioner argues that "Sourcefire discloses an operator in the form of the packet-filtering rules, which specify a keyword and associated arguments (application-layer-packet-header criteria) and the Rule Action (packet transformation function) that can be triggered." Reply 17 (citing Pet. 27). Petitioner also argues that the Petition "identified how a POSA understood that Sourcefire teaches use of the ssl_verison keyword in a packet filtering rule, specifying an application-header-field identifying a TLS-version value, e.g., TLS 1.0, for which packets should be blocked where the associated packets were encrypted using the specified TLS version, e.g., the SSL/TLS version in the associated packets matches the keyword." *Id.* at 18 (citing Pet. 39–42 (citing Ex. 1004, 827–828, 491, 597–601, 435–439; Ex. 1003 ¶ 147–149). Thus, we agree with Petitioner's argument that Sourcefire discloses an

"operator" that specifies (1) the keyword and argument that indicates "application-header-field-value criteria," e.g., TLS version 1.0, and (2) a "packet transformation function," e.g., blocking packets that match the criteria. *Id.* at 18.

Second, we are not persuaded by Patent Owner's argument that because the action of the rule is in the "rule header," it is not specified by an "operator." PO Resp. 42–43. Patent Owner states that because "the operator specifies both the application-layer-packet-header criteria and the packet transformation function, the '552 patent can use the same rule to specify **different** packet transformation functions for **different** application-layer-packet-header criteria." *Id.* Petitioner argues that Sourcefire includes the identical disclosure because Sourcefire teaches (1) the use of different ssl_version keyword arguments or criteria (Reply 18–19 (citing Ex. 1004, 828)) and (2) that for each of these keywords and arguments "a corresponding action of *pass* (allow), *alert* (and pass), or *drop* (block) can be specified" (*id.* at 19 (citing Pet. 27 (citing Ex. 1004, 761–770)). Based on the cited portions of Sourcefire, we agree with Petitioner. Although Patent Owner asserts that Petitioner "egregiously misrepresents the disclosure of Sourcefire" (Sur-Reply 16 (citing Ex. 1004, 761, 763)), Patent Owner has not provided persuasive reasoning to support its assertion that Petitioner "misrepresents" the disclosure of Sourcefire or its argument that "only one rule action may be specified per rule." Thus, we agree with Petitioner that "Sourcefire has the same functionality of the '552 [p]atent and can use the same rule to specify different packet transformation functions for different application-layer-packet-header criteria." Reply 19.

In addition, Patent Owner argues that Petitioner has not shown that Sourcefire discloses "that the operator is applied **responsive** to the determination that 'a portion of the plurality of HTTPS packets have packet-header-field values corresponding to a packet filtering rule stored in the memory,' as claimed."[20] PO Resp. at 44. Patent Owner asserts that a two-stage process is reflected in each independent claim, "wherein *first* the computing system determines that a first portion of packets has packet header data that matches a packet filtering rule," and "[s]econd, and responsive to that determination," the computing system applies an operator. *Id.* at 45. Patent Owner also argues that "Sourcefire does not disclose this claimed two-stage process" (*id.* (citing Ex. 2002 ¶ 108)), and "[n]or would it have been obvious to modify Sourcefire to meet the language of the claims" (*id.* (citing PO Resp. § VI.A.2.b)). Patent Owner further argues that "[t]his two-step process permits **different** operators to be applied to the different portions of received packets depending on the rule criteria matched in the first step." *Id.*

We are not persuaded by Patent Owner's argument. Instead, for the reasons explained by Petitioner in the Reply, we agree with Petitioner that, as set forth in the Petition, Sourcefire discloses applying an operator in two-stage packet filtering. Reply 19–22. In that regard, for example, Petitioner argues that, as set forth in the Petition, Sourcefire discloses that "[t]he rules engine implemented intrusion rules to determine whether the packet headers . . . of received packets triggered one or

20. *See, e.g.,* limitation 1[iii].

more of such rules" and describes "filtering packets based on packet header information including the 5-tuple, just like the Stage I evaluation described in the '552 patent." *Id.* at 19–20 (citing Pet. 25, 31 (citing Ex. 1004, 256–259, 761–770; *see also* Pet. 25–28, 56–58)). Petitioner also argues that these cited excerpts of Sourcefire describe that the intrusion rules, which included user customizable rule header and rule options criteria, were organized into groups or "subsets" based on commonalities in the respective rule header criteria (e.g., 5-tuple, direction indicator, etc.). *Id.* at 20 (citing Ex. 1004, 259, 761–770 (showing customizable rule header criteria)). Petitioner further argues that these excerpts of Sourcefire describe that "as packets arrive at the rules engine, it first checks whether packet-header-field values in the packets match this rule header criteria and, only if so, does it 'test' whether the remainder of the rule criteria (*e.g.,* rule keywords and arguments) match to trigger the Rule Action." *Id.* (citing Ex. 1004, 259 ("As packets arrive at the rules engine, it selects the appropriate rule subsets to apply to each packet."), 766–768 ("You can restrict packet inspection to the packets originating from [specific IP addresses/specific ports] or those destined to [a specific IP address/specific ports]."), 761 (discussing alert, pass, drop rule actions), 764 ("tests traffic" in example rule header values table), 765–766 (specifying rule actions), 358–359 ("A drop rule is an intrusion rule . . . whose rule state is set to Drop and Generate Events."))). Patent Owner does not respond to these arguments in the Sur-Reply. *See generally* Sur-Reply. In view of these disclosures of Sourcefire, we agree with Petitioner that in the language of the dependent claims, and as outlined in the Petition,

Sourcefire discloses determining whether to apply an operator in a two-stage packet filtering operation:

> if a first portion of packets match certain rule header criteria (e.g., specific addresses/specific ports), they will be evaluated against a first "subset" of rules (e.g., including the TLS-version packet-filtering rules) – some of these packets may pass and some may be blocked. Pet., 56-58. If a second portion of packets does not match this rule header criteria for the first "subset" of rules (e.g., different addresses/ different ports), they will not be evaluated against the remainder of the rule criteria (e.g., rule keywords and arguments) for the first "subset" of rules. *Id.* And, if this second portion of packets matches certain rule header criteria of a second "subset" of rules, they will instead be evaluated against the remainder of the rule criteria for the second "subset" of rules (i.e., without applying the TLS-version packet-filtering rules).

Reply 21–22.

For the above reasons and on the complete record after trial, we determine Petitioner has shown by a preponderance of the evidence that Sourcefire in view of the knowledge of a person of ordinary skill in the art teaches or suggests each limitation of claim 1.

(4) Motivation to Modify Sourcefire

Patent Owner contends that Petitioner has not demonstrated that a person of ordinary skill would have been modified Sourcefire to reach the claimed invention of the '552 patent, specifically reciting limitation 1[iv]. PO Resp. 47. Specifically, Patent Owner argues that Petitioner describes no motivation to modify Sourcefire to practice "the blocking element" of the claims because Petitioner's argument does not explain why a POSA would have written the rule recited in the claim and Petitioner's argument lacks evidentiary basis, either in Sourcefire or Dr. Staniford's declaration. *Id.* at 48–51. Patent Owner also argues that Petitioner describes no motivation to modify Sourcefire to practice "the operator element" of the claims because (1) Petitioner asserted in the Petition that a POSA understood Sourcefire taught the use of ssl_version as a keyword, and thus, it "***could be*** used as an application-layer header field value in a packet-filtering rule" (citing Pet. 40–41) and (2) as a matter of law, "the question is not whether a POSA ***could*** have modified Sourcefire," but whether a POSA would have been motivated to make the modification. *Id.* at 51–53.

We are not persuaded by Patent Owner's arguments for several reasons. Regarding Patent Owner's arguments that the Petition presents insufficient support for its assertion that a person of ordinary skill would have been motivated to practice "the blocking element" and "the operator element" (PO Resp. 47–53; Sur-Reply 17–18), "the inferences and creative steps a person of ordinary skill in the art would employ" can supply a motivation to combine

or modify teachings, and "[a] person of ordinary skill is also a person of ordinary creativity, not an automaton." *KSR*, 550 U.S. at 401, 421. In addition, Dr. Staniford's Declaration,[21] and the Petition, provide evidence of the known vulnerabilities with SSLv2, SSLv3, and TLS 1.0, which explains why a POSA would have been motivated to write an intrusion rule to block certain packets using these versions. Ex. 1003 ¶ 153; *see* Reply (citing Pet. 17, 30, 41–43). Moreover, we are not persuaded by Patent Owner's argument that the Petition failed, as a matter of law, to show a motivation to modify Sourcefire to practice "the operator element" based on the distinction between "could" and "would." A fair reading of the Petition, and Dr. Staniford's declaration, shows Petitioner argued that, given the understanding of a person of ordinary skill (i.e., what a person of ordinary skill "understood"), such a person "could" use a teaching or capability of Sourcefire (i.e, such a person had reason to use such a teaching) and that using such teaching "would" have the predictable effect of achieving the claimed feature. *See, e.g.,* Pet. 42–43 ("POSA understood that by using the ssl_version keyword, packet-filtering rules *could* be written to either pass or block the associated packets whose SSL/TLS version matched the keyword as taught by Sourcefire, and that doing so *would* have the predictable benefit of achieving increased network security by protecting a network against known vulnerabilities.") (emphasis added).

21. Based on the Petition and Dr. Staniford's Declaration as a whole, we are unpersuaded by Patent Owner's arguments that a particular paragraph of Dr. Staniford's Declaration "merely repeats the argument from the Petition," and that Petitioner improperly incorporated evidence on this issue by reference via the Declaration. *See* PO Resp. 50.

As discussed *supra*, Sourcefire explains the use of the "ssl_version" keyword in designing rules, and also teaches that rules can be drop rules that cause packets to be dropped (i.e., blocked) when triggered. We find that a person of ordinary skill would have been sufficiently motivated and informed by Sourcefire to write an intrusion rule with the ssl_version keyword to block packets whose SSL/TLS version matched the keyword, as discussed above. *See*, *e.g.*, Pet. 39–40 (citing Ex. 1004, 827–828, 491, 597–601, 435–439; Ex. 1003 ¶ 147–148); *see also id.* at 40–41 (citing Ex. 1003 ¶¶ 83–88, 149–151); *id.* at 42 (citing Ex. 1004, 254, 435–439, 697–701, 761–762; Ex. 1003 ¶¶ 83–88, 153).

(5) Objective Indicia of Nonobviousness

Before determining whether a claim is obvious in light of the prior art, we consider any relevant evidence of secondary considerations—objective indicia—of nonobviousness. *See Graham*, 383 U.S. at 17. Patent Owner presents evidence of four such considerations: (1) long-felt but unresolved need, and failure of others, (2) industry praise, (3) skepticism of experts, and (4) commercial success. PO Resp. 57–69.

"In order to accord substantial weight to secondary considerations in an obviousness analysis, the evidence of secondary considerations must have a nexus to the claims, i.e., there must be a legally and factually sufficient connection between the evidence and the patented invention." *Fox Factory, Inc. v. SRAM, LLC*, 944 F.3d

1366, 1373 (Fed. Cir. 2019) (internal quotations omitted). A nexus is presumed when "the patentee shows that the asserted objective evidence is tied to a specific product and that product 'embodies the claimed features, and is coextensive with them.'" *Id.* (quoting *Polaris Indus., Inc. v. Arctic Cat, Inc.*, 882 F.3d 1056, 1072 (Fed. Cir. 2018)). If the product is not coextensive with the claims at issue—for example, if the patented invention is only a component of the product—the patentee is not entitled to a presumption of nexus. *See id.* (citing *Demaco Corp. v. F. Von Langsdorff Licensing Ltd.*, 851 F.2d 1387, 1392 (Fed. Cir. 1988)).

(a) Long-felt but unresolved need, and failure of others

According to Patent Owner, the '552 patent "satisfied a long-felt need in the industry that others had failed to solve—namely, how to protect against '[a] category of cyber attack known as exfiltrations." PO Resp. 59. Patent Owner argues that "the long felt need for the scalable solution to the problem of exfiltration attacks provided by the '552 [p]atent was recognized as far back as 2010." *Id.* at 61–62 (citing Ex. 2013, 5–6; Ex. 2002 ¶ 126). According to Patent Owner, the failure of others in the industry to provide proactive network protection that could scale to larger networks was recognized in a White Paper, referred to as "the ESG Paper." *Id*. at 62 (citing Ex. 2006, 1, 3). Patent Owner relies on a portion of the ESG Paper that Patent Owner argues provides a "laudatory description" of Centripetal's "RuleGATE" product. *Id.* at 63 (citing Ex. 2006, 7).

With respect to nexus, Patent Owner asserts that "Centripetal's solution to the long felt need of how to meaningfully operationalize CTI is tied to the invention disclosed and claimed in the '552 [p]atent." *Id.* (citing Ex. 2002 ¶ 129). In that regard, Patent Owner argues that the claims of the '552 patent are generally directed to a two-step packet-filtering technique that allows Centripetal's solutions to scale: the second stage processing may be carried out on the subset of all received packets; and, both stages are applied to individual HTTPS packets such that there is no need for "time and resource intensive packet reassembly procedures." *Id.* at 64 (citing Ex. 2002 ¶ 129). Relying on Dr. Orso's testimony, Patent Owner further argues that the best-in-class performance of Centripetal's TIG is due "in large part to the fact that the '552 [p]atent's packet-filtering rules are applied on a packet-by-packet basis, allowing the TIG to operate as a 'network filter' rather than a traditional IPS." *Id.* at 64–65 (citing Ex. 2002 ¶ 130; Ex. 2006, 7–8).

Patent Owner's nexus arguments and evidence, however, are insufficient to establish a nexus between the alleged long-felt but unresolved need, and failure of others, and the claimed invention. First, no analysis is presented to demonstrate that the RuleGATE product is coextensive with any claim of the '552 patent. Thus, Patent Owner is not entitled to a presumption of nexus. *See Fox Factory*, 944 F.3d at 1373. Second, insufficient analysis is presented to show that the evidence of a purported long-felt but unresolved need is connected to the patented invention. Patent Owner does not adequately explain how the purported "packet-by-packet" nature of the claimed

method specifically addresses the threat of exfiltrations. Nor does Patent Owner explain how the patented invention achieves a "scalable" solution to exfiltrations. *See* Tr. 56:4–11 (Patent Owner acknowledging the claims do not require scalability or "larger rule sets" than prior devices). With respect to the "challenges" reported in the ESG Paper—i.e., "[l]ack of automation," "the inability to use feeds 'in a meaningful way to live network traffic,'" and "the ability to 'turn[] [cyber threat intelligence] into actionable insight" (PO Resp. 63)—Patent Owner provides no analysis as to how the patented invention purportedly meets those challenges. Moreover, the paper praising Centripetal's product identifies features contributing to the product's solutions that are not tied to any aspect of the challenged claims, such as "dynamically monitor[ing] for advanced threats using intelligence," and "converting indicators to rules that drive actions across a risk spectrum, i.e., logging, content capture, mirroring, redirection, shielding, and advanced threat detection." *See* Ex. 2006, 7.

Therefore, we conclude that a nexus was not proven between the purported long-felt but unresolved need identified by Patent Owner, and the patented invention of the '552 patent.

(b) Industry praise

Patent Owner cites the ESG Paper (Ex. 2006), a Gartner article (Ex. 2007), and an American Banker article (Ex. 2011) as evidence of industry praise. PO Resp. 65–66. Similar to its long-felt need contentions, however, Patent Owner does not provide sufficient analysis

or explanation to establish the requisite nexus. Patent Owner again provides no analysis demonstrating that any Centripetal product is coextensive with the challenged claims, so no presumption of nexus is applied. *See Fox Factory*, 944 F.3d at 1373. Additionally, the cited praise of Centripetal products is not linked sufficiently to the challenged claims, including because Patent Owner failed to address lauded features with no relationship to the claims.

For example, Patent Owner cites the ESG Paper as praising the "highest performance" of Centripetal's product, its ability to process "hundreds of millions of indicators from thousands of feeds," "synthesizing into a network policy," enforcing over five million "complex filtering rule[s]" with "at-least a dozen unique fields which had to be evaluated and applied bi-directionally and without state," etc. *Id.* (citing Ex. 2006, 7; Ex. 2002 ¶ 131). None of these features appear to be in the challenged claims. Patent Owner does not address whether they are part of the claimed invention or, if not, their relative contribution to the industry praise compared to any actual features of the claimed invention.

Regarding the Gartner article, Patent Owner notes that Gartner praises Centripetal's "ability to instantly detect and prevent malicious connections based on millions of threat indicators at 10-gigabit speeds," "the largest number of third-party threat intelligence service integrations," and using "5 million indicators simultaneously." *Id.* at 66 (citing Ex. 2007, 5). Again, insufficient analysis is presented to address how these

features relate to the challenged claims. Patent Owner's reference to the American Banker article similarly suffers from a lack of explanation. *Id.* (citing Ex. 2011, 14; Ex. 2002 ¶ 132).

The only nexus explanation provided is a conclusory assertion that "the salutary benefits of Centripetal's [praised product] are made possible in large part by the '552 Patent's network layer, packet-by-packet, rule enforcement that foregoes deep inspection at the application layer." *Id.* at 66 (citing Ex. 2002 ¶ 133). Dr. Orso's testimony cited in support of this statement is merely a near-verbatim copy of this conclusory statement with no additional explanation. *See* Ex. 2002 ¶ 133; *see also* 37 C.F.R. § 42.65(a) ("Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight."); *TQ Delta, LLC v. Cisco Sys., Inc.*, Nos. 2018-1766, 1767, slip op. at 10 (Fed. Cir. Nov. 22, 2019) ("Conclusory expert testimony does not qualify as substantial evidence.") (citations omitted). As a result, we find that Patent Owner has not established a sufficient nexus between the cited industry praise and the invention of the challenged claims.

(c) Skepticism of experts

Patent Owner asserts that "Dr. Staniford's skepticism regarding Centripetal's solution to the exfiltration problem as recited in the challenged claims weighs in favor of a finding that the claims are patentable." PO Resp. 68. This argument misstates Dr. Staniford's testimony because Dr. Staniford did not express "skepticism regarding the

viability of Centripetal's products, which practice the ''552 [p]atent," nor did he "opine that [Centripetal's] solution was impossible," as Patent Owner argues. *Id.* Instead, Dr. Staniford's testimony concerned Sourcefire, and he testified that he could not say "whether it's absolutely impossible to run Sourcefire in a stateless mode" and that no POSA would propose to do that "because it's not a useful way to detect attacks anytime recently." *See* Ex. 2001, 121:21–123:17. Thus, Patent Owner's argument in this regard is unsupported and conclusory. Moreover, Patent Owner does not provide sufficient analysis or explanation to establish the requisite nexus. *See Fox Factory*, 944 F.3d at 1373. Patent Owner again provides no analysis demonstrating that any Centripetal product is coextensive with the challenged claims, so no presumption of nexus is applied.

(d) Commercial success and licensing

Lastly, Patent Owner contends that the commercial success of its RuleGATE product and the license taken by Keysight Technologies to Centripetal's patent portfolio, which included the '552 patent, are compelling secondary considerations of nonobviousness. PO Resp. 68–69. We disagree.

First, we note that the sole evidence cited for the commercial success of the RuleGATE product, a declaration by Mr. Jonathan Rogers of Centripetal, makes no mention whatsoever of the '552 patent. *See* Ex. 2016. Rather, the Rogers Declaration is testimony that was submitted in a different *inter partes* review challenging

a different patent. *See id*. As such, there is no record evidence supporting any nexus between the matters in Mr. Rogers' testimony on alleged commercial success and the '552 patent.

Second, as Patent Owner itself admits (PO Resp. 69), the Keysight license was a "worldwide, royalty-bearing, non-transferable, irrevocable, nonterminable, nonexclusive license to Centripetal's worldwide patent portfolio." Ex. 2012, 83. No information is provided about crucial details of this license license—e.g., how many patents comprise the portfolio, the relative contributions of the patents in the portfolio to the value of the license—such that we could discern whether Keysight took the license "out of recognition and acceptance of the subject matter claimed" in the '552 patent. *See In re GPAC Inc.*, 57 F.3d 1573, 1580 (Fed. Cir. 1995). In fact, the record evidence indicates that this license was taken to settle litigation (Ex. 2012, 88), which diminishes its probative value as an indicator of nonobviousness. *See GPAC*, 57 F.3d at 1580. Accordingly, we find that Patent Owner has not provided sufficient evidence to establish the requisite nexus between the Keysight license and the '552 patent. *See id.*

c. Claims 2–7

Claims 2–7 depend from independent claim 1. The Petition sets forth arguments and evidentiary support for each of claims 2–7. Pet. 44–58. Patent Owner presents arguments regarding claims 2 and 7, but presents no arguments regarding claims 3–6.

