UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.
Petitioner,

v.

CENTRIPETAL NETWORKS, INC.
Patent Owner.

Case IPR2018-01559
Patent 9,686,193

PATENT OWNER'S PRELIMINARY RESPONSE UNDER 37 C.F.R. § 42.107

TABLE OF CONTENTS

Page

I. Introduction 1

II. The ’193 Patent 2

A. Overview 2

B. Challenged Claims 7

III. Claim Construction 7

IV. Specific Reasons Why The Cited References Do Not Invalidate The Claims, And Why *Inter Partes* Review Should Not Be Instituted 8

A. Petitioner Improperly Incorporates Arguments by Reference and Fails to Make Its Arguments With the Required Specificity 8

B. Sourcefire in view of knowledge, skill and creativity (“Knowledge”) of a POSA Does Not Render Obvious Claims 1–20 12

1. Petitioner Has Not Demonstrated that Sourcefire in view of the Knowledge of a POSA Discloses applying an operator “specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer” (claims 1–20) 13

(a) Sourcefire Does Not Disclose Applying an Operator Responsive to a Determination 13

(b) Sourcefire Does Not Disclose the Recited Operator 16

2. Petitioner Has Not Demonstrated That a POSA Would Have Modified Sourcefire to Reach the Invention Claimed in the ’193 Patent 19

V. CONCLUSION 23

TABLE OF AUTHORITIES

Page(s)

Cases

AG v. 511 Innovations, Inc.,
Case No. IPR2016-01792, Paper 15 (P.T.A.B. Mar. 16, 2017) 8

Belden Inc. v. Berk-Tek LLC,
805 F.3d 1064 (Fed. Cir. 2015) 20

Broadcom Corp. v. Emulex Corp.,
732 F.3d 1325 (Fed. Cir. 2013) 23

Cisco Sys., Inc., v. C-Cation Techs., LLC,
Case No. IPR2014-00454, Paper 12 (P.T.A.B. Aug. 29, 2016).....9, 11

In re Cuozzo Speed Techs., LLC,
793 F.3d 1268 (Fed. Cir. 2015) 7

DeSilva v. Dileonardi,
181 F.3d 865 (7th Cir. 1999) 9

DirectTV, LLC, v. Qurio Holdings, Inc.,
Case No. IPR2015-02006, Paper 6 (P.T.A.B. Apr. 4, 2016).....11

In re Gordon,
733 F.2d 900 (Fed. Cir. 1984) 20

Orexo AB v. Actavis Elizabeth LLC,
903 F.3d 1265 (Fed. Cir. 2018) 20

Travelocity.com L.P. v. Conos Techs., LLC,
Case No. CBM2014-00082, Paper 12 (P.T.A.B. Oct. 16, 2014) 2

Statutes

35 U.S.C. § 103 12

35 U.S.C. § 312(a)(3).....12

Regulations

37 C.F.R. § 42.6(a)(3) 9

37 C.F.R. § 42.22(a)(2) 12

37 C.F.R. § 42.100(b) 7

37 C.F.R § 42.104(b)(3) 8

37 C.F.R. § 42.104(b)(4) 11, 12, 15, 17

37 C.F.R. § 42.104(b)(5) 12

37 C.F.R. § 42.108(c) 1

Office Patent Trial Practice Guide, 77 Fed. Reg. 48756 (Aug. 14, 2012) 7

On August 21, 2018, Cisco Systems, Inc., ("Cisco" or "Petitioner") submitted a Petition to institute *inter partes* review ("IPR") of U.S. Patent No. 9,686,193 (Ex. 1001, "the '193 Patent"), challenging claims 1–20. Centripetal Networks, Inc. ("Patent Owner") requests that the Board not institute *inter partes* review because Petitioner has not demonstrated a reasonable likelihood that it would prevail in showing unpatentability of any of the challenged claims on the grounds asserted in its Petition, as required under 37 C.F.R. § 42.108(c).

I. INTRODUCTION

The Petition should be denied because the Sourcefire reference—the only reference cited against the claims—does not disclose all elements of the independent claims. For example, although Petitioner acknowledges that the '193 Patent is directed to a two-stage packet-filtering process, the sole reference cited against the claims does not disclose such a process. In particular, while challenged claims require *first* making a determination that a first portion of packets meets some rule criteria and *second* applying an operator "configured to drop packets associated with [a] particular type of data transfer," Petitioner identifies no such second-stage operator in Sourcefire.

Sourcefire also admittedly fails to disclose the actual packet-filtering rules recited in the challenged claims, which are "configured to prevent a particular type of data transfer from the first network to a second network." These claimed rules

target "[a] category of cyber attack known as exfiltrations," which "has proven to be especially difficult for conventional cyber defense systems to prevent." '193 Patent at 1:24–27. Sourcefire did not contemplate providing rules to prevent these types of exfiltrations, and Petitioner also failed to address why a POSA would modify a "conventional cyber defense system[]"—Sourcefire—to stop the types of exfiltrations addressed by the '193 Patent.

