UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KEYSIGHT TECHNOLOGIES, INC. and
PALO ALTO NETWORKS, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, LLC,
Patent Owner.

IPR2023-00446[1]
Patent 10,567,343 B2

Before KEVIN F. TURNER, AARON W. MOORE, and
STEVEN M. AMUNDSON, *Administrative Patent Judges.*

TURNER, *Administrative Patent Judge*.

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

[1] IPR2023-01353 has been joined with this proceeding.

I. INTRODUCTION

A. Background and Summary

In response to a Petition (Paper 2, "Pet."), on August 7, 2023, we instituted an *inter partes* review of claims 1–20 ("the challenged claims") of U.S. Patent No. 10,567,343 B2 (Ex. 1001, "the '343 Patent"). Paper 9 ("Dec. to Inst."). That decision was the subject of a request by Patent Owner for Director Review (Paper 12), which was later denied (Paper 14). Patent Owner subsequently filed a Patent Owner Response (Paper 15, "PO Resp."), Petitioner filed a Petitioner Reply (Paper 20, "Pet. Reply"), Patent Owner filed a Patent Owner Sur-reply (Paper 22, "PO Sur-reply"), and a transcript of an oral hearing held on May 6, 2024 (Paper 29, "Hr'g Tr.") has been entered into the record.

We have jurisdiction under 35 U.S.C. § 6. This Final Written Decision is issued pursuant to 35 U.S.C. § 318(a). We base our decision on the preponderance of the evidence. 35 U.S.C. § 316(e) (2018); 37 C.F.R. § 42.1(d) (2024).

Having reviewed the arguments of the parties and the supporting evidence, we conclude that Petitioner has demonstrated by a preponderance of the evidence that claims 1–4, 6–11, and 13–20 of the challenged claims are unpatentable.

B. Related Proceedings

The Petition states that the '343 Patent is asserted in the following litigation: *Centripetal Networks, Inc. v. Keysight Technologies, Inc.*, 2:22-cv-00002 (E.D. Va.) (filed Jan. 1, 2022), where Patent Owner cites to the same. Pet. 4; Paper 3, 1. The '343 Patent was previously the subject of another potential *inter partes* review, IPR2021-01155, with Palo Alto

Networks, Inc. as the prior petitioner, where institution was denied on the basis of that prior petitioner's petition. *See* Ex. 2004.

C. Real Party-in-Interest

Petitioner identifies itself as the sole real party-in-interest. Pet. 4. Patent Owner identifies itself as the sole real party-in-interest. Paper 3, 1.

D. The '343 Patent

The '343 Patent is directed to "filtering network data transfers" to protect data from being stolen by "exfiltrations." Ex. 1001, code (57). Exfiltrations are often facilitated using popular data transfer protocols, such as the Hypertext Transfer Protocol (HTTP), and such attacks may appear to be "normal network behavior" and interpreted by firewalls as "trusted operations." *Id*. at 1:28–51.

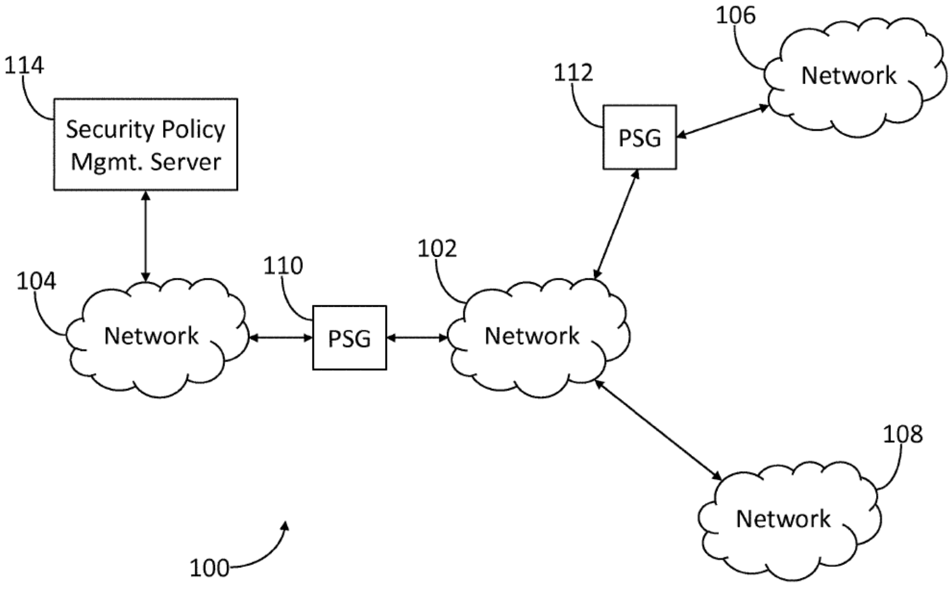
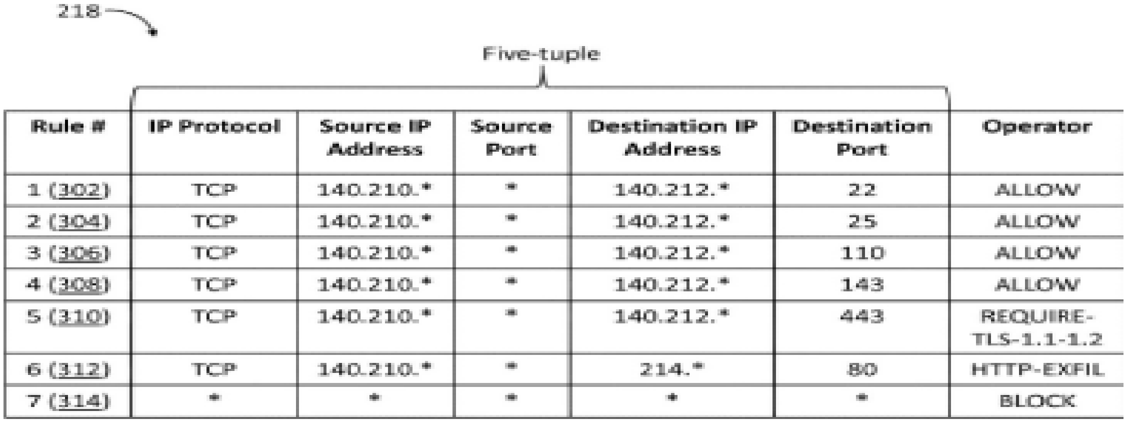


Figure 1 of the '343 Patent illustrates an exemplary network environment

The '343 Patent describes a two-stage filtering process for stopping such attacks implemented at Packet Security Gateways (PSGs, 110, 112), in network environment 100, placed at boundaries of networks they protect, and security policy management server 114. Ex. 1001, 3:62–4:41, 5:29–49, 8:39–52. As the PSG receives packets, it applies packet-filtering rules, which may implement "operators." *Id*. at 3:62–4:14, 8:39–52. In the first stage, the "5-tuple" of packet header fields (source and destination IPs and ports and transport protocol) are filtered, and in the second stage, the operators may filter application packet header field values. *Id*. at 5:20–49, 8:39–52. Exemplary packet-filtering rules are provided in Figure 3 and reproduced below:



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

The rules may specify criteria and one or more operators that may be applied to packets matching specified criteria. For example, rule 1 specifies that IP packets containing TCP packets from an IP 140.210.*, having any source port, destined for an IP 140.212.*, and destined for port 22, have an ALLOW operator. Ex. 1001, 5:63–6:24. Rules 5 and 6 have both 5-tuple criteria (first stage) and application-header-field-value criteria (second stage), where rule 6 specifies that a PSG applies an HTTP-EXFIL operator to IP packets containing TCP packets from the same sources and ports as rule 1 but destined for port 80 (associated with HTTP) on an IP address 214.*. *Id*. at 6:25–7:23, 7:41–47, 8:11–38, Fig. 3. The HTTP-EXFIL operator allows HTTP packets containing a GET method, but blocks HTTP packets containing other HTTP methods (e.g., PUT, POST, CONNECT, etc.), where attackers may often use HTTP PUT or POST methods to exfiltrate sensitive data, so that "operators such as HTTP-EXFIL [of rule 6] may be used to stop such exfiltrations." *Id.* at 7:4–23, 7:41–8:6.

