

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETSKOPE, INC.,
Petitioner,

v.

FORTINET, INC.,
Patent Owner.

IPR2023-00457
Patent 9,231,968 B2

Before JAMES P. CALVE, THOMAS L. GIANNETTI, and
STEPHEN E. BELISLE, *Administrative Patent Judges*.

CALVE, *Administrative Patent Judge*.

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

I. BACKGROUND

Netskope, Inc. (“Petitioner”) filed a Petition requesting *inter partes* review of claims 1–9 (the “challenged claims”) of U.S. Patent No. 9,231,968 B2 (“the ’968 patent”) (Ex. 1001). Paper 2, 3 (“Pet.”). Fortinet, Inc. (“Patent Owner”) filed a Preliminary Response. Paper 6 (“Prelim. Resp.”).

We have authority to determine whether to institute an *inter partes* review. *See* 35 U.S.C. § 314 (2018); 37 C.F.R. § 42.4(a) (2022) (“The Board institutes the trial on behalf of the Director.”). An *inter partes* review may not be instituted “unless . . . the information presented in the petition . . . shows that 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). Upon consideration of the evidence and arguments in the record, we determine that the information presented does not show a reasonable likelihood that Petitioner would prevail with respect to at least one of the challenged claims. We therefore deny institution of an *inter partes* review.

A. Related Proceedings

The parties identify the following proceeding in which the ’968 patent is involved: *Netskope, Inc. v. Fortinet, Inc.*, No. 3:22-cv-01852-TLT (N.D. Cal., filed Mar. 24, 2022). Pet. 1; *cf.* Paper 3, 2.

Petitioner identifies the following co-pending *inter partes* review proceedings in which Petitioner challenges other patents of Patent Owner: IPR2022-01587, IPR2023-00030, IPR2023-00175, IPR2023-00456, IPR2023-00458, and IPR2023-00459. Pet. 1–2.

B. Real Parties in Interest

Petitioner identifies Netskope, Inc. as the sole real party in interest.

Pet. 1. Patent Owner identifies Fortinet, Inc. as the sole real party in interest.
Paper 3, 2.

C. The '968 Patent (Ex. 1001)

The '968 patent describes a content detection system 100 that updates content detection modules with content detection data that is used to enforce policies for network traffic received by the content detection modules 108. Ex. 1001, 2:18–30, 4:11–18. Figure 1 is reproduced below to illustrate the content detection system, redrawn by Petitioner for clarity with annotations.

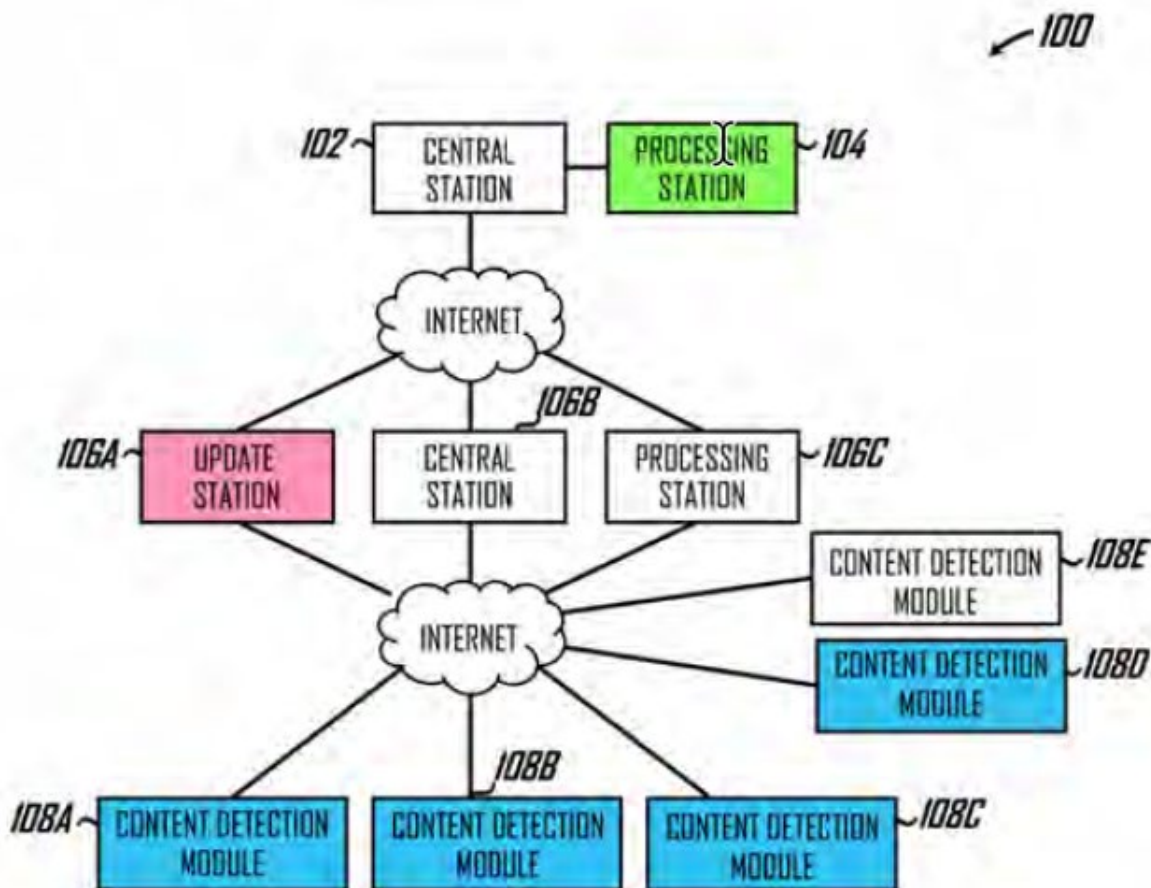


Fig.1 (Redrawn and Annotated)

Figure 1 depicts central station 102 connected to update stations 106¹ and content detection modules 108, which determine whether electronic content contains undesirable content using content detection data received from central station 102 via update stations 106. Ex. 1001, 4:11–5:20.

When content detection module 108 detects suspicious content, it sends the content to processing station 104. Ex. 1001, 6:2–7. Electronic content can be web pages, email and attachments, word files, and programs containing virus, spam, worms, and undesirable content. *Id.* at 5:60–6:2. Processing station 104 analyzes the electronic content using conventional techniques to determine whether it contains a virus, worm, spam, or other threat to be detected. *Id.* at 6:12–22. If the electronic content contains a threat, processing station 104 generates “content detection data” to send to content detection modules 108 substantially in real time for use in detecting undesirable content in received network traffic. *Id.* at 6:15–36, 8:59–9:27.

“Content detection data” includes a virus signature, virus definition, spammer identification, uniform resource locator (URL), network intrusion detection system (NIDS) signature, level of threat, and data that can be used for content detection or screening. Ex. 1001, 6:33–38. Processing station 104 transmits the content detection data that it creates to central station 102, which transmits the content detection data to update stations 106. *Id.* at 6:42–50. Update stations 106 transmit content detection data to the content detection modules 108 that they serve in an area. *Id.* at 6:50–62, 7:27–8:28.

¹ Central Station 106B and Processing Station 106C should be labelled as Update Stations 106B, 106C, which send content detection data to content detection modules 108. *See* Ex. 1001, 5:8–10 (describing Figure 1 showing three update stations 106a–106c and five content detection modules 108a–108e).

Content detection modules 108 are gateway products that enforce virus or content scanning, verification, authentication, and intrusion policies on network traffic received from *external sources* by using content detection data received from update stations 106. Ex. 1001, 5:14–59, 8:59–9:5. For content detection data of a virus signature, content detection module 108 uses the virus signature to detect a related virus. *Id.* at 8:62–65. If content detection data is a spammer identification, content detection module 108 uses the spammer identification to detect unwanted spam. *Id.* at 8:65–9:2.

Content detection modules 108 receive content detection data updates within minutes or seconds after the data are determined by processing station 104. Ex. 1001, 9:6–12. Real-time updates are important for time-sensitive virus definitions. *Id.* at 9:12–16. Whereas typical update methods require a content detection module to “poll” update stations for new updates, the ’968 patent system can “push” the latest security update data within minutes or seconds of becoming available to all content detection modules for faster responses during an outbreak and less resource consumption. *Id.* at 9:16–27.

Processing station 104 and update stations 106 are *external* to content detection module networks and send content detection data via the Internet. Ex. 1001, 4:35–5:59, Fig. 1. Update stations can service content detection modules in many ways. *See id.* at 6:42–8:23. Update stations can update one another with the latest content detection data. *Id.* at 6:63–7:26. Central station 102 can select update stations to send content detection data based on current load demands and capacities and can adjust for heavy load demand for improved efficiency. *Id.* at 7:34–8:23. Central station 102 may use an order list of primary, secondary, and tertiary update stations to cover for unavailable update stations and adjust for heavy load demand. *Id.* at 8:6–23.