Although there are a variety of reasons why the '193 Patent is valid over Petitioner's asserted prior art references, this Preliminary Response focuses on only limited reasons why *inter partes* review should not be instituted. *See Travelocity.com L.P. v. Conos Techs., LLC*, Case No. CBM2014-00082, Paper 12 at 10 (P.T.A.B. Oct. 16, 2014) ("[N]othing may be gleaned from the Patent Owner's challenge or failure to challenge the grounds of unpatentability for any particular reason."). The deficiencies of the Petition noted herein, however, are sufficient for the Board to find that Petitioner has not met its burden to demonstrate a reasonable likelihood that it would prevail in showing unpatentability of any of the challenged claims.

II. THE '193 PATENT

A. Overview

The '193 Patent generally discloses systems and methods for "filtering network data transfers." '193 Patent at Title. In particular, the '193 Patent

discloses exemplary techniques for preventing "[a] category of cyber attack known as exfiltrations (e.g., stealing sensitive data or credentials via the Internet)…." *Id*. at 1:24–25. The exemplary techniques claimed in the '193 Patent involve applying packet-filtering rules specifically crafted to prevent such exfiltrations. For example, the challenged claims explicitly recite "receiving, by a computing system and from a computing device located in a first network, a plurality of packets" and applying packet-filtering rules to those packets that "prevent a particular type of data transfer from the first network to the second network." *Id.* at claim 1.

In other words, the independent claims of the '193 Patent recite rules for preventing the transfer of a subset of packets out of the network. These rules involve implementing a two-stage process for filtering traffic:

> Conceptually, the first stage may determine if the network 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, file write, encrypted communication, etc.) between the resources.

Id. at 8:45–52 (emphasis added). In this manner, dangerous exfiltrations can be prevented on the basis of (1) detecting communications between two identified resources (*i.e.* a first and second network, as claimed) and (2) using an operator to determine whether the rule allows for the "particular type of data transfer."

Thus, the ’193 Patent discloses exemplary embodiments for preventing exfiltrations when packets match (1) a particular source and destination criteria (*e.g.* the addresses of the first and second network of each independent claim) and/or a particular transfer protocol (*e.g.* the XMPP protocol recited in claim 8) **<u>and</u>** (2) a particular type of data transfer:

> The methods described above may be modified to achieve different functionality and may be extended to other data transfer protocols or to other application-layer protocols. These methods may provide network administrators with capabilities to enforce network usage policies and network security policies that have capabilities and functionalities beyond those described above. For example, these methods may provide network administrators with capabilities to **prevent exfiltrations that are mediated by other data transfer protocols** besides HTTP and HTTPS. Examples of such protocols include File Transfer Protocol (FTP) and messaging protocols such as eXtensible Messaging and Presence Protocol (XMPP)

Id. at 8:53–65 (emphasis added). Once it is determined that a received packet matches the source/destination criteria and/or the transfer protocol criteria, the second stage (that may be performed by the operator recited in the challenged claims) occurs, wherein an operator is applied to drop packets associated with a “particular type of data transfer” (*e.g.* the HTTP POST method as recited in dependent claim 10).

Exemplary rules of the type described above and recited in the ’193 Patent are described with respect to FIG. 3, wherein each rule “may specify criteria and one or more operators that may be applied to packets associated with (e.g., matching) the specified criteria.” *Id.* at 5:49–52. For example, the claims recite a technique in which a first portion of packets is identified that includes data that “indicates that the first portion of packets [received from the first network] is destined for the second network.” For that first portion of packets an operator is applied that is “configured to drop packets associated with the particular type of data transfer.” This technique is akin to Rule 6 of FIG. 3, which specifies that an HTTP-EXFIL operator should be applied to packets received from a Source IP Address, 140.210.* (*e.g.* a first network), destined for a Destination IP Address, 214.* (*e.g.* a second network), using a particular data transfer protocol (*i.e.* TCP), and a particular destination port number (*i.e.* 80):

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

Id. at FIG. 3.

The HTTP-EXFIL operator disclosed in the ’193 Patent is an example of a type of operator. *See, e.g.*, *id.* at claim 10 (reciting a first operator that is configured to drop packets “responsive to a determination by the computing system that the first portion of packets comprises data corresponding to an HTTP POST method”). An example of an HTTP-EXFIL operator is shown below:

```
Operator HTTP-EXFIL(ip-packet):
    Inspect app-pkt(ip-packet) match GET return ALLOW;
    Inspect app-pkt(ip-packet) match POST return BLOCK;
    Inspect app-pkt(ip-packet) match PUT return BLOCK;
    Inspect app-pkt(ip-packet) match DELETE return BLOCK;
    Inspect app-pkt(ip-packet) match CONNECT return BLOCK;
    Return BLOCK;
End Operator HTTP-EXFIL;
```

Id. at 7:51–59. However, rather than only operating on specific HTTP methods such as those in the HTTP-EXFIL operator, the operators recited in the challenged claims more broadly encompass any “particular type of data transfer,” including types of data transfers associated with communications protocols other than HTTP and HTTPS (*e.g.* the FTP protocol recited in dependent claim 6). This technique furthers one of the goals of the ’193 Patent, which is to “prevent exfiltrations that are mediated by other data transfer protocols besides HTTP and HTTPS.” *Id*. at 8:61–62.

