

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Netskope, Inc.

Petitioner,

v.

Fortinet, Inc.

Patent Owner.

Case IPR2023-00457
Patent No. 9,231,968 B2

**PATENT OWNER'S PRELIMINARY RESPONSE
PURSUANT TO 35 U.S.C. § 313 AND 37 C.F.R. § 42.107**

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. OVERVIEW OF THE '968 PATENT	3
III. OVERVIEW OF THE CITED ART	7
A. Jordan (Ex-1005).....	7
B. FortiGate (Ex-1008)	9
C. Lee (Ex-1009).....	9
D. Magdych (Ex-1010)	12
E. Judge (Ex-1011)	13
F. Fang (Ex-1012).....	13
IV. LEVEL OF ORDINARY SKILL IN THE ART	14
V. CLAIM CONSTRUCTION	14
VI. PRIORITY DATE	15
A. The Challenged Claims of the '968 Patent Are Entitled To The Priority Date of the '457 Provisional Application.	15
1. "configuration data"	17
2. "user identification"	19
3. "forwarding the network traffic to an analysis process"	20
4. "policy enforcement including user identification, content identification, and at least one of source verification and destination verification"	22
B. The '968 Patent Provides Written Description Support.....	23
1. "configuration data"	23
2. "user identification"	25
VII. GROUND 1: JORDAN AND FORTIGATE DO NOT RENDER ANY CLAIM OBVIOUS.....	28
A. Jordan Does Not Qualify as Prior Art.	28
1. Jordan Provisional Does Not Provide Support For Claim 1.....	29

2.	Jordan Provisional Does Not Provide Support For The Subject Matter Relied Upon.....	30
B.	Even If Jordan is Deemed To Qualify as Prior Art, Jordan in View of FortiGate Does Not Render Any Claims Obvious.....	31
1.	Jordan Does Not Disclose or Render Obvious “Receiv[ing], Via The Network Interface Device, The Additional Content Detection Data Indirectly From the Analysis Process Via an Update Station.”	31
(a)	Network Interface Device.....	32
(b)	Indirectly From the Analysis Process Via an Update Station	36
2.	A POSITA Would Not Have Been Motivated To Combine Jordan With FortiGate.....	39
3.	Jordan Does Not Disclose “Wherein The Analysis Process Facilitates an Analysis That Includes Receiving Administrator Input.”	42
VIII.	FOUNDATIONS 2 AND 3: LEE AND MAGDYCH DO NOT RENDER ANY CLAIM OBVIOUS.....	43
A.	There is No Motivation To Combine Lee And Magdych.....	43
B.	Magdych’s Port Does Not Constitute the Claimed “Configuration Data.”	46
C.	Lee Does Not Disclose or Render Obvious Enforcing “At Least One Policy That Defines a Suspicious Category of Network Traffic.”	47
D.	Lee Does Not Disclose or Render Obvious a “Network Gateway Device” or “Data Network Device” That Performs “User Identification.”	48
E.	Lee Does Not Disclose or Render Obvious “Receiv[ing], Via The Network Interface Device, The Additional Content Detection Data Indirectly From The Analysis Process Via an Update Station.”	48
F.	Lee Does Not Disclose or Render Obvious “Stor[ing] The Additional Content Detection Data on The at Least One Memory Device.”	54