E. Illustrative Claim

As noted above, Petitioner challenges claims 1–20, with claims 1, 8, and 15 being independent claims. Claim 1 is illustrative of the challenged claims and is reproduced below:

> 1. **[1pre]** A method comprising:
>
> **[1a]** receiving, by a computing system comprising memory and at least one processor, a plurality of packets, wherein the plurality of packets comprises a first portion of packets and a second portion of packets;
>
> **[1b]** determining, based on a packet header field value, whether each packet of the plurality of packets comprises data corresponding to first criterion specified by one or more packet-filtering rules;
>
> **[1c]** responsive to a determination by the computing system that a packet header field value of the first portion of packets comprises data corresponding to the first criterion specified by at least one matching packet-filtering rule, applying, by the computing system and to each packet in the first portion of packets, one or more operators specified by the at least one matching packet-filtering rule;
>
> **[1d]** determining, based on an application header field value, the second portion of packets based on whether the first portion of packets comprises data corresponding to second criterion specified by one or more operators specified by the at least one matching packet-filtering rule; and
>
> **[1e]** responsive to determining the second portion of packets that comprises data corresponding to the second criterion specified by one or more operators specified by the at least one matching packet-filtering rule, applying, by the computing system and to each packet in the second portion of packets that match the second criterion, at least one

> packet transformation function configured to prevent an exfiltration operation, wherein the at least one packet transformation function indicates whether each packet in the second portion of packets is allowed to continue toward its destination.

Ex. 1001, 11:28–61 (with annotations provided by Petitioner, Pet. xvii).

F. Ground of Institution

Trial was instituted on the following ground:

References	35 U.S.C. §[2]	Claims Challenged
Sourcefire[3], Emerging Threats[4]	§ 103(a)	1–20

Dec. to Inst. 27. Petitioner relies on the declaration of Dr. Stuart Staniford (Ex. 1003), and Patent Owner relies on the declaration of Dr. Michael T. Goodrich (Ex. 2010) and the declaration of Pedro Marinho (Ex. 2031), with a deposition of Dr. Staniford (Ex. 2011) and depositions of Dr. Goodrich (Ex. 1100) and Mr. Marinho (Ex. 1101) entered into the record.

II. ANALYSIS

A. Level of Ordinary Skill in the Art

The level of ordinary skill in the pertinent art at the relevant time is a factor in how we construe patent claims. *See Phillips v. AWH Corp.*, 415

[2] The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011), amended 35 U.S.C. § 103 effective March 16, 2013. Because the ’343 Patent has an effective filing date prior to the effective date of the applicable AIA amendment, we refer to the pre-AIA version of § 103.

[3] Sourcefire 3D System User Guide Version 4.10 (Ex. 1004, “Sourcefire”).

[4] Emerging Threats, *available* at https://web.archive.org/web/20101202025325/http://rules.emergingthreats.net/open/snort-2.8.4/emerging-all.rules (Dec. 2, 2010). (Ex. 1020, “Emerging Threats”).

F.3d 1303, 1312–13 (Fed. Cir. 2005) (en banc). It is also one of the factors we consider when determining whether a patent claim is obvious over the prior art. *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

To assess the level of ordinary skill, we construct a hypothetical "person of ordinary skill in the art," from whose vantage point we assess obviousness and claim interpretation. *See In re Rouffet*, 149 F.3d 1350, 1357 (Fed. Cir. 1998). This legal construct "presumes that all prior art references in the field of the invention are available to this hypothetical skilled artisan." *Id.* (citing *In re Carlson*, 983 F.2d 1032, 1038 (Fed. Cir. 1993)).

Petitioner, supported by Dr. Staniford's testimony, proposes that a person of ordinary skill in the art at the time of the invention "would have had a bachelor's degree in computer science, computer engineering, or an equivalent, and four years of industry experience," and "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. 16 (citing Ex. 1003 ¶¶ 23, 25). Patent Owner does not challenge the qualifications proposed by Petitioner for a person of ordinary skill in the art. *See generally* PO Resp.

We find Petitioner's proposal consistent with the level of ordinary skill in the art reflected by the prior art of record, *see Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001); *In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995); *In re Oelrich*, 579 F.2d 86, 91 (CCPA 1978), and, therefore, we adopt Petitioner's unopposed position as to the level of ordinary skill in the art for purposes of this Decision

B. Claim Construction

In an *inter partes* review, we construe a patent claim "using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b)." 37 C.F.R. § 42.100(b). In applying such standard, claim terms are generally given their ordinary and customary meaning, as would be understood by a person of ordinary skill in the art, at the time of the effective filing date of the patent application and in the context of the entire patent disclosure. *Phillips*, 415 F.3d at 1312–13. "In determining the meaning of the disputed claim limitation, we look principally to the intrinsic evidence of record, examining the claim language itself, the written description, and the prosecution history, if in evidence." *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 469 F.3d 1005, 1014 (Fed. Cir. 2006) (citing *Phillips*, 415 F.3d at 1312–17).

In the Institution Decision, we discussed a possible construction of the claim term "operator," which Petitioner indicated needed additional discussion (Pet. 20–23), and although we discussed the use of the limitation (Dec. to Inst. 30–33), we determined that no explicit construction of "operator" was necessary (*id*. at 20).

Patent Owner brings to our attention certain claim constructions by the district court in the related litigation (Ex. 2012), where Patent Owner advocated for the plain and ordinary meaning of the terms "exfiltration," "exfiltration operation," "network exfiltration," and "network exfiltration methods" found in the '343 Patent. PO Resp. 8. Patent Owner points out that the district court adopted a construction of the term "network exfiltration methods" to mean "the unauthorized transfer of data from a computer by malware or by a malicious actor," and argues that Petitioner has failed to demonstrate that the asserted references render obvious the challenged claims under either Patent Owner's proposed claim constructions or the district court's adopted constructions. *Id.* at 8–9 (citing Ex. 2012, 11).

Petitioner responds that Patent Owner is arguing that the claims prevent exfiltrations "while still preserving the flow of normal legitimate network traffic without disruption," such that Petitioner asserts that "[Patent Owner] also argues that rules are not configured to prevent exfiltration where [Patent Owner] avers that the rule is overbroad (also blocking legitimate traffic) or too specific (also allowing some exfiltrations)." Pet. Reply 2 (citing PO Resp. 10–11, 18). Based on this, Petitioner argues that "the parties dispute whether 'configured to prevent an exfiltration operation' has its plain meaning or requires preventing exfiltrations while not having some amount of false positives or negatives, as [Patent Owner] implicitly asserts." *Id.*

Petitioner argues that we should reject Patent Owner's attempt to read additional requirements into the claim term "configured to prevent an exfiltration operation," such that it does not require preventing all exfiltrations or allowing all non-exfiltration traffic. Pet. Reply 2. Petitioner continues that the specification of the '343 Patent discloses only HTTP and HTTPS methods to prevent exfiltrations (Ex. 1001, 8:59–62), and that "construing 'prevent an exfiltration operation' to require a rule to somehow satisfy breadth or narrowness requirements would improperly exclude these embodiments." *Id.* at 2–3 (citing *MBO Lab'ys, Inc. v. Becton, Dickinson & Co.*, 474 F.3d 1323, 1333 (Fed. Cir. 2007)).

Patent Owner responds that there is no claim-construction dispute, asserting that its arguments regarding "preventing exfiltrations 'while still preserving the flow of normal legitimate network traffic without disruption' were made in the context of rebutting Petitioner's conclusory, unsupported attempts to transform Emerging Threats' alert rules into drop rules . . . or to help explain the benefits achieved by the claimed invention." PO Sur-reply 8 (citing PO Resp. 10–12, 30).

We largely agree with Patent Owner that there is no explicit claim-construction dispute. We address Patent Owner's issues of what ordinarily skilled artisans would have considered in creating and implementing packet-filtering rules in the discussion below. The preservation of the flow of normal legitimate network traffic without disruption is one aspect that those with a working knowledge of packet-switched networking, firewalls, security policies, communication protocols and layers, and the use of customized rules to address cyber-attacks would have considered. Nonetheless, overall, we determine that the plain and ordinary meaning of "configured to prevent an exfiltration operation," does not require preventing all exfiltrations from occurring, nor allowing all non-exfiltration traffic, and that we need not consider the preservation of the flow of normal legitimate network traffic without disruption in the context of that claim construction. We determine that no claim terms need to be construed expressly for purposes of this Decision.