D. Challenged Claims

Claims 1, 4, and 7 are independent. Claims 2 and 3 depend from claim 1. Claims 5 and 6 depend from claim 4. Claims 8 and 9 depend from claim 7. Ex. 1001, 12:2–14:34. Claim 1 is reproduced below with Petitioner’s annotations that identify each claim element (*see* Pet. 26–61).

1[pre] A network gateway device comprising:
1[a] at least one processor;
1[b] at least one memory device;
1[c] at least one network interface device;
1[d] content detection and configuration data stored on the
at least one memory device; and
1[e] an instruction set, stored in the at least one memory
device and executable by the at least one processor to:
1[e][i] receive network traffic via the at least one network
interface device;
1[e][ii] process the received network traffic in view of the
content detection and configuration data stored in the at
least one memory device *[e][iii]* to enforce policies
defined at least in part by the content detection and
configuration data and including at least one policy that
defines a suspicious category of network traffic, *[e][iv]*
the policy enforcement performed to determine whether
to allow the received network traffic to pass, *[e][v]* the
policy enforcement including user identification, content
identification, and at least one of source verification and
destination verification, *[e][vi]* wherein when network
traffic is determined to violate the at least one policy
defining suspicious network traffic, forwarding the
network traffic to an analysis process that will perform
analysis on network traffic to determine whether the
network traffic contains a threat desired to be detected
and, *[e][vii]* when the network traffic is determined to
contain a threat desired to be detected, the analysis
process generates additional content detection data to
detect the threat in subsequently received network traffic;

l[f] receive, via the network interface device, the additional content detection data indirectly from the analysis process via an update station;
l[g] store the additional content detection data on the at least one memory device;
l[h] process subsequently received network traffic in view of the additional content detection data;
l[i] block network traffic determined to violate at least one policy; and
l[j] allow network traffic to pass that does not violate a policy.

E. Asserted Grounds of Unpatentability

Ground	Challenged Claim(s)	35 U.S.C. §	Reference(s)
1	1–9	103(a) ²	Jordan ³ , FortiGate ⁴
2	1–9	103(a)	Lee ⁵ , Magdych ⁶
3	1–9	103(a)	Lee, Magdych, Judge ⁷
4	1–9	103(a)	Fang ⁸ , FortiGate

Petitioner also relies on a Declaration of Dr. Wenke Lee. Ex. 1002.

Patent Owner relies on a Declaration of Dr. John Black Jr. Ex. 2001.

² The Leahy-Smith America Invents Act (“AIA”) revised 35 U.S.C. §§ 102 and 103, effective March 16, 2013. Because the ’968 patent has an effective filing date before March 16, 2013, we use the pre-AIA versions of §§ 102 and 103.

³ US 11,281,775 B2, issued Mar. 22, 2022 (Ex. 1005, “Jordan”).

⁴ Fortinet’s FortiGate – 3600 User Manual, Vol. 1, dated Sept. 5, 2003 (Ex. 1008, “FortiGate”).

⁵ US 2004/0015719 A1, published Jan. 22, 2004 (Ex. 1009, “Lee”).

⁶ US 6,513,122 B1, issued Jan. 28, 2003 (Ex. 1010, “Magdych”).

⁷ US 2003/0172292 A1, published Sept. 11, 2003 (Ex. 1011, “Judge”).

⁸ US 2012/0278896 A1, published Nov. 1, 2012 (Ex. 1012, “Fang”).

II. DISCUSSION

A. Level of Ordinary Skill in the Art

Petitioner asserts that a person of ordinary skill in the art around the November 2013 filing date of the '968 patent or even around its earliest asserted filing date in 2004 “would have had at least a B.S. in computer science, computer engineering, or electrical engineering (or equivalent experience) and at least two years of practical experience with network and data security.” Pet. 20 (citing Ex. 1002 ¶ 29).

Patent Owner contends that a skilled artisan “would have a Bachelor of Science degree in electrical engineering and/or computer science, and three years of work or research experience in the fields of network and data security, or a Master’s degree in electrical engineering and/or computer science and two years of work or research experience in related fields.” Prelim. Resp. 14 (citing Ex. 2001 ¶ 18). Patent Owner points out that its proposed level of ordinary skill requires three years of experience compared to two years of experience under Petitioner’s asserted level of ordinary skill but asserts that the positions in the Preliminary Response would be the same under either party’s proposal. *Id.*

The parties substantially agree on the level of ordinary skill in the art and differ mainly in the level of experience required for different levels of education. We consider Patent Owner’s proposed level of ordinary skill to be slightly more consistent with the '968 patent and the asserted prior art, and we apply it in our obviousness analysis below. We note, however, that our decision would be the same under either party’s proposed definition of the level of ordinary skill in the art.

B. Claim Interpretation

We interpret claims “using the same claim construction standard that would be used to construe the claims in a civil action [held] under 35 U.S.C. 282(b).” 37 C.F.R. § 42.100(b). Under this standard, we construe a claim “in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.” *Id.* We construe the claims only to the extent necessary to determine whether to institute *inter partes* review. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017). The parties agree that no claim constructions are needed. Pet. 21; Prelim. Resp. 15. Having considered the record, we determine that no express claim construction is necessary to reach our decision.

C. Principles of Law

A patent claim is unpatentable under 35 U.S.C. § 103 if 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. 35 U.S.C. § 103; *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). “The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results.” *KSR*, 550 U.S. at 416. The question of obviousness is resolved based on 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) when in evidence, objective evidence of non-obviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

D. Ground 1: Alleged Obviousness Over Jordan and FortiGate

Petitioner asserts claims 1–9 are unpatentable under 35 U.S.C. § 103 over the combination of Jordan and FortiGate. Pet. 3, 21–68.

*1. Jordan (Ex. 1005)*⁹

Jordan discloses a system and method for defending a computer network by dynamically adapting to new threats in real-time or just-in-time. Ex. 1005, 2:63–3:5. Jordan provides dynamic adaptability using a traffic filter configured to handle incoming communications received from sources external to the network of the traffic filter and/or outgoing communications to devices outside of the network as a perimeter device that controls all of the communications crossing a network boundary. *Id.* at 5:21–30. Figure 1 is reproduced below to illustrate this system with traffic filter 110 configured to receive and analyze incoming communications from external network 150 to determine if the communications are “normal” and contain no anomalies, and if so, to route them to appropriate user devices 120a–d. *Id.* at 8:33–66.

⁹ Petitioner contends that Jordan is prior art because its November 17, 2004 filing date predates November 20, 2004, which Petitioner asserts to be the earliest date to which the ’968 patent can claim priority. Pet. 63. Petitioner contends that the ’968 patent cannot claim priority to the March 12, 2004 filing date of Provisional Application No. 60/662,457 (“the ’457 provisional application”) because the challenged claims lack written description support in the three-page ’457 provisional application. *Id.*; see Ex. 1005, code (22); Ex. 1001, code (60). As discussed in more detail below, Petitioner has not shown sufficiently that Jordan, alone or in combination with FortiGate, teaches or suggests limitations 1[f], 4[d], and 7[d] of independent claims 1, 4, and 7, respectively. As a result, we do not need to determine whether the ’968 patent is entitled to claim priority from the ’457 patent provisional application in order to resolve the parties’ dispute regarding Ground 1.