IX. GROUND 4: FANG IS NOT PRIOR ART.55

X. CONCLUSION.....56

TABLE OF AUTHORITIES

Page

Cases

<i>ACTV, Inc. v. Walt Disney Co.</i> , 346 F.3d 1082 (Fed. Cir. 2003)	36
<i>Ariad Pharms., Inc. v. Eli Lilly & Co.</i> , 598 F.3d 1336 (Fed. Cir. 2010)	17
<i>Bicon, Inc. v. Straumann Co.</i> , 441 F.3d 945 (Fed. Cir. 2006)	37
<i>Blue Calypso, LLC v. Groupon, Inc.</i> , 815 F.3d 1331 (Fed. Cir. 2016)	17, 25, 26
<i>Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.</i> , 800 F.3d 1375 (Fed. Cir. 2015)	28
<i>In re Giacomini</i> , 612 F.3d 1380 (Fed. Cir. 2010)	28
<i>Hynix Semiconductor Inc. v. Rambus Inc.</i> , 645 F.3d 1336 (Fed. Cir. 2011)	55
<i>Lockwood v. Am. Airlines, Inc.</i> , 107 F.3d 1565 (Fed. Cir. 1997)	55
<i>Ex Parte Robert A. Mann & Eric Colaviti</i> , No. APPEAL 2015-003571, 2016 WL 7487271	28

Statutes

35 U.S.C.A. § 120	55
35 U.S.C. § 968(b)	14

Other Authorities

37 C.F.R. §42.100(b)	14
----------------------------	----

EXHIBIT TABLE

Exhibit #	Description
2001	Declaration of John Black Jr., Ph.D.
2002	Curriculum vitae of John Black Jr., Ph.D.
2003	T. Dean, Guide to Telecommunications Technology (2003)

I. INTRODUCTION

None of the four obviousness Grounds set forth by Petitioner render any claims of U.S. Patent No. 9,231,968 (“the ’968 patent”) obvious. As a threshold matter, Jordan (*i.e.*, primary reference in Ground 1) is not prior art to the ’968 patent because, unlike the ’968 patent, Jordan is not entitled to the filing date of its provisional application. Further, Jordan and Lee (*i.e.*, primary reference in Ground 2-3) disclose fundamentally different systems in which anomalous traffic is analyzed internally within a network, and the result of that analysis is used ***in that same network*** to detect a threat in subsequent traffic. As such, neither reference discloses any concept analogous to an “update station,” much less receiving content detection data “via the network interface device” and “indirectly from the analysis process via the update station.”

Petitioner appears to recognize Jordan’s shortcoming in this respect and argues, for Ground 1, that a POSITA would have found it obvious to incorporate FortiGate’s supposed update station into Jordan. Pet., 57. But Petitioner does not explain why a POSITA would have combined Jordan with FortiGate or had reasonable expectation of success in doing so. Petitioner appears to assume that Jordan’s analytical engine (the alleged “analysis process,” from which content detection data is allegedly received “via an update station”) can simply be placed outside of the network. But communicating with an *external* analytical engine, as

Petitioner proposes, would necessitate another level of protection for the communication with the analytical engine itself. It would also take a substantial toll on the network bandwidth, undermining the “significant advantages” pursued by Jordan of quickly detecting and reacting to recently received communications. *Id.* at 9:40-50. Petitioner’s reliance on FortiGate is also misplaced because FortiGate does not disclose a FortiGate firewall forwarding suspicious traffic to the FDC (the alleged “analysis process”).

With respect to Lee (Grounds 2 and 3), Petitioner does not even acknowledge that the alleged “analysis process” is in the same network as the firewall and therefore that an “update station” is not used or even needed in Lee’s system. Instead, Petitioner only addresses another critical deficiency with Lee, namely that there is no single device (“network security device” or “data network device”) that performs the recited functions of the Challenged Claims. Attempting to overcome that deficiency, Petitioner argues that a POSITA would have been motivated to integrate the different functions disclosed in Lee into a single device. But this argument is directly contrary to Lee’s stated objective—*i.e.*, providing a “**distributed** security environment based on a number of **independent** security agents”—and the benefits Lee seeks to achieve with such a distributed environment (*e.g.*, “less cumbersome” implementation, “less overall code space,” ease of modification, etc.). Lee, ¶¶12, 40.

Lastly, Petitioner’s argument (Ground 4) that Fang renders the Challenged Claims obvious is premised on the false assumption that the Challenged Claims lack written description support in the specification of the ‘968 patent.

Accordingly, Patent Owner respectfully requests the Board deny institution of *inter partes* review.