C. Legal Standards

The question of obviousness is resolved on the basis of underlying factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) objective evidence of nonobviousness. *See Graham*, 383 U.S. at 17. Additionally, the obviousness inquiry typically requires an analysis of "whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006) (requiring "articulated reasoning with some rational underpinning to support the legal conclusion of obviousness")); *see In re Warsaw Orthopedic, Inc.*, 832 F.3d 1327, 1333 (Fed. Cir. 2016) (citing *DyStar Textilfarben GmbH & Co. Deutschland KG v. C.H. Patrick Co.*, 464 F.3d 1356, 1360 (Fed. Cir. 2006)).

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

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

In determining whether a claim is obvious in light of the prior art, when in evidence, we consider any relevant objective evidence of non-obviousness. *See Graham*, 383 U.S. at 17–18. Notwithstanding what the teachings of the prior art would have suggested to one of ordinary skill in the art at the time of the invention, the totality of the evidence submitted, including objective evidence of non-obviousness, may lead to a conclusion that the challenged claims would not have been obvious to one of ordinary skill. *In re Piasecki*, 745 F.2d 1468, 1471–72 (Fed. Cir. 1984).

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

D. Obviousness over Sourcefire and Emerging Threats

Petitioner asserts that claim 1–20 are unpatentable over Sourcefire and Emerging Threats. Pet. 17. Petitioner addresses each limitation of claim 1 and provides the testimony of Dr. Staniford in support of its position with respect to them. Pet. 46–58; Ex. 1003 ¶¶ 236–268. Petitioner also addresses the limitations of independent claims 8 and 15, referencing the analysis of independent claim 1. Pet. 46–58; Ex. 1003 ¶¶ 236–268. In addition, Petitioner argues that collateral estoppel applies to specific issues in this proceeding based on issues decided against Patent Owner in a prior proceeding. Pet. 44–46.

Patent Owner argues that the challenged claims are patentable over Sourcefire and Emerging Threats based on specific arguments: (1) that Emerging Threats is not a printed publication (PO Resp. 34–45); (2) that the combination of Sourcefire and Emerging Threats does not disclose claim limitation [1e] (PO Resp. 13–23; PO Sur-reply 3–14); (3) that Petitioner's obviousness analysis is tainted by impermissible hindsight bias (PO Resp. 23–26); and (4) that the evidence of secondary considerations demonstrates the non-obviousness of the challenged claims (PO Resp. 27–34; PO Sur-reply 16–19). Patent Owner does not provide separate arguments with respect to the other independent claims, and with respect to most of the dependent claims, only providing separate arguments with respect to dependent claims 5 and 12. PO Resp. 26–27; PO Sur-reply 14–15.

We begin with discussions of Sourcefire and Emerging Threats, consider the status of Emerging Threats as a printed publication, examine the application of collateral estoppel with respect to certain issues, consider Petitioner's assertions regarding the references' teachings with respect to independent claim 1, then consider Patent Owner's arguments countering those assertions, based on its specific arguments, and finally address the instant ground with respect to the other independent and dependent claims.

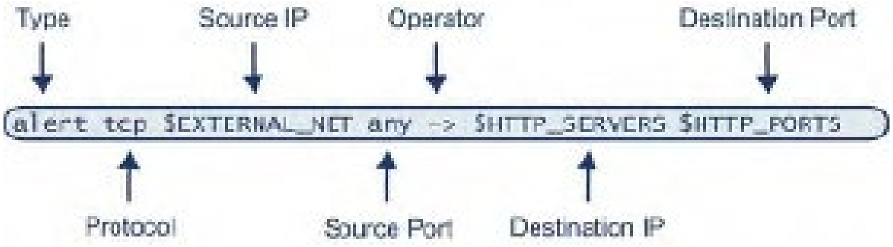
1. Sourcefire

Sourcefire is a user guide for the Sourcefire 3D System, a system that provides "real-time network intelligence for real-time network defense." Ex. 1004, 32.[5] The system operates via "3D Sensors" that can each run the Sourcefire "Intrusion Prevention System" (IPS), which allows monitoring of networks for attacks by examining packets for malicious activity. *Id.* at 33–34. Users can create custom "intrusion rules" to examine packets for attacks and manage the rules across all the 3D Sensors in the system through a centralized "Defense Center." *Id*. at 34, 254.

Intrusion rules can be "pass" rules, "alert" rules, or "drop" rules. *Id.* at 761. If a pass rule is met, the network traffic in question is ignored (and allowed to continue). *Id.* Conversely, if a drop rule is met, the packet is dropped and an "event" is generated. *Id.* Rules can be written based on "keywords" and their "arguments," i.e., the possible values of the keyword. *Id.* at 762–63.

[5] All citations to Sourcefire refer to the document's original pagination.

The rule header consists of parameters including 5-tuple criteria values (protocol, source and destination IP addresses, and source and destination ports), the rule's action or type (e.g., alert and allow, drop, or ignore and allow), and direction indicating the flow of traffic. The following figure illustrates the parts of a rule header:



```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS
```

Ex. 1004, 764.

Sourcefire also explains that users may import rules from local rule files, which are ASCII text files from a local machine. Ex. 1004, 1857–59. Sourcefire explains that once imported, a user would need to select whether rules should provide alerts, or block and provide alerts, and references the "Setting Rule States" portion of Sourcefire. *Id.* at 435–38, 1858.

2. *Emerging Threats*

Emerging Threats (Ex. 1020) is a text file of rules designed to be imported into and used with SNORT® systems. The text file contains numerous rules, where specific rules can be located therein by searching for a unique Snort ID ("SID"). Exemplary rules include SID:2002526 (search the HTTP request packets to search for the strings "TOP SECRET" or "TS" along with "NOFORN" separated by appropriate spaces and punctuation, Ex. 1020, 87), SID:2002034 (configured to detect and block unauthorized transmission of the password file from Unix/Linux systems out of an organization via a web request, Ex. 1020, 8), SID:2001328 (searching for application layer information containing social security numbers with the familiar "-XX-XXXX" ending pattern, Ex. 1020, 109), and SID:2003021 (to detect/prevent transmissions of encrypted data on an usual port via SSLv3, Ex. 1020, 109).

3. Status of Emerging Threats as a Printed Publication

With respect to Emerging Threats, Petitioner asserts that the text file qualifies as a "printed publication" under § 102(b) as it 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." Pet. 18 (quoting *SRI Int'l, Inc. v. Internet Sec. Sys., Inc.*, 511 F.3d 1186, 1194 (Fed. Cir. 2008) (quoting *Bruckelmyer v. Ground Heaters, Inc.*, 445 F.3d 1374, 1378 (Fed. Cir. 2006))). Petitioner further asserts that the Internet Archive's Wayback Machine shows the public accessibility of Emerging Threats on December 2, 2010 by preserving Emerging Threats as it was "made available to the public" on that date. *Id.* Petitioner also cites to the testimony of Dr. Staniford, detailing that, based on his experience, the Emerging Threats rules appear to be true copies of rules that existed in 2010. *Id.* at 19 (citing Ex. 1003 ¶¶ 204–206). Petitioner also asserts that Emerging Threats was a well-known independent clearinghouse of Snort rules that were available to persons of ordinary skill in the art. *Id.* (citing Ex. 1003 ¶¶ 202–203, 206; Ex. 1018; Ex. 1050; Ex. 1051; Ex. 1082).

Patent Owner argues that Petitioner has not met its burden to prove that Emerging Threats is a prior-art printed publication. PO Resp. 34. Patent Owner argues that Petitioner has not shown that a person of ordinary skill in the art, exercising reasonable diligence, would have been able to locate Emerging Threats, and that such artisans would not have recognized the relevance of Emerging Threats without the need for further research or experimentation. *Id*. Patent Owner also argues that while the existence of a Wayback Machine archive might mean the Emerging Threats reference was technically accessible, public accessibility requires more than technical accessibility. *Id*. at 35 (citing *Samsung Elecs. Co. v. Infobridge Pte. Ltd.*, 929 F.3d 1363, 1369 (Fed. Cir. 2019)). Patent Owner argues that "[a] reference is publicly accessible only if it was 'disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, can locate it.'" *Id*. (quoting *Acceleration Bay, LLC v. Activision Blizzard Inc.*, 908 F.3d 765, 772 (Fed. Cir. 2018) (citations omitted)). *See also id*. at 37–40 (expanding on this argument).