Notably, Petitioner misrepresents the claims of the ’193 Patent, stating that “Claim 1, while verbose, is directed to providing two rules, one for ‘dropping’ (*i.e.* blocking) packets and one for ‘forwarding’ (*i.e.* allowing) packets.” Petition at 11. Petitioner thereby ignores that the claimed **operator** is “configured to drop packets associated with the particular type of data transfer” and that the operator is applied **responsive** to an initial determination that, for example, the packet is destined for a particular network. In other words, Petitioner rewrites the claims to ignore the second stage of the filtering process that it acknowledges is part of the ’193 Patent. *See* Petition at 7 (describing the exemplary two-stage packet-filtering process of the ’193 Patent); *see also id.* at 8 (same).

B. Challenged Claims

Petitioner challenges claims 1–20 of the ’193 Patent, of which claims 1, 8, 18, and 19 are independent. A list of the challenged claims is provided in Appendix A.

III. CLAIM CONSTRUCTION

In an *inter partes* review proceeding, claims are given their broadest reasonable interpretation (“BRI”) in light of the specification of the patent in which they appear. 37 C.F.R. § 42.100(b); Office Patent Trial Practice Guide, 77 Fed. Reg. 48756 at 48766 (Aug. 14, 2012); *see also In re Cuozzo Speed Techs., LLC*,

793 F.3d 1268, 1278 (Fed. Cir. 2015) ("We conclude that Congress implicitly approved the broadest reasonable interpretation standard in enacting the AIA.").

The Petition should be rejected because Petitioner fails to identify "[h]ow the challenged claim is to be construed" under 37 C.F.R § 42.104(b)(3). By not providing any explicit constructions for any claim terms, "Petitioner improperly attempts to shift the burden of construing the claim… to the Board." *ams AG v. 511 Innovations, Inc.,* Case No. IPR2016-01792, Paper 15 at 8 (P.T.A.B. Mar. 16, 2017).

IV. SPECIFIC REASONS WHY THE CITED REFERENCES DO NOT INVALIDATE THE CLAIMS, AND WHY *INTER PARTES* REVIEW SHOULD NOT BE INSTITUTED

Petitioner proposes that claims 1–20 of the '193 Patent are obvious over the Sourcefire reference in view of the knowledge of a POSA. As detailed below, however, the Petition should be denied at least for the several reasons set forth below.

A. Petitioner Improperly Incorporates Arguments by Reference and Fails to Make Its Arguments With the Required Specificity

Petitioner certifies that the Petition includes 13,994 words. *See* Petition at "Certificate of Compliance." However, the Petition incorporates vast amounts of information from other documents by reference and fails to explain with the required specificity how that information renders the challenged claims obvious.

Under the Board's rules, "[a]rguments must not be incorporated by reference from one document into another document." 37 C.F.R. § 42.6(a)(3). And in one of the Board's informative opinions on this topic, the Board found that the citing "large portions of another document, without sufficient explanation of those portions, amounts to incorporation by reference." *See Cisco Sys., Inc., v. C-Cation Techs., LLC*, Case No. IPR2014-00454, Paper 12 at 8 (P.T.A.B. Aug. 29, 2016) (informative opinion). Nevertheless, Petitioner consistently makes conclusory assertions and then cites to large page ranges of its exhibits, including the Staniford Declaration, without making the underlying evidence available in the Petition. This tactic is improper because it fails to make the actual evidence "accessible to the judges" and "amounts to a self-help increase in the length of the brief." *See Cisco*, IPR2014-00454, Paper 12 at 10 (informative opinion) (citing *DeSilva v. Dileonardi*, 181 F.3d 865, 866-67 (7th Cir. 1999) ("Incorporation by reference amounts to a self-help increase in the length of the brief, and is a pointless imposition on the court's time. A brief must make all arguments accessible to the judges, rather than ask them to play archeologist with the record.") (modifications omitted)).

The overwhelming majority of paragraphs in the Petition follow the same format: Sourcefire discloses X, followed by a string-cite to vast page ranges of the Sourcefire reference as well as one or more paragraphs of the Staniford

declaration. For example, the following paragraph contains one conclusory statements that baldly cites to **46** pages of the Sourcefire reference and a paragraph of the Staniford declaration, without actually presenting the evidence disclosed therein:

> Thus, Sourcefire teaches that various packet-filtering rules could be configured to prevent a particular type of data transfer from the first network to a second network, wherein the data satisfies criteria based on HTTP method, FTP command, IM content, multimedia content (*e.g.*, RTP streams), TLS_version, or any other criteria designed to prevent data transfer subject to a known vulnerability or exploit. *CS-1004* pp.333-335, 435-439, 491-492, 538-542, 546-560, 597-601, 697-701, 765, 785-786, 807, 827-828; *CS-1003* ¶171.

Petition at 43. Because Petitioner fails to make the underlying evidence available in the Petition itself, it is impossible to gauge whether Petitioner's assertions accurately characterize the underlying information without scouring each page of the many pages and paragraphs cited for the many conclusory assertions made in the Petition.

