

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 B2

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

LEE, *Administrative Patent Judge*.

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

INTRODUCTION

Cisco Systems, Inc. (“Petitioner”) filed a Petition (Paper 1, “Pet.”) requesting an *inter partes* review of claims 1–20 (“the challenged claims”) of U.S. Patent No. 9,686,193 B2 (Ex. 1001, “the ’193 Patent”). Centripetal Networks, Inc. (“Patent Owner”) timely filed a Preliminary Response (Paper 6, “Prelim. Resp.”).

We have authority to institute an *inter partes* review only if the information presented in the Petition shows “there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314(a). An *inter partes* review may not be instituted on fewer than all claims challenged in the Petition. *SAS Inst., Inc. v. Iancu*, 138 S. Ct. 1348, 1359–60 (2018).

Upon consideration of the Petition and Preliminary Response, we determine that the information presented does not show there is a reasonable likelihood that Petitioner would prevail in establishing the unpatentability of any of the challenged claims. Accordingly, we do not institute an *inter partes* review, and the Petition is *denied*.

A. *Related Cases*

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

B. *The ’193 Patent*

The ’193 Patent relates to filtering network data transfers. Ex. 1001, 1:58–59. When multiple data packets are received by a system, “[a] determination may be made that a portion of the packets have packet header

field values corresponding to a packet filtering rule.” *Id.* at 1:59–62. A “network packet filter” located at the boundary between a secured and unsecured network may be used to compare certain information in packet headers to packet filtering rules. *Id.* at 2:6–16. Packet filtering rules may in turn be associated with an “operator” that may be applied to a packet that matches a rule’s criteria. *Id.* at 2:16–19. For example, such operators may include “identity” operators, which allow packets to continue to their destination; “null” operators, which prevent packets from continuing; and other operators that are capable of analyzing application-level header information in a packet. *Id.* at 2:20–29. An operator may be associated with one or more rules to enforce, for example, a particular Web usage policy. *Id.* at 2:43–50.

C. Challenged Claims

Petitioner challenges all of the claims of the ’193 Patent. Claims 1, 8, 18, and 19 are the independent claims. Claim 1 is illustrative and is reproduced below:

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.

D. Asserted Ground of Unpatentability and Asserted Prior Art

Petitioner asserts that each of the challenged claims is unpatentable as obvious under 35 U.S.C. § 103(a) in view of the Sourcefire 3D System User Guide, Version 4.10 (Ex. 1004, “Sourcefire”). Pet. 24. According to Petitioner, Sourcefire is prior art under 35 U.S.C. § 102(b), and was publicly accessible at least as early as April 2011 through physical distribution to buyers of the Sourcefire 3D System, as well as being made available for

download from the Sourcefire website. *Id.* at 27.¹ Petitioner offers the Declaration of John Leone, which presents testimony to support Petitioner’s assertions regarding public accessibility. Ex. 1005. In addition, Petitioner further relies on the Declaration of Dr. Stuart Staniford (Ex. 1003).

ANALYSIS

A. *Claim Construction*

For petitions filed before November 13, 2018, claim terms in an unexpired patent are given their broadest reasonable construction in light of the specification of the patent in which they appear. 37 C.F.R. § 42.100(b); *see Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2144–46 (2016).

Petitioner asserts that “no specific construction of any claim term is required.” Pet. 14. Patent Owner argues the Petition should be denied because Petitioner did not provide any explicit claim constructions, as required under 37 C.F.R. § 42.104(b)(3). Prelim. Resp. 7–8 (citing *ams AG v. 511 Innovations, Inc.*, Case IPR2016-01792, slip op. at 8 (PTAB Mar. 16, 2017) (Paper 15)). Patent Owner does not, however, specify any claim terms it contends require express construction, or offer any explicit constructions of its own for any terms.

As explained below, we determine that a claim construction analysis of the term “operator” is required to resolve the issues raised by Petitioner’s unpatentability arguments. The Petition states that “each claim term in the

¹ At this stage of the case, Patent Owner has not disputed Petitioner’s assertion that Sourcefire qualifies as prior art. For purposes of this Decision, we determine Petitioner has made a sufficient showing that Sourcefire is prior art to the ’193 Patent.