Petitioner responds that the 2010 version of the Emerging Threats website (Ex. 1102) rebuts Patent Owner's assertions. Pet. Reply 18. Petitioner illustrates a search functionality, and a documentation wiki, which corroborates that Emerging Threats was known to those of skill in the art. *Id*. at 18–19 (citing Ex. 1102, 1). Petitioner also points out that the webpage contained a link to navigate and download rule sets, including the emerging-all.rules file. *Id*. at 19.

We agree with Petitioner. The identified aspects of Emerging Threats website would have allowed interested parties to locate the rule sets, download the rule sets and make determinations regarding what rule to use in a packet-handling system, such as Sourcefire. Emerging Threats need not be indexed or broadly searchable under Petitioner's theory of the ground of unpatentability, namely that Emerging Threats was known, one of ordinary skill in the art would have gone to Emerging Threats, and downloaded the emerging-all.rules file, guided by the documentation wiki. As such, we do not agree with Patent Owner's argument that "the record evidence of this case shows the Emerging Threats reference was not publicly accessibly because it was buried on a website that was not searchable or meaningful indexed." *See* PO Resp. 36.

Further, we distinguish *Acceleration Bay* from the instant facts, where in the former a technical report was determined to not be a printed publication when a website allowed a user to view a list of technical reports indexed only by author or year. *Acceleration Bay*, 908 F.3d at 773. Based on the comparison with the website in *Acceleration Bay*, Patent Owner argues that "[t]he Emerging Threats rules website's plain homepage, lacking any useful scheme or labelling, was not meaningfully indexed such that a POSITA might have located the reference even when exercising reasonable diligence." PO Resp. 39 (citing Ex. 2010 ¶ 51; Ex. 2030). Although we have agreed that "persons proceeding to the website without knowledge of a specific SID would have found this to be of little help [in locating specific rules]" (Dec. to Inst. 27), we are not persuaded that is what Petitioner has articulated in the ground of unpatentability. Rather than searching for a single rule, Petitioner is advocating that persons of ordinary skill would have gone to Emerging Threats and would have been guided to download a comprehensive set, and then determine the applicable rules through the commenting provided in the rule set. As such, we are not persuaded that this is analogous to the situation in *Acceleration Bay*.

Patent Owner also argues that Emerging Threats was not publicly accessible and that the testimony of Petitioner's expert, Dr. Staniford, is conclusory. PO Resp. 40–42. Patent Owner argues that his testimony does not provide support that Emerging Threats was disseminated, that a skilled artisan could have located the Emerging Threats reference using reasonable diligence, or that a person ordinarily interested in the art would have been aware of the Emerging Threats website generally. *Id.* (citing *Blue Calypso, LLC v. Groupon, Inc.*, 815 F.3d 1331, 1349–50 (Fed. Cir. 2016)).

Petitioner responds that Patent Owner's declarant, Mr. Marinho, testifies that he became aware of Emerging Threats and downloaded rule sets, demonstrating that an interested artisan exercising reasonable diligence would have been aware of Emerging Threats and known how to download the rules. Pet. Reply 20–21 (citing Ex. 1011, 14:15–17:17, 17:25–20:12, 45:11–22). Petitioner also argues that Mr. Marinho's testimony corroborates Dr. Staniford's recollection and shows public availability. *Id.* at 24 (citing Ex. 1011, 18:6–21, 22:8–23:13).

We agree with Petitioner that Mr. Marinho's testimony supports Dr. Staniford's testimony, and we are persuaded that one of ordinary skill in the art, prior to the effective filing date of the '343 Patent, would have known to look to the Emerging Threats website for Snort rules that could be applied to conventional cyber-defense systems. Dr. Staniford's testimony provides that Snort was begun as an open source project in the late 1990s, that the Bleeding Snort project launched in 2004 as an independent clearing house for Snort rules, and that the project continues as Emerging Threats. *See* Ex. 1003 ¶¶ 202–203. The presence of the Internet Archive's Wayback Machine copy suggests that the document was available and was accessible on December 2, 2010, prior to the March 12, 2013 effective filing date of the '343 Patent.

Lastly, Patent Owner argues that persons interested and ordinarily skilled in the art must be able to "recognize and comprehend therefrom the essentials of the claimed invention without need of further research or experimentation." PO Resp. 42 (quoting *Cordis Corp. v. Boston Scientific Corp.*, 561 F.3d 1319, 1333 (Fed. Cir. 2009) (citing *In re Wyer*, 655 F.2d

221, 226 (CCPA 1981))). Patent Owner argues that persons of ordinary skill in the art would not have recognized the relevance of Emerging Threats without the need of further research or experimentation. *Id*. at 42–45. Patent Owner argues that such persons would have needed to review the 11,000+ rules disclosed in Emerging Threats, that keyword searching would not have proved useful, and such persons could not have determined the relevance of Emerging Threats without further research or experimentation. *Id*. Patent Owner argues that "reviewing thousands of rules far outweighs the reasonable diligence exercised by a POSITA in determining whether a printed publication is potentially relevant." *Id*. at 45.

Petitioner responds, as discussed above, that interested parties would have been able to have searched the contents of Emerging Threats and find the rules contained thereon. Pet. Reply 25–26. Petitioner also argues that "Emerging Threats was published as a listing of 'emerging-all.rules' shows that interested artisans would have downloaded the entire ruleset and reviewed it to determine which rules they wanted to use," and that the comments in the ruleset would have allowed a user to decide which to use. *Id*. at 26.

We agree with Petitioner that it would not have required further experimentation or undue research to have located the necessary aspects of Emerging Threats and accessed any necessary materials. We also agree with Petitioner that the citations made by Patent Owner address whether references qualify as prior-art publications and not with the ease of locating a specific teaching within a publication. Further, a reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill in the art, including nonpreferred embodiments. *Merck & Co. v. Biocraft Lab'ys, Inc.* 874 F.2d 804 (Fed. Cir. 1989). We discuss the likelihood of whether persons of ordinary skill in the art would have incorporated specific rules of Emerging Threats into the system of Sourcefire below, but we remain persuaded that Emerging Threats was publicly accessible. Weighing the evidence of the public accessibility of Emerging Threats in the relevant timeframe, we continue to determine that Petitioner has established that Emerging Threats qualifies as a printed publication under § 102(b). *See* Dec. to Inst. 25–28.

4. *Collateral Estoppel with Respect to Certain Issues*

The ’343 Patent is a continuation of US Application 14/625,486, which issued as US 9,686,193 B2 (“the ’193 patent,” Ex. 1063). Ex. 1001, code (63). The ’193 patent is a continuation of US Application 13/795,822, which issued as US 9,124,552 B2 (“the ’552 patent”). Ex. 1001, code (63). US 9,160,713 B2 (“the ’713 patent”) is also a continuation of this application. IPR2018-01437, Ex. 1001, code (63). The ’552 patent was challenged by a petitioner in IPR2018-01436 (“the ’552 IPR”), and the Board determined all of the ’552 patent’s claims were unpatentable over Sourcefire. Ex. 1067, 2, 15–17, 66–67. The Board also found all claims of the ’713 patent unpatentable over Sourcefire in IPR2018-01437. Ex. 1068. These decisions were affirmed by the U.S. Court of Appeals for the Federal Circuit in *Centripetal Networks, Inc. v. Cisco Sys., Inc.*, 847 F. App’x 869 (Fed. Cir. 2021). Ex. 1069.

Petitioner asserts that the issues decided in the ’552 IPR against Patent Owner and affirmed by the Federal Circuit are binding in this proceeding. Pet. 45–46 (citing *Amazon.com, Inc., v. M2M Solutions LLC*, IPR2019-01205, Paper 43 at 45 (PTAB Jan. 25, 2021); *Webpower, Inc. v. WAG Acquisition, LLC*, IPR2016-01239, Paper 21 at 27 (PTAB July 8, 2020); *Alphatec Holdings, Inc. v. Nuvasive, Inc.*, 2020 Pat.App. LEXIS 12487, *31

(PTAB July 8, 2020)). Based on this, Petitioner asserts that the findings that Sourcefire is prior art and that it teaches materially similar elements of the ’552 patent claims are binding in this proceeding.