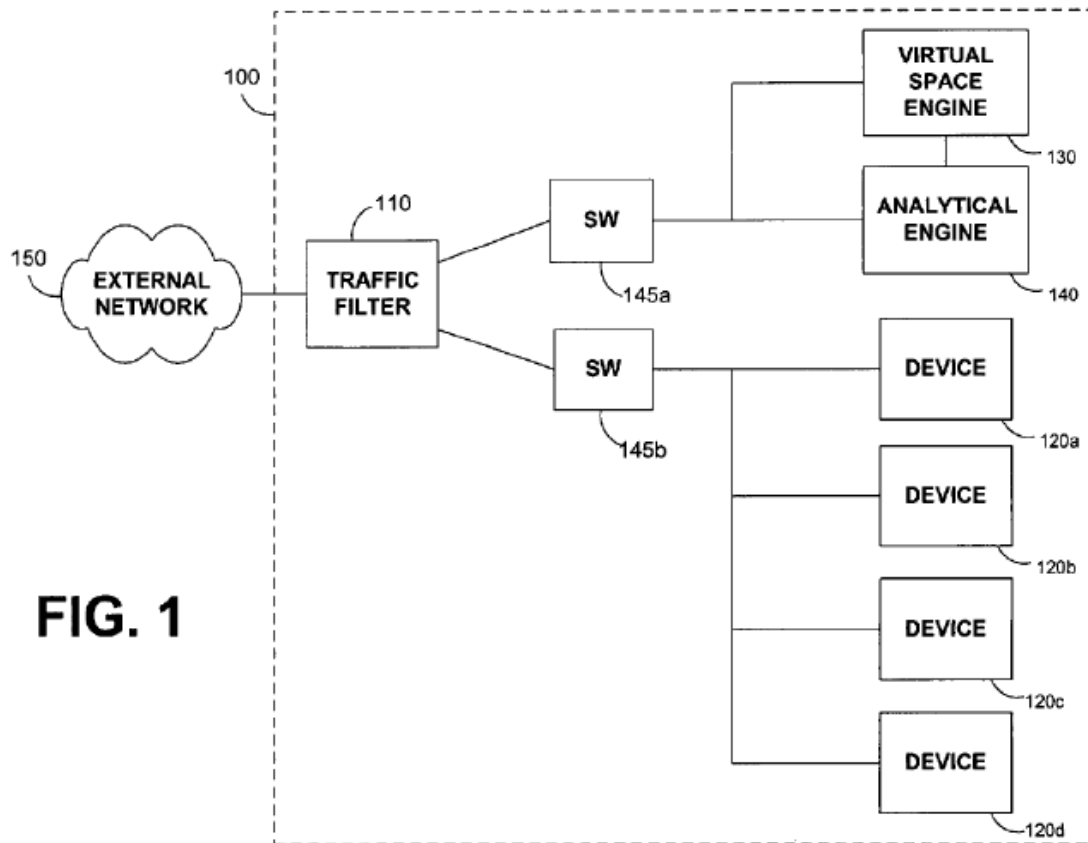


Figure 1 depicts network system 100. Traffic filter 110 filters external communications received from external sources over external network 150. It routes normal communications to devices 120a–d and sends anomalous or malicious communications to virtual space engine 130 and analytical engine 140. Ex. 1005, 5:21–33, 8:33–9:64. Traffic filter 110 communicates with analytical engine 140, which is a part of network system 100 that generates and communicates predetermined rules dynamically to traffic filter 110 to use in preventing malicious payloads from being delivered to devices 120. *Id.* at 9:33–64. Analytical engine 140 can generate or modify filtering rules used by traffic filter 110 to filter incoming network communications based on recently received communications with malicious payloads to adapt to the most recently received communications. *Id.* at 9:38–64.

2. *FortiGate (Ex. 1008)*

The FortiGate Antivirus Firewall User Manual (FortiGate) supports network-based deployment of application-level services that include antivirus protection and full-scan content filtering that improve network security and reduce network misuse and abuse. Ex. 1008, 13.

3. *Motivation to Combine*

Petitioner contends that a skilled artisan would have been motivated to combine Jordan and FortiGate because FortiGate analyzes content in real-time and downloads new or updated virus definitions to identify suspicious network traffic, and this capability would improve Jordan's complementary system, which generates and updates rules for malware detection. Pet. 25.

4. *Independent Claims 1, 4, and 7*

a. *1[pre]: "A network gateway device comprising:"*

Petitioner asserts that Jordan discloses a network gateway device as traffic filter 110 that sits between an external network and local network. Petitioner contends that traffic filter 110 is "used as a **perimeter device** to ***control all communications crossing a network boundary***," and FortiGate describes a "gateway" as something "that links different networks." Pet. 26–27 (citing Ex. 1005, 5:20–23, 5:28–30, Fig. 1; Ex. 1008, 297 (Glossary); Ex. 1002 ¶¶ 90–92). These contentions, which Patent Owner does not contest, are supported sufficiently by record evidence.

b. *4[pre]: "A method comprising:"*

Petitioner contends that Jordan discloses a "method for defending a computer network." Pet. 27 (citing Ex. 1005, 2:63–65; Ex. 1002 ¶ 93). This contention, which Patent Owner does not contest, is supported sufficiently by record evidence.

- c. 7[pre]: “A non-transitory computer-readable medium with instructions stored thereon which when executed by at least one processor of a data network device, causes the data network device to:”
1[a]: “at least one processor;” and 1[b]: “at least one memory device;”

Petitioner asserts that Jordan discloses “a processor-readable medium comprising code representing instructions to cause a processor” to perform functions of the invention, and Jordan’s traffic filter is a data network device that uses a processor-readable medium, instructions, and a processor to perform data network functions “such as controlling communications that crossed a network boundary.” Pet. 27–28 (citing Ex. 1005, 3:6–40, 3:25–30, 5:28–30, 25:29–32, Figs. 11, 14; Ex. 1001, 10:49–51; Ex. 1002 ¶¶ 94–96). These contentions, which Patent Owner does not contest, are supported sufficiently by record evidence.

- d. 1[c]: “at least one network interface device;”

Petitioner contends that Jordan discloses that traffic filter 110 has a network interface device that “received traffic from an external network and routed it accordingly” and “communicated with ‘other devices or network components within its network by *any suitable means* . . . via standard wired or wireless communication protocols.” Pet. 28–31 (citing Ex. 1005, 3:14–40, 14:19–36, 11:1–24, 17:46–49, 17:53–57, 25:40–42, Figs. 1, 3, 5, 11; Ex. 1002 ¶¶ 97–101). These contentions, which Patent Owner does not contest, are supported sufficiently by record evidence. Traffic filter 110 is a perimeter device that is configured to handle communications from sources external to network 100 and received over external network 150. Traffic filter 110 routes normal traffic to devices 120 within network 100. Ex. 1005, 5:21–44, 8:33–57.

- e. *1[e]/4[a]/7[a]: “receive[ing] network traffic via the at least one network interface device;”*

Petitioner asserts that Jordan’s traffic filter is “***configured to receive communications*** from the external network 150” and skilled artisans would understand that the communications were network traffic transmitted over a network and received by traffic filter 110 using a network interface for receiving such communication. Pet. 38–39 (citing Ex. 1005, 5:23–25, 8:39–42, 14:9–11, 15:50–53, Fig. 3; Ex. 1002 ¶¶ 117–120). Dr. Lee testifies that Jordan’s “***traffic filter 110 receive[d] a communication such as a network communication*** from a device external to the network system 100,” and a skilled artisan “would have understood that the communications were network traffic because they were data transmitted over a network” and “those communications were received over the network interface.” Ex. 1002 ¶¶ 119, 120 (citing Ex. 1005, Fig. 3, 14:9–11, 15:50–53 (The “traffic filter 110 receive[d] a communication, such as a network communication from a device external to the network system 100 (e.g., via an external network 150.”))). These contentions, which Patent Owner does not contest, are supported sufficiently by record evidence.

- f. *1[f]/4[d]/7[d]: “receive[ing], via the [at least one] network interface device, the additional content detection data indirectly from the analysis process via an update station;”*

Petitioner contends that Jordan’s traffic filter 110 received new or updated rules containing additional content detection data such as virus lists from analytical engine 140 via switch 145. Pet. 57–58 (citing Ex. 1005, 9:38–40, 14:54–56, Figs. 1, 14; Ex. 1002 ¶¶ 154–156). Petitioner did not identify a network interface device in traffic filter 110 that receives this data.

Petitioner contends that FortiGate’s FortiResponse Distribution Center receives threats from Fortinet customers, updates virus definitions, and sends updates to update stations called FortiResponse Distribution Servers, which push updates to FortiGate firewalls. Petitioner asserts that a skilled artisan would have been motivated to incorporate FortiGate’s update stations into Jordan to improve Jordan’s scalability so “whenever the analytical engine generated additional content detection data, it could send the information to the update station, which could coordinate pushing the update to the various traffic filters/gateways.” Pet. 58–59 (citing Ex. 1008, 335, 336; Ex. 1001, 4:53–5:13; Ex. 1002 ¶¶ 154–157).

Patent Owner argues that Jordan does not disclose or render obvious a “network gateway device” (in claim 1) or “data network device” (in claims 4 and 7) that “receiv[es], *via the network interface device*, the additional content detection indirectly from the analysis process via an update station.” Prelim. Resp. 31 (emphasis added). In particular, Patent Owner argues:

Jordan discloses a fundamentally different system in which suspicious traffic is analyzed and new rules are generated *internally* within the network protected by the traffic filter. See Jordan at 9:34-35, Fig. 1. This stands in contrast to the invention of the ‘968 patent, in which additional content detection data is received externally “via the network interface device” and “indirectly from the analysis process via an update station.” Indeed, *having an update station in the external network is key to the claimed invention because it allows different update stations to serve network gateway devices in different geographical regions and improve load demands and capacities.*

Id. (emphasis added in last sentence); see also *id.* at 32 (“But critically, Petitioner does not identify a ‘network interface device’ via which the ‘additional content detection data’ is received.”).