II. OVERVIEW OF THE ‘968 PATENT

The ‘968 patent, titled “Systems and Methods For Updating Content Detection Devices and Systems,” is directed to an improved technique for managing and utilizing content detection data to detect threats in network traffic. “The generation and spreading of computer viruses are major problems in computer systems and computer networks.” *Id.* at 1:27-28. “With new attacks reported almost weekly, organizations are constantly exposed to virus attacks, and spend significant resources ensuring that all hosts are constantly updated with new antivirus information.” *Id.* at 1:42-46. The ‘968 patent describes that existing software did not address the challenges of detecting constantly-evolving viruses. *Id.* at 1:46-56.

The ‘968 patent addresses these challenges by providing an innovative architecture in which content detection data—*e.g.*, virus signatures, virus definitions, etc. (*id.* at 6:33-38)—is generated in an “analysis process” and then received via an “update station” to process subsequently received network traffic. Fig. 1 illustrates

an embodiment of a content detection system, in which update stations 106¹ distribute, via the Internet, content detection data to content detection modules 108:

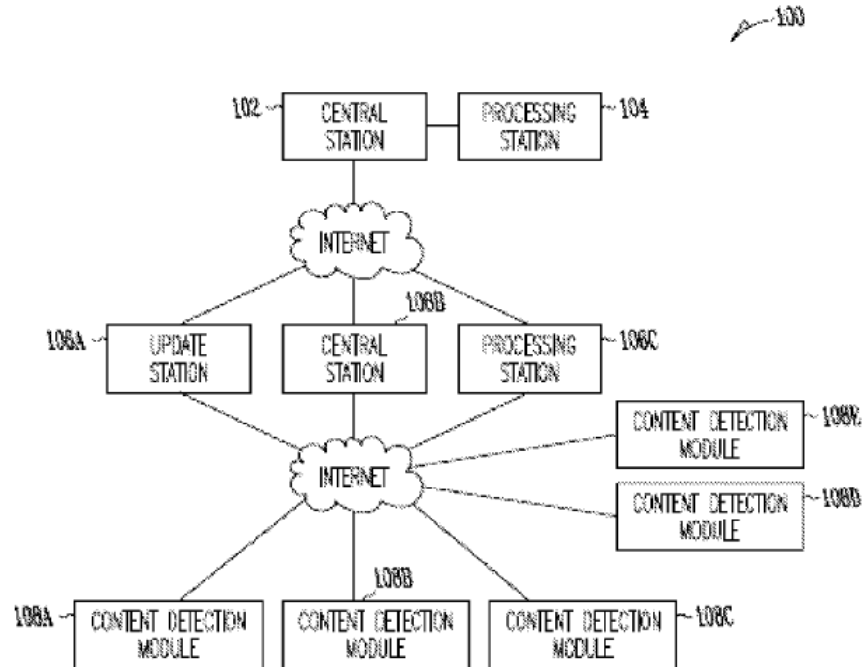


Fig. 1

Id., Fig. 1.

The ‘968 patent describes that “[u]pdate stations 106 receive the content detection data from central station 102, and send the content detection data to content detection modules 108 (e.g., through the Internet).” *Id.* at 4:53-55. “Each of the update stations 106 is located at a geographical location that is different from

¹ Elements 106B-C should read “update station.” Petitioner erroneously states that elements 108B-C should read an “update station.” Pet., 11 n.1.

others,” such as at a different building, city, or country. *Id.* at 4:56-60. The update stations can be configured to serve (e.g., send content detection data to and/or from) different content detection modules. *Id.* at 6:50-62. The configuration can be “pre-assigned” (*id.* at 7:27-33) or determined “based on a condition during use, e.g., based on load demands and/or capacities of update stations.” *Id.* at 7:34-39. For example, “if update station 106a has high load demand” and/or “if its remaining capacity to handle additional traffic is low,” update stations 106b and 106c can be used to transmit content detection data to content detection modules 108a-108e. *Id.* at 7:47-53. Further, when content detection modules of an organization are inside the Intranet and do not have access to the Internet, a customized update station can be provided outside the Intranet of the organization, and the customer can “configure an update station to serve its own content detection module(s).” *Id.* at 9:42-52.