This tactic improperly forces Patent Owner and the Board to "play archaeologist with the record" to determine whether or not the conclusory assertion made in the paragraph is actually supported by the record evidence. And, as demonstrated below, Petitioner abuses this tactic to mischaracterize the Sourcefire

reference in many respects. *See* § VI.B.1–2, *infra* (detailing numerous mischaracterizations of Sourcefire with respect to the "applying… an operator" element of the challenged claims).

While the Board in the informative *Cisco* case, cited above, determined that the proper course of action would be to "not consider arguments that are not made in the Petition, but are instead incorporated by reference," the problem is so pervasive in this Petition that it is unclear whether **any** arguments would remain standing, and outright denial of *inter partes* review is warranted here. *Cisco*, IPR2014-00454, Paper 12 at 10. Indeed, to the extent that Petitioner's "arguments" are actually made in the Petition, those arguments so completely torture the underlying evidence as to become unreliable sources for the Board to find a reasonable likelihood that any claim of the '193 Patent is obvious over Sourcefire.

Furthermore, Petitioner's tactic of making a conclusory assertion and allegedly supporting that assertion with bare citations to large portions of the record evidence also results in the Petition failing to comply with "the particularity and specificity required of supporting evidence under [the Board's] governing statute and rules," including 37 C.F.R. § 42.104(b)(4). *DirectTV, LLC, v. Qurio Holdings, Inc.*, Case No. IPR2015-02006, Paper 6 at 10 (P.T.A.B. Apr. 4, 2016). When Petitioner makes conclusory assertions and cites to large portions of a

document that allegedly supports that assertion, without making the evidence available in the Petition or explaining how the evidence actually supports the assertion, the Petition cannot satisfy the Board's "governing statute and rules," including 35 U.S.C. § 312(a)(3) and 37 C.F.R. §§ 42.22(a)(2), 42.104(b)(4)–(5). *Id.*

Thus, due to the pervasive and improper incorporation by reference of arguments and evidence not presented in the Petition and Petitioner's failure to meet their burden to state their challenge with "particularity and specificity," Patent Owner requests that the Board decline to institute *inter partes* review of the '193 Patent.

B. Sourcefire in view of knowledge, skill and creativity ("Knowledge") of a POSA Does Not Render Obvious Claims 1–20

The Board should decline to institute a *inter partes* review at least because the Sourcefire reference does not render challenged claims 1–20 obvious under 35 U.S.C. § 103.

The Petition should be denied because Sourcefire fails to disclose or suggest "responsive to [the] determination… applying, by the computing system and to each packet in the first portion of packets, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer," as recited in each independent claim of the '193 Patent. Petitioner also has not met its burden to demonstrate that it would have

been obvious to modify Sourcefire in order to prevent the type of exfiltrations targeted by the ’193 Patent.

1. Petitioner Has Not Demonstrated that Sourcefire in view of the Knowledge of a POSA Discloses applying an operator “specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer” (claims 1–20)

The ’193 Patent teaches and claims, **responsive** to a determination that a first portion of packets is destined for the second network, applying an **operator** that specified by the packet-filtering rules that is “configured to drop packets associated with the particular type of data transfer.” *See, e.g.*, ‘193 Patent at 8:10-17 (“Conceptually, the first stage may determine if the network 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, file write, encrypted communication, etc.) between the resources.”) (emphasis added); *see also id.* at 8:53–65. Petitioner has not met its burden to demonstrate that Sourcefire discloses applying the claimed operator, let alone that the operator is applied **responsive** to the determination that the “first portion of packets is destined for the second network,” as claimed.

(a) Sourcefire Does Not Disclose Applying an Operator Responsive to a Determination

As acknowledged by Petitioner, the ’193 Patent discloses and claims a two-stage packet-filtering process. *See* Petition at 5 (“The ’193 Patent describes a two-

stage filtering process for addressing such attacks implemented at a Packet Security Gateway (PSG) examining packets that are exiting a trusted network towards an external network."); *id.* at 7 ("In operation, each PSG performs a two-stage filtering process for received packets.").

This two-stage process is reflected in each independent claim, wherein *first* the computing system determines that a first portion of packets [received from a first network] is destined for the second network or uses a particular type of protocol:

> a **determination** by the computing system that **the first portion of packets comprises data corresponding to criteria** specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network, wherein **the data indicates that the first portion of packets is destined for the second network**

'193 Patent at claim 1 (emphasis added); *see also id.* at claim 8 (reciting making a determination that the packet received from the first includes data associated with the XMPP protocol).

Second, and **responsive** to that determination, the computing system applies an operator that is "configured to drop packets associated with the particular type of data transfer." Petitioner does not allege that Sourcefire discloses this claimed two-stage process, let alone that it would have been obvious to modify Sourcefire

to meet the language of the claims, as is its obligation under 37 C.F.R. § 42.104(b)(4).