The plain meaning of the claims is the “at least one network interface device” that receives network traffic in elements 1[e][i]/4[a]/7[a] is also “the network interface device” in claim 1 and “the at least one network interface device” in claims 4 and 7 that receives “the additional content detection data indirectly from the analysis process via an update station” in elements 1[f]/4[d]/7[d]. Antecedent basis for “the network interface device” or “the at least one network interface device” that receives additional content detection data in elements 1[f]/4[d]/7[d] is provided by “at least one network interface device” that receives network traffic in elements 1[e][i]/4[a]/7[a]. Ex. 1001, 12:2–14:19; *Wi-Lan, Inc. v. Apple, Inc.*, 811 F.3d 455, 462 (Fed. Cir. 2016) (“Subsequent use of the definite articles ‘the’ or ‘said’ in a claim refers back to the same term recited earlier in the claim.”); *see also Univ. of Mass. v. L’Oréal USA, Inc.*, 36 F.4th 1374, 1380 (Fed. Cir. 2022) (the use of “*the* adenosine concentration applied to the dermal cells” invoked an antecedent for repeating the claim’s prior reference to “a concentration of adenosine”).

This meaning is consistent with the ’968 patent specification, which discloses that “each content detection module 108 is configured to receive electronic content (content data), and determine[] whether the electronic content contains undesirable content based on the content detection data it receives from update station 106.” Ex. 1001, 5:14–20. A content detection module is a perimeter device that receives (1) external network traffic and (2) content detection data from external update stations via the same network interface device and the Internet. It receives both types of data from sources external to the network (network traffic, update stations) that it protects. It receives network traffic and content detection data from external sources via the same network interface and Internet. *Id.* at 4:53–55, 5:14–6:62, Fig. 1.

The '968 patent describes the content detection module receiving the network traffic and content detection data from external sources. Central station 102 “send[s] the content detection data to update stations 106 (e.g., through the Internet).” Ex. 1001, 4:35–38. Update stations 106 receive the content detection data from central station 102, and send content detection data to content detection modules 108 (e.g., *through the Internet*). *Id.* at 4:53–55, Fig. 1. External central station 102 and update stations 106 push the latest security update data to content detection modules 108. *Id.* at 4:53–55, 9:6–60. “After content detection modules 108 received the content detection data (e.g., a virus signature), content detection modules 108 can then utilize the content detection data to detect content.” *Id.* at 8:59–62.¹⁰

Petitioner asserts that a network interface device in Jordan’s traffic filter 110 receives network traffic from *external networks* in elements 1[e]/4[a]/7[a]. Pet. 38–39. Petitioner asserts that traffic filter 110 is a network gateway and perimeter device that controls all communications crossing a network boundary. *Id.* at 26–27 (citing Ex. 1005, 5:28–30). Petitioner also asserts that traffic filter 110 includes “at least one network interface device” because “the traffic filter received traffic from an external network and routed it accordingly” (*id.* at 28–29 (citing Ex. 1005, 3:14–40, 11:1–24, 14:19–36, Figs. 1, 3, 5, 11)), and traffic filter 110 is “***configured to receive communications*** from the external network 150” via a network interface device in elements 1[e][i]/4[a]/7[a] (*id.* at 38–39 (citing Ex. 1005, 5:23–25, 8:39–42, 14:9–11, 15:50–53, Fig. 3)).

¹⁰ The original claims of Application No. 14/072,184, filed on November 5, 2013, as a continuation of Application No. 13/795,407, filed on March 12, 2013, recited this claimed subject matter. Ex. 1003, 340–344.

Petitioner asserts that traffic filter 110 receives content detection data *via Jordan's switch* for elements 1[f]/4[d]/7[d] without identifying a network interface that does so. Petitioner asserts, “Jordan disclosed that the traffic filter received new/updated rules via a switch.” Pet. 57 (citing Figure 14 to show “the analytical engine sending new/updated rules to the traffic filter”).

Petitioner further contends as follows:

The additional content detection data went indirectly from the analytical engine to the traffic filter. Figure 1 (below) showed that a switch (145a) intermediated traffic between analytical engine (140) and the traffic filter (110). Accordingly, the traffic filter received the data indirectly from the analytical engine because it went through the switch.

Pet. 58. Petitioner illustrates its contentions in Figure 1, reproduced below.

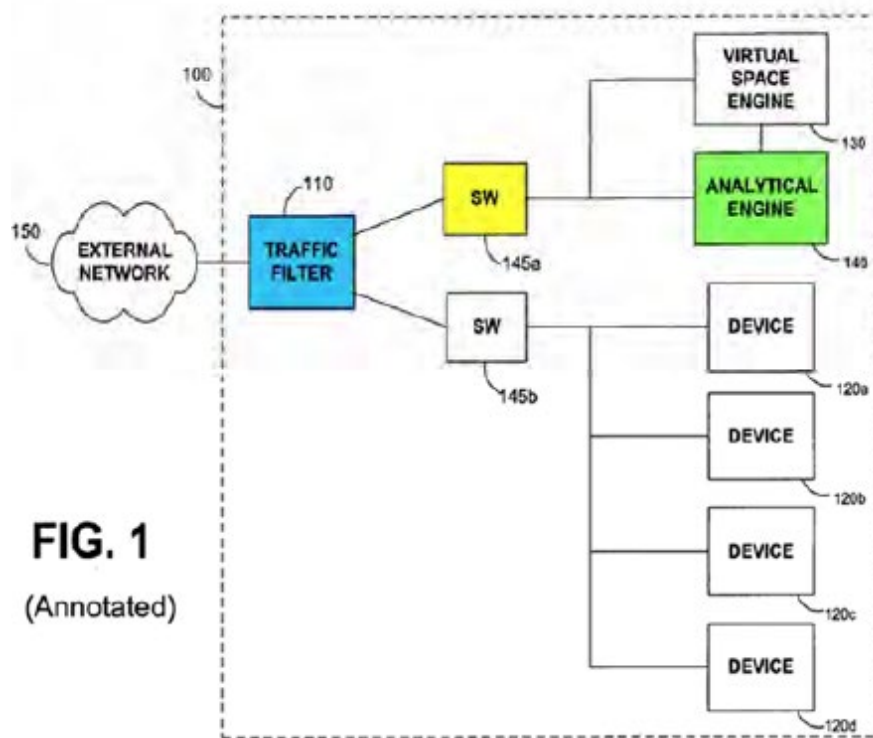


Figure 1 of Jordan includes Petitioner’s annotations to show that analytical engine 140 sends content detection data to traffic filter 110 “indirectly” via switch 145a *within network 100*. Pet. 58.

Petitioner does not explain how the *same network interface device* that receives external network traffic in elements 1[e][i]/4[a]/7[a] also receives content detection data at traffic filter 110 for elements 1[f]/4[d]/7[d].

For elements 1[e][i]/4[a]/7[a], Dr. Lee testifies that “the network system 100 include[d] a traffic filter 110, which [was] ***configured to receive communications*** from the external network 150” and route communications “within the network system 100.” Ex. 1002 ¶ 118 (quoting Ex. 1005, 8:39–42). Dr. Lee testifies that Jordan’s traffic filter 110 “handle[s] incoming communications (i.e., communications received from sources external to the network of the traffic filter).” *Id.* (quoting Ex. 1005, 5:23–25). Dr. Lee further testifies that Figure 3 of Jordan shows traffic filter 110 receiving network communications “from a device *external to the network system 100.*” *Id.* ¶ 119 (citing Ex. 1005, 15:50–53, Fig. 3) (emphasis added).

For elements 1[f]/4[d]/7[d], Dr. Lee switches course and testifies that “Jordan discloses that the traffic filter received the new/updated rules via switch” and “[i]f Jordan’s switch does not constitute an ‘update station,’ a [skilled artisan] would have found it obvious to incorporate FortiGate’s update station into Jordan.” Ex. 1002 ¶ 154. Relying on an annotated copy of Figure 1, which we reproduced above, Dr. Lee testifies, “[t]he additional content detection data went indirectly from the analytical engine to the traffic filter” and “a switch (145a) intermediated traffic between analytical engine (140) and the traffic filter (110).” Ex. 1002 ¶ 156. Dr. Lee testifies that traffic filter 110 receives content detection data via switch 145 (or a FortiGate update station) *within network 100* in elements 1[f]/4[d]/7[d], rather than via the network interface device that received external network traffic in elements 1[e][i]/4[a]/7[a]. Ex. 1002 ¶¶ 97, 98, 117–120, 154–157.

Neither Petitioner nor Dr. Lee explains how traffic filter 110 receives network traffic from external network 150 in elements 1[e]/4[a]/7[a] and “additional content detection data indirectly from the analysis process via an update station” in elements 1[f]/4[d]/7[d] *via the same network interface device*. Figure 14 of Jordan, reproduced below, illustrates how analytical engine 140 sends new or updated rules as content detection data to traffic filter 110 *internally within network 100* without passing through the network interface device that receives network traffic from external network 150.

