Trials@uspto.gov
571.272.7822

Paper No. 40
Entered: January 23, 2020

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, INC.,
Patent Owner.

IPR2018-01436
Patent 9,124,552 B2

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)

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.

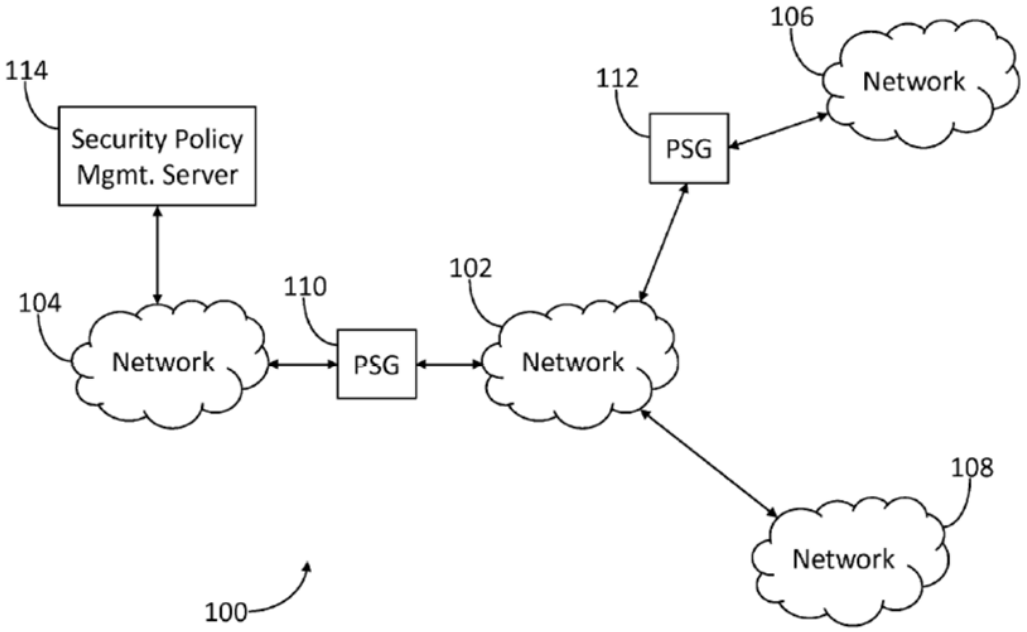
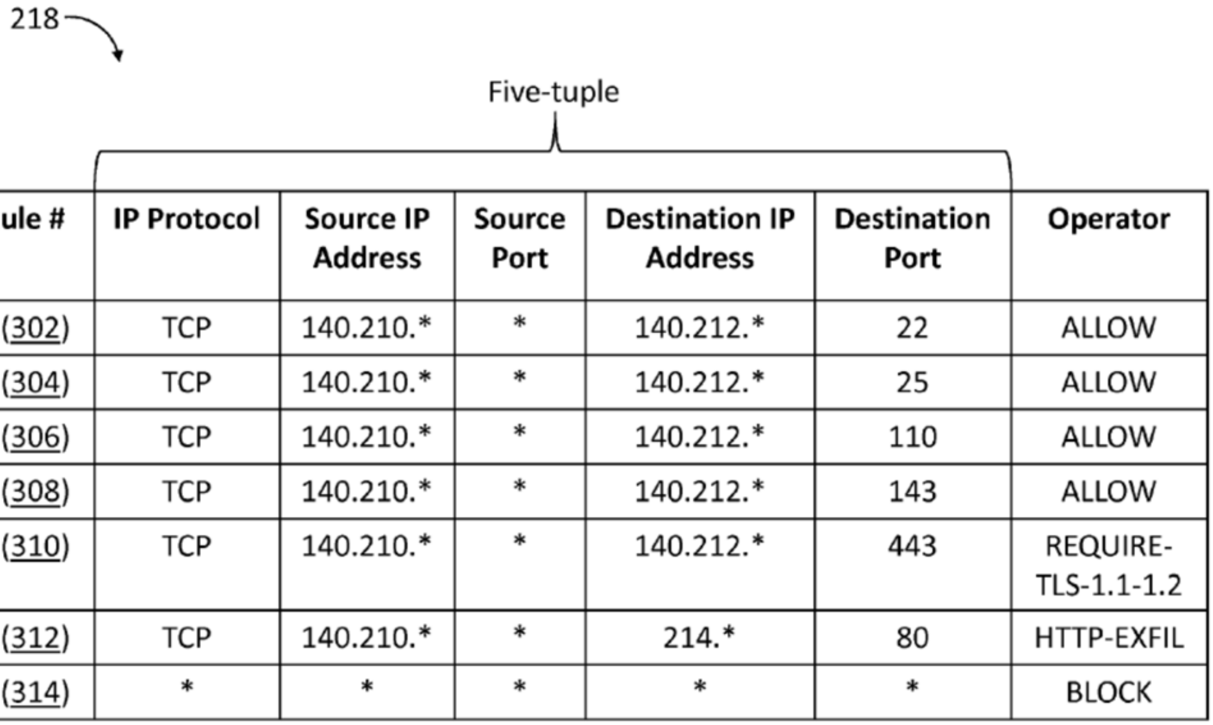