Petitioner provides three examples from the Sourcefire reference that allegedly meet this claim element. *See* Petition at 43–44 (referring to an alleged "HTTP method drop rule," "FTP command drop rule," and "ssl_version drop rule"). However, Petitioner does not explain how such rules—which, as discussed in more detail below, are not actually disclosed in Sourcefire—are applied **responsive** to a determination that a first portion of packets comprises data indicating "that the first portion of packets is destined for the second network" or "comprises data associated with eXtensible messaging and presence protocol (XMPP)," as claimed.

Petitioner's argument ignores the "applying… a first operator" elements of the challenged claims and effectively argues that this element is met by a rule that incorporates information other than the 5-tuple criteria. *See generally* Petition at 37–41. But Petitioner does not allege that any of this information is part of an operator that is applied responsive to a determination that a first portion of packets includes "data indicat[ing] that the first portion of packets is destined for the second network" or "data associated with eXtensible messaging and presence protocol (XMPP)," as required under 37 CFR. § 42.104(b)(4).

This two-step process permits **different** operators to be applied to the different portions of received packets depending on the destinations associated with those packets or the presence of other criteria, such as whether the packets are associated with a particular messaging protocol. *See, e.g.*, '193 Patent, claim 1 (reciting determining that the **second** portion of packets is destined for a different network than the first portion and applying **different** operators to those packets); *see also id*. at claim 8 (reciting determining whether packets use the XMPP protocol and applying **different** operators depending on the determination).

Petitioner does not argue that Sourcefire teaches a similar two-stage packet-filtering process. Nevertheless, to the extent that Petitioner argues that Sourcefire discloses this claim element simply by applying a "drop" operator responsive to matching some rule criteria, that argument fails for the reasons presented directly below.

(b) Sourcefire Does Not Disclose the Recited Operator

Petitioner has not met its burden to demonstrate that Sourcefire discloses applying an operator configured to drop packets associated with the particular type of data transfer," as recited in independent claims 1, 8, 18, and 19 of the '193 Patent.

As a preliminary matter, Petitioner failed to meet its burden to "specify where each element of the claim is found in the prior art patents or printed

publications relied upon." 37 C.F.R. § 42.104(b)(4). In particular, although Petitioner cites three examples from the Sourcefire reference under the heading for this claim element, there is no allegation that any of the examples are operators "configured to drop packets associated with the particular type of data transfer." *See* Petition at 43–44 (referring to an alleged "HTTP method drop rule," "FTP command drop rule," and "ssl_version drop rule"). At best, Petitioner alleges that Sourcefire discloses an operator "configured to drop packets" rather than an operator "configured to drop packets **associated with the particular type of data transfer**." *Id.* (emphasis added) (referring to "a *drop* operator") (emphasis in Petition).

The '193 Patent does not **only** disclose "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." '193 Patent at 2:20–24 (emphasis added). Rather, the '193 Patent also introduced the concept of applying an operator that can determine whether the packet is associated with a particular type of data transfer:

> 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. at 2:24–29 (emphasis added). The ’193 Patent gives two examples of this type of operator, which is “configured to drop packets associated with the particular type of data transfer”: the HTTP-EXFIL operator and the “REQUIRE-TLS-1.1-12 operator”:

HTTP-EXFIL Operator	REQUIRE-TLS-1.1-1.2 Operator
Operator HTTP-EXFIL(ip-packet): Inspect app-pkt(ip-packet) match GET return ALLOW; Inspect app-pkt(ip-packet) match POST return BLOCK; Inspect app-pkt(ip-packet) match PUT return BLOCK; Inspect app-pkt(ip-packet) match DELETE return BLOCK; Inspect app-pkt(ip-packet) match CONNECT return BLOCK; Return BLOCK; End Operator HTTP-EXFIL;	Operator REQUIRE-TLS-1.1-1.2(ip-packet): Inspect app-pkt(ip-packet) match 1.0 return BLOCK; Inspect app-pkt(ip-packet) match 1.1 return ALLOW; Inspect app-pkt(ip-packet) match 1.2 return ALLOW; Return BLOCK; End Operator REQUIRE-TLS-1.1-1.2;

See, generally, id. at 7:38–8:38. As should be appreciated, these types of operators are “configured to drop packets associated with [a] particular type of data transfer” (*e.g.*, an HTTP POST type or TLS 1.0 type). In other words, the relevant claims of the ’193 Patent state that the operator is “configured to drop packets **associated with the particular type of data transfer**,” and Petitioner identifies no such operator in Sourcefire.

For at least the foregoing reasons, Petitioner has not demonstrated that Sourcefire discloses “apply[ing]… a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer,” as recited in each independent claim of the ’193 Patent. Accordingly, Patent Owner respectfully requests that the Board decline to institute *inter partes* review of the ’193 Patent.