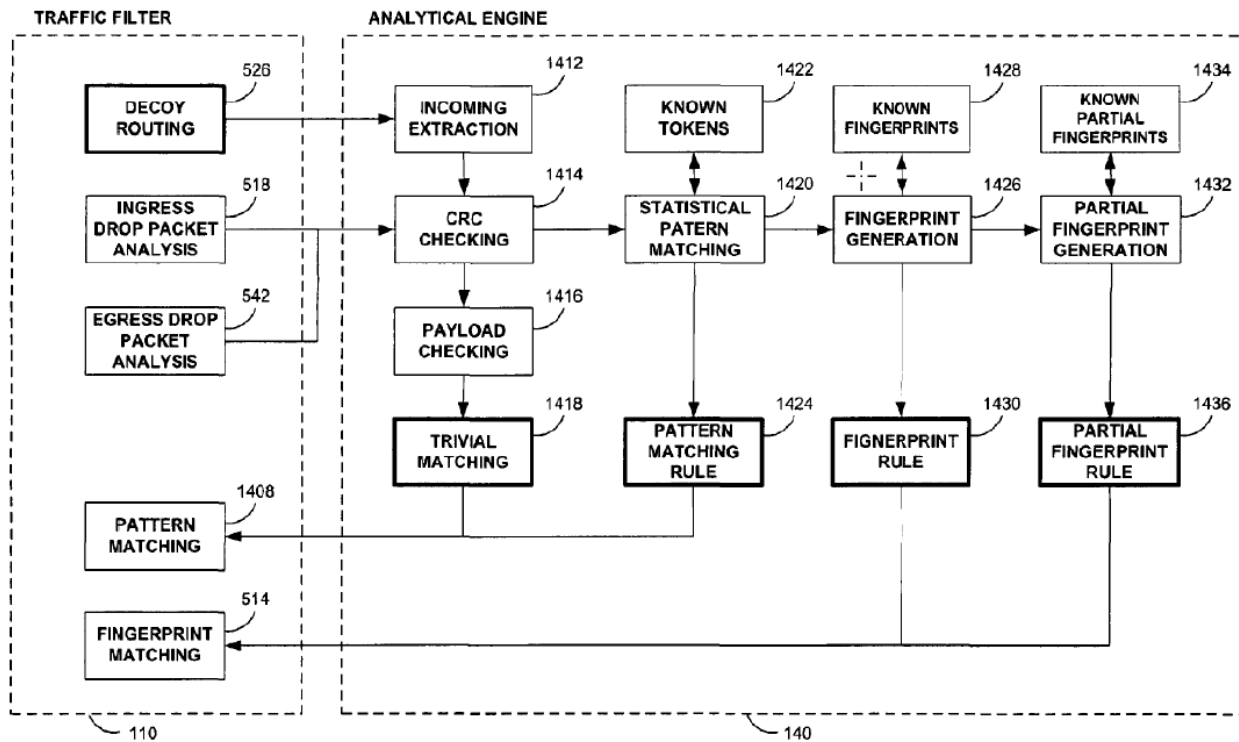


Figure 14 of Jordan depicts content detection data sent by analytical engine 140 to traffic filter 110 *within network 100*, rather than via a network interface device that receives network traffic from external network 150. Ex. 1005, 29:39–64; *id.* at 9:34–35 (the traffic filter communicates with an analysis engine 140, which is part of the network system 100), Fig. 1; *cf. id.* at 5:23–25 (traffic filter is configured to receive external network traffic).

Even if Jordan is modified “to incorporate FortiGate’s update stations to improve Jordan’s scalability” [so that] “whenever the analytical engine generated additional content detection data, it could send the information to the update station, which could coordinate pushing the update to the various traffic filters/gateways” (Pet. 59), Petitioner has not explained sufficiently how the network interface device in traffic filter 110 that receives network traffic from *external* network 150 also receives content detection data from *internal* analytical engine 140 via a FortiGate update station (Pet. 58–59).

As Patent Owner argues, “Jordan’s traffic filter is served directly by its dedicated analytical engine, which is in the same network as the traffic filter,” so adding a FortiGate “update station” between the traffic filter and analytical engine would be unnecessary, detrimental to speed and reliability, and add an extraneous layer. Prelim. Resp. 40. Content detection data sent from analytical engine 140 to traffic filter 110 via a FortiGate update station would travel *within network 100* rather than via external network 150 to the network interface device of traffic filter 110 that receives external network traffic in elements 1[e]/4[a]/7[a].¹¹ As discussed in Section I.C. above and argued by Patent Owner (Prelim. Resp. 38–39), externally situated update stations offer many benefits compared to update stations located internally to a network that is protected by a content detection module as in Jordan.

We find that Petitioner has not shown sufficiently that Jordan, alone or in combination with FortiGate, teaches elements 1[f], 4[d], and 7[d]. We find that Petitioner has not established a reasonable likelihood that at least one of claims 1, 4, and 7 is unpatentable over Jordan and Fortigate.

¹¹ Petitioner’s contentions regarding FortiGate are not clear, as they cite to pages 335 and 336 of Exhibit 1008, which only comprises 329 pages.

5. *Dependent Claims 2, 3, 5, 6, 8, and 9*

Petitioner's contentions for dependent claims 2, 3, 5, 6, 8, and 9 do not resolve the deficiency in its contentions for claims 1, 4, and 7. Indeed, Petitioner continues to assert that traffic filter 110 and analytical engine 140 are distinct devices that are separated by a switch *within network 100* and does not address how content detection data sent by analytical engine 140 to traffic filter 110 is received via the network interface device in traffic filter 110 that receives network traffic from external network 150. Pet. 61.

Accordingly, we find that Petitioner has not established a reasonable likelihood that any of claims 2, 3, 5, 6, 8, and 9 are unpatentable over Jordan and FortiGate.

E. *Ground 2: Alleged Obviousness Over Lee and Magdych*

Petitioner asserts claims 1–9 are unpatentable under 35 U.S.C. § 103 over the combination of Lee and Magdych. Pet. 3, 68–93. As discussed in more detail below, Petitioner's contentions for Lee and Magdych suffer from the same defects as Jordan and FortiGate in Ground 1, namely, that even if Lee's firewall is modified to include a Network Security Agent (NSA) that receives content detection data from a Security Policy Manager (SPM) 54 and Intelligent Security Engine (ISE) 52, this content detection data is received through the *internal network* that the firewall protects rather than via a network interface device in firewall 20 that receives network traffic from data sources 80 via an unsecured *external network 10*. Once again, the Petition fails to identify *a single* network interface device that (1) receives external network traffic in elements 1[e]/4[a]/7[a] and (2) receives content detection data in elements 1[f]/4[d]/7[d] as recited in independent claims 1, 4, and 7.

1. Lee (Ex. 1009)

Lee discloses a security system with firewall 20 protecting an internal network 30, 60 from external users as shown in Figure 1, reproduced below.