Challenged Claims [should] be given its plain and ordinary meaning,” but we conclude this assertion is inadequate at least with respect to the term “operator.” It is apparent from the Specification of the ’193 Patent that this term either has a special meaning in the context of the patent, or at least has a specific technical meaning (e.g., as a term of art) that is not apparent from the term itself. As such, it was incumbent upon Petitioner to provide a proposed construction for “operator,” or at least to explain what the “plain and ordinary meaning” of the term is in the relevant field. Petitioner’s failure to do so weighs in favor of denying the Petition.

B. Alleged Unpatentability Under § 103(a)

A claim is unpatentable under § 103 if the differences between the claimed subject matter and the prior art are “such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) objective evidence of nonobviousness, i.e., secondary considerations. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

Additionally, the obviousness inquiry typically requires an analysis of “whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006) (requiring “articulated reasoning with some rational underpinning to support the legal conclusion of obviousness”)); see *In re Warsaw Orthopedic, Inc.*, 832 F.3d 1327, 1333

(Fed. Cir. 2016) (citing *DyStar Textilfarben GmbH & Co. Deutschland KG v. C. H. Patrick Co.*, 464 F.3d 1356, 1360 (Fed. Cir. 2006)).

1. *Overview of Sourcefire*

Sourcefire is a user guide for the Sourcefire 3D System, a system that provides “real-time network intelligence for real-time network defense.” Ex. 1004, 32.² The system operates via “3D Sensors” that can each run the Sourcefire “Intrusion Prevention System” (IPS), which allows monitoring of networks for attacks by examining packets for malicious activity. *Id.* at 33–34. Users can create custom “intrusion rules” to examine packets for attacks and manage the rules across all the 3D Sensors in the system through a centralized “Defense Center.” *Id.* at 34, 254.

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

The Sourcefire 3D System also features “preprocessors” that can facilitate processing of network traffic by identifying and decoding certain types of traffic, such as HTTP (hypertext transfer protocol) and SSL (secure sockets layer) traffic. *Id.* at 513–514. The SSL preprocessor, for example, can be used to identify encrypted traffic that IPS cannot analyze, thereby

² All citations to Sourcefire refer to the document’s original pagination.

enabling IPS to ignore (pass) the encrypted packets and avoid wasting resources trying to inspect them. *Id.* at 596.

2. Level of Ordinary Skill

Petitioner asserts that a person of ordinary skill in the art would have had a bachelor's degree in computer science, computer engineering or an equivalent, as well as four years of industry experience. Pet. 15 (citing Ex. 1003 ¶¶ 21–24, 64–65). In addition, Petitioner indicates a person of ordinary skill would have had “a working knowledge of packet-switched networking, firewalls, security policies, communication protocols and layers, and the use of customized rules to address cyber attacks.” *Id.*

At this stage of the case, Patent Owner does not dispute Petitioner's formulation of the level of skill in the art. Based on the information presented in the Petition and Dr. Staniford's testimony, we adopt Petitioner's formulation for purposes of this Decision.

3. Secondary Considerations of Non-Obviousness

Neither party presented any evidence or argument regarding secondary considerations of non-obviousness at this stage of the case. Thus, we do not consider any such considerations in our analysis for this Decision.

4. Independent Claim 1

Claim 1 recites receiving first and second portions of packets, and a determination regarding each portion. For the first portion of packets, the claim recites 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.” Thus, the system determines that the first portion of packets comprises data corresponding to criteria specified by one or more packet-filtering rules.

Claim 1 then recites that “responsive to” this determination, a “first operator” is applied to the first portion of packets. This first operator is configured to drop packets associated with the type of data transfer that the recited packet-filtering rules are configured to prevent. Then, claim 1 recites that the packets in the first portion are dropped.