FIG. 1

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.


218
Five-tuple

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.

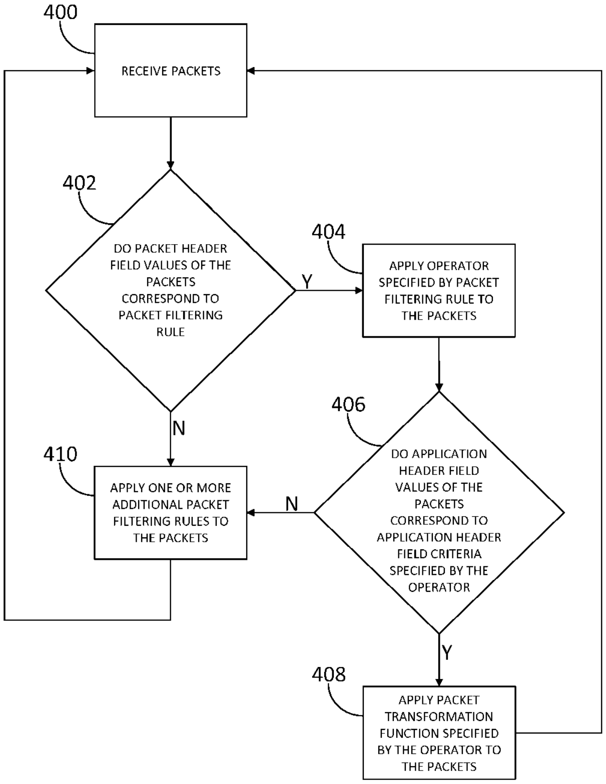

400
RECEIVE PACKETS
402
DO PACKET HEADER FIELD VALUES OF THE PACKETS CORRESPOND TO PACKET FILTERING RULE
Y
404
APPLY OPERATOR SPECIFIED BY PACKET FILTERING RULE TO THE PACKETS
N
406
DO APPLICATION HEADER FIELD VALUES OF THE PACKETS CORRESPOND TO APPLICATION HEADER FIELD CRITERIA SPECIFIED BY THE OPERATOR
410
APPLY ONE OR MORE ADDITIONAL PACKET FILTERING RULES TO THE PACKETS
N
Y
408
APPLY PACKET TRANSFORMATION FUNCTION SPECIFIED BY THE OPERATOR TO THE PACKETS

FIG. 4

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:
>
> [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. § 103. Because the '552

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 computer science or a related field." Ex. 2002 ¶¶ 42–43. In the Institution Decision, we adopted Petitioner's proposed description of the level of

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

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 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

[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).

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.* 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

[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.

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

[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 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 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 POSA understood 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.

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

[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*.

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).

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.

[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

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 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

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.