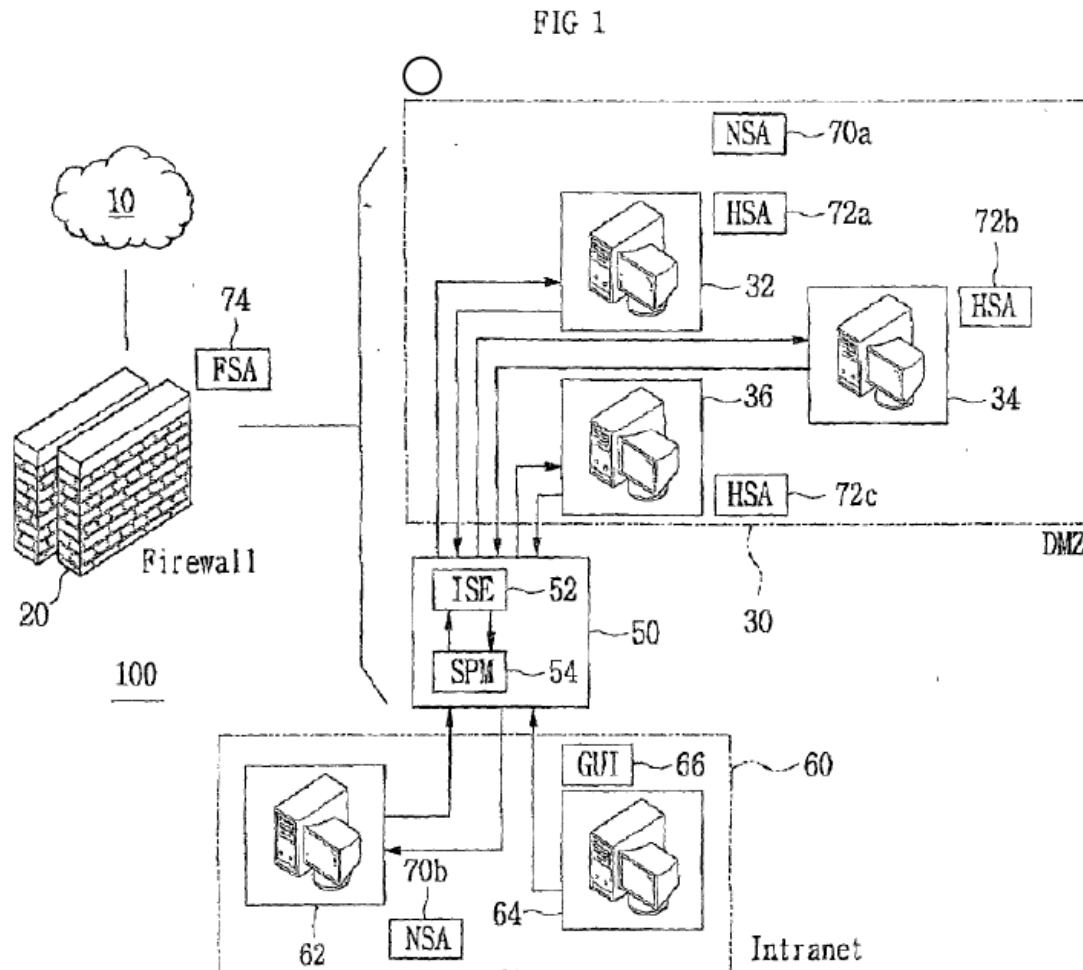


Figure 1 shows firewall 20, Firewall Security Agent (FSA) 74, and Network Security Agents (NSAs) 70a, 70b, Host Security Agents (HSAs) 72a–c, Security Policy Manager (SPM) 54, and Intelligent Security Engine (ISE) 52 forming an integrated security system to protect *internal network* 30, 60 from outside users and public network 10. Ex. 1009 ¶¶ 34–41.

De-Militarized Zone (DMZ) 30 offers customers or outsiders access to public information without accessing internal user system 62 and manager system 64 of intranet 60 of the internal network. Ex. 1009 ¶¶ 35, 36, 38.

NSA 70 and HSA 72 are active agents. NSA 70 confronts threats to internal network security and analyzes suspicious traffic and alert messages for known attacks. Ex. 1009 ¶ 41. HSA 72 reacts to threats against servers in the network and responds to requests from ISE 52 to analyze system status, activities, and security functions. *Id.* NSA 70 and HSA 72 perform monitoring and alerts using detection signatures generated by ISE 52. *Id.*

ISE 52 and SPM 54 are part of an intelligent security management module 50. Ex. 1009 ¶ 38. ISE 52 is an analysis engine that analyzes alert messages received from agents installed within each individual security system and generates a new detection signature through learning. *Id.* ¶ 48. SPM 54 applies dynamic security policies from ISE 52 to associated agents according to the detection signatures generated by ISE 52. *Id.* ¶ 49.

Firewall 20 blocks traffic from *external attackers 80* using policies that FSA 74 receives from ISE 52 and SPM 54. Ex. 1009 ¶¶ 14, 46, 51, 52.

Figure 2 of Lee is reproduced below to depict an operational flow of this security system as it protects internal network 30, 60. Ex. 1009 ¶ 20.

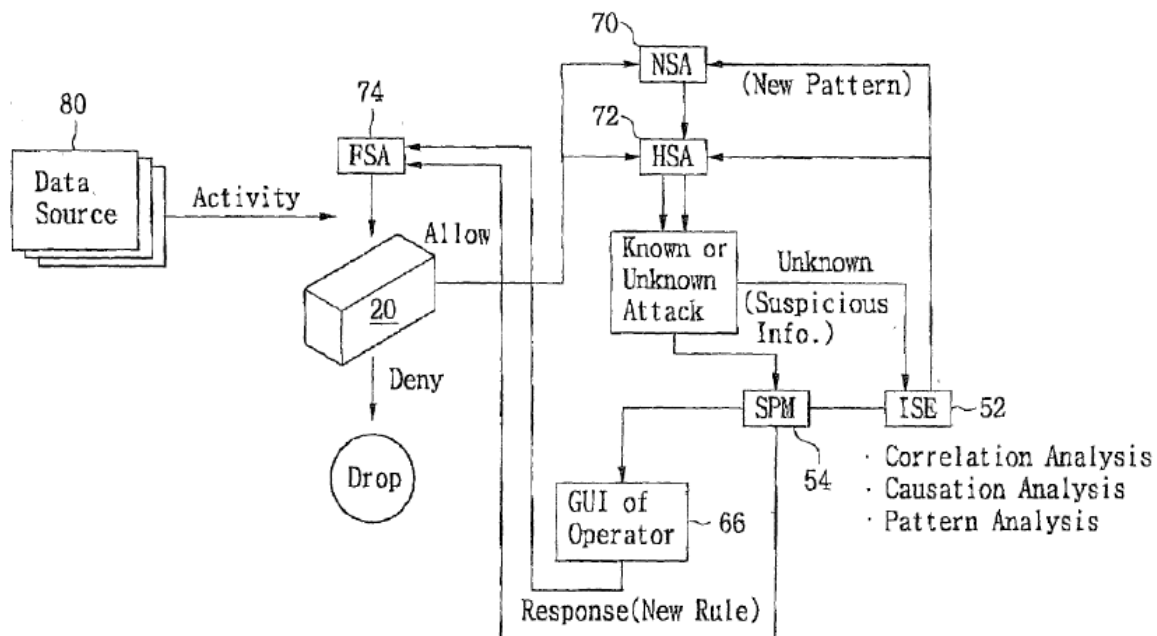


Figure 2 illustrates firewall 20 and active agents NSA 70, HSA 72, FSA 74, ISE 52, and SPM 54 arranged to protect internal network 30, 60. Ex. 1009 ¶ 51. NSA 70 and HSA 72 agents detect *known* attacks and also suspicious data and traffic and generate reports to ISE 52 and SPM 54. *Id.* When SPM 54 receives detection of an attack, it sends new rules *internally* to FSA 74 so firewall 20 blocks traffic from external attack data source 80. *Id.* ¶¶ 51, 52.

2. Magdych (Ex. 1010)

Magdych discloses firewalls that detect network attacks by passing data through a firewall portion 402 that discards some data using rules, and an intrusion detection system 404 that compares other data to a list of text associated with attacks. Ex. 1010, 1:9–10, 2:39–54. Figure 4 of Magdych is reproduced below to illustrate this firewall configuration.

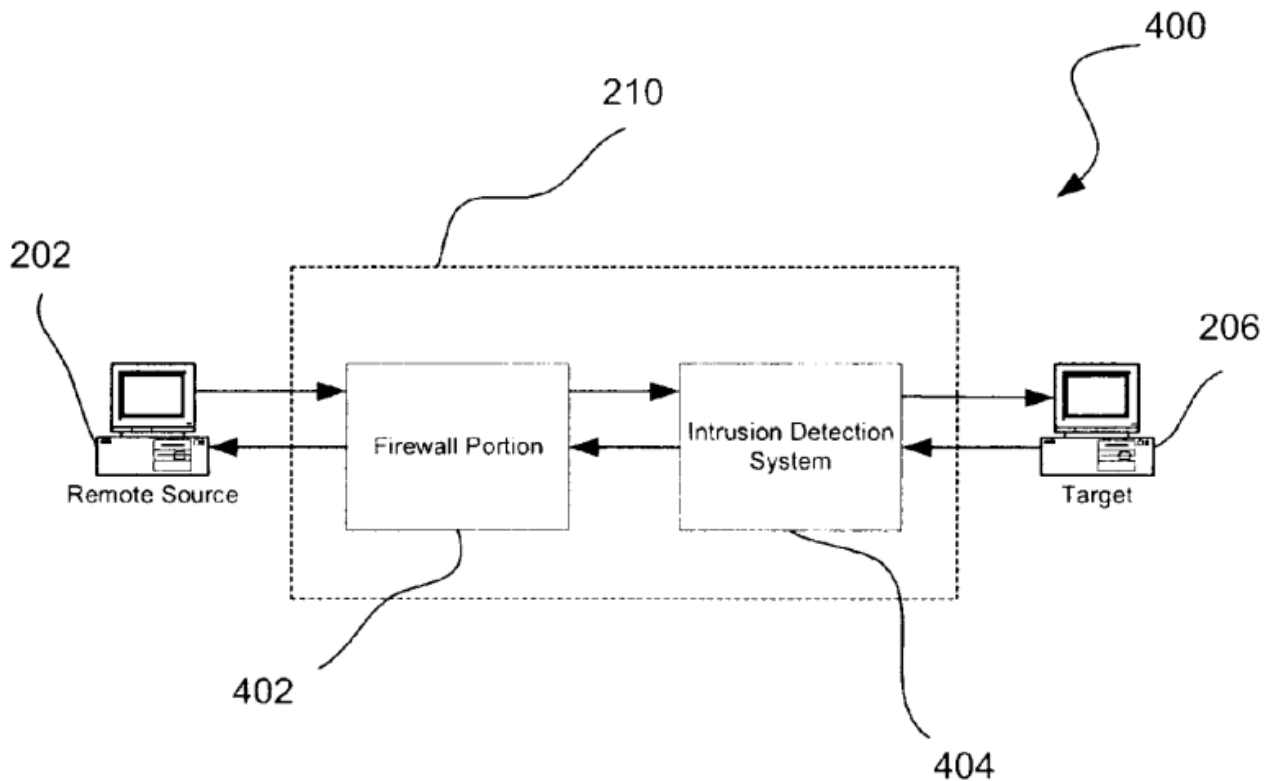


Figure 4

Figure 4 depicts firewall portion 402 and intrusion detection system 404 serially coupled between remote source 202 and target 206. Firewall portion 402 filters packets with rules based on source, destination, and/or port. Intrusion detection system 404 compares other text data to a list of data representing text associated with attacks. *See* Ex. 1010, 4:17–5:63.