2. Petitioner Has Not Demonstrated That a POSA Would Have Modified Sourcefire to Reach the Invention Claimed in the '193 Patent

Petitioner admits that Sourcefire does not explicitly disclose the type of packet-filtering rules recited in the claims of the '193 Patent. Instead, the Petition relies on what it describes as Sourcefire's "very flexible approach to customizing Sourcefire-provided intrusion rules" to suggest that a POSA would have written rules corresponding to the claims of the '193 Patent. Petition at 32; *see also id.* at 35 (arguing that a user would have "modif[ied] various parameters of rules to customize them as appropriate or desired for a network and/or to write their own custom intrusion rules tuned to the user's specific network environment and the types of anomalies and malicious activities that such network environment is likely to encounter"); *id.* at 38 (arguing that "a user would have written a rule using the HTTP Method option of the HTTP content keyword as part of the criteria"); *id*. at 39 (arguing that "a user would have written a rule using content keywords as part of the rule criteria to identify a first portion of packets using the particular PORT FTP command type").

In an attempt to substantiate this argument, Petitioner points to "guidance" in the Sourcefire reference stating "[i]f none of the existing intrusion rules meet your needs, write new rules that inspect for intrusion attempts." Petition at 37 (citing *CS-1004* pp.333-335). Petitioner then puts forward several arguments

allegedly describing why a POSA would have written rules to "identify and block" certain types of data transfer methods, including an HTTP PUT method, a PORT FTP command, or a particular SSL version. *See* Petition at 39–41.

However, Petitioner presents no explanation as to why a POSA would modify Sourcefire to write rules designed to prevent the type of threats described and protected against by the techniques recited in the claims of the '193 Patent. The Board should therefore deny the Petition because the question is not whether a POSA **could** have modified Sourcefire to practice the invention claimed in the '193 Patent—which Petitioner has not satisfied—but whether a POSA would have been motivated to make the asserted modification. *See Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064, 1073 (Fed. Cir. 2015) ("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.") (citation and emphasis omitted); *see also Orexo AB v. Actavis Elizabeth LLC*, 903 F.3d 1265, 1272-73 (Fed. Cir. 2018) (citing *In re Gordon*, 733 F.2d 900, 902 (Fed. Cir. 1984)) ("The mere fact that the prior art could be so modified would not have made the modification obvious unless the prior art suggested the desirability of the modification."). Petitioner makes no pretense at explaining why a POSA would be motivated to make such a modification, and thus its argument fails as a matter of law.

As Petitioner explicitly notes, the ’193 Patent is capable of preventing “a category of cyber-attacks known as exfiltrations”:

> The ’193 Patent is directed to systems and methods for filtering data packets **leaving a network to ensure that the packets are not improperly transferring sensitive data from the network, a category of cyber-attacks known as exfiltrations**. For example, exfiltrations are often facilitated by using popular network data transfer protocols, such as the Hypertext Transfer Protocol (HTTP) used by the Web. Such attacks may appear to a casual observer as normal network behavior; older network trust models (*e.g.*, those used by firewalls that do not interpret application-layer data like HTTP) may interpret exfiltrations as trusted operations.

Petition at 5 (citing ’193 Patent at 1:24–47, *CS-1003* ¶ 33) (emphasis added). Indeed, the claim language reciting “packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network” may prevent exfiltrations because they prevent the “attempt to transfer data from one or more” networks associated with the computing device to a particular second network:

> Enterprise X may desire to prevent cyber attacks (e.g., exfiltrations) from one or more of its networks (e.g., network 104 or 106). Accordingly, it may locate one or more packet security gateways at each boundary between its networks and one or more public interconnect networks (e.g., network 102), which may be utilized by a cyber criminal, such as organization Z, to attempt to remotely access

> its networks (e.g., network 104 or 106), and which may, for example, potentially be used to attempt **to transfer data from one or more of its networks** (e.g., network 104 or 106) **to one or more networks affiliated with organization Z** (e.g., network 108). For example, packet security gateway 110 may protect network 104 from one or more cyber attacks (e.g., exfiltrations) mediated by network 102 (e.g., the Internet), and packet security gateway 112 may protect network 106 from one or more cyber attacks (e.g., exfiltrations) mediated by network 102.

'193 Patent at 4:21–37 (emphasis added).

On the other hand, the Sourcefire reference is the user manual for an "Intrusion Prevention System," or "IPS":

> Sourcefire IPS™ (Intrusion Prevention System) provides best-in-class intrusion detection and prevention by harnessing the power of the industry-standard Snort® rules-based detection engine. Backed by the acclaimed Sourcefire Vulnerability Research Team™ (VRT), Sourcefire delivers its customers unrivaled protection against known and unknown threats.

Sourcefire at 33 (highlighting added). The entirety of the 2123-page Sourcefire reference fails to mention the term exfiltration and explicitly touts itself as "provid[ing] best-in-class ***intrusion*** detection and prevention." *Id.* (emphasis added).

Petitioner also makes no attempt to explain why a POSA would have modified the Sourcefire Intrusion Prevention System to make a system that is capable of protecting against exfiltrations. Indeed, the several example rules that

Petitioner asserts would or could have been written by a user are all dedicated to preventing **intrusions**, not exfiltrations. *See* Petition at 35 ("Sourcefire discloses that IPS allowed a user to modify various parameters of rules to customize them as appropriate or desired for a network and/or to write their own custom **intrusion rules** tuned to the user's specific network environment and the types of anomalies and malicious activities that such network environment is likely to encounter.") (emphasis added). Nor does Petitioner cite any reference demonstrating that there were known exfiltration vulnerabilities that would or could be addressed by rules that map onto the claims of the '193 Patent. Thus, the Petition fails to demonstrate sufficient motivation to modify Sourcefire. *See Broadcom Corp. v. Emulex Corp.*, 732 F.3d 1325, 1334 (Fed. Cir. 2013) (finding invention nonobvious when an allegedly invalidating prior art reference did not disclose all elements of the claims and addressed a different problem from the challenged patent).