Patent Owner did not contradict Petitioner’s position, but did assert that whether the second “determining” step of claim 1 is taught or suggested by Sourcefire was not litigated in the ’552 IPR in the context of the discussion of limitation [1e]. Prelim. Resp. 50–51. We respond to Patent Owner’s argument below, in the discussion of limitation [1e].

With respect to Petitioner’s assertions of collateral estoppel, notably in the Petition at pages 47, 49, 51, 52, and 54, with respect to limitations [1a] through [1d], we agree with Petitioner that Patent Owner is estopped from asserting that Sourcefire is not prior art to the challenged claims, and also estopped from asserting that those limitations are not taught or suggested by Sourcefire, to the extent that the limitations “do not materially alter the question” of patentability relative to the elements of the claims of the ’552 patent. *See Soverain Software LLC v. Victoria’s Secret Direct Brand Mgmt., LLC*, 778 F.3d 1311, 1319 (Fed. Cir. 2015).

5. *Independent Claim 1*

a. Petitioner’s Assertions

As discussed above, we concur with Petitioner that collateral estoppel exists with respect to limitations [1a] through [1d]. Thus, we begin with a discussion of Petitioner’s assertions regarding claim limitation [1e].

Claim limitation [1e] is directed to applying at least one packet transformation function configured to prevent an exfiltration operation, wherein the at least one packet transformation function indicates whether each packet in the second portion of packets is allowed to continue toward its destination, when the packet in the second portion of packets matches the second criterion. Petitioner asserts that Sourcefire discloses that rules may be set to alert (i.e., generate events) or drop (i.e., drop packets that trigger the rule), such that the "Sourcefire rules specify a packet transformation function that will 'indicate whether each packet in the second portion of packets is allowed to continue toward its destination' as claimed." Pet. 56 (citing Ex. 1004, 435–38; Ex. 1003 ¶¶ 162, 262).

Petitioner also asserts that Emerging Threats contains numerous rules targeting exfiltration operations, including rule SID:2003021, that determines whether a second portion of packets comprise data corresponding to the second criterion specified by operators specified by the matching packet-filtering rule. Pet. 56–57 (citing Ex. 1003 ¶¶ 211–229, 263–267). Petitioner asserts that persons of ordinary skill in the art would have recognized the cited rule as a rule configured to prevent an exfiltration operation by detecting attempts to transmit traffic to unusual ports using an out-of-date and insecure encryption protocol. *Id.* at 57 (citing Ex. 1003 ¶¶ 128, 228–229, 263–264).

Petitioner also asserts that while Emerging Threats ships all rules set to "alert" for initial evaluation on a user network, an ordinarily skilled artisan would have been motivated to change rules to "drop" — and therefore prevent an exfiltration operation — when tuning the rules to their network environment. Pet. 57 (citing Ex. 1003 ¶¶ 268–269). Once done, Petitioner asserts that this would have the effect of blocking suspected exfiltration operations of this particular kind, while packets in connections that match the same 5-tuple, but that did not show this pattern would be allowed through. *Id.* at 57–58 (citing Ex. 1003 ¶ 268).

Petitioner further asserts that the Board previously found, in the '552 IPR, that Sourcefire discloses applying an operator that specifies one or more application-header-field-value criteria and a packet transformation function. Pet. 58 (citing Ex. 1067, 16–17, 48–49). Based on this, Petitioner asserts that an Emerging Threats rule imported into Sourcefire therefore also includes an operator that specifies one or more application-header-field-criteria (i.e., second criteria) and a packet transformation function, and that persons of ordinary skill in the art would have understood that numerous of those Emerging Threats rules are configured to detect or prevent exfiltration operations, and would have found it obvious to configure Sourcefire using such rules to prevent exfiltration operations. *Id*.

b. Patent Owner's Arguments

1) Claim Limitation [1e]

Patent Owner argues that, before the '343 Patent, attempts to prevent data exfiltration were often too coarse or overbroad because they would simply block all traffic to/from a given network, regardless of the actual threat, resulting in a negative impact to the subject computer network and ultimately to business operations. PO Resp. 11. Patent Owner argues that persons of ordinary skill in the art would have understood that Snort rules are usually commented out for having "excessive false positive" or "poor performance." *Id*. at 12 (citing Ex. 2010 ¶¶ 68–70). Patent Owner argues that the application of the commented rules from Emerging Threats, changing the rules to enable the dropping of packets in the network environment, would have made the network unusable. *Id*. at 12; PO Sur-reply 4, 7. Patent Owner also argues that Rule 2003021 from Emerging Threats cannot prevent exfiltration operations because it is not only merely an "alert" rule, which cannot block traffic, but also commented out. PO Resp. 15.

Petitioner responds that a Sourcefire user would import rules and tune them to the network environment, including selectively activating and setting rules to block or alert. Pet. Reply 3–4 (citing Ex. 1003 ¶¶ 268–269). Petitioner also relies on testimony by Dr. Staniford that uncommenting rules that were commented-out would enable them, and was disclosed by Emerging Threats. *Id*. at 4 (citing Ex. 2011, 67:10–68:24, 69:8–72; Ex. 1020, 109). Petitioner also argues that "Emerging Threats' teachings of rules configured to detect exfiltration operations (even if disabled) in combination of Sourcefire's teaching of loading and enabling rules to inspect and block or allow packets render the claims obvious." *Id*. (citing *In re Mouttet*, 686 F.3d 1322, 1332 (Fed. Cir. 2012); *In re Etter*, 756 F.2d 852, 859 (Fed. Cir. 1985) (en banc)).

Patent Owner responds that it was incumbent on Petitioner to explain how and why persons of ordinary skill in the art would have modified the existing rules to prevent exfiltrations. PO Sur-reply 3. Patent Owner also argues that Petitioner's assertions to make them "drop" rules, per Sourcefire, relies on what an administrator *could* have done, not what they would have been motivated to do. *Id*. at 4–5 (citing Pet. 57–58).

We disagree with Patent Owner's arguments. We continue to be persuaded that one of ordinary skill in the art, combining Sourcefire and Emerging Threats, would have understood that downloaded rules should be reviewed, and it would have been obvious to enable rules that such persons deemed appropriate. We find Dr. Staniford's testimony to be persuasive on this point. *See* Ex. 2011, 67:10–68:24, 69:8–72; Ex. 1020, 109. We acknowledge that downloading all of a particualr ruleset from Emerging Threats and enabling all the rules, might have resulted in a drop in performance of the network appliance, but, at the same time, we are persuaded that individual rules might have been enabled without a significant drop in performance, especially if a potential threat might be sufficient to warrant a minor performance hit. Patent Owner's counsel acknowledged at oral hearing that instituting all rules of a set in "alert" mode would not result in a decrease in performance, even though some computational outlay must be engaged to engage those alert rules. *See* Hr'g Tr. 24:24–25:4. We are persuaded that judiciously implementing certain rules would not necessary result in a network device that is unusable. Additionally, there is testimony from Dr. Staniford that "you start out with your rules in alert because there might be false positives. I mean, for the best rule in the world, Snort wasn't known for false positives in the rules, when you apply them to a large network." Ex. 2011, 68:2–7. As such, we continue to determine that it would have been obvious, in combining Sourcefire with Emerging Threats, for one of ordinary skill in the art to have downloaded rules and implemented specific rules.

Patent Owner also argues that the plain language of Rule 2003021 indicates that the rule is not configured to prevent exfiltration operations, and the message parameter of the rule indicates that it was intended to target encrypted traffic having an "Unusual Port." PO Resp. 15–16 (citing Ex. 2010 ¶ 77; Ex. 1020, 109); PO Sur-reply 3. Patent Owner also argues that the intent of the rule was to capture traffic from a particular new bot that generated encrypted traffic on a high port, and persons of ordinary skill in the art would have understood that the goal of this rule was to catch a particular bot, not prevent an exfiltration operation. PO Resp. 16–17 (citing Ex. 2010 ¶ 80). Patent Owner also argues that there is no support for Dr. Staniford's testimony that Rule 2003021 would have been understood as preventing exfiltration. *Id*. at 18–19 (citing Ex. 2011, 93:8, 94:2–6, 97:4–16, 103:22–104:6).