3. *Motivation to Combine*

Petitioner asserts that a skilled artisan would add Lee’s NSA and FSA into a firewall, as Magdych teaches, to apply security policies and to detect known attacks. Pet. 71. Petitioner asserts the following motivation is found:

A POSITA would have made this combination for several reasons. First, it would save rack space and combining software into a single module would have been feasible given increased processor speeds and memory. Second, it would have improved Lee’s efficiency by having a single device perform at least two levels of analysis (firewall-level and content-level analyses). Third, it would have improved Lee’s security. Currently, Lee’s architecture has the NSA behind the FSA—i.e., deeper within the network. But it was standard practice to deploy traffic filters at a network’s perimeter to minimize any potential damage in the event of an attack.

Pet. 72 (citing Ex. 1002 ¶¶ 190, 191).

Patent Owner argues, “this is contrary to Lee’s teachings” because

Lee expressly states that an “object of the invention” is “to implement a *distributed* security environment based on a number of *independent* security agents” such as an NSA and FSA. Lee, ¶¶ 12, 14. Lee explains that, “[b]ecause agents are independent of one another, the implementation is less cumbersome and preferably requires less overall code space. *Id.*, ¶ 40. Furthermore, independence allows “different agents” to be “easily added, removed, or modified as necessary to fulfill the requirements of network security.” *Id.*

Prelim. Resp. 45 (quoting Ex. 1009 ¶ 40).

Petitioner relies on Magdych’s teachings to add a content intrusion device to a firewall to augment the network security features of the firewall and improve Lee’s firewall where Lee teaches that different agents are “easily added, removed, or modified as necessary to fulfill the requirements of network security,” as Patent Owner recognizes. Pet. 71–72; Ex. 1009 ¶ 40; Prelim. Resp. 45. Using a known technique to improve similar devices in the same or similar way is obvious unless its application is beyond the level of ordinary skill in the art. *KSR*, 550 U.S. at 417.

4. *Independent Claims 1, 4, and 7*

a. *1[c] “at least one network interface device”*

Petitioner contends that Lee discloses that the firewall had a network interface device because it “intermediated traffic between a secure network connected and the insecure outside world.” Pet. 75. Petitioner contends that Lee’s “Figure 1 . . . depicted firewall 20 receiving traffic from an outside network (e.g., the Internet)” and “Lee explained that firewall 20 had ‘three network interfaces: one [went] to the inside of the intranet; one [went] to the unsecured external network 10; and the third [went] to the DMZ 30.” *Id.* (citing Ex. 1009 ¶¶ 7, 35, 36, Fig. 1; Ex. 1002 ¶¶ 199, 200).

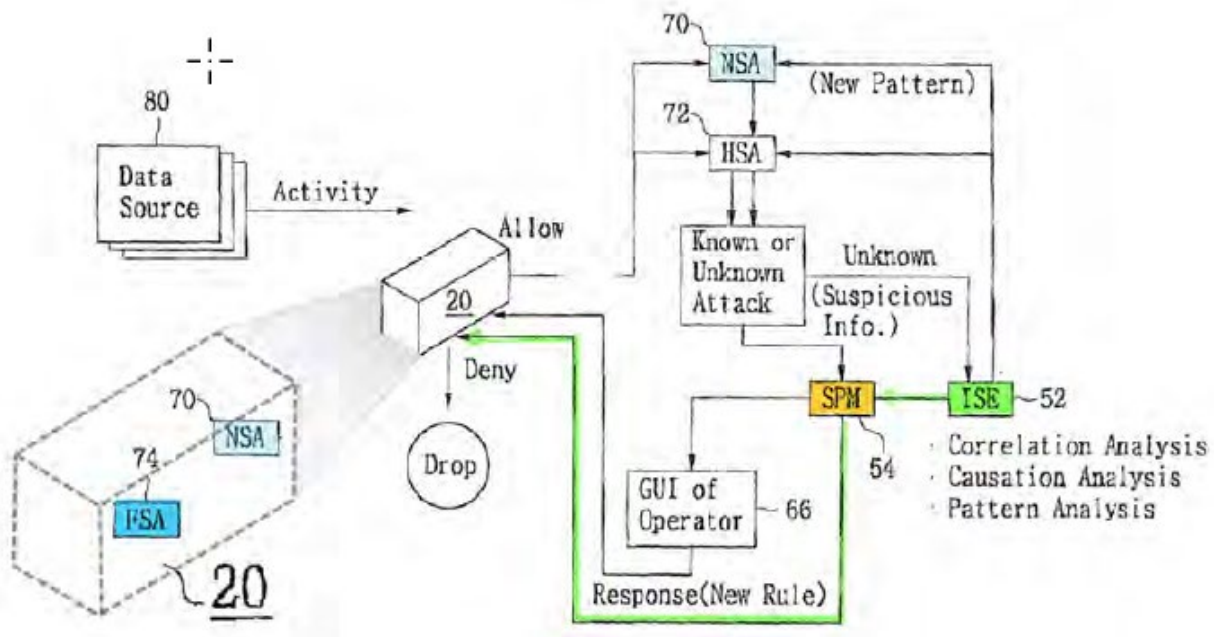
b. *1[e][i]/4[a]/7[a] “receive[ing] network traffic via the at least one network interface device”*

Petitioner contends that “Lee disclosed that the firewall received data via the network interface device,” “Lee explained that firewall 20 had a network interface that went to an *unsecured external network*,” and “as illustrated in Figure 1 . . . , Lee disclosed that firewall 20 received traffic from an *outside network (10)*.” Pet. 79 (citing element 1[c]; Ex. 1009 ¶¶ 35, 36, 51, Fig. 1; Ex. 1002 ¶¶ 209, 210) (emphasis added).

- c. 1[f]/4[d]/7[d]: “receive[ing], via the network interface device, the additional content detection data indirectly from the analysis process via an update station”

Petitioner asserts that “Lee’s SPM acted as an update station by providing new rules generated by the ISE to the agents, including the FSA in firewall (20),” and “Lee disclosed that a generated signature from the ISE was transferred to the NSA (70) and FSA (74) in firewall (20) . . . shown in Figure 2 (annotated below), where the ‘new pattern’ was transmitted from ISE to SPM, then SPM to FSA.” Pet. 88 (citing Ex. 1009 ¶¶ 46, 49, 56, Fig. 2 (annotated)). We reproduce Petitioner’s annotated Figure 2 below.

FIG 2 (Redrawn and Annotated)



Annotated Figure 2 of Lee shows Petitioner’s assertion that Lee with Magdych’s teachings would transmit content detection data from ISE 52 to NSA 70 and FSA 74 in firewall 20 *via the internal network*. Pet. 88–89.

Regarding elements 1[f]/4[d]/7[d], Petitioner asserts:

While Lee did not explicitly describe that the new rules [were] received via a network interface device, a POSITA would have found it obvious because the SPM transferred digital information to firewall (20) and firewall (20) had a *network interface for the internal part of the network*.

Pet. 89 (citing Ex. 1009 ¶¶ 36, 46; Ex. 1002 ¶¶ 231–232) (emphasis added).

Petitioner asserts that Lee disclosed firewall 20 with three network interface devices (one to the inside of the intranet 60, one to the unsecured *external network 10*, and one to internal DMZ 30), and that Lee’s firewall 20 as modified by Magdych’s teachings to include NSA 70, would receive content detection data from ISE 52 and SPM 54 via the *network interface device* “for the *internal part of the network*.” Pet. 75, 89 (emphasis added).