With respect to claim 2, Patent Owner argues that "Petitioner has not explained how Sourcefire can utilize a single packet filtering rule that specifies two different packet transformation functions (each specified by the operator), as required by claims 2, 9, and 16." *See* PO Resp. 53–55. We are not, however, persuaded by this argument because, as discussed *supra*, we determine that Sourcefire "can use the same rule to specify different packet transformation functions for different application-layer-packet-header criteria." *See* § II.B.3.b.(3)(b)(ii).

Regarding claim 3, Petitioner contends that Sourcefire discloses that rules could be written, which included the most common HTTP methods of GET, PUT, POST, and CONNECT as one or more of the rule criteria. Pet. 47 (citing Ex. 1004, 568, 786; Ex. 1003 ¶ 172). Petitioner also contends that Sourcefire discloses that such rules can be implemented by the HTTP inspect preprocessor and by the rules engine and provides a specific keyword option just to access the HTTP method. *Id.* at 48 (citing Ex. 1004, 785–786, 807, 435–439, 491; Ex. 1003 ¶¶ 173, 124). We find Petitioner's arguments and evidence to be persuasive.

Regarding claim 4, Petitioner contends that a POSA understood that Sourcefire disclosed how a user would have written a rule using the HTTP Method option of the HTTP content keyword as part of the application-layer rule criteria to invoke the HTTP inspect preprocessor to identify a packet using the "PUT" HTTP method and to block such a packet with certain application payload content posing a threat from continuing towards its destination." *Id.* at 51–52 (citing Ex. 1004, 560, 568, 786; Ex. 1003 ¶ 184). We find Petitioner's arguments and evidence to be persuasive.

Regarding claim 5, Petitioner asserts that Sourcefire in view of the knowledge of a POSA discloses the limitations of claim 5 for the reasons set forth with respect to claims 3 and 4. *Id.* at 53–54. We agree with Petitioner's assertions and find Petitioner's arguments and evidence to be persuasive.

Regarding claim 6, Petitioner argues that Sourcefire discloses each of the recited "comparing" limitations because (1) Sourcefire defines the information contained in the rule header of the packet-filtering rule (*id.* at 54–55 (citing Ex. 1004, 764, Ex. 1003 ¶ 194)) and the Rule Header Values table provides examples of values found in the packet header (*id.* at 55 (citing Ex. 1004, 764, Ex. 1003 ¶ 195)) and (2) Sourcefire explains that the rule triggered when the step of "comparing" the rule header value with the packet header value of the packet received produced a match (*id.* (citing Ex. 1004, 403, Ex. 1003 ¶ 196)). We find Petitioner's arguments and evidence to be persuasive.

With respect to claim 7, Patent Owner argues there is no allegation in the Petition that Sourcefire discloses a rule or that such a rule would have been obvious to a POSA "that blocks all packets that do not 'have packet-header-field values corresponding to [the] packet-filtering rule'" of claim 1. PO Resp. 56–57. We are not persuaded by this argument. As discussed *supra* (*see* § II.B.3.b.(3)(b)(ii)), as set forth in the Petition, Sourcefire describes "filtering packets based on packet header information including the 5-tuple, just like the Stage I evaluation described in the '552 patent." *See* Reply 19–20 (citing Pet. 25, 31 (citing Ex. 1004, 256–259, 761–770; *see also*

Pet. 25–28, 56–58)). Sourcefire also describes that "as packets arrive at the rules engine, it first checks whether packet-header-field values in the packets match this rule header criteria and, only if so, does it 'test' whether the remainder of the rule criteria (*e.g.,* rule keywords and arguments) match to trigger the Rule Action." *Id.* (citing Ex. 1004, 259 ("As packets arrive at the rules engine, it selects the appropriate rule subsets to apply to each packet.")). Moreover, Sourcefire describes that "[y]ou can restrict packet inspection to the packets originating from [specific IP addresses/specific ports] or those destined to [a specific IP address/specific ports]." *Id.* at 20 (citing Ex. 1004, 766–768, 761 (discussing alert, pass, drop rule actions)). Thus, as we determine *supra*, Sourcefire discloses that if a second portion of packets does not match the rule header criteria for the first "subset" of rules (e.g., different addresses/different ports), they will not be evaluated against the remainder of the rule criteria and can be dropped or blocked as disclosed in Sourcefire. *See* Ex. 1004, 761; § II.B.3.b.(3)(b)(ii). As such, we find that Sourcefire in light of the knowledge of one of ordinary skill in the art would have taught the limitations of claim 7.

d. Claims 8–21

Independent claim 8 recites an apparatus comprising a processor and a memory storing instructions that, when executed, performs substantially the same steps recited in claim 1. Claims 9–14 depend from claim 8 and recite limitations substantially the same as those of claims 2–7. Petitioner relies on the same arguments and evidence for claims 8–14 as for the corresponding claims 1–7. Pet. 58–63.

Independent claim 15 recites non-transitory computer readable media comprising instructions that, when executed, cause substantially the same steps recited in claim 1 to be performed. Similarly, claims 16–21 depend from claim 15 and recite limitations substantially the same as those of claims 2–7. Petitioner relies on the same arguments and evidence for claims 15–21 as for the corresponding claims 1–7. *Id.* at 63–69.

Patent Owner presents no arguments for independent claims 8 and 15 other than those discussed *supra* for claim 1. Similarly, Patent Owner presents no arguments for claims 9 and 16, and claims 14 and 21, other than those discussed *supra* for claims 2 and 7, respectively.

e. Conclusion as to Obviousness

Based on Petitioner's arguments and evidence discussed above, we determine Petitioner has shown by a preponderance of the evidence that Sourcefire in view of the knowledge of a person of ordinary skill in the art teaches or suggests each limitation of each challenged claim. We further determine that Petitioner's showing that the claims are taught or suggested by Sourcefire in view of the knowledge of a person or ordinary skill was very strong, particularly in comparison to Patent Owner's showing with respect to the asserted objective indicia of nonobviousness. As discussed above, we find that Patent Owner has not established the requisite nexus between the challenged claims and *any* of the asserted secondary considerations. As such, we are unable to accord them any substantial weight. *See Fox Factory*, 944 F.3d at 1373. Therefore, in weighing the totality of the evidence

of record and the strength of the parties' showings on the inquiries underlying the question of obviousness, we conclude that Petitioner has met its overall burden of proving by a preponderance of the evidence that each of the challenged claims would have been obvious in view of Sourcefire and the knowledge of a person of ordinary skill.

C. Motions to Exclude

1. Petitioner's Motion to Exclude (Paper 29, "Pet. Mot.")

Petitioner moves to exclude Exhibits 2003, 2005–2007, 2011–2013, and 2016. Pet. Mot. 1. Exhibits 2003 and 2005 did not form the basis for any aspect of this Decision. As such, Petitioner's Motion with respect to those exhibits is moot.

For Exhibit 2016, the Rogers Declaration, Petitioner asserts that it should be excluded under Rules 401, 402, 403, and 602 of the Federal Rules of Evidence. Pet. Mot. 10–11. We agree with Patent Owner that exclusion is unwarranted. Paper 33, 4–5. Mr. Rogers testifies in the Declaration about his position at Centripetal, his responsibilities ("overseeing all operations of the business"), and his familiarity with Centripetal's licensing practices. Ex. 2016 ¶ 3. We are satisfied that this testimony establishes sufficient personal knowledge of the subject matter of his testimony, which concerns Centripetal's customers and its RuleGATE product. *See generally* Ex. 2016. Thus, we deny Petitioner's objection under Rule 602. With regard to Rules 401, 402, and 403, we note that Patent Owner relies on Exhibit 2016 to support its arguments for

commercial success, which specifically note the alleged success of the RuleGATE product. PO Resp. 68. Although the Rogers Declaration addresses a different patent than the '552 patent, its testimony regarding Centripetal's customers for the RuleGATE product generally meets the threshold for relevance, and its purported shortcomings as evidence go to its persuasive weight rather than its admissibility. We also discern no risk of unfair prejudice. Thus, Petitioner's objection under Rules 401, 402, and 403 also are denied.

With respect to Exhibits 2005–2007 and 2011–2013, Petitioner argues they should be excluded under Rules 401, 402, 403, 901, and as hearsay (under Rule 802). Pet. Mot. 7–9. We are not persuaded. Each of these exhibits is cited by Patent Owner as evidence supporting its arguments regarding objective considerations of nonobviousness, including as evidence of industry praise and the existence of a relevant license. *See* PO Resp. 46–53. Although they may not identify the '552 patent (Pet. Mot. 7), we determine that they meet the threshold for relevance nonetheless, and we discern no risk of unfair prejudice, confusion, or waste of time. Regarding authentication, we note that the Declaration of Jeffrey H. Price (Ex. 2017) provides evidence of the source of each of these exhibits, and we find that this information along with the distinctive characteristics of the exhibits themselves (including dates, titles, publication names, etc.) provide the necessary basis for authentication.[22] With respect to Petitioner's hearsay

22. We further note that Exhibits 2007 and 2011 are printed material purporting to be from news sources, which are self-authenticating under Rule 902(6).

objections, we conclude first that Exhibits 2007 and 2011 are not hearsay because they are not relied on for the truth of the matters asserted. *See* Fed. R. Evid. 801(c). These exhibits are cited only as evidence of industry praise; their relevance lies in that they include statements from the industry allegedly praising Centripetal and its products, not in whether that praise is true or accurate. *See* PO Resp. 65–66. For the remaining exhibits, we deny Petitioner's hearsay objection under Rule 807 because we conclude that the totality of the circumstances provides sufficient indicia of trustworthiness—for example, these exhibits are contemporaneous documents by third parties produced for purposes that indicate their statements are likely reliable (e.g., Keysight's official Annual Report (Ex. 2012))—and these exhibits generally are highly probative on the points underlying Patent Owner's secondary considerations allegations (e.g., industry praise) compared to different evidence reasonably available to Patent Owner. For the above reasons, we are not persuaded that any of these exhibits should be excluded and, thus, we deny Petitioner's Motion to Exclude.

2. Patent Owner's Motion to Exclude (Paper 30, "PO Mot.")

Patent Owner moves to exclude Exhibits 1010, 1011, 1013–1039, and 1044. PO Mot. 1. With the exception of Exhibit 1034, none of the other exhibits formed the basis for any aspect of this Decision. Thus, Patent Owner's Motion is moot as to those exhibits.

For Exhibit 1034, Patent Owner objects on the basis of Rule 901. *Id*. We agree with Petitioner, however, that the distinctive characteristics of Exhibit 1034—e.g., the BusinessWire logo and trademarks, URL, date, and general appearance of the document—provide the necessary basis for authentication. *See* Paper 31, 7. We further agree that Exhibit 1034 is sufficiently akin to a newspaper or periodical article such that the exhibit is self-authenticating under Rule 902(6). *See id.* at 7–8.

For the above reasons, we are not persuaded that any of these exhibits should be excluded and, thus, we deny Patent Owner's Motion to Exclude.

III. CONCLUSION[23]

For the foregoing reasons, Petitioner has proven by a preponderance of the evidence that the challenged claims of the '552 patent are unpatentable, as summarized in the following table:

---

23. 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).

Appendix C

Claims	35 U.S.C. §	Reference(s)
1–21	103(a)	Sourcefire
Overall Outcome		

Claims Shown Unpatentable	Claims Not Shown Unpatentable
1–21	
1–21	

IV. ORDER

In consideration of the foregoing, it is:

ORDERED that the challenged claims of the '552 patent are held unpatentable as obvious under 35 U.S.C. § 103(a) in view of Sourcefire and the knowledge of a person of ordinary skill in the art;

FURTHER ORDERED that Petitioner's Motion to Exclude (Paper 29) is *denied* as set forth above;

FURTHER ORDERED that Patent Owner's Motion to Exclude (Paper 30) is *denied* as set forth above;

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

APPENDIX D — JUDGMENT OF THE UNITED STATES PATENT AND TRADEMARK OFFICE, PATENT TRIAL AND APPEAL BOARD, IPR2018-01437, DATED JANUARY 23, 2020

UNITED STATES PATENT
AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL
AND APPEAL BOARD

IPR2018-01437
Patent 9,160,713 B2

CISCO SYSTEMS, INC.,

Petitioner,

v.

CENTRIPETAL NETWORKS, INC.,

Patent Owner.

Before BRIAN J. McNAMARA, J. JOHN LEE, and JOHN P. PINKERTON, *Administrative Patent Judges.*

LEE, *Administrative Patent Judge.*

JUDGMENT

Final Written Decision
Determining All Challenged Claims Unpatentable
Denying Petitioner's Motion to Exclude
Denying Patent Owner's Motion to Exclude
35 U.S.C. § 318(a)

Appendix D

INTRODUCTION

Cisco Systems, Inc. ("Petitioner") filed a Petition (Paper 1, "Pet.") requesting an *inter partes* review of claims 1–20 ("the challenged claims") of U.S. Patent No. 9,160,713 B2 (Ex. 1001, "the '713 Patent"). An *inter partes* review of all challenged claims was instituted on January 24, 2019. Paper 7 ("Inst. Dec."). After institution, Centripetal Networks, Inc. ("Patent Owner") filed a Patent Owner Response (Paper 18, "PO Resp."), Petitioner filed a Reply (Paper 25, "Pet. Reply"), and Patent Owner filed a Sur-reply (Paper 27, "PO Sur-reply"). The parties also filed additional motions that remain pending, which are addressed below. An oral hearing was held on December 2, 2019. Paper 39 ("Tr.").

We have jurisdiction under 35 U.S.C. § 6. This Final Written Decision is issued pursuant to 35 U.S.C. § 318(a). As explained below, Petitioner has shown by a preponderance of the evidence that all challenged claims of the '713 Patent are unpatentable.

A. Related Cases

The parties identify as related to the present case *Centripetal Networks, Inc. v. Cisco Systems, Inc.*, Case No. 2:18-cv-00094-MSD-LRL (E.D. Va.). Pet. 2; Paper 4, 1.

B. The '713 Patent

The '713 Patent relates to filtering network data transfers. Ex. 1001, 1:57–58. When multiple data packets

are received by a system, "[a] determination may be made that a portion of the packets have packet header field values corresponding to a packet filtering rule." *Id.* at 1:58–61. The specification discloses an embodiment in which a determination is made as to whether one or more of the received packets have header field values corresponding to, for example, particular versions of Transport Layer Security (TLS) protocol specified in a packet filtering rule. *Id.* at 6:11–19, 9:19–28. Based on that determination, the packets in question may be allowed to continue to their destinations (*id.* at 9:34–42), or blocked from continuing to their destinations (*id.* at 9:56–10:1). The specification further discloses other criteria that can be applied in packet filtering rules, such as network address, port number, or protocol type. *Id.* at 5:38–7:9, Fig. 3.

C. Challenged Claims

Petitioner challenges all of the claims of the '713 Patent. Claims 1, 8, and 15 are the only independent claims. Claim 1 is illustrative and is reproduced below:

> 1. A method comprising:
>
> receiving, by a computing system provisioned with a plurality of packet-filtering rules, a first packet and a second packet;
>
> responsive to a determination by the computing system that the first packet comprises data corresponding to a transport layer security (TLS)-version value for which one or more

> packet-filtering rules of the plurality of packet-filtering rules indicate packets should be forwarded toward their respective destinations, forwarding, by the computing system, the first packet toward its destination; and
>
> responsive to a determination by the computing system that the second packet comprises data corresponding to a TLS-version value for which the one or more packet-filtering rules indicate packets should be blocked from continuing toward their respective destinations, dropping, by the computing system, the second packet.

Ex. 1001, 11:8–25.

D. Instituted Ground of Unpatentability and Asserted Prior Art

Trial was instituted on the sole ground of unpatentability asserted in the Petition:

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

Inst. Dec. 16; *see* Pet. 26–27. The parties dispute whether Sourcefire qualifies as prior art under 35 U.S.C. § 102(b), specifically whether it was publicly accessible in (or before)

1. Sourcefire 3D System User Guide, Version 4.10 (Ex. 1004, "Sourcefire").

April of 2011. *See* Pet. 27; PO Resp. 2–7; Pet. Reply 2–6; PO Sur-reply 1–7.

ANALYSIS

A. Level of Ordinary Skill

Petitioner asserts that a person of ordinary skill in the art would have had a bachelor's degree in computer science, computer engineering or an equivalent, as well as four years of industry experience. Pet. 15. In addition, Petitioner indicates a person of ordinary skill would have had "a working knowledge of packet-switched networking, firewalls, security policies, communication protocols and layers, and the use of customized rules to address cyber attacks." *Id*. Patent Owner does not dispute Petitioner's proposed definition of the level of skill in the art.[2] We agree with Petitioner's definition, and apply it herein, based on the testimony of Petitioner's expert witness, Dr. Stuart Staniford, which we find supports Petitioner's view. *See* Ex. 1003 ¶¶ 23, 62.

B. Claim Construction

For petitions filed before November 13, 2018, as here, claim terms in an unexpired patent are given their broadest reasonable construction in light of the specification of the patent in which they appear. *See* 37

2. Patent Owner's expert witness, Dr. Alessandro Orso, testified to a slightly different definition of the level of ordinary skill. *See* Ex. 2002 ¶ 43. We note that our Decision would be unchanged were we to apply Dr. Orso's proposal instead.

C.F.R. § 42.100(b) (2018); *Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2144–46 (2016); Changes to the Claim Construction Standard for Interpreting Claims in Trial Proceedings Before the Patent Trial and Appeal Board, 83 Fed. Reg. 51,340 (Oct. 11, 2018).

Patent Owner argues that the term "packet" should be construed as "IP packet." PO Resp. 18–20; PO Sur-reply 7–8. According to Patent Owner, the proper construction of "packet" within the meaning of the challenged claims excludes other types of packets, including packets that are encapsulated within an IP packet—e.g., TCP packets, application packets. *See* PO Sur-reply 7–8; Tr. 76:24–77:19. Petitioner disagrees, arguing that Patent Owner's proposed construction is too narrow and inconsistent with the Specification of the '713 Patent. We agree with Petitioner.

First, the intrinsic evidence cited by Patent Owner does not support its proposed construction. Patent Owner does not identify any special definition of "packet" in the Specification. Further, Patent Owner does not identify any aspect of the Specification that clearly indicates the term "packet," in fact, excludes certain types of packets. Instead, Patent Owner relies (PO Resp. 18–19) on a description of several kinds of packets, including "IP packets," "application packets," and "TLS Record Protocol packets." Ex. 1001, 7:62–8:2. Nothing in that description indicates the term "packet" refers only to one of those types of packets, much less to "IP packets" in particular. *See id.*

Patent Owner also relies on dependent claims 4, 11, and 18, which require that the recited "packet" further "comprises a network address." *See* PO Resp. 19. But Patent Owner does not explain sufficiently why the limitation of comprising a network address in certain dependent claims requires a "packet" *generally* to include only an "IP packet" and not other types of packets. *See id.* Indeed, these dependent claims underscore that a "packet" within the meaning of the broader independent claims, for example, is *not* necessarily required to comprise a network address. Moreover, the fact that the Specification uses both the terms "packet" and "IP packet" indicates that the '713 Patent distinguishes between a "packet" generally and specific types of packets, such as an "IP packet." *See* Pet. Reply 6–7 (noting that the Specification refers to multiple types of packets). Patent Owner's citation of certain examples in the Specification (PO Resp. 19–20) also is unpersuasive because it is axiomatic that limitations should not be read into the claims from mere embodiments. *See Superguide Corp. v. DirecTV Enters., Inc.*, 358 F.3d 870, 875 (Fed. Cir. 2004).

In addition, Patent Owner argues claim 1 requires that "the HTTPS packets are received 'by a computing system,'" which indicates they must be IP packets given that a computing system's interface receives IP packets (whereas other types of packets encapsulated within IP packets are targeted at particular "destination program[s]" on the system rather than the system itself). *See* PO Resp. 20 (citing Ex. 2002 ¶ 68). Neither Patent Owner nor Dr. Orso explains adequately, however, why a person of ordinary skill would have understood

an application packet, for example, *not* to have been received by a computing system (including the destination application on the system) when the IP packet containing that application packet *is* received by the system. *See* Pet. Reply 7.

For the above reasons, we are not persuaded that the correct construction of "packet," as recited in the challenged claims, should be limited only to "IP packet." No further express construction of this or any other claim term of the '713 Patent is necessary to resolve the issues in this case.[3] *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (holding that only claim terms in controversy require express construction, and only to the extent necessary to resolve the controversy).