Petitioner responds that Patent Owner's declarant, Mr. Marinho, confirmed that malware attempting to exfiltrate data would trigger Rule 2003021, and Dr. Goodrich, Patent Owner's expert, acknowledged that attempted exfiltration using SSLv3 on a high port would trigger the rule. Pet. Reply 5 (citing Ex. 1101, 77:16–78:11; Ex. 1100, 62:18–25). Petitioner also responds that "Rule 2003021 triggers when an application header field value includes content indicating an out-of-date SSL/TLS version—exactly how the '343 patent's HTTPS method prevents exfiltrations." *Id.* Petitioner also asserts that reading Rule 2003021 in conjunction with those before it in the ruleset shows that Emerging Threats teaches preventing exfiltrations while preserving the flow of legitimate network traffic on known ports. *Id*. at 6–7.

As we discussed in the Institution Decision, we continue to find that Patent Owner's discussion of exfiltration relies on only a portion of what is disclosed in the Specification of the '343 Patent. *See* Dec. to Inst. 32 (citing Ex. 1001, 1:28–45). Under this fuller appreciation of "exfiltration," we continue to find that Rule 2003021 would be triggered by exfiltration attempts. As discussed above, both Dr. Goodrich and Mr. Marinho agree that, under specific conditions, certain exfiltration attempts would trigger that rule. We continue to be persuaded that persons of ordinary skill in the art would have understood that the rule was configured to identify attempted exfiltration of encrypted data via the use of a vulnerable SSL/TLS version, and that the rule checks application header field values to identify traffic using a vulnerable encryption protocol, which indicates that the rule detects attempted exfiltrations. *See* Pet. 54; Ex. 1003 ¶ 267; Ex. 2011, 102:5–23.

Based on these findings, we are not persuaded by Patent Owner's arguments that Rule 2003021 does not prevent an exfiltration operation.

Patent Owner also argues that the combination fails to teach or suggest the challenged claims because none of its rules prevent exfiltration operations ***responsive to*** "determining, based on an application header field value" the first portion of packets corresponds to the claimed one or more operators' second criterion. PO Resp. 21 (citing Ex. 2010 ¶¶ 86–89). Patent Owner argues that no rule in Emerging Threats is written to trigger based on the application layer header field. *Id*. at 22–23.

Petitioner responds that Patent Owner's arguments attack the teachings of Emerging Threats alone, whereas the Petition shows the combined teachings of Sourcefire and Emerging Threats render the "responsive to" element obvious. Pet. Reply 10 (citing Pet. 56–58). Petitioner also cites to other rules disclosed by Emerging Threats that apply a packet transformation function responsive to a determination based on an application header field value. *Id*. (citing Pet. 56–57, 61–62, 64–65).

As discussed above, we agree with Petitioner that Rule 2003021 prevents an exfiltration operation, and that the rule identifies exfiltrations by checking an application header field value for traffic using an out-of-date encryption version. *See* Pet. Reply 5 (citing Pet. 57–58). As we have determined previously, other rules cited by Petitioner in the Petition are not argued as being applicable to the limitations of claim 1, and, as such, "are immaterial to the ground and discussion made with respect to limitation [1e] in the Petition." Dec. to Inst. 31.

Nonetheless, we also agree with Petitioner that specific rules disclosed in Emerging Threats generally teach the application of a packet transformation function responsive to a determination based on an application header field value. We agree with Petitioner that Rules 2005319 and 2010234 do just that. Pet. Reply 10 (citing Pet. 56–57, 61–62, 64–65). Although the Petition does not rely on those rules to show exfiltration, the process of triggering other rules lends support that rules that trigger on an application header field value can be employed in Sourcefire to achieve filtering. As the Board has found previously, Sourcefire discloses applying an operator that specifies one or more application-header-field-value criteria and a packet transformation function. *See* Ex. 1067, 16–17, 48–49; Ex. 1069, 20. Therefore, depending on the type of rule being implemented in Sourcefire, it would certainly have the capacity to apply a packet transformation function responsive to a determination based on an application header field value. Based on these findings, we are not persuaded by Patent Owner's arguments.

Patent Owner also argues that other rules of Emerging Threats cited in the Petition also do not match an application layer header field. PO Resp. 19–21. Making similar arguments in the Sur-reply, Patent Owner notes that Petitioner does not dispute that the other rules do not render obvious the claim limitation, but argues that Petitioner has shifted its theory asserting those other rules. PO Sur-reply 12 (citing Pet. Reply 8–9). Patent Owner argues that any new arguments by Petitioner should be rejected as untimely and improper. *Id*. at 12–14.

We disagree with Patent Owner. The arguments raised by Petitioner in the Reply are directly responsive to Patent Owner's arguments that other rules do not match any application layer header field, based on its argument that no rule in Emerging Threats is written to trigger based on the application layer header field. *See* PO Resp. 19–21. Although we continue to be persuaded that Petitioner has not argued the applicability of rules other than Rule 2003021 with respect to this limitation (Dec. to Inst. 31), Petitioner is permitted to argue that other rules match on application header information to show how Rule 2003021 does as well. We are not persuaded that these contentions made in the Reply are untimely or improper, and we have considered them in our discussion above.

2) Impermissible Hindsight Bias

Patent Owner argues that the Petition's reliance on Emerging Threats is based on impermissible hindsight gleaned from Patent Owner's disclosure, as well as prior invalidity proceedings against related patents. PO Resp. 23–26. Patent Owner asserts that Petitioner distilled the '343 Patent down to its "gist," but the inventor's intent was not merely to stop exfiltrations, but to do so "without completely hampering the user's ability to surf the web." *Id.* at 23. Patent Owner also argues that the rationale for SID: 2003021 was combatting "a new bot that's using standard ssl for a command and control session on a high port," according to its author, and it was not recognized at the time to have anything to do with exfiltration prevention. *Id*. at 24 (citing Ex. 2018, 1). Patent Owner continues that without the impermissible hindsight gleaned from Patent Owner's disclosure, there would be no reason to use application header field values to achieve the objective of the '343 Patent. *Id*. Patent Owner also argues that Petitioner's hindsight bias is further demonstrated by its use of evidence dated *after* the time of invention to support its theory that a skilled artisan would have applied the Emerging Threats reference to render the challenged claims obvious. *Id*. at 25.

Petitioner responds that the '343 Patent discloses two methods for preventing exfiltrations and that Emerging Threats disclosed rules that were likewise configured to identify exfiltration operations by detecting packets with application header field values indicating the use of an out-of-date encryption protocol and HTTP POST methods. Pet. Reply 10–11. Petitioner also argues that the rules' comments, as well as Mr. Marinho's and Dr. Goodrich's testimonies, confirmed that the cited rules in Emerging Threats are designed to be triggered by outbound traffic associated with malware that could be used for exfiltration. *Id.* at 11 (citing Pet. 57; Ex. 1100, 62:18–25; Ex. 1101, 77:16–78:11, 104:22–105:3, 106:2–9, 109:5–110:13). Petitioner also relies on Dr. Staniford's recognition of the Snort rules in Emerging Threats as being applicable to preventing exfiltration, which Petitioner asserts were grounded in his experience, and not hindsight. *Id.* at 11–12 (citing Ex. 1003 ¶¶ 128, 208, 284; Ex. 2011, 23:23–24, 26:14–27, 65:15–21, 99:9–101:10, 102:5–23, 113:13–116:6).