For at least the foregoing reasons, Petitioner has not met its burden to demonstrate that a POSA would have modified Sourcefire to reach the claims of the '193 Patent.

V. CONCLUSION

Petitioner has not established a reasonable likelihood that it will prevail in establishing that claims 1–20 of the '193 Patent are invalid. Centripetal

accordingly requests that the Board deny institution of *inter partes* review of the ’193 Patent.

Respectfully submitted,

Dated: January 4, 2018

/James Hannah/

James Hannah (Reg. No. 56,369)
Michael Lee (Reg. No. 63,941)
Kramer Levin Naftalis & Frankel LLP
990 Marsh Road
Menlo Park, CA 94025
Tel: 650.752.1700 Fax: 212.715.8000

Jeffrey H. Price (Reg. No. 69,141)
Kramer Levin Naftalis & Frankel LLP
1177 Avenue of the Americas
New York, NY 10036
Tel: 212.715.7502 Fax: 212.715.8302

Bradley C. Wright (Reg. No. 38,061)
Banner & Witcoff, Ltd.
1100 13th Street NW, Suite 1200,
Washington, DC 20005.
Tel: 202.824.3160. Fax: 202.824.3000.
Email: bwright@bannerwitcoff.com

(Case No. IPR2018-01559) *Attorneys for Patent Owner*

Appendix A
Challenged Claims

1. A method comprising:

receiving, by a computing system and from a computing device located in a first network, a plurality of packets, wherein the plurality of packets comprises a first portion of packets and a second portion of packets;

responsive to a determination by the computing system that the first portion of packets comprises data corresponding to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network, wherein the data indicates that the first portion of packets is destined for the second network:

applying, by the computing system and to each packet in the first portion of packets, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and

dropping, by the computing system, each packet in first portion of packets; and

responsive to a determination by the computing system that the second portion of packets comprises data that does not correspond to the criteria wherein the data indicates that the second portion of packets is destined for a third network:

applying, by the computing system and to each packet in the second portion of packets, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, a second operator configured to forward packets not associated with the particular type of data transfer toward the third network; and

forwarding, by the computing system, each packet in the second portion of packets toward the third network.

2. The method of claim 1, wherein

the first portion of packets comprises data indicating: a protocol type associated with the particular type of data transfer, and corresponding to the criteria specified by the one or more packet-filtering rules; and

the second portion of packets comprises data indicating a protocol type not associated with the particular type of data transfer.

3. The method of claim 1, wherein:

the first portion of packets comprises data indicating a first destination port number associated with the particular type of data transfer, and corresponding to the criteria specified by the one or more packet-filtering rules; and

the second portion of packets comprises data indicating a second destination port number not associated with the particular type of data transfer.

4. The method of claim 1, wherein:

the first portion of packets comprises data associated with hypertext transfer protocol (HTTP), and corresponding to the criteria specified by the one or more packet-filtering rules; and

the second portion of packets does not comprise data associated with HTTP.

5. The method of claim 1, wherein:

the first portion of packets comprises data associated with hypertext transfer protocol secure (HTTPS), and corresponding to the criteria specified by the one or more packet-filtering rules; and

the second portion of packets does not comprise data associated with HTTPS.

6. The method of claim 1, wherein:

the first portion of packets comprises data associated with file transfer protocol (FTP), and corresponding to the criteria specified by the one or more packet-filtering rules; and

the second portion of packets does not comprise data associated with FTP.

7. The method of claim 1, wherein:

the first portion of packets comprises data associated with real-time transport protocol (RTP), and corresponding to the criteria specified by the one or more packet-filtering rules; and

the second portion of packets does not comprise data associated with RTP.

8. A method comprising:

receiving, by a computing system and from a computing device located in a first network, a plurality of packets;

responsive to a determination by the computing system that a first packet of the plurality of packets comprises data associated with eXtensible messaging and presence protocol (XMPP) and the data corresponds to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network;

applying, by the computing system and to the first packet, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and

dropping, by the computing system, the first packet; and

responsive to a determination by the computing system that a second packet of the plurality of packets does not comprise data associated with XMPP:

applying, by the computing system, to the second packet, and without applying the one or more packet-filtering rules configured to prevent the particular

type of data transfer from the first network to the second network, a second operator configured to forward packets not associated with the particular type of data transfer toward the second network; and

forwarding, by the computing system, the second packet toward the second network.

9. The method of claim 1, wherein:

receiving the plurality of packets comprises receiving packets comprising data associated with hypertext transfer protocol (HTTP);

the first portion of packets comprises a first type of data associated with HTTP;

the second portion of packets comprises a second type of data associated with HTTP; and

applying the first operator configured to drop packets associated with the particular type of data transfer is performed responsive to a determination by the computing system that the first portion of packets comprises the first type of data.