C. Whether Sourcefire Qualifies as Prior Art

Patent Owner asserts that Sourcefire does not qualify as applicable prior art because it is not a printed publication. *See* PO Resp. 2–7 (citing 35 U.S.C. § 311(b)); PO Sur-reply 1–7. In determining whether a prior art reference constitutes a printed publication,

---

3. Patent Owner argues that the proper construction of "packet" excludes "reassembled application layer messages." *See*, *e.g.*, PO Resp. 19. Neither party has asserted at any time in this case that "packet" should be construed to include such messages. As discussed below, this issue relates to whether certain disclosures of the asserted prior art (involving reassembled messages) would have taught or suggested the recited "packet[s]." Thus, we address this issue in the context of our obviousness analysis below.

"the touchstone is public accessibility." *In re Bayer*, 568 F.2d 1357, 1359 (CCPA 1978); *see Blue Calypso, LLC v. Groupon, Inc.*, 815 F.3d 1331, 1348 (Fed. Cir. 2016). "A given reference is 'publicly accessible' upon a satisfactory showing that such document has been disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art exercising reasonable diligence, can locate it." *SRI Int'l, Inc. v. Internet Sec. Sys., Inc.*, 511 F.3d 1186, 1194 (Fed. Cir. 2008) (quoting *Bruckelmyer v. Ground Heaters, Inc.*, 445 F.3d 1374, 1378 (Fed. Cir. 2006))

Petitioner contends that Sourcefire was publicly available because (1) it was actually disseminated to hundreds of customers who purchased Sourcefire 3D System products, and (2) it was available on Sourcefire's support website. *See* Pet. 27; Pet. Reply 2. As explained below, we conclude that Petitioner has shown sufficiently that Sourcefire was publicly available due to its actual dissemination to customers.

According to Petitioner, Sourcefire was enclosed on a CD-ROM disk that was "included with each [Sourcefire] 3D System product offered for sale, including actual sales, beginning . . . in April 2011 through the priority date of the '713 Patent." Pet. Reply 2. Petitioner relies on the testimony of John Leone, a former employee of Sourcefire's manufacturer. Pet. 27 (citing Ex. 1005). Mr. Leone testified that Sourcefire was included with every Sourcefire 3D System product in that timeframe, and that "approximately 586 customers purchased the Sourcefire 3D System from April 2011 through March 2013 and had

access to the Sourcefire 3D System User Guide." Ex. 1005 ¶¶ 11, 19.

Additionally, Petitioner cites a press release about the relevant Sourcefire 3D System published in BusinessWire in April 2011 (Ex. 1034), a product review for the Sourcefire 3D System published by ITPro in January 2007 (Ex. 1042), and a product review for the system published by SC Media in May 2006 (Ex. 1043), as evidence establishing that the Sourcefire 3D System (including its accompanying user manual, the Sourcefire reference) was publicly marketed and sold. Pet. Reply 3–4. Patent Owner does not dispute the above facts. Rather, Patent Owner argues that these facts are insufficient to establish public accessibility under controlling case law. *See* PO Sur-reply 2–5.

Petitioner relies on *Mass. Inst. of Tech. v. AB Fortia*, 774 F.2d 1104 (Fed. Cir. 1985) ("*MIT*"). Pet. Reply 2–3. In *MIT*, a paper was orally presented at a scientific conference attended by "50 to 500 cell culturists." 774 F.2d at 1108. Copies of the paper "were distributed on request, without any restrictions, to as many as six persons." *Id.* at 1108–09. The Federal Circuit held that these facts were sufficient to establish public accessibility. *Id.* at 1109; *see also In re Klopfenstein*, 380 F.3d 1345, 1349 (Fed. Cir. 2004) ("The key to the court's finding [in *MIT*] was that actual copies of the presentation were distributed."). Petitioner also cites *Garrett Corporation v. United States*, 422 F.2d 874, 878 (Ct. Cl. 1970). Pet. Reply 3. In *Garrett*, the court held that a government report was a "printed publication" under § 102(b) because approximately 80 copies were disseminated, including to six commercial companies. 422

F.2d at 878. The court held, "distribution to commercial companies without restriction on use clearly" established that the report is a printed publication. *Id.*

Patent Owner relies on *Medtronic, Inc. v. Barry*, 891 F.3d 1368 (Fed. Cir. 2018). PO Sur-reply 2–3. In *Medtronic*, the prior art at issue was disseminated to attendees of three conferences. 891 F.3d at 1379. The Federal Circuit distinguished *Medtronic* from past cases involving references stored in repositories (e.g., libraries)—rather than considerations like indexing and cataloguing, the relevant inquiry was whether the *distribution* of the reference to certain groups of people was sufficient for public accessibility. *Id.* at 1379–80. Issues underlying that inquiry include, for example, "whether there is an expectation of confidentiality between the distributor and the recipients of the materials," as well as "[t]he expertise of the target audience." *Id.* at 1381–82. Although agreeing with the Board that "[d]istributing materials to a group of experts" is not enough for public accessibility "simply by virtue of the relative expertise of the recipients," the Federal Circuit held that the Board in that case had not sufficiently considered all of the recipients of the distributed materials, or whether all the recipients were expected to hold the distributed materials in confidence. *Id.* at 1382–83.

Based on the above facts and case law, we conclude that Sourcefire was publicly accessible based on undisputed facts. It is undisputed that the Sourcefire 3D System was publicly marketed and sold, and that the Sourcefire reference was actually distributed to over

500 customers of the Sourcefire 3D System. Ex. 1005 ¶¶ 11, 19. This vastly exceeds the distribution to six people in *MIT* and distribution of 80 copies in *Garrett*. It is also undisputed that the customers who received Sourcefire included entities interested in network security products, including persons of ordinary skill in the art. *See* Tr. 54:5–17; *see also* Ex. 1004, 1, 32–33 (identifying Sourcefire as a "User Guide" and indicating Sourcefire provides information for network administrators); Ex. 1005 ¶ 5 (indicating Sourcefire was drafted in consultation with, and reviewed by, engineers who designed the Sourcefire system). Moreover, similar to *MIT* and as discussed in *Medtronic*, the record indicates that the recipients of Sourcefire were not subject to confidentiality requirements restricting use or further distribution. *See* Ex. 1004, 2 (Sourcefire copyright page stating, "You may use . . . and otherwise copy and distribute [Sourcefire] solely for non-commercial use").[4,5] Patent Owner has not identified any evidence of such restrictions on recipients of Sourcefire. Although Patent Owner asserts that *MIT* and *Klopfenstein* are distinguishable because they

4. All citations to Sourcefire refer to the document's original pagination.

5. Both of the decisions by Board panels cited by Patent Owner (PO Sur-reply 3–4) are distinguishable on their facts, including because both involved references that were subject to restrictions prohibiting their reproduction or further dissemination. *See ASM IP Holding B.V., v. Kokusai Elec. Corp.*, IPR2019-00369, Paper 8, at 18 (PTAB June 27, 2019); *VMAC Global Techs. Inc., v. Vanair Mfg, Inc.*, IPR2018-00670, Paper 9, at 13–14 (PTAB Aug. 10, 2018). In *ASM*, the panel further noted that no evidence of actual dissemination to interested artisans. *See ASM*, Paper 8, at 17.

involved "the free distribution of academic documents to conference and meeting attendees" (PO Sur-reply 4–5), case law indicates that distribution to commercial entities also may be sufficient. *See Garrett*, 422 F.2d at 878; Pet. Reply 3.

Patent Owner argues, however, that dissemination is insufficient and that Petitioner must additionally demonstrate that a person of ordinary skill would have been able to locate Sourcefire through reasonable diligence. PO Resp. 3, 5–7; PO Sur-reply 2 (citing *Acceleration Bay, LLC v. Activision Blizzard, Inc.*, 908 F.3d 765, 772 (Fed. Cir. 2018)). The Federal Circuit has indicated that public accessibility is established by showing that the reference was "disseminated *or otherwise* made available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, can locate it." *Acceleration Bay*, 908 F.3d at 772 (quoting *Jazz Pharm., Inc. v. Amneal Pharm., LLC*, 895 F.3d 1347, 1355–56 (Fed. Cir. 2018)) (emphasis added). Here, Petitioner has shown that Sourcefire was "disseminated" to interested artisans; thus, it is unnecessary to additionally show that it was also "otherwise" made available to them. *See Klopfenstein*, 380 F.3d at 1349 ("The key to the court's finding [in *MIT*] was that actual copies of the presentation were distributed."). We note the Federal Circuit has held that if the latter is shown (i.e., accessibility through reasonable diligence), it is unnecessary to show actual access or dissemination. *See*, *e.g.*, *Jazz Pharm.*, 895 F.3d at 1356 ("If accessibility is proved, there is no requirement to show that particular members of the public actually received the information.").

Consequently, we are unpersuaded that Sourcefire was not publicly accessible due to various issues surrounding whether the Sourcefire website made the reference adequately accessible, given the evidence of actual dissemination through sales and commercial distribution. *See* PO Resp. 5–7; PO Sur-reply 2–3, 5–7. Nor are we persuaded by Patent Owner's contention that the cost of the Sourcefire 3D System was too high and, thus, a skilled artisan would not have been able to access Sourcefire. *See* PO Sur-reply 4. The cost did not prevent over 500 customers from actually obtaining Sourcefire by purchasing Sourcefire 3D System products. Moreover, there is no evidence in the record indicating that sales of the relevant Sourcefire products were restricted or limited to only certain customers, or that the cost[6] of acquiring a Sourcefire 3D System product was prohibitively high to the relevant artisans.

Additionally, Patent Owner cites *In re Bayer*, 568 F.2d 1357 (CCPA 1978), arguing the prior art in *Bayer* (a thesis) was held not to have been publicly accessible despite actual distribution to faculty on a graduate committee reviewing the thesis. PO Sur-reply 3. In *Bayer*, the relevant issue was whether the appellant's "uncatalogued, unshelved thesis, by virtue of its accessibility to the graduate committee,"

6. The record includes evidence of a range of prices for various configurations of Sourcefire 3D System products, from $1,385 to £25,000. Ex. 1042, 1; Ex. 1043, 1. Based on Mr. Leone's testimony, Sourcefire would have been distributed with the purchase of any of these products. Ex. 1005 ¶ 11 (testifying that Sourcefire was "included with each Sourcefire 3D System appliance (*e.g.*, 3D Sensor, Defense Center) sold to a customer").

constituted a printed publication. 568 F.2d at 1359. The Federal Circuit has clarified *Bayer*, explaining that the thesis was held not publicly accessible because "a work is not publicly accessible if the only people who know how to find it are the ones who created it," such as the faculty on the graduate committee reviewing and advising on student theses. *See Samsung Elecs. Co. v. Infobridge Pte. Ltd.*, 929 F.3d 1363, 1371–72 (Fed. Cir. 2019). Thus, *Bayer* is inapposite here, where Sourcefire was distributed to over 500 customers.

In summary, we find that a preponderance of the evidence establishes that Sourcefire was distributed commercially through sales of the Sourcefire 3D System to over 500 customers, including interested persons of ordinary skill, and that those customers were not subject to any restriction or expectation of confidentiality with regard to its use or further distribution. Therefore, we conclude that Sourcefire was publicly accessible, and that it constitutes prior art under § 102(b).

D. Alleged Unpatentability Under § 103(a)

A claim is unpatentable under § 103 if the differences between the claimed subject matter and the prior art are "such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). 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 skill in the art; and (4) objective evidence of nonobviousness, i.e., secondary considerations. *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*, 550 U.S. at 418 (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)).

1. Overview of 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. The system operates via "3D Sensors" that can each run the Sourcefire "Intrusion Prevention System" (IPS), which allows monitoring of networks for attacks by examining packets for malicious activity. *Id.* at 33–34. Users can create custom "intrusion rules" to examine packets for attacks and manage the rules across all the 3D Sensors in the system through a centralized "Defense Center." *Id*. at 34, 254.

Intrusion rules can be "pass" rules, "alert" rules, or "drop" rules. *Id.* at 761. If a pass rule is met, the network

traffic in question is ignored (and allowed to continue). *Id.* Conversely, if a drop rule is met, the packet is dropped and an "event" is generated. *Id.* Rules can be written based on "keywords" and their "arguments," i.e., the possible values of the keyword. *Id.* at 762–763.

The Sourcefire 3D System also features "preprocessors" that can facilitate processing of network traffic by identifying and decoding certain types of traffic, such as HTTP (hypertext transfer protocol) and SSL (secure sockets layer) traffic. *Id.* at 513–514. The SSL preprocessor, for example, can be used to identify encrypted traffic that IPS cannot analyze, thereby enabling IPS to ignore (pass) the encrypted packets and avoid wasting resources trying to inspect them. *Id.* at 596.

2. Independent Claim 1

Claim 1 recites a three-step method. According to Petitioner, Sourcefire teaches a computing system provisioned with a plurality of packet-filtering rules that receives first and second packets, as recited in the first step of claim 1, in its description of the Sourcefire 3D System applying intrusion rules to incoming network traffic. Pet. 40–42 (citing Ex. 1003 ¶¶ 135–139). Patent Owner does not dispute that Sourcefire teaches this limitation. Sourcefire discloses a system with 3D Sensors "us[ing] intrusion rules to examine the decoded packets for attacks based on patterns." Ex. 1004, 254. The packets are captured from the network packet stream by the 3D Sensor, which decodes them to enable its preprocessors and rules engine to inspect packet headers to determine

whether any rules are triggered. *Id*. at 257–259. We find that Sourcefire teaches the first step of the method of claim 1.

With respect to the second and third steps, Petitioner contends that Sourcefire teaches forwarding packets or dropping them, based on rules that indicate whether they should be forwarded or dropped, in its description of "pass" and "drop" rules that, when triggered, allow packets to continue to their destination or drop them, respectively. Pet. 42–45 (citing Ex. 1004, 761; Ex. 1003 ¶¶ 141–142, 150–151). Further, according to Petitioner, Sourcefire teaches that a pass or drop rule can be triggered by a determination that a packet's header indicates a particular TLS version. *Id.* at 43–44. Specifically, Petitioner asserts that Sourcefire teaches the crafting of intrusion rules using the "ssl_version keyword," which can be set to detect particular SSL or TLS versions. *Id.* (citing Ex. 1004, 597–601, 697–701, 827–828; Ex. 1003 ¶¶ 124–128, 142–144).

Patent Owner contends that Sourcefire fails to teach the second and third steps of claim 1 because Sourcefire does not teach any determination that a first or second packet "comprises data corresponding to a transport layer security (TLS)-version value." *See* PO Resp. 24–36. According to Patent Owner, Sourcefire instead teaches only determining whether a reconstructed *message* (and associated session) corresponds to a particular TLS version, not individual packets within that message. *See id.* at 24–25 (citing Ex. 2002 ¶¶ 77–78). Further, Patent Owner maintains that Sourcefire extracts TLS version information, before any intrusion rules are applied,

from a reassembled handshake message. *Id.* at 25–28 (citing Ex. 2002 ¶ 82). Specifically, Patent Owner asserts that intrusion rules do not assess whether any packet comprises TLS version information but rather just receive that information, which was previously extracted by an SSL preprocessor from the handshake message for the session. *Id.* at 26–27.

As an initial matter, even assuming *arguendo* that Patent Owner is correct that Sourcefire discloses only obtaining TLS version information from reconstructed TCP *messages*, we find that Sourcefire still teaches a determination that a *packet* comprises TLS version information. It is undisputed that such reconstructed messages consist of packets. *See* Tr. 35:4–6, 39:14–16; Ex. 1041, 161:22–162:10; Ex. 2001, 122:13–17. According to Patent Owner, the technology of the claimed invention "works because the [TLS version] information we're looking for is always going to be in the first packet." Tr. 35:6–8. In other words, as Patent Owner acknowledged, a person of ordinary skill would have understood that when TLS protocol is used, information about TLS version always is located in the packet header of the first packet in the message. *See id.* at 42:10–43:1; Ex. 1041, 194:17–23.

The sole difference in this regard between claim 1 and the teachings of Sourcefire, according to Patent Owner, is that claim 1 recites determining that a packet (e.g., the first packet of a message) comprises TLS version data, whereas Sourcefire teaches determining that a message comprises TLS version data *by extracting that data from the first packet of the message*. *See* Tr. 40:3–12. We find

that a person of ordinary skill would have understood that, in both instances, the relevant data is located in the first packet of the message (e.g., a handshake message). Whether the system of Sourcefire itself recognizes that fact or deduces it is irrelevant; the relevant question is whether a *person of ordinary skill* would have been taught the recited determination (i.e., determining that a packet comprises TLS version data) based on Sourcefire and his/her own knowledge. *See In re Keller*, 642 F.2d 413, 425 (CCPA 1981) ("The test for obviousness is not . . . that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art."). Furthermore, as Petitioner notes (Pet. Reply 11–12), claim 1 does not require "inspection" of "application header values" of packets (*see* PO Resp. 22–23), and instead it broadly encompasses any method of making the recited determination.[7]

Additionally, we also are unpersuaded by Patent Owner's argument that the rules using the "ssl_version keyword" in Sourcefire do not teach the recited determination because the TLS version information was extracted earlier by the SSL preprocessor. PO

7. To the extent Patent Owner contends that claim 1 should be limited by a particular example in the Specification of the '713 Patent, which purportedly describes "how to determine that a packet comprises" TLS version data (PO Sur-reply 10–11), Patent Owner has not persuasively explained why doing so is warranted, and we decline to read any such limitations into the claim. *See Superguide*, 358 F.3d at 875.

Resp. 26–29; PO Sur-reply 12–13. This argument is not commensurate with the scope of the claim. Claim 1 recites a "determination . . . that the [first/second] packet comprises data corresponding to a [TLS version] for which one or more packet-filtering rules . . . indicate packets should be [forwarded/blocked]." The claim does not require that the determination be performed by the rule itself, or that the determination of the TLS version and whether it meets the criterion of the rule must be performed at the same time or by the same structure.

Instead, we find that a preponderance of the evidence supports Petitioner's view that Sourcefire teaches the recited "determination[s]" of claim 1. We agree with Petitioner (Pet. 42–44) that Sourcefire teaches both "pass" (i.e., forward) and "drop" (i.e., block) versions of intrusion rules using the ssl_version keyword, which examines TLS version data. Ex. 1004, 761, 827–828; Ex. 1003 ¶¶ 141–144. As discussed above, Sourcefire describes obtaining the TLS version data from the first packet of a message using TLS protocol (e.g., a handshake message), and that data is provided to the rule engine applying the intrusion rules (*see* Ex. 1004, 827), thereby teaching a determination that the message—and, thus, the first *packet* of the message—corresponds to a TLS version that an intrusion rule indicates should be forwarded or blocked. Whether or not there are *other* packets that do not undergo such a determination is inapposite and outside the scope of claim 1. *See* PO Sur-reply 12; Tr. 37:7–17, 38:12–16.

We also find persuasive Petitioner's argument that, even after the handshake is completed to establish

an encrypted session, Sourcefire teaches that each subsequent TLS-encrypted message in the session (and, thus, the first packet of each such message) can be assessed by the intrusion rules. *See* Pet. Reply 17–18. If the SSL preprocessor detects that the session is encrypted (i.e., it uses SSL or TLS protocol), IPS "can" be set to ignore (i.e., pass/forward) all packets in the session. *See* Ex. 1004, 597–599. As Petitioner notes, however, Sourcefire's disclosure that IPS "can" be set to do this indicates that it can also *not* be set to do this, i.e., the system can be set such that packets are *not* passed based solely on the fact that the session was determined to be a TLS session. *See* Pet. Reply 17–18. Consequently, we are unpersuaded by Patent Owner's argument that Sourcefire is deficient because it teaches only that TLS version for an entire session is determined solely by the handshake. *See* PO Resp. 25–27.

We further find that preponderant evidence establishes that Sourcefire teaches the forwarding or blocking of the packet (and message) responsive to the determination, as recited in claim 1. *See* Ex. 1004, 761. Patent Owner argues, however, that Sourcefire does not disclose blocking packets based on SSL/TLS version. PO Resp. 36–38; PO Sur-reply 15–16. Specifically, Patent Owner asserts that "Sourcefire vaguely references identifying, but not blocking, traffic using SSL version 2." PO Resp. 36–37 (citing Ex. 1004, 827). Patent Owner also faults Petitioner for failing to allege that Sourcefire makes such a disclosure rather than merely indicating Sourcefire "could have" been modified to block packets. *See* PO Sur-reply 15. The question, however, is not whether Sourcefire explicitly

discloses an example of blocking packets based on SSL/TLS version, but rather whether Sourcefire would have taught or suggested doing so to a person of ordinary skill in the art. *See Keller*, 642 F.2d at 425. As discussed above, Sourcefire describes designing both pass and drop rules, and also describes the use of the ssl_version keyword in rules. *See* Ex. 1004, 761 ("For a *drop* rule . . . IPS drops the packet and generates an event."), 827–828. We find that these disclosures would have been sufficient to teach an artisan of ordinary skill to block packets based on the SSL/TLS version of the packet. *See* Ex. 1003 ¶¶ 141–144, 150–152.