Reviewing all of the evidence of record, we are persuaded that the Petition's obviousness rationale based on Sourcefire and Emerging Threats is not guided by impermissible hindsight bias. We find persuasive Dr. Staniford's testimony that one of ordinary skill in the art would have understood that "this rule [SID:2003021] was not directed to looking for instances of exploits or attacks (which would be invisible within the encryption) but rather was looking for exfiltration of some kind of encrypted data." Ex. 1003 ¶ 228. As discussed by Petitioner, such recognition was also made by Mr. Marinho and Dr. Goodrich, such that the rule would have been understood to possibly prevent exfiltrations. We continue to be persuaded that Petitioner provides that a correspondence exists between the REQUIRE-TLS-1.1-1.2 operator in the '343 Patent and SID:2003021 in Emerging Threats, in that both detect an SSL/TLS version in application packet header field values to detect exfiltration attempts using out-of-date encryption protocols. Pet. 43 (citing Ex. 1003 ¶¶ 229–230). We are persuaded that this correspondence can be made, i.e., to determine if the ’343 Patent discloses the interruption of a similar type of exfiltration, without resorting to impermissible hindsight bias, that Patent Owner asserts. Patent Owner has provided no evidence that Petitioner used the specification of the ’343 Patent to find an applicable rule in Emerging Threats, as opposed to the testified-version provided by Dr. Staniford that he recalls “working on a similar feature where we looked for large encrypted transmissions outbound from the network on non-HTTP ports as a possible symptom of exfiltration of large amounts of data.” Ex. 1003 ¶ 228. Thus, we are not persuaded by Patent Owner’s arguments.

3) Evidence of Secondary Considerations

Patent Owner argues that objective evidence of secondary considerations demonstrates that the challenged claims are not obvious. PO Resp. 27–34. Patent Owner argues that “[t]he ’343 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.’” *Id*. at 28 (quoting Ex. 2010 ¶ 104; citing Ex. 1001, 1:28–51). Patent Owner indicates that it was a known, ongoing problem, and that Patent Owner “solved this long-felt, unsolved need with its RuleGATE, Advanced Cyber Threat, and QuickTHREAT system components, which practices the ’343 Patent.” *Id*. at 28–29 (citing Ex. 2010 ¶ 105). Patent Owner argues that the claims of the ’343 Patent recite techniques that address this long-felt but unresolved problem of data exfiltrations, with processes that “succeeded where traditional, overbroad techniques failed because it permitted normal business network traffic, like allowing a web browser to download web pages hosted by web servers, while still preventing data exfiltrations.” *Id*. at 29–30 (citing Ex. 2010 ¶¶ 107–108).

Petitioner responds that Patent Owner's secondary consideration arguments lack merit and do not show a nexus with the challenged claims. Pet. Reply 13–17. Petitioner argues that Patent Owner has not established a long-felt need because the Petitioner demonstrates that this need was solved earlier by Sourcefire and Emerging Threats. *Id*. at 14. Petitioner also asserts that Patent Owner does not present any evidence that shows that the asserted products embody the claims, instead relying on assertions by its declarant, who does not base his opinions on his own analysis, but relies "on a conclusory declaration from PO's Chief Technology Officer and the named inventor on the patent, Dr. Sean Moore." *Id*. at 15 (citing Ex. 2010 ¶¶ 104–112, Ex. 1081 ¶¶ 5–6, 11–12). Lastly, Petitioner points out that Patent Owner has asserted in other proceedings that its products embody Patent Owner's other patents that do not mention exfiltration. *Id*. (citing IPR2018-01386, Paper 14 at 63; IPR2018-01443, Paper 12 at 70; *Fox Factory, Inc. v. SRAM, LLC*, 944 F.3d 1366, 1375 (Fed. Circ. 2019) ("A patent claim is not coextensive with a product that includes a 'critical' unclaimed feature that is claimed by a different patent.")).

Reviewing all of the evidence of record, we are not persuaded that Patent Owner has demonstrated sufficient nexus between the asserted products and the instant claims. We agree with Petitioner that Dr. Goodrich's testimony relies solely on Dr. Moore's declaration in its assertions about what the asserted products do, where Dr. Moore is the named inventor. *See* Ex. 2010 ¶¶ 105, 107–108. Examining the portions of Dr. Moore's declaration relied upon by Dr. Goodrich (Ex. 1081 ¶¶ 5–6, 11–12), it is clear that Patent Owner's asserted products prevent exfiltrations, but it is not clear that they do so according to the methods of the challenged claims. Dr. Moore also talks about what the '343 Patent recites as its exfiltration processes (Ex. 2010 ¶¶ 110–111), but those specific processes are not mapped to the asserted products by any testimony from Dr. Moore. As such, although we do not doubt the success of the asserted products produced by Patent Owner, and that the success could have met a long-felt, unsolved need, we do not have sufficient proof of nexus to demonstrate that the ’343 Patent resulted in that success.

Patent Owner also argues that evidence of industry praise, specifically for products embodying the invention, demonstrates the nonobviousness of the challenged claims. PO Resp. 32–34. Patent Owner cites to an ESG white paper (Ex. 2025), mentioning Patent Owner’s RuleGATE and CleanINTERNET products, and a Security Innovation Network (“SINET”) Innovator for 2017 award (Ex. 2028), that Patent Owner argues is tied to the technologies in the ’343 Patent because they provide techniques for preventing malicious exfiltration. *Id*. at 32–33 (citing 2010 ¶ 115); PO Sur-reply 19–20. Patent Owner also cites to an industry periodical (Ex. 2027), that praises it as “currently ha[ving] the largest number of third-party threat intelligence service integrations in the network security market” (quoting *id*. at 5), and states that it was American Banker’s “Top 10 FinTech Companies to Watch” for 2014 (Ex. 2026) because of its specific products. *Id*. at 33–34 (citing 2010 ¶ 116).

Petitioner responds that industry praise identified by Patent Owner also lacks nexus with the claims of the ’343 Patent. Pet. Reply 16–17. Petitioner asserts that the “ESG Paper provides nothing more than generalities unrelated to the subject matter of the ’343 Patent claims,” and asserts that the paper was “commissioned by Centripetal Networks,” such that it cannot be considered objective indicia. *Id*. at 16. Petitioner also points out that the “SINET article also lacks a nexus and says nothing about exfiltration," and the Gartner and American Banker articles also lack nexus, and recite generalities not tied to the'343 Patent claims. *Id.* at 16–17.

Reviewing all of the evidence of record, we are not persuaded that Patent Owner has demonstrated sufficient nexus between the asserted industry praise and the instant claims. We agree with Petitioner that although the articles are laudatory toward Patent Owner and its products, they are not specific to the '343 Patent claims. The assertions in the articles, such as the highest performance network filter, automated enforcement of millions of IOC policies against live network traffic, and instantly detect and prevent malicious network connections, are laudatory, but are not presented as being related to exfiltration prevention, nor any other aspects of the challenged claims. Without further support, Patent Owner's assertion that "[t]he evidence of industry praise discussed above is reasonably commensurate with the scope of the claims of the '343 Patent and that there is a nexus between the merits of the claimed invention and the evidence of secondary considerations, as the praise is directed at Centripetal's products which embody the claimed features of the '343 Patent," is just a mere conclusion. Without more, we are not persuaded that Patent Owner has demonstrated a nexus between the instant claims and its cited industry praise.

Patent Owner also argues that "[t]he Office has already confirmed that objective indicia of nonobviousness supports the conclusion that Centripetal's exfiltration technology is patentable." PO Sur-reply 16 (citing Ex. 1085, 7). Although we accept that the Office has made such prior determinations, those determinations were made in view of other evidence, with regard to different claims, and not in the context of the instant obviousness ground over Sourcefire and Emerging Threats. As such, although we consider the evidence presented by Patent Owner fully, those prior determinations carry little weight as to whether the secondary-consideration arguments overcome the instant obviousness ground. As discussed above, we do not find the arguments sufficient to overcome the obviousness of claim 1 in view of Sourcefire and Emerging Threats.

c. Conclusion Regarding Obviousness of Claim 1

Based on the record presented, and for the foregoing reasons, we determine that Petitioner has demonstrated that the combination of Sourcefire and Emerging Threats teaches or suggests all the limitations of independent claim 1 and conclude that a preponderance of the evidence establishes that claim 1 is unpatentable as being obvious over Sourcefire and Emerging Threats.

6. Independent Claims 8 and 15

As noted above, Petitioner also addresses the limitations of independent claims 8 and 15, referencing the analysis of independent claim 1. Pet. 46–58. Patent Owner does not provide separate arguments with respect to the elements of independent claims 8 and 15, except with respect to similar elements argued with respect to claim 1. *See* PO Resp.; PO Sur-reply. We find persuasive Petitioner's arguments regarding the correspondences of elements of independent claims 8 and 15 with those of independent claim 1. Pet. 46–58.