According to Petitioner, Sourcefire teaches the recited packet-filtering rules and the recited determination regarding the first portion of packets in its disclosure of custom “intrusion rules.” Pet. 35–43. Specifically, Petitioner alleges that Sourcefire teaches the use of “keywords” to craft customized intrusion rules that, for example, specify particular data transfer types, such as HTTP or FTP. *Id.* at 37. Petitioner asserts that a skilled artisan would have been motivated to follow these teachings to write a rule, for example, to block packets associated with an HTTP PUT method, packets associated with an FTP PORT command, packets associated with vulnerable SSL data transfers, or packets associated with streaming audio or video content. *Id.* at 38–42. As Petitioner notes, Sourcefire discloses that an intrusion rule may be an “alert rule” (generates an intrusion event), “pass rule” (ignores the packet), or “drop rule” (drops the packet and generates an event). *E.g.*, Ex. 1004, 761.

With respect to the first operator limitation, Petitioner’s only statements are reproduced below in their entirety:

Using the HTTP method drop rule discussed above as an example, a drop operator would be applied to the first portion

of packets that include an HTTP method of PUT. *CS-1003* ¶174.

Likewise, using the FTP command drop rule discussed above as an example, a drop operator would be applied to the first portion of packets that include an FTP command of PORT. *CS-1003* ¶175.

Likewise, using the `ssl_version` drop rule discussed above as an example, a drop operator would be applied to the first portion of packets having a version of TLS 1.0, SSLv2, or SSLv3. *CS-1003* ¶176.

Pet. 44. The three cited paragraphs of Dr. Staniford’s Declaration are essentially identical to the above and do not provide further explanation. *See* Ex. 1003 ¶¶ 174–176.

Neither the Petition nor the cited portions of Dr. Staniford’s Declaration identifies the source of the referenced term “drop operator,” and Petitioner does not direct us to any specific portion of Sourcefire, much less a portion that uses that term. Neither Petitioner nor Dr. Staniford explains sufficiently what aspects of Sourcefire teach a “drop operator” being “applied to the first portion of packets” in any of the three referenced examples. The preceding discussion of an HTTP method drop rule, FTP command drop rule, and `ssl_version` drop rule did not mention a “drop operator,” or indeed any “operator.” *See* Pet. 38–43.

The three examples of drop *rules* refer to the custom intrusion rules that Petitioner maps to the recited packet-filtering rules. *See id.* To the extent Petitioner intends to also map the same intrusion rules to the recited first operator, no explanation is provided as to how the same rule teaches both limitations, or why an ordinary artisan would understand Sourcefire’s intrusion rules to teach or suggest a method with both steps. Nor does Petitioner explain sufficiently how Sourcefire teaches an operator applied

“responsive to” the determination based on the packet-filtering rules, as recited in claim 1, if both steps are taught by the same intrusion rules. *See* Prelim. Resp. 13–15. Presumptively, the first operator refers to something other than the recited packet-filtering rule(s) because a different term is used, including within the same claim limitation—e.g., claim 1 recites that the “first operator” is “specified by the one or more packet-filtering rules.” *See Ethicon Endo-Surgery, Inc. v. U.S. Surgical Corp.*, 93 F.3d 1572, 1579 (Fed. Cir. 1996). Although this presumption may be rebutted, Petitioner makes no attempt to do so.

The Specification of the ’193 Patent also indicates that the recited operators may be distinct from the recited packet-filtering rules. For example, the Specification indicates that some packet-filtering rules are associated with an operator, but others are not. *See* Ex. 1001, 2:16–19 (stating that one or more rules “may” be associated with an operator). In addition, an operator may be associated with multiple rules. *See id.* at 2:43–45. The Specification describes that rules are used by a network packet filter to determine whether a packet meets certain criteria, while some operators themselves have the capability to analyze packets for certain information. *See id.* at 2:24–29, 2:35–43. Network filters that utilize this additional functionality of operators (packet security gateways) are distinguished from filters that do not. *See id.* at 2:29–34.