Moreover, to the extent Patent Owner argues that a motivation is needed (and was not proven) to "modify" Sourcefire to teach the recited blocking of packets (PO Resp. 38; PO Sur-reply 15–16), we find that no "modification" would have been required. As discussed above, Sourcefire explains the use of the ssl_version keyword in designing rules based on TLS version information, and also teaches that rules can be drop rules that cause packets to be dropped when triggered. Thus, designing drop rules that drop packets based on TLS version information would have constituted following the direct teachings of Sourcefire without "modification," and, thus, no additional "motivation" to modify Sourcefire would have been required. Moreover, even if we assume *arguendo* that such a motivation were required, we note that "the inferences and creative steps a person of ordinary skill in the art would employ" can supply a motivation to combine or modify teachings, and "[a] person of ordinary skill is also a person of ordinary creativity, not

an automaton." *KSR*, 550 U.S. at 401, 421. Based on the evidence of Sourcefire's teachings regarding this aspect of claim 1, we find that a person of ordinary skill would have been sufficiently motivated and informed by Sourcefire to design intrusion rules with the ssl_version keyword as discussed above. *See*, *e.g.*, Pet. 45 (citing Ex. 1004, 254, 435–439, 761; Ex. 1003 ¶¶ 150–151); *see also id.* at 30–32 (citing Ex. 1004, 762–763; Ex. 1003 ¶¶ 109, 112–116), 36–39 (citing Ex. 1004, 597–601, 697–701, 827–828; Ex. 1003 ¶¶ 124–128).[8]

For the above reasons and on the complete record after trial, we conclude Petitioner has shown that a preponderance of the evidence indicates that Sourcefire teaches each limitation of claim 1.

3. Dependent Claims 2–7

Claims 2–7 depend from claim 1. The Petition sets forth arguments and evidentiary support for each of the claims. Pet. 45–57. Petitioner explains that Sourcefire discloses rules other than TLS version rules—including "5-tuple" rules based on protocol type, and source or destination IP addresses or ports—which teaches that a second portion

8. Patent Owner argues that record evidence indicates that a skilled artisan would have been taught not to block data traffic using TLS version 1.0, despite known security vulnerabilities, because more secure versions of TLS protocol were not yet widely used. PO Resp. 37–38 (citing Ex. 2002 ¶ 95; Ex. 1037, 8). Claim 1, however, is not limited to blocking TLS version 1.0 packets, and we find that Sourcefire's teachings similarly encompass designing rules to pass or drop packets based on any TLS version.

of packets (as well as the first portion) can be filtered to be forwarded or dropped (based on such other rules) without applying the TLS version rule applied to the first portion of packets, as recited in claims 2–4. *Id.* at 46–50 (citing Ex. 1003 ¶¶ 154, 157, 160–161, 163, 165, 168, 171). The Petition also explains how Sourcefire discloses an "HTTP inspect preprocessor" that can detect HTTP methods such as GET, PUT, POST, and CONNECT, which teaches determining that a packet comprises data corresponding to such HTTP methods, as recited in claims 5 and 6. *Id.* at 50–55 (citing Ex. 1003 ¶¶ 174–180, 183). Petitioner further explains how a person of ordinary skill would have understood Sourcefire to teach determining that certain packets comprise data associated with Hypertext Transfer Protocol Secure (HTTPS), as recited in claim 7, by teaching that TCP port 443 (a standard HTTPS port) or TLS version value (indicating TLS data, which is also HTTPS data) can be used in designing and applying rules. *Id.* at 55–57 (citing Ex. 1003 ¶¶ 186, 187, 190). We agree with Petitioner's analysis and find that the cited evidence supports its contentions by a preponderance of the evidence that Sourcefire teaches all of the limitations of claims 2–7.

Patent Owner does not present any arguments specific to claims 5–7. With regard to claims 2–4, Patent Owner argues that Petitioner failed to show that "Sourcefire explicitly discloses applying the TLS-version value packet-filtering rules recited in in the independent claims to a first portion of packets and not a second portion of packets," or "that a [person of ordinary skill] ***would*** have written such a rule." PO Resp. 41. Explicit disclosure is not, however,

required for obviousness. Petitioner, in response, explains (Pet. Reply 21–24) how Sourcefire teaches applying different sets of intrusion rules to different groups of packets. *See* Ex. 1004, 259, 766–768. Patent Owner does not respond to this evidence. Upon reviewing the relevant arguments and evidence, we find Petitioner's position persuasive.

4. Claims 8–20

Independent claim 8 recites a system comprising a processor and a memory storing instructions that, when executed, perform substantially the same steps recited in claim 1. Similarly, claims 9–14 depend from claim 8 and recite limitations substantially the same as those of claims 2–7. The Petition explains how Sourcefire discloses that each 3D Sensor includes a processor, memory, and disk storage with the instructions that control the operations of the 3D Sensor. Pet. 57–58 (citing Ex. 1004, 33–34, 106–107; Ex. 1003 ¶ 192). Petitioner then relies on the same arguments and evidence as for claims 1–7 for the remaining elements of claims 8–14 that correspond to the limitations of claims 1–7. *Id.* at 57–62.

Independent claim 15 recites non-transitory computer readable media comprising instructions that, when executed, cause substantially the same steps recited in claim 1 to be performed. Similarly, claims 16–20 depend from claim 15 and recite limitations substantially the same as those of claims 2–7 (the limitations of claim 19 correspond to the limitations of both claims 5 and 6). Petitioner relies on the disk storage containing the

instructions controlling the operation of a 3D Sensor as teaching the recited computer readable media. *Id.* at 63 (citing Ex. 1004, 33–34, 106–107; Ex. 1003 ¶ 199). As with the system claims, Petitioner then relies on the same arguments and evidence as for claims 1–7 for the remaining elements of claims 15–20 that correspond to the limitations of claims 1–7. *Id.* at 62–67.

Patent Owner presents no arguments regarding these claims other than those for claim 1–4, discussed above. For essentially the same reasons as for claims 1–7, the arguments and evidence in the Petition are persuasive as to claims 8–20, and we find a preponderance of the cited evidence supports Petitioner's contentions that Sourcefire teaches each of the limitations of claims 8–20.

5. Secondary Considerations of Non-Obviousness

Before determining whether a claim is obvious in light of the prior art, we consider any relevant evidence of secondary considerations—i.e., objective indicia—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 presents evidence of three such considerations: (1) long-felt but unmet need, (2) industry praise, and (3) commercial success/licensing. PO Resp. 42–53.

"In order to accord substantial weight to secondary considerations in an obviousness analysis, the evidence of secondary considerations must have a nexus to the claims, i.e., there must be a legally and factually sufficient connection between the evidence and the patented invention." *Fox Factory, Inc. v. SRAM, LLC*, 944 F.3d 1366, 1373 (Fed. Cir. 2019) (internal quotations omitted). A nexus is presumed when "the patentee shows that the asserted objective evidence is tied to a specific product and that product 'embodies the claimed features, and is coextensive with them.'" *Id.* (quoting *Polaris Indus., Inc. v. Arctic Cat, Inc.*, 882 F.3d 1056, 1072 (Fed. Cir. 2018)). If the product is not coextensive with the claims at issue—e.g., if the patented invention is only a component of the product—the patentee is not entitled to a presumption of nexus. *See id.* (citing *Demaco Corp. v. F. Von Langsdorff Licensing Ltd.*, 851 F.2d 1387, 1392 (Fed. Cir. 1988)).

a. Long-Felt But Unmet Need and Failure of Others

According to Patent Owner, "the '713 Patent satisfied a long-felt need . . . namely, how to protect against '[a] category of cyber attack known as exfiltrations,'" which others had failed to meet. PO Resp. 44. With respect to nexus, Patent Owner asserts that the challenged claims "are applied on a packet-by-packet basis" and are "applied to individual packets" such that "time- and resource-intensive packet reassembly procedures" are unnecessary. *Id.* at 49–50 (citing Ex. 2002 ¶¶ 108–109); *see also* PO Sur-reply 18–19. Further, Patent Owner points to "leveraging [cyber threat intelligence] in a manner that applied

TLS-version value criteria to only those packets meeting specified packet header criteria," and that the claimed techniques are "scalable." *Id.* at 45–46. Patent Owner also relies on a paper (the "ESG Paper") that praises Patent Owner's "RuleGATE" product while identifying certain purported challenges to "operationalizing threat intelligence." *Id.* at 48–49 (citing Ex. 2006, 4).[9]

Patent Owner's nexus arguments and evidence, however, are insufficient to establish a nexus between the alleged long-felt but unmet need, and the claimed invention. First, no analysis is presented to demonstrate that the RuleGATE product is coextensive with any claim of the '713 Patent. Thus, Patent Owner is not entitled to a presumption of nexus. *See Fox Factory*, 944 F.3d at 1373. Second, insufficient analysis is presented to show that the evidence of a purported long-felt but unmet need is connected to the patented invention. Patent Owner does not adequately explain how the purported "packet-by-packet" nature of the claimed method specifically addresses the threat of exfiltrations. Nor does Patent Owner explain how "cyber threat intelligence" is related to any challenged claim, or how the patented invention achieves a "scalable" solution to exfiltrations. *See* Tr. 56:4–11 (Patent Owner acknowledging the claims do not require

9. Petitioner argues that the ESG Paper is not objective evidence of non-obviousness because it is a report commissioned and paid for by Patent Owner. Pet. Reply 24–25. We decline to disregard this evidence, or Dr. Orso's testimony about it, entirely. We find, however, that the nature and circumstances around the genesis of the ESG Paper diminish the persuasive weight it should be accorded.

scalability or "larger rule sets" than prior devices). With respect to the "challenges" reported in the ESG Paper—i.e., "[l]ack of automation," "the inability to use feeds 'in a meaningful way to live network traffic,'" and "the ability to 'turn[] [cyber threat intelligence] into actionable insight'" (PO Resp. 48)—Patent Owner provides no analysis as to how the patented invention purportedly meets those challenges. Moreover, the paper praising Patent Owner's product identifies features contributing to the product's solutions that are not tied to any aspect of the challenged claims, such as "dynamically monitor[ing] for advanced threats using intelligence," and "converting indicators to rules that drive actions across the risk spectrum, i.e., logging, content capture, mirroring, redirection, shielding, and advanced threat detection." Ex. 2006, 7.

Therefore, we conclude that a nexus was not proven between the purported long-felt but unmet need(s) identified by Patent Owner and the patented invention of the '713 Patent.

b. Industry Praise

Patent Owner cites the ESG Paper (Ex. 2006) as well as a Gartner article (Ex. 2007) and an American Banker article (Ex. 2011) as evidence of industry praise. PO Resp. 50–52. Similar to its long-felt need contentions, however, Patent Owner does not provide sufficient analysis or explanation to establish the requisite nexus. Patent Owner again provides no analysis demonstrating that any Centripetal product is coextensive with the challenged claims, so no presumption of nexus is applied. *See Fox*

Factory, 944 F.3d at 1373. Additionally, the cited praise of Centripetal products is not linked sufficiently to the challenged claims, including because Patent Owner failed to address lauded features with no relationship to the claims.

For example, Patent Owner cites the ESG Paper as praising the "high performance" of its product, its ability to process "hundreds of millions of indicators from thousands of feeds," "synthesizing into a network policy," "complex filtering rule[s]" with "at-least a dozen unique fields which had to be evaluated and applied bi-directionally and without state," etc. Ex. 2006, 7. None of these features appear to be in the challenged claims. Patent Owner does not address whether they are part of the claimed invention or, if not, their relative contribution to the industry praise compared to any actual features of the claimed invention.

Regarding the Gartner article, Patent Owner notes that Gartner praises its product's "ability to instantly detect and prevent malicious network connections based on millions of threat indicators at 10-gigabit speeds," "the largest number of third-party threat intelligence service integrations," and using "5 million indicators simultaneously." Ex. 2007, 5; *see* PO Resp. 51. Again, insufficient analysis is presented to address how these features relate to the challenged claims. Patent Owner's reference to the American Banker article similarly suffers from a lack of explanation. *See* PO Resp. 51.

The only nexus explanation provided is a conclusory assertion that "the salutary benefits of Centripetal's

[praised products] are made possible in large part by the '713 Patent's network layer, packet-by-packet, rule enforcement that foregoes deep inspection at the application layer." PO Resp. 51–52. Dr. Orso's testimony cited in support of this statement is merely a near-verbatim copy of this conclusory statement with no additional explanation. *See* Ex. 2002 ¶ 112; 37 C.F.R. § 42.65(a) ("Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight."). As a result, we find that Patent Owner has not established a sufficient nexus between the cited industry praise and the invention of the challenged claims.

c. Commercial Success and Licensing

Finally, Patent Owner contends that the commercial success of its RuleGATE product as well as a license to the '713 Patent taken by Keysight Technologies are compelling secondary considerations of non-obviousness. PO Resp. 52–53. We disagree.

First, we note that the sole evidence cited for the commercial success of the RuleGATE product, a declaration by Mr. Jonathan Rogers of Centripetal, makes no mention whatsoever of the '713 Patent. *See* Ex. 2016. Rather, the Rogers Declaration is testimony that was submitted in a different *inter partes* review challenging a different patent. *See id*. As such, there is no record evidence supporting any nexus between the matters in Mr. Rogers' testimony on alleged commercial success and the '713 Patent.

Second, as Patent Owner itself admits (PO Resp. 53), the Keysight license was a "worldwide, royalty-bearing, non-transferable, irrevocable, nonterminable, nonexclusive license to Centripetal's worldwide patent portfolio." Ex. 2012, 88. No information is provided about the relevant details of this license—e.g., how many patents comprise the portfolio, the relative contributions of the patents in the portfolio to the value of the license—such that we could discern whether Keysight took the license "out of recognition and acceptance of the subject matter claimed" in the '713 Patent. *See In re GPAC Inc.*, 57 F.3d 1573, 1580 (Fed. Cir. 1995). In fact, the record evidence indicates that this license was taken to settle litigation (Ex. 2012, 88), which diminishes its probative value as an indicator of non-obviousness. *See GPAC*, 57 F.3d at 1580. As such, we find that Patent Owner has not provided sufficient evidence to establish the requisite nexus between the Keysight license and the '713 Patent. *See id.*

6. Conclusion as to Obviousness

As discussed above, Petitioner has shown by a preponderance of the evidence that Sourcefire teaches each limitation of each challenged claim. We further determine that Petitioner's showing that the claims are taught by Sourcefire is very strong, particularly in comparison to Patent Owner's showing with respect to the asserted secondary considerations of obviousness. As discussed above, we find that Patent Owner has not established the requisite nexus between the challenged claims and *any* of the asserted secondary considerations. As such, we are unable to accord them any substantial weight. *See Fox Factory*, 944 F.3d at 1373. Therefore,

in weighing the totality of the evidence of record and the strength of the parties' showings on the inquiries underlying the question of obviousness, we conclude that Petitioner has met its overall burden of proving by a preponderance of the evidence that each of the challenged claims would have been obvious in view of Sourcefire.

E. Motions to Exclude

1. Petitioner's Motion to Exclude (Paper 29, "Pet. Mot.")

Petitioner moves to exclude Exhibits 2003, 2005–2007, 2011–2013, and 2016. Pet. Mot. 2. Exhibits 2003 and 2005 did not form the basis for any aspect of this Decision. As such, Petitioner's Motion with respect to those exhibits is moot.

For Exhibit 2016, the Rogers Declaration, Petitioner asserts that it should be excluded under Rules 401, 402, 403, and 602 of the Federal Rules of Evidence. Pet. Mot. 10–11. We agree with Patent Owner that exclusion is unwarranted. Paper 33, 4–5. Mr. Rogers testifies in the Declaration about his position at Centripetal, his responsibilities ("overseeing all operations of the business"), and his familiarity with Centripetal's licensing practices. Ex. 2016 ¶ 3. We are satisfied that this testimony establishes sufficient personal knowledge of the subject matter of his testimony, which concerns Centripetal's customers and its RuleGATE product. *See generally* Ex. 2016. Thus, we deny Petitioner's objection under Rule 602. With regard to Rules 401, 402, and 403, we note that Patent Owner relies on Exhibit 2016 to support its arguments for

commercial success, which specifically note the alleged success of the RuleGATE product. PO Resp. 52. Although the Rogers Declaration addresses a different patent than the '713 Patent, its testimony regarding the RuleGATE product and Centripetal's customers generally meets the threshold for relevance, and its purported shortcomings as evidence go to its persuasive weight rather than its admissibility. We also discern no risk of unfair prejudice. Thus, Petitioner's objection under Rules 401, 402, and 403 also are denied.

With respect to Exhibits 2005–2007 and 2011–2013, Petitioner argues they should be excluded under Rules 401, 402, 403, 901, and as hearsay (under Rule 802). Pet. Mot. 7–9. We are not persuaded. Each of these exhibits is cited by Patent Owner as evidence supporting its arguments regarding secondary considerations of non-obviousness, including as evidence of industry praise and the existence of a relevant license. *See* PO Resp. 46–53. Although they may not identify the '713 Patent specifically (Pet. Mot. 7), we determine that they meet the threshold for relevance nonetheless, and we discern no risk of unfair prejudice, confusion, or waste of time. Regarding authentication, we note that the Declaration of Jeffrey H. Price (Ex. 2017) provides evidence of the source of each of these exhibits, and we find that this information along with the distinctive characteristics of the exhibits themselves (including dates, titles, publication names, etc.) provide the necessary basis for authentication.[10] With respect to Petitioner's hearsay

10. We further note that Exhibits 2007 and 2011 are printed material purporting to be from news sources, which are self-authenticating under Rule 902(6).

objections, we conclude first that Exhibits 2007 and 2011 are not hearsay because they are not relied on for the truth of the matters asserted. *See* Fed. R. Evid. 801(c). These exhibits are cited only as evidence of industry praise; their relevance lies in that they include statements from the industry allegedly praising Centripetal's invention, not in whether that praise is true or accurate. *See* PO Resp. 51. For the remaining exhibits, we deny Petitioner's hearsay objection under Rule 807 because we conclude that the totality of the circumstances provides sufficient indicia of trustworthiness—for example, these exhibits are contemporaneous documents by third parties produced for purposes that indicate their statements are likely reliable (e.g., Keysight's official Annual Report (Ex. 2012))—and these exhibits generally are highly probative on the points underlying Patent Owner's secondary considerations allegations (e.g., industry praise) compared to different evidence reasonably available to Patent Owner.

For the above reasons, we are not persuaded that any of these exhibits should be excluded and, thus, we deny Petitioner's Motion to Exclude.

2. Patent Owner's Motion to Exclude (Paper 30, "PO Mot.")

Patent Owner moves to exclude Exhibits 1010, 1011, 1013–1039, and 1044. PO Mot. 1. With the exception of Exhibit 1034, none of the other exhibits formed the basis for any aspect of this Decision. Thus, Patent Owner's Motion is moot as to those exhibits.

For Exhibit 1034, Patent Owner objects on the basis of Rule 901. *Id.* We agree with Petitioner, however, that the distinctive characteristics of Exhibit 1034—e.g., the BusinessWire logo and trademarks, URL, date, and general appearance of the document—provide the necessary basis for authentication. *See* Paper 31, 7. We further agree that Exhibit 1034 is sufficiently akin to a newspaper or periodical article such that the exhibit is self-authenticating under Rule 902(6). *See id.* at 7–8.

For the above reasons, we are not persuaded that any of these exhibits should be excluded and, thus, we deny Patent Owner's Motion to Exclude.

CONCLUSION[11]

For the foregoing reasons, Petitioner has shown by a preponderance of the evidence that the challenged claims of the '713 Patent are unpatentable, as summarized in the following table:

---

11. 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).