Thus, for the same reasons discussed above with respect to claim 1, based on the current record, Petitioner has demonstrated that the combination of Sourcefire and Emerging Threats teaches or suggests of all the limitations of independent claims 8 and 15, and conclude that a preponderance of the evidence establishes that claims 8 and 15 are unpatentable as being obvious over Sourcefire and Emerging Threats.

7. Dependent Claims 2–7, 9–14, and 16–20

Petitioner asserts that dependent claims 2–7, 9–14, and 16–20 are obvious under 35 U.S.C. § 103(a) over Sourcefire and Emerging Threats. *See* Pet. 59–69. We address these dependent claims in groups, per the discussions in the Petition. Patent Owner does not separately address the limitations of the dependent claims, with the exception of dependent claims 5 and 12, where Patent Owner addresses separate, specific arguments. *See* PO Resp. 26–27; PO Sur-reply 14–15.

With respect to dependent claims 2, 9, and 16, each of those claims recites, in part, that the packet header field indicates a protocol type, corresponding to the first criterion specified by the at least one matching packet-filtering rule. Petitioner explains that Sourcefire discloses that the IP protocol field is part of the 5-tuple specification in the header of each rule that would have indicated a protocol type associated with a particular type of data transfer, and that Emerging Threats rules also have a protocol specified in their rule header. Pet. 59 (citing Ex. 1004, 766; Ex. 1020, 109; Ex. 1003 ¶¶ 270–272). We agree with Petitioner and determine that the combination of Sourcefire and Emerging Threats also teaches or suggests the limitations of dependent claims 2, 9, and 16.

With respect to dependent claims 3, 10, and 17, each of those claims recites, in part, that the first portion includes a destination port number associated with a particular type of data transfer. Petitioner explains that both Sourcefire and Emerging Threats disclose that the destination port is a part of their rule headers. Pet. 60–61 (citing Ex. 1004, 768–69; Ex. 1020, 109; Ex. 1003 ¶¶ 263–264, 267, 273–275). We agree with Petitioner and determine that the combination of Sourcefire and Emerging Threats also teaches or suggests the limitations of dependent claims 3, 10, and 17.

With respect to dependent claims 4, 11, and 18, each of those claims recites, in part, that specific HTTP methods are identified within the flow of the packets, and the packets corresponding to "GET" requests would be allowed to continue and packets corresponding to "POST" requests would be blocked. Petitioner explains that the combination of Sourcefire and Emerging Threats teaches that a rule looks for a 5-tuple consistent with requests to HTTP servers, and that a user would be motivated to set the rule to drop traffic that would have been identified a threatening. Pet. 61–63 (citing Ex. 1004, 438, 1857–59; Ex. 1020, 45; Ex. 1003 ¶¶ 277–280). We agree with Petitioner and determine that the combination of Sourcefire and Emerging Threats also teaches or suggests the limitations of dependent claims 4, 11, and 18.

With respect to dependent claims 5 and 12, each of those claims recites, in part, allowing or blocking packets, based on a determination that the application header field value indicates either a request for specified resource data, or a request to submit data to be processed by a specified resource, respectively. For the "allowing" of claim 5, Petitioner points to "Emerging Threats rule SID:2010234" ("Rule 2010234"), which "in the first stage, looks for connections outbound from the local network to external networks on HTTP ports (e.g. port 80)," contending that if "the request method was a GET, the rule would not trigger and the packets would be allowed through to continue toward their respective destinations" (Pet. 64–65), and that if the request "had a request method of POST, then this would match the rule," and be blocked, and that the "HTTP POST request would be a 'request to submit data to be processed by a specified resource,'" where the resource is "the URL '/senm.php?data='" (*id.* at 65–66). Petitioner further asserts that persons of ordinary skill in the art would have understood that this rule is an exfiltration rule because it is designed to detect and either allow or block HTTP POST methods. *Id*. at 64 (citing Ex. 1003 ¶ 283).

Dependent claims 5 and 12 depend from their respective independent claims, independent claims 1 and 8, and thus recite all of the elements of those independent claims. With respect to independent claims 1 and 8, Petitioner relies upon Rule 2003021, which, as discussed above, we agree prevents an exfiltration operation. *See* Pet. 56–68. With respect to dependent claims 5 and 12, Petitioner relies upon Rule 2010234, a different rule. *See* Pet. 63–66. The Petition does not, however, provide any explanation why one of ordinary skill in the art would have utilized both rules or how both rules would have functioned together. The different rules of Emerging Threats are, in effect, different embodiments. Although we agree that one of ordinary skill in the art would have downloaded a rule set from Emerging Threats, and would have understood that downloaded rules should be reviewed, and that it would have been obvious to enable rules that such persons deemed appropriate, the Petition is devoid of explanation of why both rules, Rules 2003021 and 2010234, should have been enabled and what effect, if any, enabling both rules would have entailed. Such an explanation would be required even if we accepted Petitioner's assertion that "[a] POSA would understand that this rule [Rule 2010234] is an exfiltration rule." Pet. 64. As such, we are not persuaded that the Petition has demonstrated the obviousness of dependent claims 5 and 12 by a preponderance of the evidence.

With respect to dependent claims 6, 13, and 19, each of those claims recites, in part, the dropping of packets if it is determined they correspond to a particular transport layer security version value. Petitioner explains that Emerging Threats' Rule 2003021 looks for a particular SSL/TLS record header that includes a version value, and it would have been obvious to have employed that value to drop packets in the combination of Sourcefire and Emerging Threats. Pet. 66–67 (citing Ex. 1004, 783; Ex. 1020, 109; Ex. 1037, 16–17; Ex. 1003 ¶¶ 287–289). We agree with Petitioner and determine that the combination of Sourcefire and Emerging Threats also teaches or suggests the limitations of dependent claims 6, 13, and 19.

With respect to dependent claims 7, 14, and 20, each of those claims recites, in part, the dropping of packets if it is determined they correspond to a particular real-time transport protocol. Petitioner explains that Emerging Threats detects a buffer overflow attack and that persons of ordinary skill in the art would have understood that RTSP conditions could be detected to drop packets based on an analogous rule. Pet. 67–69 (citing Ex. 1020, 211; Ex. 1099, 1; Ex. 1098; Ex. 1003 ¶¶ 290–295). We agree with Petitioner and determine that the combination of Sourcefire and Emerging Threats also teaches or suggests the limitations of dependent claims 7, 14, and 20.

As such, we conclude that Petitioner has demonstrated that the combination of Sourcefire and Emerging Threats teaches or suggests of all the limitations of claims 2–4, 6, 7, 9–11, 13, 14, and 16–20, and that a preponderance of the evidence establishes that claims 2–4, 6, 7, 9–11, 13, 14, and 16–20 are unpatentable as being obvious over Sourcefire and Emerging Threats. In addition, we conclude that Petitioner has not demonstrated that the combination of Sourcefire and Emerging Threats teaches or suggests of all the limitations of claims 5 and 12.

III. CONCLUSION[6]

Having reviewed all the evidence and arguments of record, we determine that Petitioner has demonstrated by a preponderance of the evidence that claims 1–4, 6–11, and 13–20 of the ’343 Patent are unpatentable, but has not shown that claims 5 and 12 are unpatentable. In summary:

Claims	**35 U.S.C. §**	**Basis**	**Claims Shown Unpatentable**	**Claims Not Shown Unpatentable**
1–20	103(a)	Sourcefire, Emerging Threats	1–4, 6–11, 13–20	5, 12
Overall Outcome			1–4, 6–11, 13–20	5, 12

IV. ORDER

In consideration of the above it is:

ORDERED that claims 1–4, 6–11, and 13–20 of the ’343 Patent are unpatentable;

FURTHER ORDERED that claims 5 and 12 of the ’343 Patent have not been shown to be unpatentable; and

[6] 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).

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

FOR PETITIONER (Keysight Technologies):

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

For PETITIONER (Palo Alto Networks):
James L. Davis, Jr.
ROPES & GRAY LLP
james.l.davis@ropesgray.com

FOR PATENT OWNER:

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

Bradley Wright
Scott M. Kelly
John. R. Hutchins
BANNER & WITCOFF, LTD.
bwright@bannerwitcoff.com
skelly@bannerwitcoff.com
jhutchins@bannerwitcoff.com