"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. *See Medtronic*, 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]

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

[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 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.

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 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).

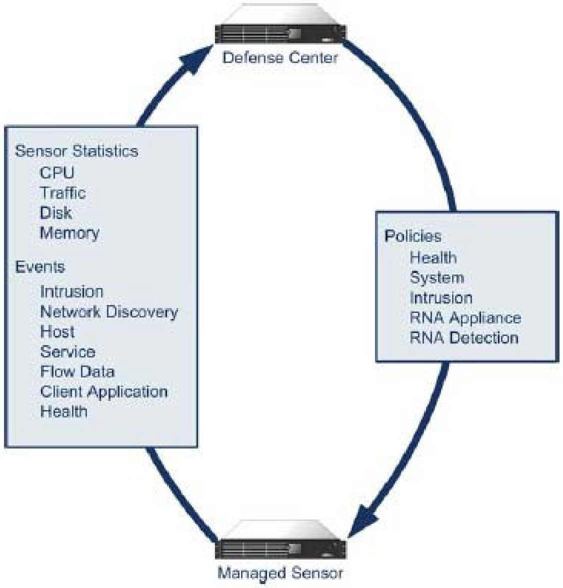
2. Overview of Sourcefire

Sourcefire is a user manual for the Sourcefire 3D System. Pet. 23; Ex. 1004. Sourcefire describes that the 3D System could identify changing

[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").

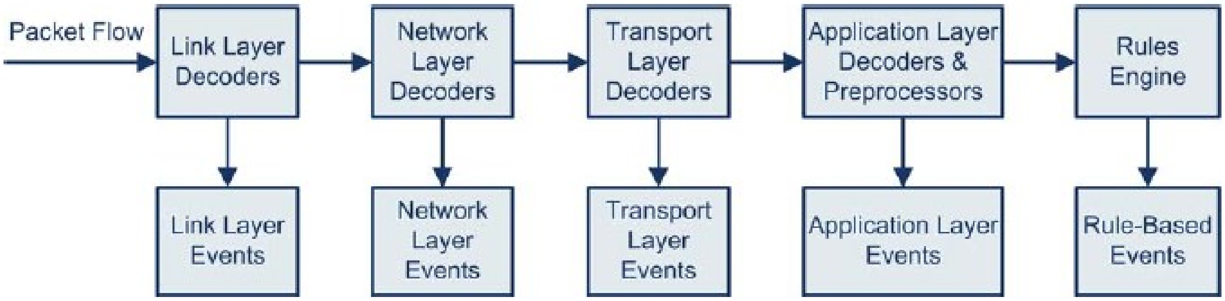
assets and vulnerabilities on the network, determine the types of attacks against the network and their impact, and defend the network in real time. Ex. 1004, 32.

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 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.



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.

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 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.

[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).

[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.

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 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.

According to Patent Owner, Petitioner incorrectly argues that "a POSA understood that Sourcefire describes the use of SSL/TLS rule

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

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

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 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,

[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 Superguide Corp. v. DirecTV Enters., Inc.*, 358 F.3d 870, 875 (Fed. Cir. 2004).

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 '"[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, 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

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

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 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

[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.

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 that such reassembled or reconstructed messages 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

[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.

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 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

[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.*).

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"

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

(*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 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 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.

[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).

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:

Claims	**35 U.S.C. §**	**Reference(s)**	**Claims Shown Unpatentable**	**Claims Not Shown Unpatentable**
1–21	103(a)	Sourcefire	1–21	
Overall Outcome			1–21	

[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).

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.

For PETITIONER:

Patrick McPherson
Christopher Tyson
Joseph Powers
DUANE MORRIS LLP
pdmcpherson@duanemorris.com
cjtyson@duanemorris.com
japowers@duanemorris.com

For PATENT OWNER:

James Hannah
Jeffrey Price
Michael Lee
KRAMER LEVIN NAFTALIS & FRANKEL LLP
jhannah@kramerlevin.com
jprice@kramerlevin.com
mhlee@kramerlevin.com

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