Appendix D

Claims	35 U.S.C. §	Reference(s)
1–20	103(a)	Sourcefire
Overall Outcome		

Claims Shown Unpatentable	Claims Not Shown Unpatentable
1–20	
1–20	

ORDER

In consideration of the foregoing, it is hereby:

ORDERED that the challenged claims of the '713 Patent are held unpatentable as obvious under 35 U.S.C. § 103(a) in view of Sourcefire;

FURTHER ORDERED that Petitioner's Motion to Exclude (Paper 29) is *denied* as set forth above;

FURTHER ORDERED that Patent Owner's Motion to Exclude (Paper 30) is *denied* as set forth above;

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

APPENDIX E — JUDGMENT OF THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE PATENT TRIAL AND APPEAL BOARD, IPR2018-01437, DATED MAY 18, 2020

UNITED STATES PATENT
AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL
AND APPEAL BOARD

CISCO SYSTEMS, INC.,

Petitioner,

v.

CENTRIPETAL NETWORKS, INC.,

Patent Owner.

IPR2018-01760

Patent 9,413,722 B1

Before BRIAN J. McNAMARA, J. JOHN LEE, and JOHN P. PINKERTON, *Administrative Patent Judges.*

LEE, *Administrative Patent Judge.*

Appendix E

JUDGMENT
Final Written Decision
Determining Some Challenged Claims Unpatentable
Denying Petitioner's Motion to Exclude
Denying Patent Owner's Motion to Exclude
35 U.S.C. § 318(a)

INTRODUCTION

Cisco Systems, Inc. ("Petitioner") filed a Petition (Paper 1, "Pet.") requesting an *inter partes* review of claims 1–25 ("the challenged claims") of U.S. Patent No. 9,413,722 B1 (Ex. 1001, "the '722 Patent").[1] An *inter partes* review of all challenged claims was instituted on May 20, 2019. Paper 9 ("Inst. Dec."). After institution, Centripetal Networks, Inc. ("Patent Owner") filed a Patent Owner Response (Paper 14, "PO Resp."), Petitioner filed a Reply (Paper 20, "Pet. Reply"), and Patent Owner filed a Sur-reply (Paper 26, "PO Sur-reply"). The parties also filed motions to exclude evidence, which are addressed below. An oral hearing was held on February 20, 2020. Paper 40 ("Tr.").

We have jurisdiction under 35 U.S.C. § 6. This Final Written Decision is issued pursuant to 35 U.S.C. § 318(a). As explained below, Petitioner has shown by a preponderance of the evidence that all challenged claims of the '722 Patent are unpatentable.

1. On its face, the '722 Patent indicates the earliest effective filing date is April 17, 2015. Ex. 1001, code (63). Consequently, for all purposes relevant to this Decision, we apply statutes as they stand after the Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011).

Appendix E

A. Related Cases

The parties identify as related to the present case: *Centripetal Networks, Inc. v. Cisco Systems, Inc.*, Case No. 2:18-cv-00094-MSD-LRL (E.D. Va); and *Centripetal Networks, Inc. v. Keysight Techs., Inc.*, Case No. 2:17-cv-00383-HCM-LRL (E.D. Va). Pet. 8; Paper 3, 1.

B. The '722 Patent

The '722 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.

Appendix E

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.

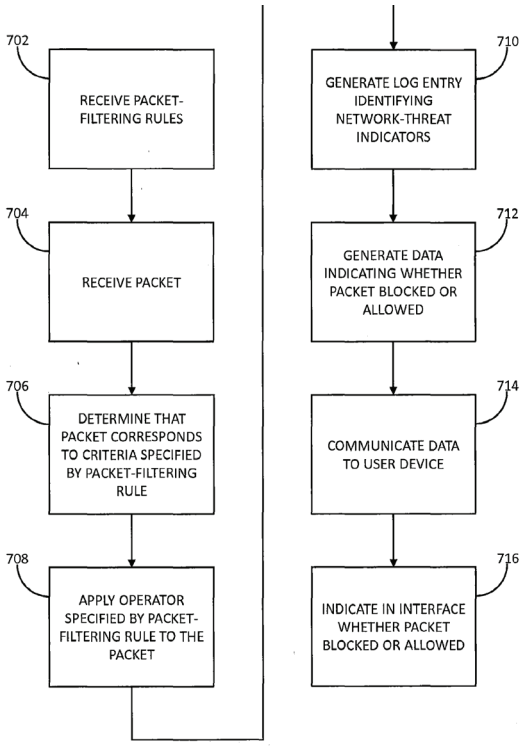


FIG. 7

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).

C. Challenged Claims

Petitioner challenges all of the claims of the '722 Patent. Claim 1, the only independent claim, is illustrative and is reproduced below (letters in brackets added for ease of reference):

> 1. A method comprising:
>
> [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;
>
> [b]receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;
>
> [c] 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:
>
> [d] 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;

[e] 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;

[f] 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 packet-filtering rule and the one or more network-threat indicators;

[g] 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;

and responsive to receiving the instruction:

> [h] 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
>
> [i] responsive to a determination by the packet-filtering device that the second

packet corresponds to the one or more criteria:

> [j] preventing, by the packet-filtering device, the second packet from continuing toward a destination of the second packet;
>
> [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] 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.

D. Instituted Ground of Unpatentability and Asserted Prior Art

Trial was instituted on the sole ground of unpatentability asserted in the Petition:

Claim(s) Challenged	**35 U.S.C. §**	**Reference(s)/ Basis**
1–25	103	Sourcefire[2]

2. Sourcefire 3D System User Guide, Version 4.10 (Ex. 1004, "Sourcefire").

Inst. Dec. 27; *see* Pet. 24. The parties dispute whether Sourcefire qualifies as prior art under 35 U.S.C. § 102(a)(1), specifically whether it was publicly accessible in (or before) April of 2011. *See* Pet. 24; PO Resp. 2–11; Pet. Reply 2–7; PO Sur-reply 2–10.

Petitioner relies on the Declaration of John Leone (Ex. 1005) and the Declaration of Jacob H. Baugher III (Ex. 1042), which present testimony to support Petitioner's assertions regarding public accessibility. In addition, Petitioner further relies on the Declaration of Dr. Stuart Staniford (Ex. 1003), its proffered expert witness. Similarly, Patent Owner relies on a declaration by its proffered expert witness, Dr. Alessandro Orso (Ex. 2002).

ANALYSIS

A. Level of Ordinary Skill in the Art

Petitioner asserts that a person of ordinary skill in the art would have had a bachelor's degree in computer science, computer engineering or an equivalent, as well as four years of industry experience. Pet. 15 (citing Ex. 1003 ¶¶ 21–24 (Dr. Staniford's testimony)). In addition, Petitioner asserts that a person of ordinary skill would have had "a working knowledge of packet-switched networking, firewalls, security policies, communication protocols and layers, user interfaces, and the use of customized rules to address cyber-attacks." *Id.*

In its Response, Patent Owner does not dispute Petitioner's definition of the level of skill in the art.[3] Based on the complete trial record, we find Dr. Staniford's testimony credible and persuasive (Ex. 1003 ¶¶ 21–24), and we adopt Petitioner's definition as a result.

B. Claim Construction

For petitions filed before November 13, 2018, as here, claim terms in an unexpired patent are given their broadest reasonable construction in light of the specification of the patent in which they appear. 37 C.F.R. § 42.100(b) (2018); *see Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2144–46 (2016). In the Decision on Institution, we preliminarily construed the term "network-threat indicator" as an "indicator that represents the identity of a resource associated with a network threat." Inst. Dec. 8. During trial, neither party disputed this preliminary construction. *See* PO Resp. 25; Pet. Reply 7–8; Tr. 10:22–11:9. We do not discern any evidence in the full record after trial indicating that this construction is incorrect or should be modified. Moreover, the Specification supports this construction, indicating that "network addresses, ports, fully qualified domain names (FQDNs), uniform resource

3. Dr. Orso testified to a slightly different description of the level of skill in the art (Ex. 2002 ¶ 36), but Patent Owner did not argue during trial that Dr. Orso's description should be adopted instead of Petitioner's description and waived any such argument as a result. *See In re NuVasive, Inc.*, 842 F.3d 1376, 1380–81 (Fed. Cir. 2016). Moreover, Dr. Orso testified that his opinions would be unchanged under Petitioner's description of the level of ordinary skill. Ex. 2002 ¶ 36.

locators (URLs), uniform resource identifiers (URIs), or the like" are examples of "network-threat indicators." Ex. 1001, 3:18–26. Thus, we apply this construction in this Decision.

At the oral hearing, Patent Owner belatedly argued that the Specification indicates the above examples are insufficient by themselves to constitute "network-threat indicators" because the Specification further mentions "other information associated with the network threats," such as threat type and geographic location. *See* Tr. 45:9–25, 62:10–64:23, 80:15–82:2. As an initial matter, Patent Owner did not make this argument in its claim construction positions advanced during trial and, thus, it is untimely. *See* PO Resp. 25–28; PO Sur-reply 10–12; *NuVasive*, 842 F.3d at 1380–81.

Even were we to consider this argument, we disagree and decline to modify our construction to require such "other information." The Specification describes that "[n]etwork-threat-intelligence providers" disseminate "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." Ex. 1001, 3:18–33 (emphasis added). In other words, the "other information" is included in network-threat-intelligence reports *along with* network-threat indicators, *not* as part of them, which also is evidenced by how the "other information" is *not* included in the parenthetical

listing the examples of such indicators. In fact, Patent Owner itself admits that the '722 Patent "makes clear that the network-threat indicator is the identity of the resource associated with the threat *and not the threat itself or other information associated with the threat*." PO Sur-reply 12–13 (quoting Ex. 1001, 3:18–33) (emphasis added).

We note that the parties disagree further about whether our construction of "network-threat indicator" encompasses certain specific examples potentially relevant to the prior art, particularly ports. *See* PO Resp. 27–28; Pet. Reply 10; PO Sur-Reply 11–12. As this dispute concerns the application of our construction rather than the construction itself, we address it to the extent necessary to determine the patentability of the challenged claims in our obviousness analysis below.

No other claim terms in the '077 Patent require express construction for purposes of this Decision. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (holding that only claim terms in controversy require express construction, and only to the extent necessary to resolve the controversy).

C. Alleged Unpatentability Under § 103

Petitioner's sole asserted ground of unpatentability as to all challenged claims is obviousness in view of Sourcefire. Pet. 24. A claim is unpatentable under § 103 if the differences between the claimed subject matter and the prior art are "such that the subject matter as a whole would have been obvious at the time the invention was

made to a person having ordinary skill in the art to which said subject matter pertains." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). 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 skill in the art; and (4) objective evidence of nonobviousness, i.e., secondary considerations. *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*, 550 U.S. at 418 (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)).

1. Overview of 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.[4] The system operates via "3D Sensors" that can each run the Sourcefire "Intrusion Prevention System" (IPS), which allows monitoring of networks for attacks

4. All citations to Sourcefire refer to the document's original pagination.

by examining packets for malicious activity. *Id.* at 33–34. Users can create custom "intrusion rules" to examine packets for attacks and manage the rules across all the 3D Sensors in the system through a centralized "Defense Center." *Id.* at 34, 254.

Intrusion rules can be "pass" rules, "alert" rules, or "drop" rules. *Id.* at 761. If a pass rule is met, the network traffic in question is ignored (and allowed to continue). *Id.* Conversely, if a drop rule is met, the packet is dropped and an "event" is generated. *Id.* Rules can be written based on "keywords" and their "arguments," i.e., the possible values of the keyword. *Id.* at 762–763.

The Sourcefire 3D System also features "preprocessors" that can facilitate processing of network traffic by identifying and decoding certain types of traffic, such as HTTP (hypertext transfer protocol) and SSL (secure sockets layer) traffic. *Id.* at 513–514. The SSL preprocessor, for example, can be used to identify encrypted traffic that IPS cannot analyze, thereby enabling IPS to ignore (pass) the encrypted packets and avoid wasting resources trying to inspect them. *Id.* at 596.

2. Public Accessibility of Sourcefire

Petitioner asserts that Sourcefire qualifies as prior art under § 102(a)(1). Pet. 24. Patent Owner asserts that Sourcefire does not qualify as applicable prior art because it is not a printed publication. *See* PO Resp. 2–11 (citing 35 U.S.C. § 311(b)); PO Sur-reply 2–10. In determining whether a prior art reference constitutes a

printed publication, "the touchstone is public accessibility." *In re Bayer*, 568 F.2d 1357, 1359 (CCPA 1978); *see Blue Calypso, LLC v. Groupon, Inc.*, 815 F.3d 1331, 1348 (Fed. Cir. 2016). "A given reference is 'publicly accessible' upon a satisfactory showing that such document has been disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art exercising reasonable diligence, can locate it." *SRI Int'l, Inc. v. Internet Sec. Sys., Inc.*, 511 F.3d 1186, 1194 (Fed. Cir. 2008) (quoting *Bruckelmyer v. Ground Heaters, Inc.*, 445 F.3d 1374, 1378 (Fed. Cir. 2006)).

Petitioner contends that Sourcefire was publicly available because (1) it was actually disseminated to hundreds of customers who purchased Sourcefire 3D System products, and (2) it was available on Sourcefire's support website. *See* Pet. 24; Pet. Reply 2. As explained below, we conclude that Petitioner has shown sufficiently that Sourcefire was publicly available due to its actual dissemination to customers.

According to Petitioner, Sourcefire was enclosed on a CD-ROM disk that was "included with each [Sourcefire] 3D System appliance sold, and offered for sale, from April 2011 through at least March 2013 – no less than two years before the '722 Patent." Pet. Reply 3. Specifically, Petitioner asserts there were "586 sales of the [Sourcefire] 3D System that included [the Sourcefire reference]" during this time period. *Id.* Petitioner relies on the testimony of John Leone and Jacob H. Baugher III, two former employees of Sourcefire's manufacturer. *Id.* (citing Ex. 1005 (Leone Declaration); Ex. 1042 (Baugher

Declaration)). Mr. Leone testified that Sourcefire was included with every Sourcefire 3D System product in that timeframe, and that "approximately 586 customers purchased the Sourcefire 3D System from April 2011 through March 2013 and had access to the Sourcefire 3D System User Guide." Ex. 1005 ¶¶ 11, 19. Mr. Baugher provided corroborating testimony in which he explained how Sourcefire sales records were kept and that, based on those records, "there were approximately 586 customers that purchased the Sourcefire 3D System from April 2011 through March 2013." Ex. 1042 ¶¶ 5–8. He further testified that "[t]hese 586 customers include entities having large network security teams," including Microsoft, Symantec, and various other technology companies, as well as governmental organizations such as the U.S. Department of Defense, the U.S. Department of Homeland Security, and the North Atlantic Treaty Organization (NATO). *Id.* ¶ 9.

Additionally, Petitioner cites a press release about the relevant Sourcefire 3D System published in BusinessWire in April 2011 (Ex. 1034), a product review for the Sourcefire 3D System published by ITPro in January 2007 (Ex. 2009), and a product review for the system published by SC Media in May 2006 (Ex. 2010), as evidence establishing that the Sourcefire 3D System (including its accompanying user manual, the Sourcefire reference) was publicly marketed and sold to customers. Pet. Reply 4. Patent Owner argues that these facts and Petitioner's evidence are insufficient to establish public accessibility under controlling case law. *See* PO Sur-reply 3–10.

Appendix E

Petitioner relies on *Mass. Inst. of Tech. v. AB Fortia*, 774 F.2d 1104 (Fed. Cir. 1985) ("*MIT*"). Pet. Reply 3. In *MIT*, a paper was orally presented at a scientific conference attended by "50 to 500 cell culturists." 774 F.2d at 1108. Copies of the paper "were distributed on request, without any restrictions, to as many as six persons." *Id.* at 1108–09. The Federal Circuit held that these facts were sufficient to establish public accessibility. *Id.* at 1109; *see also In re Klopfenstein*, 380 F.3d 1345, 1349 (Fed. Cir. 2004) ("The key to the court's finding [in *MIT*] was that actual copies of the presentation were distributed."). Petitioner also cites *Garrett Corporation v. United States*, 422 F.2d 874, 878 (Ct. Cl. 1970). Pet. Reply 3. In *Garrett*, the court held that a government report was a "printed publication" under § 102(b) because approximately 80 copies were disseminated, including to six commercial companies. 422 F.2d at 878. The court held that "distribution to commercial companies without restriction on use clearly" established that the report is a printed publication. *Id.*

Patent Owner relies on *Medtronic, Inc. v. Barry*, 891 F.3d 1368 (Fed. Cir. 2018). PO Sur-reply 4–5. In *Medtronic*, the prior art at issue was disseminated to attendees of three conferences. 891 F.3d at 1379. The Federal Circuit distinguished *Medtronic* from past cases involving references stored in repositories (e.g., libraries)—rather than considerations like indexing and cataloguing, the relevant inquiry was whether the *distribution* of the reference to certain groups of people was sufficient for public accessibility. *Id.* at 1379–80. Issues underlying that inquiry include, for example, "whether there is an expectation of confidentiality between the distributor and the recipients of the materials," as well as "[t]he expertise

of the target audience." *Id.* at 1381–82. Although agreeing with the Board that "[d]istributing materials to a group of experts" is not enough for public accessibility "simply by virtue of the relative expertise of the recipients," the Federal Circuit held that the Board in that case had not sufficiently considered all of the recipients of the distributed materials, or whether all the recipients were expected to hold the distributed materials in confidence. *Id.* at 1382–83.

Based on the above facts and case law, we conclude that Sourcefire was publicly accessible. The evidence of record indicates that the Sourcefire 3D System was publicly marketed and sold, and that the Sourcefire reference was actually distributed to over 500 customers of the Sourcefire 3D System. Ex. 1005 ¶¶ 11, 19; Ex. 1042 ¶¶ 5–9. This vastly exceeds the distribution to six people in *MIT* and distribution of 80 copies in *Garrett*. Record evidence also supports Petitioner's contention that the customers who received Sourcefire included entities interested in network security products, including persons of ordinary skill in the art. *See* Ex. 1042 ¶ 9; *see also* Ex. 1004, 1, 32–33 (identifying Sourcefire as a "User Guide" and indicating Sourcefire provides information for network administrators); Ex. 1005 ¶ 5 (indicating Sourcefire was drafted in consultation with, and reviewed by, engineers who designed the Sourcefire system). Moreover, similar to *MIT* and as discussed in *Medtronic*, the record indicates that the recipients of Sourcefire were not subject to confidentiality requirements restricting use or further distribution. *See* Ex. 1004, 2 (Sourcefire copyright page stating, "You may use . . . and otherwise

copy and distribute [Sourcefire] solely for non-commercial use").[5] Although Patent Owner asserts that *MIT* and *Klopfenstein* are distinguishable because they involved "the free distribution of academic documents to conference and meeting attendees" (PO Sur-reply 7), case law indicates that distribution to commercial entities also may be sufficient. *See Garrett*, 422 F.2d at 878; Pet. Reply 3.[6]

Patent Owner argues that Mr. Leone's testimony regarding the number of customers who purchased relevant Sourcefire products (and, thus, received the Sourcefire reference) is not credible. *See* PO Resp. 6–7; PO Sur-reply 8. According to Patent Owner, insufficient

5. Patent Owner asserts that "Mr. Baugher reveals that each sale of a Sourcefire product was subject to licensing restrictions," arguing that such restrictions preclude public accessibility. PO Sur-reply 9–10 (citing Ex. 2017, 47:6–18). Mr. Baugher, however, does not mention any "licensing restrictions," instead indicating only that a "signed sales order" or a "purchase order" was required. Ex. 2017, 47:6–21. He also mentions that customers would "click through an agreement to agree to our terms and conditions," but Patent Owner does not identify any evidence about those terms and conditions or otherwise explain how they show restrictions on the dissemination of Sourcefire.

6. Both decisions by Board panels relied on by Patent Owner (PO Sur-reply 5–6) are distinguishable on their facts, including because both involved references that were subject to restrictions prohibiting their reproduction or further dissemination. *See ASM IP Holding B.V., v. Kokusai Elec. Corp.*, IPR2019-00369, Paper 8, at 18 (PTAB June 27, 2019); *VMAC Global Techs. Inc., v. Vanair Mfg, Inc.*, IPR2018-00670, Paper 9, at 13–14 (PTAB Aug. 10, 2018). In *ASM*, the panel further noted that there was no evidence of actual dissemination to interested artisans. *See ASM*, Paper 8, at 17.

explanation was provided as to "how many 'documentation disks' were provided with the product and whether the documentation disks were indexed in any meaningful way," and Mr. Leone's role does not indicate sufficient personal knowledge about sales or customers. *See* PO Resp. 6–7; PO Sur-reply 8.