Figure 2 of the ’193 Patent depicts both rules and operators, and is reproduced below:

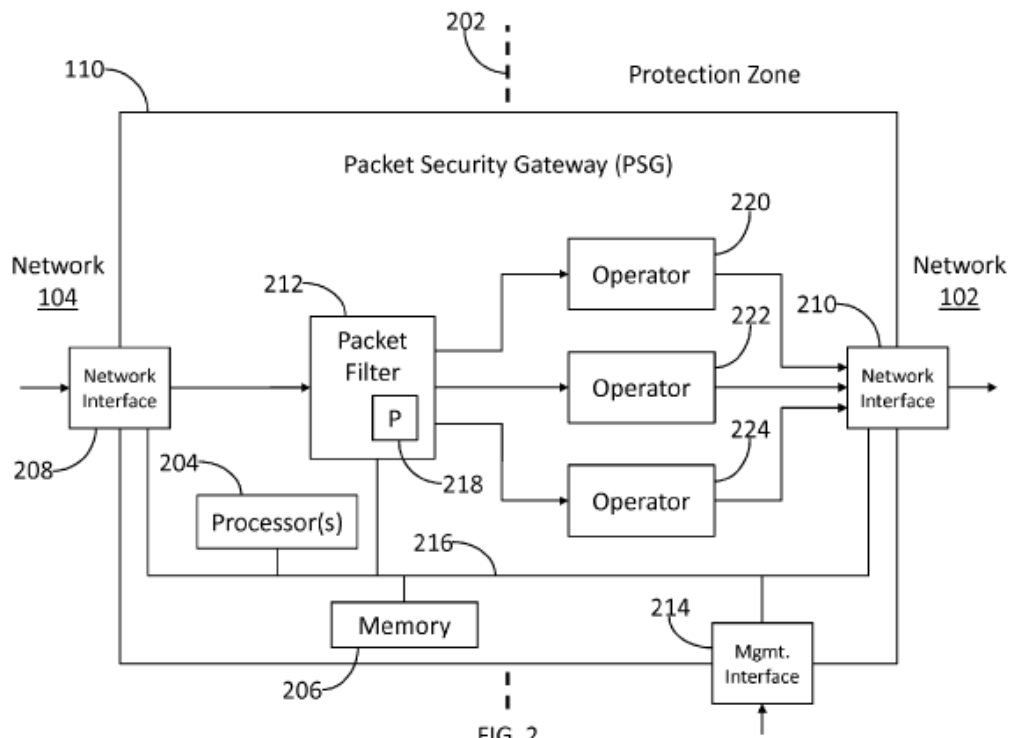


FIG. 2

Figure 2 is a diagram of a packet security gateway. *Id.* at 3:4. As shown in Figure 2, packet filter 212 is configured based on dynamic security policy 218, which houses the one or more rules. *Id.* at 5:25–28. These rules, when triggered, may cause packet filter 212 to forward packets to operator 220, operator 222, or operator 224, each of which is depicted as distinct from packet filter 212 (and dynamic security policy 218) and may in turn perform one or more functions on the packets. *Id.* at 5:29–45, Fig. 2.

It is unclear to what extent the recited packet-filtering rules and first operator may nonetheless be related, e.g., two parts of the same structure or software code. But therein lies the problem with the Petition as to the first operator limitation—it does not provide adequate explanation. *See* 37 C.F.R. § 42.104(b)(3)–(5). Consequently, we determine Petitioner has failed to establish a reasonable likelihood of prevailing as to claim 1.

5. *Remaining Challenged Claims*

Each of the remaining independent claims—claims 8, 18, and 19—recite substantially the same “first operator” limitation. For each of these claims, Petitioner relies on the same arguments regarding that limitation as for claim 1, without any further explanation or other support. *See* Pet. 56 (claim 8), 66 (claim 18), 67 (claim 19). Petitioner also does not provide any information with regard to any dependent claim that remedies the issue discussed above. Thus, we determine Petitioner also has failed to establish a reasonable likelihood of prevailing as to all remaining challenged claims.

CONCLUSION

For the foregoing reasons and on the present record, we determine that the information presented in the Petition does not demonstrate there is a reasonable likelihood that Petitioner would prevail in establishing the unpatentability of claims 1–20 of the ’193 Patent.

ORDER

In consideration of the foregoing, it is hereby:

ORDERED that the Petition is *denied* and no trial is instituted.

PETITIONER:

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

PATENT OWNER:

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

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