Petitioner has not shown that Lee’s firewall receives network traffic and content detection data via the same network interface device as claimed. Instead, Petitioner asserts that Lee’s firewall 20 (1) receives network traffic via a network interface device that interfaces to unsecured *external network 10* for elements 1[e]/4[a]/7[a] but (2) receives content detection data via a different network interface device “for the *internal part of the network*” for elements 1[f]/4[d]/7[d]. Pet. 75, 89 (emphasis added); *see* Prelim. Resp. 51.

The ’968 patent describes numerous benefits of the external update configuration. Update stations can be distributed geographically to serve multiple content detection modules. Ex. 1001, 7:27–33. Central station 102 can distribute content detection data to content detection modules via update stations that have more capacity. *Id.* at 7:34–8:5. Update stations can share loads, back up one other, and update one another with content detection data to send to content detection modules. *Id.* at 8:6–9:41; Section I.C. above.

We find that Petitioner has not shown sufficiently that Lee, alone or in combination with Magdych, teaches elements 1[f], 4[d], and 7[d]. We also find that Petitioner has not established a reasonable likelihood that any of claims 1, 4, and 7 is unpatentable over Lee and Magdych.

d. Dependent Claims 2, 3, 5, 6, 8, and 9

Petitioner's contentions for dependent claims 2, 3, 5, 6, 8, and 9 do not resolve the deficiency in its contentions for claims 1, 4, and 7. Pet. 91–93. Accordingly, we find that Petitioner has not established a reasonable likelihood that any of claims 2, 3, 5, 6, 8, and 9 are unpatentable over Lee and Magdych.

F. Ground 3: Alleged Obviousness Over Lee, Magdych, and Judge

Petitioner asserts claims 1–9 are unpatentable under 35 U.S.C. § 103 over the combination of Lee, Magdych, and Judge. Pet. 3, 93–95.

1. Judge (Ex. 1011)

Petitioner relies on Judge to disclose the knowledge of a skilled artisan to use configuration data in detection systems. Pet. 93–94.

2. Analysis

Petitioner asserts it would have been obvious to incorporate Judge's configuration data examples into the Lee-Magdych combination to increase the parameters, features, accuracy, and control of Lee's modified system. Pet. 95 (“Incorporating goals and threat types of interest (e.g., configuration data) into the applied policies would help better protect networks.”).

Petitioner's reliance on Judge to disclose configuration data does not cure the deficiencies in Lee and Magdych for Ground 2. Thus, we find that Petitioner has not established a reasonable likelihood that any of claims 1–9 are unpatentable over Lee, Magdych, and Judge.

G. Ground 4: Alleged Obviousness Over Fang and FortiGate

Petitioner asserts claims 1–9 are unpatentable under 35 U.S.C. § 103 over the combination of Fang and FortiGate. Pet. 3, 96–112.

1. Priority

The '968 patent issued from U.S. Patent Application No. 14/072,184, filed November 5, 2013. Ex. 1001, codes (21), (22). The '968 patent claims priority as a continuation of U.S. Patent Application No. 13/795,407, which was filed March 12, 2013 (“the '407 application”; Ex. 1004), and through a series of continuation applications (with identical written descriptions) back to U.S. Patent Application No. 11/000,703, filed November 30, 2004 (“the '703 application”). Ex. 1001, code (63).

Petitioner argues that “the challenged claims lack written description support in the '407 application because, *inter alia*, it does not disclose (1) “configuration data” and operations that implicate configuration data, or (2) “user identification” and operations that implicate user identification.” Pet. 14 (“[T]he challenged claims are entitled to a priority date of no earlier than November 5, 2013, the date the '968 patent was filed.”).

2. Fang (Ex. 1012)

Petitioner asserts that Fang is prior art to the '968 patent because “Fang has the same description as the '968 patent, and precisely like the '968 patent, disclosed ‘systems and methods for updating content detection devices and systems.’” Pet. 96. *Id.* Fang was published on November 1, 2012. Ex. 1012, code (43); *see* Pet. 96 n.6 (“Fang is the printed publication . . . and has the same figures and detailed description as the '968 Patent.”).

As discussed below, we are not persuaded that the '968 patent lacks written description support in the '407 application and prior continuations.

a. “configuration data”

Petitioner asserts that the “content detection data” and “configuration data” define and enforce policies for processing received network traffic, but “configuration data” is not disclosed in the ’968 patent, the ’407 application, or any other application in the priority chain of the ’968 patent. Pet. 15. In addition, Petitioner argues that every mention of a content detection module processing network traffic describes the module processing the traffic using only “content detection data” but not “configuration data.” *Id.* at 15–16.

Claim 1 recites a network gateway device that can “process received network traffic in view of content detection and configuration data stored in” a memory device “to enforce policies defined at least in part by the content detection and configuration data.” Ex. 1001, 12:12–16. Independent claims 4 and 7 contain similar limitations. *Id.* at 12:54–59, 13:32–35.

The ’407 application describes gateway content detection module 108 is *configured* to perform policy enforcement and determine if content data is undesirable based on content detection data. Ex. 1004, 175–176 (¶ 29). To configure a content detection module to process network traffic for policy enforcement describes “configuration data” as indicated by the following:

each content detection module 108 is *configured* to receive electronic content (content data), and determines whether the electronic content contains undesirable content based on the content detection data it receives from update station 106. For example, content detection module 108 can be *configured* to detect virus based on a virus signature received from update station 106. [M]odule 10[8] is implemented as a component of a gateway (or gateway product), which is *configured* to perform policy enforcement . . . which creates a result that can be used to determine whether to pass data to the user

Ex. 1004, 175–176 (¶ 29); *see* Ex. 1001, 5:14–35 (same).

The '407 application describes a content detection module 108 that is *configured* to enforce policies for different types of web traffic including viruses, spam, and worms based on content detection data such as a virus signature, virus definition, spammer identification, a URL, and a NIDS signature. *See* Ex. 1004, 175–176 (¶ 29), 177 (¶¶ 31, 32), 181–182 (¶ 39); Prelim. Resp. 24–25; Ex. 2001 ¶ 62. This description matches the '968 patent and supports claims to configuration data and content detection data used to enforce policies at a network gateway device or data network device in claims 1, 4, and 7. *See* Ex. 1001, 5:13–31, 5:60–6:7, 6:28–36, 8:59–92.

A specification does not have to provide literal or verbatim support for claimed subject matter. *See Union Oil Co. of Cal. v. Atl. Richfield Co.*, 208 F.3d 989, 997 (Fed. Cir. 2000); *In re Gosteli*, 872 F.2d 1008, 1012 (Fed. Cir. 1989); *In re Kaslow*, 707 F.2d 1366, 1375 (Fed. Cir. 1983).

b. “user identification”

The claimed policy enforcement also includes user identification and content identification. Ex. 1001, 12:2–14:27. The '968 patent and '407 application describe subscription data that includes user identification of a content detection module 108 and level of protection desired by a user from a processing station 104 or update station 106 for policy enforcement that identifies particular content to be detected by a content detection module. Ex. 1004, 174–176 (¶¶ 27–29); Ex. 1001, 4:38–5:35; Prelim. Resp. 25–27; Ex. 2001 ¶¶ 65–69.

We find that this subject matter is described in the '407 application and the '968 patent sufficiently to convey to a skilled artisan that the inventors possessed this claimed subject matter. *See* Prelim. Resp. 25–27.

c. Conclusion

Patent Owner has shown that claims 1, 4, and 7 of the '968 patent, reciting “configuration data” and “user identification,” are supported by the written description in the '407 application and can claim priority to that application as well as to other continuation applications not challenged by Petitioner, to November 30, 2004. *See* Prelim. Resp. 23–27; Ex. 1001, code (63). Because Patent Owner has shown that the challenged claims are entitled to claim priority to the '407 application and the earlier continuation applications, including U.S. Patent Application No. 11/000,703, Fang is not prior art to the '968 patent, and Petitioner has not established a reasonable likelihood that any of claims 1–9 are unpatentable over Fang.

III. CONCLUSION

For the reasons discussed above, we are not persuaded that Petitioner has demonstrated a reasonable likelihood of prevailing in establishing that any of claims 1–9 of the '968 patent is unpatentable.

IV. ORDER

In consideration of the foregoing, it is hereby:

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

IPR2023-00457
Patent 9,231,968 B2

PETITIONER:

Thomas Millikan
Babak Tehranchi
Cory Owan
PERKINS COIE LLP
Milikan-ptab@perkinscoie.com
Tehranchi-ptab@perkinscoie.com
Owan-ptab@perkinscoie.com

PATENT OWNER:

James Glass
John McKee
Quincy Lu
Andrew Holmes
Ognjen Zivojnovic
QUINN EMANUEL URQUHART & SULLIVAN LLP
jimglass@quinnemanuel.com
johnmckee@quinnemanuel.com
quincylu@quinnemanuel.com
drewholmes@quinnemanuel.com
ogizivojnovic@quinnemanuel.com