The relevant question, however, is not whether Sourcefire was publicly accessible on a certain number or format of "documentation disks," but rather whether Sourcefire was adequately disseminated. Regarding Mr. Leone's credibility, we find his testimony to be credible and persuasive, particularly as supported by the testimony of Mr. Baugher, who also confirmed the number of customers who purchased the Sourcefire system. *See* Ex. 1042 ¶¶ 5–8. We note that Patent Owner declined to depose Mr. Leone to determine the extent of his personal knowledge or the manner in which he informed himself of the facts necessary for his testimony. *See* Pet. Reply 3–4. Patent Owner also is not seeking to exclude any aspect of Mr. Leone's testimony for any reason, including for lack of personal knowledge under Rule 602. *See* Paper 28 (Patent Owner's motion to exclude); Fed. R. Evid. 602.

Patent Owner also challenges Mr. Baugher's testimony, asserting that Mr. Baugher's methodology for determining the relevant customers was flawed. *See* PO Sur-reply 8–9. We are not persuaded, however, because Patent Owner's assertions are not consistent with Mr. Baugher's testimony. For example, according to Patent Owner, Mr. Baugher's "method of analysis relied entirely on a SKU (stock keeping unit) scheme in which certain SKUs

contained the '3D' prefix in its value," which allegedly undermines his testimony because he could not "verify that he specifically analyzed sales record having a product description naming Sourcefire 3D **Sensor** products, i.e., specific products named in Mr. Leone's declaration as . . . containing the Sourcefire reference." *Id.* (citing Ex. 2017, 53:5–25 (emphasis added by Patent Owner)).

Mr. Baugher testified, however, that the records he relied on included both SKU descriptions and product descriptions. *See* Ex. 2017, 52:24–53:4; *see also id.* at 51:4–52:23 (indicating the records were identified based on "product family" rather than "SKU alone," and that each SKU was accompanied by "a description of the product . . . which would also identify it as a 3D product type"). Additionally, Mr. Leone's Declaration named "3D Sensor" products as only one *example* of products that included the Sourcefire reference, i.e., "each Sourcefire 3D System appliance (*e.g.*, 3D Sensor, Defense Center)." Ex. 1005 ¶ 11. Thus, whether Mr. Baugher could recall that "3D Sensor" products specifically were included is of limited relevance given his explanation that the records were identified based on the Sourcefire 3D System *product family*. *See* Ex. 2017, 51:4–53:4.

Patent Owner also argues that, even if sales of Sourcefire products (including the Sourcefire reference) were established, such dissemination is insufficient, and that Petitioner must additionally demonstrate that a person of ordinary skill would have been able to locate Sourcefire through reasonable diligence. PO Resp. 2–3, 7–8; PO Sur-reply 4–6, 7–8 (citing *Acceleration Bay,*

LLC v. Activision Blizzard, Inc., 908 F.3d 765, 772 (Fed. Cir. 2018)). The Federal Circuit has indicated that public accessibility is established by showing that the reference was "disseminated *or otherwise* made available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, can locate it." *Acceleration Bay*, 908 F.3d at 772 (quoting *Jazz Pharm., Inc. v. Amneal Pharm., LLC*, 895 F.3d 1347, 1355–56 (Fed. Cir. 2018)) (emphasis added). Here, Petitioner has shown that Sourcefire was "disseminated" to interested artisans; thus, it is unnecessary to additionally show that it was also "otherwise" made available to them. *See Klopfenstein*, 380 F.3d at 1349 ("The key to the court's finding [in *MIT*] was that actual copies of the presentation were distributed."). We note the Federal Circuit has held that if the latter is shown (i.e., accessibility through reasonable diligence), it is unnecessary to show actual access or dissemination. *See*, *e.g.*, *Jazz Pharm.*, 895 F.3d at 1356 ("If accessibility is proved, there is no requirement to show that particular members of the public actually received the information.").

Consequently, we are unpersuaded that Sourcefire was not publicly accessible due to various issues surrounding whether the Sourcefire website made the reference adequately accessible, given the evidence of actual dissemination through sales and commercial distribution. *See* PO Resp. 3–5; PO Sur-reply 2–3. Nor are we persuaded by Patent Owner's contention that the cost of the Sourcefire 3D System was too high and, thus, a skilled artisan would not have been able to access Sourcefire. *See* PO Resp. 8–9; PO Sur-reply 6–7. The

cost did not prevent over 500 customers from actually obtaining Sourcefire by purchasing Sourcefire 3D System products. Moreover, there is no evidence in the record indicating that sales of the relevant Sourcefire products were restricted or limited to only certain customers, or that the cost[7] of acquiring a Sourcefire 3D System product was prohibitively high to the relevant artisans.

Additionally, Patent Owner cites *In re Bayer*, 568 F.2d 1357 (CCPA 1978), arguing the prior art in *Bayer* (a thesis) was held not to have been publicly accessible despite actual distribution to faculty on a graduate committee reviewing the thesis. PO Sur-reply 5. In *Bayer*, the relevant issue was whether the appellant's "uncatalogued, unshelved thesis, by virtue of its accessibility to the graduate committee," constituted a printed publication. 568 F.2d at 1359. The Federal Circuit has clarified *Bayer*, explaining that the thesis was held not publicly accessible because "a work is not publicly accessible if the only people who know how to find it are the ones who created it," such as the faculty on the graduate committee reviewing and advising on student theses. *See Samsung Elecs. Co. v. Infobridge Pte. Ltd.*, 929 F.3d 1363, 1371–72 (Fed. Cir. 2019). Thus, *Bayer* is inapposite here, where Sourcefire was distributed to over 500 customers.

---

7. The record includes evidence of a range of prices for various configurations of Sourcefire 3D System products, from $1,385 to £25,000. Ex. 2009, 1; Ex. 2010, 1. Based on Mr. Leone's testimony, Sourcefire would have been distributed with the purchase of any of these products. Ex. 1005 ¶ 11 (testifying that Sourcefire was "included with each Sourcefire 3D System appliance (*e.g.*, 3D Sensor, Defense Center) sold to a customer").

In summary, we find that a preponderance of the evidence establishes that Sourcefire was distributed commercially through sales of the Sourcefire 3D System to over 500 customers, including interested persons of ordinary skill, and that those customers were not subject to any restriction or expectation of confidentiality with regard to its use or further distribution. Therefore, we conclude that Sourcefire was publicly accessible, and that it constitutes prior art under § 102(a)(1).

3. Independent Claim 1

Petitioner contends claim 1 of the '722 Patent would have been obvious in view of Sourcefire. As explained in more detail below, we find that Petitioner has shown by a preponderance of the evidence that Sourcefire teaches each limitation of claim 1.

a. Limitation 1[a]

Limitation 1[a] of claim 1 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."

Petitioner identifies Sourcefire's 3D Sensor with IPS as the recited "packet-filtering device," and the rules received by the 3D Sensor via, for example, intrusion policies imported from a centralized Defense Center as the recited "packet-filtering rules." Pet. 36–39 (citing *inter alia* Ex. 1004, 34, 105, 338–350, 2001–2002). With respect to the

recited "network-threat indicators," Petitioner relies on Sourcefire's disclosures regarding rules using IP addresses or ports, for example, to take an action (e.g., passing or dropping) on a data packet. *Id.* at 39 (citing Ex. 1004, 762–769). Specifically, Petitioner identifies Sourcefire's discussion of "source or destination IP address, source or destination port, protocol, keyword (*e.g.*, malicious URL/URI), etc.[] associated with the particular exploit that the rule was designed to protect" as examples of "data . . . corresponding to characteristics associated with malicious activities" that teach the recited "network-threat indicators." *Id.* at 38–39 (citing Ex. 1004, 34, 762–769). The Petition explains that Sourcefire, thus, teaches receiving the recited "packet-filtering rules" configured to cause a 3D Sensor device to identify packets corresponding to, for example, certain IP addresses identifying a source of malicious activity ("network-threat indicators"). *Id.*

We are persuaded by Petitioner's reasoning and evidence. Patent Owner's arguments, discussed in more detail below, are unpersuasive and are inconsistent with the weight of the record evidence. Thus, we find that Sourcefire teaches limitation 1[a] of claim 1.

In particular, Sourcefire discloses that "[b]y placing 3D Sensors with IPS on key network segments, you can examine the packets that traverse your network for malicious activity," and that the 3D Sensors use "rules . . . to look for the broad range of exploits that attackers have developed." Ex. 1004, 34. Further, Sourcefire describes these rules as follows:

Appendix E

> An *intrusion rule* is a specified set of keywords and arguments on a 3D Sensor with the IPS component that detects attempts to exploit vulnerabilities on your network by analyzing network traffic to check if it matches the criteria in the rule. 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.

Id. at 761. Consequently, we find that Sourcefire teaches the recited "packet-filtering device" (3D Sensor with IPS), which examines packets using "packet-filtering rules" (intrusion rules). Sourcefire also teaches that intrusion rules are "received" by the packet-filtering device (3D Sensor) from a Defense Center, which is used to manage multiple 3D Sensors and provide them with intrusion policies that include intrusion rules. *See id.* at 34, 105, 338–350, 2001–2002.

Sourcefire indicates that an intrusion rule may specify "source and destination IP addresses," "source and destination ports," and "keywords and their parameters and arguments." *Id.* at 762. Using these aspects of a rule, a user can "restrict packet inspection to the packets originating from specific IP addresses." *Id.* at 766–767; *see also id.* at 768–769 (teaching similar restrictions for packets originating from specific ports). Based on these disclosures, we find that Sourcefire teaches packet-filtering rules that are "configured to cause the packet-filtering device to identify packets corresponding to," for example, specific source IP addresses (e.g., computers located at those IP addresses).

Appendix E

We further find that Sourcefire teaches the recited "network-threat indicators." As discussed above, a "network-threat indicator" is properly construed as an "indicator that represents the identity of a resource associated with a network threat." The source IP address discussed in Sourcefire identifies the source of a packet. *See id.* at 768–769. As noted above, Sourcefire indicates intrusion rules are used to identify "exploits" from attackers such that 3D Sensors employing those rules examine packets for "malicious activity." *Id.* at 34, 761. Thus, we are persuaded that a person of ordinary skill would understand these disclosures of Sourcefire to teach packet-filtering rules (intrusion rules) configured to cause a packet-filtering device (3D Sensor with IPS) to identify packets corresponding to at least one of a plurality of indicators (source IP addresses) that represent the identity of a resource (computer located at the source IP address) associated with a network threat (exploit or other malicious activity). *See* Ex. 1003 ¶¶ 114–116. Indeed, we note that the Specification of the '722 Patent itself identifies "network addresses" associated with network threats as examples of "network-threat indicators." Ex. 1001, 3:23–24.

Patent Owner disputes that Sourcefire teaches the recited "network-threat indicators" for a number of reasons, all of which are unpersuasive. *See* PO Resp. 29–48. First, Patent Owner asserts that "the source IP address specified in the Rule Header is used merely to 'restrict packet inspection'" and "not because the IP addresses and ports are associated with a network threat." *Id.* at 32–33. Further, Patent Owner notes that Sourcefire indicates source and destination IP addresses are used, at least in part, to

"remov[e] the possibility of the rule triggering against packets whose source and destination addresses *do not* indicate suspicious behavior." *Id.* at 32–33, 40–42 (citing Ex. 1004, 766–767 (emphasis added)). These arguments, however, ignore Sourcefire's teachings about using intrusion rules to detect exploits and malicious activity (*see* Ex. 1004, 34, 761), rather than only identifying "known trusted IP addresses" on a "whitelist" that should not be inspected, as Patent Owner suggests (PO Resp. 40–42). We find that an ordinary artisan would have been taught by Sourcefire's disclosures to use source and destination IP addresses to configure the rule to more accurately target only packets with IP addresses that *do* indicate suspicious behavior, consistent with our construction of "network-threat indicators."

Next, Patent Owner cites particular examples in Sourcefire that it alleges support its position—for instance, the example of a rule shown on pages 763–764 of Sourcefire indicates the rule applies to "traffic coming from any host that is not on your internal network," and that example rule specifies various other criteria that are applied instead of specific network-threat indicators. PO Resp. 33–35, 45–46. Petitioner does not, however, rely solely on that particular example rule—other aspects of the same sections of Sourcefire undermine Patent Owner's position and support Petitioner's view, as discussed above. For example, Sourcefire also provides examples of rule header syntax that would configure the intrusion rule to apply to a specific source IP address. *See* Ex. 1004, 766–767. As a result, Patent Owner's argument is not persuasive.

Similarly, Patent Owner's arguments regarding the example of an "intrusion event" on pages 282–283 of

Sourcefire also are unpersuasive because they erroneously focus on only part of Sourcefire's disclosure. *See* PO Resp. 35–38, 46–48. For instance, Patent Owner argues that certain "5-tuple information" (including source IP address) in that particular example was not used in the relevant intrusion rule and, thus, could not teach the network-threat indicator. *Id.* at 36–38. This argument, however, ignores Sourcefire's teachings regarding rules in which source IP addresses *are* used as a network-threat indicator, as discussed above—whether Sourcefire *also* includes examples that may not disclose limitation 1[a] is inapposite. Moreover, we note that Petitioner does not rely on the "intrusion event" disclosure for limitation 1[a], but rather cites it in its arguments relating to limitation 1[e]. *See* Pet. 42–44. Likewise, Patent Owner's argument (PO Resp. 43) that Sourcefire's "Rule Categories" do not include a category based on "traffic identified based upon the identity of a resource associated with a network threat" also is unpersuasive because Petitioner does not rely on those disclosures of Sourcefire.[8]

Patent Owner further argues that "Sourcefire does not disclose any source of information for constructing rules that identify **resources** associated with a network attack." PO Resp. 41 (citing Ex. 2002 ¶ 94) (emphasis in original). According to Patent Owner, "[t]hat concept is simply missing

8. We note that the "Rule Categories" cited by Patent Owner include categories for rules detecting traffic identified based on, for example, specific communications protocols (e.g., FTP, POP2, NNTP, SNMP), "UNIX or Linux-based remote services," whether the traffic "originate[s] from telnet servers," and whether the traffic is "suspicious traffic sent to or from web servers," as well as a category for "[u]ser-defined rules" created based on the rule customization instructions described in Sourcefire. Ex. 1004, 427–430.

from Sourcefire because Sourcefire is not designed to operate on the basis of network threat indicators, but rather on the basis of inspecting content in received traffic for exploits." *Id.* (citing Ex. 2002 ¶ 94). No further explanation is given to support these conclusory statements. For example, Patent Owner does not address why a computer located at a specific source address would not constitute a "resource," or explain why operating on the basis of network-threat indicators and inspecting content in received traffic are mutually exclusive. *See id.* The only evidence cited is the testimony of Dr. Orso, but that testimony likewise fails to provide more than the same conclusory statements—indeed, the cited testimony is nearly a verbatim repetition of Patent Owner's brief, which undermines its credibility. *See id.*; Ex. 2002 ¶ 94; 37 C.F.R. § 42.65(a) ("Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight."). As a result, we find this argument unpersuasive and insufficiently supported compared to Petitioner's contentions and evidence, discussed above.

The next argument advanced by Patent Owner is that Sourcefire's teachings do not satisfy the proper construction of "network-threat indicator" because Sourcefire allegedly teaches that the IP addresses used in intrusion rules are only "retroactively discovered to be associated with a network threat after an exploit is found in content received from that IP address."[9] PO Resp. 42 (citing Ex. 2002 ¶ 95); *see* PO Sur-reply 14–15. Aside from Dr. Orso's near-

9. Patent Owner also raises related issues regarding disclosures about the "Sourcefire VRT." PO Resp. 42–43. As Petitioner relies on such disclosures for certain dependent claims, we address them below in the context of those dependent claims.

verbatim repetition of these arguments, however, Patent Owner cites no evidence to support its allegation.

Moreover, Patent Owner's characterization of Sourcefire is undercut by the disclosures of Sourcefire relied on by Petitioner. As discussed above, Sourcefire teaches 3D Sensor devices that use intrusion rules to identify exploits and other malicious activity. *See* Ex. 1004, 34, 761. According to Sourcefire, packets are examined to determine whether they match the criteria specified by the rules, in which case the rule would be triggered. *Id.* at 761. Sourcefire also teaches that rules can be selected and enabled "that would detect the attacks you think most likely to occur on your network," including "custom intrusion rules tuned to your environment." *Id.* at 34.

We find that this evidence supports Petitioner's contention that Sourcefire teaches the recited "network-threat indicator" because Sourcefire is describing measures to be taken to protect the system from malicious activity.[10] *See id.* at 34, 761. Patent Owner's allegation essentially characterizes Sourcefire's system as incapable of proactive protection, instead only "retroactively" identifying malicious activity that has already penetrated the system. That characterization, however, is inconsistent with Sourcefire's disclosures discussed above.

Patent Owner additionally argues that a person of ordinary skill "would distinguish between the use of

10. As discussed in more detail below, Sourcefire indicates that the rule may be configured as a "drop rule" such that the packet is dropped instead of being passed through, thereby preventing the packet from causing damage. *See* Ex. 1004, 761.

network-threat indicators in the claimed invention and Sourcefire's use of signature or patterns," citing a document describing one of Petitioner's products. PO Sur-reply 13–14 (citing Ex. 2001, 3). But Patent Owner does not explain adequately how a description of Petitioner's product—which does not reference Sourcefire or use the term "network-threat indicator"—bears on Sourcefire's teachings or limitation 1[a] (or any specific language of claim 1). *See id.*

In addition, Patent Owner challenges Dr. Staniford's testimony on the grounds that Dr. Staniford applied a different claim construction of "network-threat indicator" than our construction, allegedly construing the term as "any rule that utilizes an IP address, port number, or URL as part of the rule criteria . . . even if the IP address is not associated with a network threat." PO Resp. 39 (citing Ex. 2008, 49:2–50:14). Patent Owner mischaracterizes Dr. Staniford's testimony, however. Dr. Staniford instead testified that he relied on examples of network-threat indicators provided in the Specification of the '722 Patent, indicating that "all of those certainly can be potentially network-threa[t] indicators under the right circumstances." Ex. 2008, 49:2–50:14. In fact, although Dr. Staniford provided his Declaration before our preliminary construction in the Decision on Institution (or, indeed, Patent Owner's Preliminary Response that proposed that construction), he confirmed that he subsequently reviewed our construction and that it does not change his opinions regarding obviousness. *Id.* at 7:23–25, 9:12–18. Thus, we discern no defect in Petitioner's reliance on the testimony of Dr. Staniford here.

For the reasons explained above, we find that Petitioner has shown by a preponderance of the evidence that Sourcefire teaches limitation 1[a].

b. Limitations 1[b]–1[d]

For limitations 1[b] through 1[d], Petitioner relies on Sourcefire's description of applying intrusion rules to packets and taking actions on those packets as specified by the rules. Pet. 39–42. Aside from its arguments discussed above with respect to limitation 1[a], which we addressed above, Patent Owner raises no further arguments regarding claim 1.

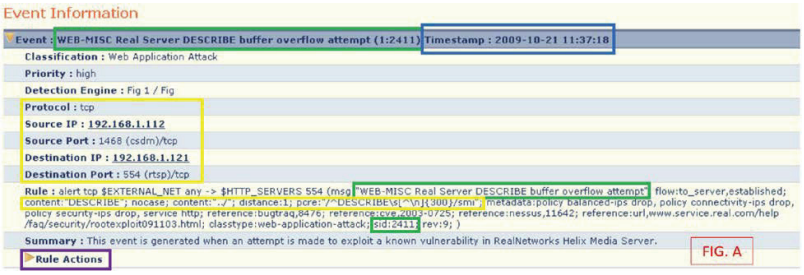
More specifically, as discussed above as well for limitation 1[a], Petitioner contends Sourcefire discloses rules that identify packets corresponding to particular source IP addresses, including the IP addresses of network threats (network-threat indicators). *Id.* at 40–41. According to Petitioner, this teaches the recited "determination by the packet-filtering device that the first packet satisfies one or more criteria . . . that correspond to one or more network-threat indicators." *Id.* We agree. Sourcefire discloses that its 3D Sensor devices "analyz[e] network traffic to check if it matches the criteria in the rule." Ex. 1004, 761. As discussed above, Sourcefire teaches the use of source IP addresses as network-threat indicators. Further, Sourcefire expressly teaches using such source IP addresses as criteria for intrusion rules. *See id.* at 764–766.

Petitioner also identifies, as the recited "operator," the "rule actions" that are specified by each rule, which are applied to a packet if the packet triggers the rule based on, for example, its source IP address (i.e., "responsive to" the determination that the rule criteria is met). *Id.* at 41–42 (citing Ex. 1004, 276–277, 761, 765). These rule actions include "pass" or "alert," which cause the packet to continue toward its destination. *Id.* We find that this evidence supports Petitioner's contention that Sourcefire teaches applying an operator specified by the packet-filtering rule and configured to cause the first packet to continue toward its destination, as recited in claim 1.