10. The method of claim 9, wherein applying the first operator configured to drop packets associated with the particular type of data transfer is performed responsive to a determination by the computing system that the first portion of packets comprises data corresponding to an HTTP POST method.

11. The method of claim 9, wherein applying the first operator configured to drop packets associated with the particular type of data transfer is performed responsive to a determination by the computing system that the first portion of packets comprises data corresponding to an HTTP PUT method.

12. The method of claim 9, wherein applying the first operator configured to drop packets associated with the particular type of data transfer is performed responsive to a determination by the computing system that the first portion of packets comprises data corresponding to an HTTP DELETE method.

13. The method of claim 9, wherein applying the first operator configured to drop packets associated with the particular type of data transfer is performed responsive to a determination by the computing system that the first portion of packets comprises data corresponding to an HTTP CONNECT method.

14. The method of claim 9, wherein applying the first operator configured to forward packets not associated with the particular type of data transfer toward the second network is performed responsive to a determination by the computing system that the second portion of packets comprises the second type of data.

15. The method of claim 9, wherein applying the first operator configured to forward packets not associated with the particular type of data transfer toward the second network is performed responsive to a determination by the computing system that the second portion of packets comprises data corresponding to an HTTP GET method.

16. The method of claim 1, wherein applying the first operator configured to drop packets associated with the particular type of data transfer is performed responsive to a determination by the computing system that the first portion of packets comprises data corresponding to a particular transport layer security (TLS) version value.

17. The method of claim 1, wherein applying the first operator configured to forward packets not associated with the particular type of data transfer toward the second network is performed responsive to a determination by the computing system that the second portion of packets comprises data corresponding to a particular transport layer security (TLS) version value.

18. A system comprising:

at least one processor; and

a memory storing instructions that when executed by the at least one processor cause the system to:

receive, from a computing device located in a first network, a plurality of packets wherein the plurality of packets comprises a first portion of packets and a second portion of packets;

responsive to a determination that the first portion of packets comprises data corresponding to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network, wherein the data indicates that the first portion of packets is destined for the second network:

apply, to each packet in the first portion of packets, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and

drop each packet in the first portion of packets; and

responsive to a determination that the second portion of packets comprises data that does not correspond to the criteria, wherein the data indicates that the second portion of packets is destined for a third network:

apply, to each packet in the second portion of packets, and without applying the one or more packet-filtering rules configured to prevent the

particular type of data transfer from the first network to the second network, a second operator configured to forward packets not associated with the particular type of data transfer toward the third network; and

forward each packet in the second portion of packets toward the third network.

19. One or more non-transitory computer-readable media comprising instructions that when executed by one or more computing devices cause the one or more computing devices to:

receive, from a computing device located in a first network, a plurality of packets wherein the plurality of packets comprises a first portion of packets and a second portion of packets;

responsive to a determination that the first portion of packets comprises data corresponding to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network, wherein the data indicates that the first portion of packets is destined for the second network:

apply, to each packet in the first portion of packets, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and

drop each packet in the first portion of packets; and

responsive to a determination that the second portion of packets comprises data that does not correspond to the criteria, wherein the data indicates that the second portion of packets is destined for a third network:

apply, to each packet in the second portion of packets, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, a second

operator, configured to forward packets not associated with the particular type of data transfer toward the third network; and

forward each packet in the second portion of packets toward the third network.

20. The method of claim 1, wherein:

the first portion of packets comprises data indicating: a first source port number associated with the particular type of data transfer, and corresponding to the criteria specified by the one or more packet-filtering rules; and

the second portion of packets comprises data indicating a second source port number not associated with the particular type of data transfer.

CERTIFICATE OF COMPLIANCE WITH 37 C.F.R. § 42.24

This paper complies with the type-volume limitation of 37 C.F.R. § 42.24. The paper includes 4,881 words, excluding the parts of the paper exempted by § 42.24(a).

This paper also complies with the typeface requirements of 37 C.F.R. § 42.6(a)(ii) and the type style requirements of § 42.6(a)(iii)&(iv).

/James Hannah/

James Hannah (Reg. No. 56,369)
Kramer Levin Naftalis & Frankel LLP
990 Marsh Road,
Menlo Park, CA 94025
(650) 752-1700

CERTIFICATE OF SERVICE

The undersigned certifies, in accordance with 37 C.F.R. § 42.6(e), that service was made on the Petitioner as detailed below.

Date of service	January 4, 2019
Manner of service	Electronic Mail (PDMcPherson@duanemorris.com; CJTyson@duanemorris.com; JAPowers@duanemorris.com; and PCMuldoon@duanemorris.com).
Documents served	PATENT OWNER'S PRELIMINARY RESPONSE
Persons Served	Patrick D. McPherson; Joseph A. Powers; and Christopher Tyson Patrick Muldoon

/James Hannah/
James Hannah
Registration No. 56,369
Counsel for Patent Owner