For the above reasons, we find that a preponderance of the evidence establishes that Sourcefire teaches limitations 1[b] through 1[d] of claim 1.

c. Limitations 1[e] and 1[f]

With respect to limitations 1[e] and 1[f], Petitioner relies on Sourcefire's disclosures relating to intrusion events. Pet. 42–46. For example, Petitioner cites the figure on page 283 of Sourcefire, which is presented with annotations in the Petition (reproduced below):



Pet. 43; *see* Ex. 1004, 283 (original figure). This figure is a screenshot of Sourcefire's "packet view" interface displaying information for an intrusion event (Ex. 1004, 282–283), with Petitioner's annotations. As Petitioner asserts (Pet. 42–44), Sourcefire indicates that its 3D Sensor devices communicate such intrusion event information to the Defense Center. Ex. 1004, 253–254, 290.

Sourcefire discloses that the packet view "indicates why a specific packet was captured by providing information about the intrusion event that the packet triggered, including . . . the rule that generated the event." Ex. 1004, 290. Petitioner notes Sourcefire's teaching that the intrusion event information includes source and destination IP addresses. Pet. 43; *see* Ex. 1004, 282–283. In light of the teachings of Sourcefire discussed above regarding using, for example, source IP addresses associated with malicious activity as network-threat indicators, we are persuaded that Sourcefire's intrusion event disclosures teach a packet-filtering device (3D Sensor) communicating information from a packet-filtering rule (intrusion rule) that identified a network-threat indicator (e.g., source IP address associated with malicious activity).

As already noted, Patent Owner argues that the specific rule depicted in the example intrusion event above does not use a network-threat indicator. *See* PO Resp. 35–38, 46–48. This argument, however, ignores the other disclosures in Sourcefire identified by Petitioner that teach using source IP addresses and similar information to detect malicious traffic, as discussed above. When

taken together, we agree with Petitioner that Sourcefire's disclosures regarding both intrusion rules and intrusion events teach communicating information from a rule that identified a network-threat indicator, as recited in limitation 1[e].

For the recited "data indicative that the first packet was allowed to continue toward the destination of the first packet," Petitioner cites the figure on page 281 of Sourcefire, which is presented with annotations in the Petition (reproduced below):

Pet. 44–45; *see* Ex. 1004, 281 (original figure). This figure is a screenshot of Sourcefire's "table view of intrusion events" (Ex. 1004, 280–281), with Petitioner's annotations. Petitioner notes that this table shows for each event (i.e.,

each packet), an icon (annotated in red) indicating the result of the rule action applied to that packet. Pet. 44–45. For example, a black down arrow indicates the packet was dropped, whereas no icon indicates the packet was not dropped, i.e., allowed to continue. Ex. 1004, 276–277. We agree with Petitioner that this evidence shows that Sourcefire teaches communicating "data indicative that the first packet was allowed to continue toward the destination of the first packet," as recited in limitation 1[e].

Additionally, we agree with Petitioner that the packet view and table view described and depicted in Sourcefire teach "display of the information . . . corresponding to the packet-filtering rule and the one or more network-threat indicators," as recited in limitation 1[f]. *See* Pet. 45–46; Ex. 1004, 126, 280–283.

For the above reasons, we find that a preponderance of the evidence demonstrates that Sourcefire teaches limitations 1[e] and 1[f] of claim 1.

d. Limitations 1[g]–1[l]

For the remaining limitations of claim 1, Petitioner relies on Sourcefire's description of how a user can use the Sourcefire intrusion event interface to modify rules, which are then applied to packets going forward. Pet. 46–51. The Petition includes a step-by-step explanation of how Sourcefire describes using the intrusion event interface of Sourcefire to select a particular event, select the "Rule Actions" menu in packet view, and change the rule action to drop triggering packets (instead of "alert," which

allows a packet to continue while generating an event) such that intrusion policies are updated with the modified rule. *Id.* at 46–49 (citing Ex. 1004, 281–283, 290–297, 358, 359; Ex. 1003 ¶¶ 132–136). According to Petitioner, these disclosures teach "modifying . . . at least one operator specified by the packet-filtering rule to reconfigure the packet-filtering device to prevent packets . . . from continuing toward their respective destinations," and doing so "responsive to" receiving an instruction from a user "invoking an element in . . . the interface," as recited in claim 1. We agree and find that the cited evidence supports Petitioner's contention.

Petitioner further explains how Sourcefire teaches that the rule, when modified to drop packets as described, would prevent a second packet from continuing toward its destination. *Id.* at 50. We agree with Petitioner. In fact, Sourcefire expressly describes "two scenarios" in which a rule is initially set to generate events (but allow a malicious packet through) in a first scenario, but is instead set to drop packets in a second scenario, in which case the "malicious packet" is dropped and "never reaches its target." Ex. 1004, 435. Further, because drop rules also generate events, we agree with Petitioner that Sourcefire teaches "communicating . . . data indicative that the second packet was prevented from continuing," and displaying that data in the intrusion event interface, as with other intrusion events. *See id.* at 50–51 (citing Ex. 1004, 276, 290; Ex. 1003 ¶ 138).

Patent Owner does not advance any arguments regarding these limitations. We determine that the

evidence cited by Petitioner supports its contentions with respect to limitations 1[g] through 1[l], and we find that Sourcefire teaches each of these limitations based on that evidence, as explained above.

e. Conclusion on Claim 1

For the reasons explained above, we find Petitioner has shown by a preponderance of the evidence that Sourcefire teaches each limitation of claim 1.

4. Dependent Claims

a. Claims 8 and 9

Claim 8 recites, "for each packet in the second portion of packets, generating the packet-log entry *while the packet-filtering device is generating one or more flow-log entries for one or more packets in the first portion of packets*" (emphasis added). Thus, claim 8 requires that the packet-log entries for the second portion of packets be generated *at the same time* that flow-log entries for the first portion of packets are generated. Claim 9 depends from claim 8.

Petitioner's argument regarding the above limitation of claim 8 refers to its arguments regarding claim 6. Pet. 65. Claim 6 recites "updating, . . . based on a packet-log entry, a packet-flow log to indicate" that a packet satisfies one or more criteria and whether the packet was prevented from continuing, or allowed to continue, toward its destination. In its arguments for claim 6, Petitioner mentions a "refresh interval":

> Sourcefire discloses that this count (and therefore the packet-flow log in which it is contained) could be periodically updated. Specifically, Sourcefire discloses that "event preferences" could be selected by the user to configure basic characteristics of event views in the Sourcefire 3D System. [Ex. 1004, 46-47]; [Ex.]1003 ¶ 162. One of these characteristics was the "refresh [or update,] interval" which updated event information (e.g., count (orange)) displayed in the packet flow log at the user-selected refresh interval.

Pet. 60. As to claim 8, Petitioner refers to the above argument and states the following:

> As discussed above with respect to Claim 6, a user could set a "refresh interval" for the event data being displayed such that a packet log entry and a flow log entry was refreshed at a selected time interval which caused the flow log entry to be generated while the packet log entry was being generated. [Ex.]1003 ¶173.

Id. at 65. These largely conclusory arguments, however, fail to explain how refreshing an event view or event summary page, whether at a regular interval or otherwise, teaches *generating* different types of log entries *at the same time* for different portions of packets in the manner claimed. The cited testimony of Dr. Staniford does not provide any further illumination, instead repeating essentially the same conclusory statements made in the Petition. *See* Ex. 1003 ¶¶ 162, 173; 37 C.F.R. § 42.65(a).

Petitioner's Reply also fails to supply the necessary explanation or supporting evidence. Petitioner notes that "flow-log entries are generated from the packet-logs"—thus, flow-log entries must be generated after the corresponding packet-log entries and would reflect any changes made to those entries. Pet. Reply 19–21. Although true, these facts pertain only to a single portion of packets, i.e., that their packet-log entries are generated first, and that the related flow-log entries are generated afterward. The same is true even considering that this process can occur at a predetermined "refresh interval." Petitioner does not identify any specific teaching or suggestion in Sourcefire that indicates how the generation of log entries for two different portions of packets would operate. Instead, Petitioner relies on a bare assertion—without any specific basis in Sourcefire—that "the processing of the packet-logs and the flow-logs are continually being updated or refreshed." Without sufficient supporting evidence, that bare assertion and the conclusory testimony of Dr. Staniford are inadequate to meet Petitioner's burden to prove the unpatentability of these claims by a preponderance of the evidence.

b. Claims 10 and 14

Claim 10 depends from claim 1 and recites that "each of the plurality of network-threat indicators corresponds to at least one network threat of a plurality of network threats," and that "each of the plurality of packet-filtering rules corresponds to a different network threat of the plurality of network threats." For the latter limitation, Petitioner cites Sourcefire's disclosure of event messages

that identify a plurality of network threats (e.g., exploits). Pet. 68 (citing Ex. 1004, 278, 281). Patent Owner does not dispute that Sourcefire teaches this limitation. We find that Petitioner's showing is sufficient because Sourcefire discloses that event messages, such as those cited by Petitioner, are "pulled from the rule" for rule-based intrusion events and, thus, demonstrate a correspondence between a plurality of rules and a plurality of different network threats. *See* Ex. 1004, 278.

For the "network-threat indicators" limitation of claim 10, Petitioner relies *inter alia* on its arguments for claim 1 regarding network-threat indicators associated with network threats. *See* Pet. 67. For similar reasons discussed above for claim 1, we find those arguments and supporting evidence persuasive. Aside from its arguments relating to claim 1, which we addressed above, Patent Owner additionally argues that an example event message cited in the Petition does not teach the recited network-threat indicators. PO Resp. 48–50 (citing Pet. 67–68). Whether or not that specific example alone teaches network-threat indicators, however, is not the proper inquiry for obviousness. Rather, we consider all of the teachings identified by Petitioner, which we determine support Petitioner's contention that Sourcefire teaches the limitations of claim 10 as explained above.

Claim 14, which also depends from claim 10, recites "determining, by the packet-filtering device, an ordering of the plurality of network threats," and "indicating, in the interface, the ordering." In addition to its arguments for claims 1 and 10, Petitioner relies on Sourcefire's

description of its event interface, which allows ordering of displayed intrusion events (and, thus, their associated network threats) in ascending or descending order. Pet. 72 (citing Ex. 1004, 1611–1612). Specifically, Petitioner notes that the "table view" of the interface displays the identification of the network threat associated with each intrusion event, which is ordered when the table entries are ordered. *See* Pet. Reply 23–24 (citing Ex. 1004, 1611–1612; Pet. 45).

Patent Owner argues that the disclosures identified by Petitioner teach only the ordering of events, not network threats. PO Resp. 56–57; PO Sur-reply 22–23. This argument, however, does not cite or rely on any evidence and, thus, constitutes mere attorney argument, which we find unpersuasive. Upon review of the arguments and evidence presented by Petitioner, we agree with Petitioner's analysis and find that Sourcefire teaches the limitations of claim 14 on that basis.

c. Claims 13, 22, and 23

Claim 13 recites that generating the data indicating whether a packet was prevented from continuing, or allowed to continue, to its destination comprises "generating the data *based on the packet-flow-log entry* that corresponds to the particular network threat" (emphasis added). Petitioner's sole statement regarding this limitation in the Petition is: "The indication in Sourcefire's flow log regarding whether the packets were dropped was generated from data in the event log corresponding to the network threat." Pet. 71. This statement is conclusory,

and neither it nor the material cited in support explains sufficiently how Sourcefire teaches the recited limitation.

In its Reply, Petitioner adds that an annotated figure it provided regarding claim 12 shows a depiction in Sourcefire of a flow-log that identifies rules, associated network threats, and associated "block option[s]." Pet. Reply 22–23. But again, Petitioner fails to adequately explain how that figure teaches generating data indicating whether a packet was blocked or allowed *based on the packet-flow-log entry*—indeed, the figure simply depicts packet-flow-log entries. *See id.* Nor do we find persuasive Petitioner's conclusory statement that "[t]his is the same information that is used to generate an entry in the packet-log," for which no evidentiary support is identified. *See id.* at 23. Thus, we conclude that Petitioner did not show that Sourcefire teaches the limitations of claim 13 by a preponderance of the evidence.

Claim 22 recites, "determining an order of the first network threat relative to the second network threat based on a determination that the first portion of the plurality of network-threat-intelligence reports was received from a greater number of the one or more network-threat-intelligence providers than the second portion of the plurality of network-threat-intelligence reports." Although admitting that Sourcefire does not disclose prioritizing network threats based on the number of network-threat-intelligence providers providing reports, Petitioner asserts doing so would have been obvious because "it was well known and a matter of common sense that agreement between sources would serve to

increase confidence in the network threat." Pet. 83–84. The only evidence cited is a paragraph of Dr. Staniford's Declaration, which is essentially identical to the Petition and does not provide any further explanation or evidence. *See* Ex. 1003 ¶ 212.

In its Reply, Petitioner points to arguments it made with respect to claim 21, but again admits that Sourcefire does not disclose prioritizing or ordering network threats based on the *number* of network-threat-intelligence providers, as recited in claim 22. *See* Pet. Reply 24–25. Petitioner also does not identify or present any additional evidence. We conclude that Petitioner did not meet the burden of demonstrating by a preponderance of the evidence that Sourcefire teaches the limitations of claim 22.

Similarly, claim 23 recites ordering network threats "based on data . . . indicating a number of the plurality of different packet-filtering devices that have reconfigured an operator of the first packet-filtering rule to prevent packets . . . from continuing toward their respective destinations." As with claim 22, Petitioner's contentions regarding this limitation are conclusory and supported only with a citation to testimony from Dr. Staniford that merely parrots the same contentions without providing further explanation or evidence. *See* Pet. 86; Ex. 1003 ¶ 216.

In its Reply, Petitioner directs us to arguments it made with respect to claim 10 regarding Sourcefire's disclosure of event information including "counts" of the number of times a given rule was triggered to produce an event. *See* Pet. Reply 25–26 (citing Pet. 67–68). We are not persuaded, however,

that a count of how many times a rule was triggered teaches the recited "number of . . . *different packet-filtering devices* that have *reconfigured an operator*" (emphases added). Petitioner presents only unsupported attorney argument on that issue. *See id.* Thus, we conclude that Petitioner has not met its burden to show the unpatentability of claim 23 by a preponderance of the evidence.

d. Claim 19

Claim 19 depends from claim 10 and recites that receiving the plurality of packet-filtering rules comprises "receiving a plurality of packet-filtering rules generated based on a plurality of network-threat-intelligence reports produced by one or more network-threat-intelligence providers." Petitioner relies on Sourcefire's teachings regarding the "Sourcefire Vulnerability Research Team" ("Sourcefire VRT"). Pet. 75–78. Specifically, Sourcefire describes how the Sourcefire VRT "regularly sends out updates called Security Enhancement Updates, or SEUs, that can contain *new intrusion rules* . . . so you can be sure that you are detecting the most recently released attacks." Ex. 1004, 254. The Sourcefire VRT "continues to add rules as new vulnerabilities and exploits are discovered." *Id.* at 869. Petitioner also explains how Sourcefire teaches adding information to intrusion rules that reflect reports and other information about a network threat.[11] *See* Pet.

11. In the Reply, Petitioner asserts for the first time that Sourcefire's SEUs teach the recited "network-threat-intelligence reports." Pet. Reply 18. We do not consider this argument because it is was not included in the Petition and, thus, is untimely. Moreover,

76–77. We are persuaded by Petitioner's arguments and find that the evidence discussed above shows that Sourcefire teaches receiving a plurality of packet-filtering rules (intrusion rules) generated based on a plurality of network-threat-intelligence reports (information on network threats) produced by one or more network-threat-intelligence providers (the Sourcefire VRT or others who produce the information on network threats referenced in the rules). *See* Ex. 1003 ¶¶ 198–199.

Patent Owner disputes that Sourcefire teaches these limitations of claim 19, but we find its arguments unpersuasive. Specifically, Patent Owner asserts that Petitioner has not shown that the information about reports on network threats described in Sourcefire include network-threat indicators. PO Resp. 51–52. As Patent Owner notes (*id.*), the Specification of the '722 Patent describes an embodiment in which "[n]etwork-threat-intelligence providers 130, 132, and 134 may . . . disseminate (e.g., to subscribers) network-threat-intelligence reports that include network-threat indicators . . . associated with the network threats." Ex. 1001, 3:18–26. As discussed above, however, the evidence supports Petitioner's contention that Sourcefire teaches generating intrusion rules to detect network threats based on information about those threats. *See* Pet. 76–78. And as discussed with respect to claim 1 above, Sourcefire teaches intrusion rules based on network-threat indicators. Thus, we are persuaded that a person of ordinary skill

---

Petitioner does not explain how intrusion rules are "generated based on" the SEUs when the rules in question are themselves contained in the SEUs. *See* Ex. 1004, 254.

in the art would have understood Sourcefire to teach generating rules based on information about network threats, including information constituting network-threat indicators that form part of the criteria applied by the rule (e.g., source IP address). *See* Ex. 1003 ¶¶ 198–199.

For the above reasons, we conclude that Petitioner has shown by a preponderance of the evidence that Sourcefire teaches the limitations of claim 19.

e. Claims 2–7, 11, 12, 15–18, 20, 21, 24, and 25

Claims 2–7, 24, and 25 depend from claim 1; claims 11 and 12 depend from claim 10; claims 15–18 depend from claim 14; and claims 20 and 21 depend from claim 19. Petitioner contends these claims are obvious in view of Sourcefire. Pet. 51–65, 69–75, 86–89. Aside from its arguments regarding the claims from which they depend, which are unpersuasive for the same reasons discussed above, Patent Owner raises no other arguments with respect to the limitations of these claims.

Having reviewed Petitioner's arguments and the evidenced cited in support, we agree with the reasoning set forth in the Petition regarding claims 2–7, 11, 12, 15–18, 20, 21, 24, and 25, and determine that the record evidence supports Petitioner's contentions. Therefore, based on the Petition's analysis and the evidence relied on therein, we find that a preponderance of the evidence shows that Sourcefire teaches each limitation of claims 2–7, 11, 12, 15–18, 20, 21, 24, and 25.

f. Conclusion on Dependent Claims

For the reasons explained above, we find Petitioner has shown by a preponderance of the evidence that Sourcefire teaches each limitation of claims 2–7, 10–12, 14–21, 24, and 25. We find that Petitioner has not shown by a preponderance of the evidence that Sourcefire teaches each limitation of claims 8, 9, 13, 22, and 23.

5. Secondary Considerations of Non-Obviousness

Before determining whether a claim is obvious in light of the prior art, we consider any relevant evidence of secondary considerations—i.e., objective indicia—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 presents evidence of three such considerations: (1) long-felt but unmet need/failure of others, (2) industry praise, and (3) commercial success/licensing. PO Resp. 58–67.

"In order to accord substantial weight to secondary considerations in an obviousness analysis, the evidence of secondary considerations must have a nexus to the claims, i.e., there must be a legally and factually sufficient connection between the evidence and the patented invention." *Fox Factory, Inc. v. SRAM, LLC*, 944 F.3d

1366, 1373 (Fed. Cir. 2019) (internal quotations omitted). A nexus is presumed when "the patentee shows that the asserted objective evidence is tied to a specific product and that product 'embodies the claimed features, and is coextensive with them.'" *Id.* (quoting *Polaris Indus., Inc. v. Arctic Cat, Inc.*, 882 F.3d 1056, 1072 (Fed. Cir. 2018)). If the product is not coextensive with the claims at issue—e.g., if the patented invention is only a component of the product—the patentee is not entitled to a presumption of nexus. *See id.* (citing *Demaco Corp. v. F. Von Langsdorff Licensing Ltd.*, 851 F.2d 1387, 1392 (Fed. Cir. 1988)).

a. Long-Felt But Unmet Need and Failure of Others

According to Patent Owner, "[t]he '722 Patent satisfied a long-felt need in the industry that others had failed to solve—namely, how to operationalize threat intelligence to proactively identify network threats." PO Resp. 59. Patent Owner presents evidence praising Patent Owner's "RuleGATE" product while identifying certain purported challenges to "provid[ing] proactive network protection that could scale to larger networks" and "operationalizing threat intelligence." *Id.* at 59–62. Further, Patent Owner identifies evidence about purported advantages of its products, such as "processing hundreds of millions of indicators from thousands of feeds," "better manag[ing] traffic by leveraging [cyber threat intelligence (CTI)] context with highly granular rules in the form of policies that can be automatically enforced," dynamic updating of intelligence, real time reporting of results for "live analytics," "best-in-class performance [due to] the fact

that the dynamic security policies implement rules on a packet-by-packet basis." *Id.*

Patent Owner's arguments and evidence, however, are insufficient to establish a nexus between the alleged long-felt but unmet need, and the claimed invention. First, no analysis is presented to demonstrate that any product, including RuleGATE, is coextensive with any claim of the '722 Patent. Thus, Patent Owner is not entitled to a presumption of nexus. *See Fox Factory*, 944 F.3d at 1373. Patent Owner's conclusory assertion that its "RuleGATE product practices [the '722 Patent and other patents]" is insufficient and unpersuasive. *See* PO Sur-reply 25–26; PO Resp. 62–63.

Second, insufficient analysis is presented to show that the evidence of a purported long-felt but unmet need is connected to the patented invention. The only mention of any challenged claim is a conclusory statement that limitation 1[a] of claim 1 corresponds to "converting indicators to rules that drive actions across a risk spectrum." PO Resp. 62. Patent Owner does not explain how limitation 1[a], or any aspect of any challenged claim, relates to a "risk spectrum." The paper from which Patent Owner derived the reference to a "risk spectrum" (the "ESG Paper") indicates that "converting indicators to rules that drive actions across a risk spectrum" refers to "logging, content capture, mirroring, redirection, shielding, and advanced threat detection." Ex. 2006, 7.[12] Patent Owner makes no

12. Petitioner argues that the ESG Paper is not objective evidence of non-obviousness because it is a report commissioned and paid for by Patent Owner. Pet. Reply 26–27. We decline to disregard this evidence, or Dr. Orso's testimony about it, entirely. We find,

attempt to demonstrate that limitation 1[a], or any aspect(s) of any challenged claim, relates to, for example, "content capture" or "mirroring." With respect to other "challenges" reported in the ESG Paper—e.g., "[l]ack of automation" and "the inability to use feeds 'in a meaningful way to live network traffic'" (PO Resp. 61)—Patent Owner provides no analysis as to how the patented invention purportedly meets those challenges.

Further, Patent Owner also does not explain how the challenged claims relate to processing "hundreds of millions of indicators," or "leveraging CTI context with highly granular rules in the form of policies that can be automatically enforced," or "dynamic security policies [that] implement rules on a packet-by-packet basis." PO Resp. 62–63. Indeed, these seem clearly outside the scope of the challenged claims. For example, claim 1 recites, at most, a "plurality of network-threat indicators" (i.e., as few as two indicators), not hundreds of millions.

Therefore, we conclude that a nexus was not proven between the purported long-felt but unmet need(s) identified by Patent Owner and the patented invention of the '722 Patent.

b. Industry Praise

Patent Owner cites the ESG Paper (Ex. 2006) as well as a Gartner article (Ex. 2007) and an American Banker article (Ex. 2011) as evidence of industry praise. PO Resp. 63–65. Similar to its long-felt need contentions,

---

however, that the nature and circumstances around the genesis of the ESG Paper diminish the persuasive weight it should be accorded.

however, Patent Owner does not provide sufficient analysis or explanation to establish the requisite nexus. Patent Owner again provides no analysis demonstrating that any Centripetal product is coextensive with the challenged claims, so no presumption of nexus is applied. *See Fox Factory*, 944 F.3d at 1373. Additionally, the cited praise of Centripetal products is not linked sufficiently to the challenged claims, including because Patent Owner failed to address lauded features with no relationship to the claims.

For example, Patent Owner cites the ESG Paper as praising the "high performance" of its product, its ability to process "hundreds of millions of indicators from thousands of feeds," "synthesizing into a network policy," "complex filtering rule[s]" with "at-least a dozen unique fields which had to be evaluated and applied bi-directionally and without state," etc. Ex. 2006, 7. None of these features appear to be in the challenged claims. Patent Owner does not address whether they are part of the claimed invention or, if not, their relative contribution to the industry praise compared to any actual features of the claimed invention.

Regarding the Gartner article, Patent Owner notes that Gartner praises its product's "ability to instantly detect and prevent malicious network connections based on millions of threat indicators at 10-gigabit speeds," "the largest number of third-party threat intelligence service integrations," and using "5 million indicators simultaneously." Ex. 2007, 5; *see* PO Resp. 64. Again, insufficient analysis is presented to address how these features relate to the challenged claims. Patent Owner's

reference to the American Banker article similarly suffers from a lack of explanation. *See* PO Resp. 64–65.

The only nexus explanation provided is a conclusory assertion that "the salutary benefits of [the praised products] are made possible in large part by the '722 Patent's packet-filtering rules, which transform network-threat indicators into actionable rules." *Id.* at 65. Dr. Orso's testimony cited in support of this statement is merely a near-verbatim copy of this conclusory statement with no additional explanation. *See* Ex. 2002 ¶ 123; 37 C.F.R. § 42.65(a). As a result, we find that Patent Owner has not established a sufficient nexus between the cited industry praise and the invention of the challenged claims.

c. Commercial Success and Licensing

Finally, Patent Owner contends that the commercial success of its RuleGATE product as well as a license to the '722 Patent taken by Keysight Technologies are compelling secondary considerations of non-obviousness. PO Resp. 65–67. We disagree.

First, we note that the sole evidence cited for the commercial success of the RuleGATE product, a declaration by Mr. Jonathan Rogers of Centripetal, makes no mention whatsoever of the '722 Patent. *See* Ex. 2016. Rather, the Rogers Declaration is testimony that was submitted in a different *inter partes* review challenging a different patent. *See id*. As such, there is no record evidence supporting any nexus between the matters in Mr. Rogers' testimony on alleged commercial success and the '722 Patent.

Second, as Patent Owner itself admits (PO Resp. 66), the Keysight license was a "worldwide, royalty-bearing, non-transferable, irrevocable, non-terminable, non-exclusive license to Centripetal's worldwide patent portfolio." Ex. 2012, 88. No information is provided about the relevant details of this license—e.g., how many patents comprise the portfolio, the relative contributions of the patents in the portfolio to the value of the license—such that we could discern whether Keysight took the license "out of recognition and acceptance of the subject matter claimed" in the '713 Patent. *See In re GPAC Inc.*, 57 F.3d 1573, 1580 (Fed. Cir. 1995). In fact, the record evidence indicates that this license was taken to settle litigation (Ex. 2012, 88), which diminishes its probative value as an indicator of non-obviousness. *See GPAC*, 57 F.3d at 1580. As such, we find that Patent Owner has not provided sufficient evidence to establish the requisite nexus between the Keysight license and the '722 Patent. *See id.*

6. Conclusion as to Obviousness

As discussed above, Petitioner has shown by a preponderance of the evidence that Sourcefire teaches each limitation of claims 1–7, 10–12, 14–21, 24, and 25. We further determine that Petitioner's showing that the claims are taught by Sourcefire is strong, particularly in comparison to Patent Owner's weak showing with respect to the asserted secondary considerations of obviousness. As discussed above, we find that Patent Owner has not established the requisite nexus between the challenged claims and *any* of the asserted secondary considerations. As such, we are unable to accord them any substantial weight. *See Fox Factory*, 944 F.3d at 1373. Therefore,

in weighing the totality of the evidence of record and the strength of the parties' showings on the inquiries underlying the question of obviousness, we conclude that Petitioner has met its overall burden of proving by a preponderance of the evidence that 1–7, 10–12, 14–21, 24, and 25 would have been obvious in view of Sourcefire.

Also as discussed above, we determine that Petitioner has not shown that Sourcefire teaches each limitation of claims 8, 9, 13, 22, and 23. Thus, we conclude that Petitioner has not met its overall burden to prove the unpatentability of these claims.

E. Motions to Exclude and Other Matters

1. Petitioner's Motion to Exclude (Paper 29, "Pet. Mot.")

Petitioner moves to exclude Exhibits 2003, 2005–2007, 2011–2013, and 2016. Pet. Mot. 2. Exhibits 2003 and 2005 did not form the basis for any aspect of this Decision. As such, Petitioner's Motion with respect to those exhibits is moot.

For Exhibit 2016, the Rogers Declaration, Petitioner asserts that it should be excluded under Rules 401, 402, and 403 of the Federal Rules of Evidence. Pet. Mot. 10–11. We agree with Patent Owner that exclusion is unwarranted. Paper 32, 5–7. We note that Patent Owner relies on Exhibit 2016 to support its arguments for commercial success, which specifically note the alleged success of the RuleGATE product. PO Resp. 65. Although the Rogers Declaration addresses a different patent than

the '722 Patent, its testimony regarding the RuleGATE product and Centripetal's customers generally meets the threshold for relevance, and its purported shortcomings as evidence go to its persuasive weight rather than its admissibility. We also discern no risk of unfair prejudice. Thus, Petitioner's objections under Rules 401, 402, and 403 are denied.

Petitioner argues that Exhibits 2006, 2007, and 2011–2013 should be excluded under Rules 401, 402, 403, 901, and as hearsay (under Rule 802). Pet. Mot. 7–9. We are not persuaded. Each of these exhibits is cited by Patent Owner as evidence supporting its arguments regarding secondary considerations of non-obviousness, including as evidence of industry praise and the existence of a relevant license. *See* PO Resp. 59–66. Although they may not identify the '722 Patent specifically (Pet. Mot. 7), we determine that they meet the threshold for relevance nonetheless, and we discern no risk of unfair prejudice, confusion, or waste of time. Regarding authentication, we note that the Declaration of Jeffrey H. Price (Ex. 2018) provides evidence of the source of each of these exhibits, and we find that this information along with the distinctive characteristics of the exhibits themselves (including dates, titles, publication names, etc.) provide the necessary basis for authentication.[13] With respect to Petitioner's hearsay objections, we conclude first that Exhibits 2007 and 2011 are not hearsay because they are not relied on for the truth of the matters asserted. *See* Fed. R. Evid. 801(c). These exhibits are cited only as evidence of industry praise; their

13. We further note that at least Exhibits 2007 and 2011 are printed material purporting to be from news sources, which are self-authenticating under Rule 902(6).

relevance lies in that they include statements from the industry allegedly praising Centripetal's invention, not in whether that praise is true or accurate. *See* PO Resp. 64–65. For the remaining exhibits, we deny Petitioner's hearsay objection under Rule 807 because we conclude that the totality of the circumstances provides sufficient indicia of trustworthiness—for example, these exhibits are contemporaneous documents by third parties produced for purposes that indicate their statements are likely reliable (e.g., Keysight's official Annual Report (Ex. 2012))—and these exhibits generally are highly probative on the points underlying Patent Owner's secondary considerations allegations (e.g., industry praise) compared to different evidence reasonably available to Patent Owner.

For the above reasons, we are not persuaded that any of these exhibits should be excluded and, thus, we deny Petitioner's Motion to Exclude.

2. Patent Owner's Motion to Exclude (Paper 28, "PO Mot.")

Patent Owner moves to exclude Exhibits 1038 and 1042. PO Mot. 1. Exhibit 1038 did not form the basis for any aspect of this Decision. Thus, Patent Owner's Motion is moot as to that exhibit.

For Exhibit 1042 (the Baugher Declaration), Patent Owner objects on the basis of Rule 403 and 37 C.F.R. § 42.61. *Id.* The crux of Patent Owner's objections is that the Baugher Declaration was submitted with Petitioner's Reply instead of the Petition, which Patent Owner considers to be untimely. *Id.* at 1–4. According to Patent

Owner, the timing of the Baugher Declaration's submission was unfairly prejudicial to Patent Owner, including because Patent Owner was denied an opportunity to seek additional discovery related to his testimony. *Id.*

As an initial matter, we note that Patent Owner's objections to the Baugher Declaration did not include any objection based on Rule 403. *See* Paper 21, 3. Thus, Patent Owner did not preserve a Rule 403 objection to the Baugher Declaration, and we deny that objection at least for that reason. *See* 37 C.F.R. § 42.64 (b)(1), (c).

We also agree with Petitioner, however, that the Baugher Declaration was not unfairly prejudicial. *See* Paper 31. As Petitioner explains (*id.* at 2–5), the Baugher Declaration was submitted to address arguments raised in the Patent Owner Response in compliance with our rules. *See* 37 C.F.R. § 42.23(b) ("A reply may only respond to arguments raised in the corresponding opposition, patent owner preliminary response, or patent owner response."). Specifically, the Patent Owner Response asserted that another declarant, Mr. Leone, had insufficiently accounted for his testimony regarding the amount of sales of Sourcefire products. *See* PO Resp. 6–7. Mr. Baugher's testimony corroborated Mr. Leone's testimony and provided information regarding the source for that testimony, which addressed issues raised by Patent Owner. *See* Paper 31, 3.

Although the substance of Mr. Baugher's testimony was known to Petitioner at the time the Petition was filed (*see* PO Mot. 3), that subject matter *was* presented with the Petition in the form of Mr. Leone's testimony. The

Baugher Declaration did not introduce any new theory of unpatentability, or any new factual issue regarding the public accessibility of Sourcefire. The issue of whether Sourcefire was disseminated as part of sales of Sourcefire products, and the scope of those sales, was properly raised in the Petition and supported by the Leone Declaration. *See* Pet. 24 (citing Ex. 1005); *cf. Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1369 (Fed. Cir. 2016) (approving of the Board's exclusion of new arguments raised *for the first time* in a reply). Although the Baugher Declaration provided additional evidence relevant to those issues, it was appropriately provided to address specific arguments and allegations in the Patent Owner Response, as explained above. Thus, we determine that the Baugher Declaration was not untimely filed.

Moreover, we note that Patent Owner had the opportunity to depose Mr. Baugher, and did so. *See* Ex. 2017. Patent Owner also had the opportunity to address Mr. Baugher's testimony in its Sur-reply, and did so, including by presenting testimony it elicited during Mr. Baugher's deposition. *See* PO Sur-reply 8–10. Thus, we disagree that Patent Owner was unfairly prejudiced by the timing of the Baugher Declaration.

Patent Owner also asserts that it was prevented from obtaining discovery on purported "restrictions" on the dissemination of Sourcefire that Mr. Baugher allegedly disclosed at this deposition. PO Mot. 3–4. We note that this issue was raised by Mr. Baugher's deposition testimony under questioning by Patent Owner, not the Baugher Declaration. *See id.* Additionally, we note that Patent Owner was previously aware of the issue of restrictions

on dissemination and access, which Patent Owner itself raised in its Response. *See* PO Resp. 3–5, 10. Patent Owner did not, however, avail itself of an earlier opportunity to seek discovery on that issue, declining to depose Petitioner's original declarant on public accessibility issues, Mr. Leone. As a result, we conclude that the totality of the circumstances indicates that Patent Owner was not unfairly prejudiced.

For the above reasons, we are not persuaded that any of the exhibits challenged by Patent Owner should be excluded and, thus, we deny Patent Owner's Motion to Exclude.

3. Patent Owner's Request to File a Motion for Supplemental Information

Just prior to the oral hearing, Patent Owner contacted the Board to request authorization to file a motion to submit supplemental information, which was considered at the prehearing conference. *See* Ex. 1046, 4:3–7. Specifically, Patent Owner sought to introduce evidence of the allowance of a patent stemming from a continuation of the application that led to the '722 Patent. *See id.* at 5:23–6:9. We denied the request, principally because the request came very late in the case and, thus, would unfairly prejudice Petitioner as well as disrupt the parties' and the Board's preparations for the oral hearing and the case schedule. *See id.* at 10:3–11:1, 11:23–12:13. Under those circumstances, we were not persuaded that the potential probative value of the proposed evidence—which concerned a related but different patent with different

claims[14]—outweighed the potential prejudice to Petitioner and disruption to the case. *See id.*

We note, however, that Patent Owner nonetheless raised the proposed evidence during the oral hearing, our ruling on its request notwithstanding. *See* Tr. 34:14–35:6. We emphasize that the proposed evidence is not part of the record of this case, and we do not consider any arguments pertaining to such evidence. Further, we expect all parties appearing before the Board to comply with our rules, and all rulings made by the Board during one of our proceedings.

CONCLUSION[15]

For the foregoing reasons, Petitioner has shown by a preponderance of the evidence that certain challenged claims of the '722 Patent are unpatentable, as summarized in the following table:

---

14. We note that the patent application in question was, at the time, still unpublished and not publicly available. *See id.* at 5:14–19.

15. 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).

Appendix E

Claims	35 U.S.C. §	Reference(s)	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1–25	103	Sourcefire	1–7, 10–12, 14–21, 24, 25	8, 9, 13, 22, 23
Overall Outcome			1–7, 10–12, 14–21, 24, 25	8, 9, 13, 22, 23

ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1–7, 10–12, 14–21, 24, and 25 of the '722 Patent are held unpatentable as obvious under 35 U.S.C. § 103 in view of Sourcefire;

FURTHER ORDERED that claims 8, 9, 13, 22, and 23 of the '722 Patent are not held as obvious under 35 U.S.C. § 103 in view of Sourcefire;

FURTHER ORDERED that Petitioner's Motion to Exclude (Paper 29) is *denied* as set forth above;

FURTHER ORDERED that Patent Owner's Motion to Exclude (Paper 28) is *denied* as set forth above;

Appendix E

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

PETITIONER:

Patrick McPherson
Patrick Muldoon
Joseph Powers
Christopher Tyson
pdmcpherson@duanemorris.com
pcmuldoon@duanemorris.com
japowers@duanemorris.com
cjtyson@duanemorris.com

PATENT OWNER:

James Hannah
Jeffrey Price
Jonathan Caplan
Michael Lee
Bradley Wright
jhannah@kramerlevin.com
jprice@kramerlevin.com
mhlee@kramerlevin.com
bwright@bannerwitcoff.com

APPENDIX F — 35 U.S.C. 102

35 U.S.C. 102 (PRE-AIA)

CONDITIONS FOR PATENTABILITY; NOVELTY AND LOSS OF RIGHT TO PATENT.

[Editor Note: With the exception of subsection (g)),* ***not applicable*** *to any patent application subject to the first inventor to file provisions of the AIA (see* ***35 U.S.C. 100 (note)****). See* ***35 U.S.C. 102*** *for the law otherwise applicable.]*

A person shall be entitled to a patent unless —

- (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for patent, or

- (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of the application for patent in the United States, or

- (c) he has abandoned the invention, or

- (d) the invention was first patented or caused to be patented, or was the subject of an inventor's certificate, by the applicant or his legal representatives or assigns in a foreign country prior to the date of the application for patent in this country on an application for patent or inventor's

certificate filed more than twelve months before the filing of the application in the United States, or

- (e) the invention was described in — (1) an application for patent, published under ***section 122(b)***, by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in ***section 351(a)*** shall have the effects for the purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under ***Article 21(2)*** of such treaty in the English language; or

- (f) he did not himself invent the subject matter sought to be patented, or

- (g)(1) during the course of an interference conducted under ***section 135*** or ***section 291***, another inventor involved therein establishes, to the extent permitted in ***section 104***, that before such person's invention thereof the invention was made by such other inventor and not abandoned, suppressed, or concealed, or (2) before such person's invention thereof, the invention was made in this country by another inventor who had not abandoned, suppressed, or concealed it. In determining priority of invention under this subsection, there shall be considered not only the respective dates of conception and reduction to

practice of the invention, but also the reasonable diligence of one who was first to conceive and last to reduce to practice, from a time prior to conception by the other.

(Amended July 28, 1972, Public Law 92-358, sec. 2, 86 Stat. 501; Nov. 14, 1975, Public Law 94-131, sec. 5, 89 Stat. 691; subsection (e) amended Nov. 29, 1999, Public Law 106-113, sec. 1000(a)(9), 113 Stat. 1501A-565 (S. 1948 sec. 4505); subsection (g) amended Nov. 29, 1999, Public Law 106-113, sec. 1000(a)(9), 113 Stat. 1501A-590 (S. 1948 sec. 4806); subsection (e) amended Nov. 2, 2002, Public Law 107-273, sec. 13205, 116 Stat. 1903.)

(Public Law 112-29, sec. 14, 125 Stat. 284 (Sept. 16, 2011) provided that tax strategies are deemed to be within the prior art (see ***AIA § 14***).)

NOTE:** The provisions of ***35 U.S.C. 102(g), as in effect on March 15, 2013, shall apply to each claim of an application for patent, and any patent issued thereon, for which the first inventor to file provisions of the AIA apply (see ***35 U.S.C. 100 (note)***, if such application or patent contains or contained at any time—

(A) a claim to an invention having an effective filing date as defined in section ***100(i)*** of title 35, United States Code, that occurs before March 16, 2013; or

(B) a specific reference under section ***120***, ***121***, or ***365(c)*** of title 35, United States Code, to any patent or application that contains or contained at any time such a claim.