“[E]ach 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 stations 106.” *Id.* at 5:14-18. “For example, content detection module 108 can be configured to detect virus based on a virus signature received from update station 106.” *Id.* at 5:18-20. When suspicious content is detected, it “sends the electronic content to processing station 104 for processing.” *Id.* at 6:3-7. Processing station 104 “analyzes such information to determine whether the content contains/is a

threat” and, if so, “generates content detection data,” such as “a virus signature, a virus definition, a spammer identification, a URL, a NIDS signature.” *Id.* at 6:12-19, 6:33-38. The generated content detection data is transmitted, through the Internet, to update stations, which as discussed above distribute the content detection data to the respective content detection modules they serve. *Id.* at 4:35-37, 6:42-62, *see also id.* at 6:63-8:58. “Content detection modules 108 can then utilize the content detection data to detect content.” *Id.* at 8:59-9:5.

This novel architecture achieves numerous improvements over prior art approaches. *First*, it simplifies the security update process and reduces the reliance on users’ diligence in keeping the security software on their computers up-to-date. *Id.* at 9:16-19 (“[T]he responsibility to keep up with the latest security update (e.g., content detection data) is shifted from users of content detection modules to processing station 104 and/or central station 102.”). *Second*, the claimed invention achieves “faster response time during an outbreak and less resource consumption” because, for example, an “update station” can “‘push’ the latest security update within minutes (or even seconds)” after the update is made available. *Id.* at 9:19-27. *Third*, an “update station” from which the “additional content detection data” is received can be added or removed “at run-time without causing service interruption.” *Id.* at 9:28-37. The configurability and scalability of these update stations lead to increased reliability of the security update. *Id.* at 9:37-41.

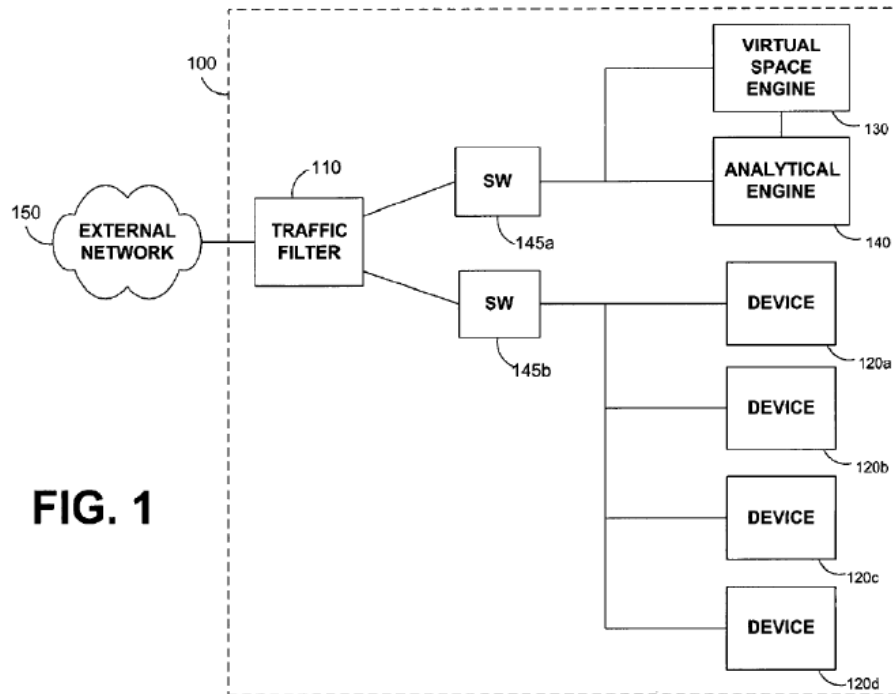
III. OVERVIEW OF THE CITED ART

The petition challenges claims 1 through 9 (the “Challenged Claims”) on four grounds. Ground 1 asserts that the combination of Jordan and FortiGate renders the Challenged Claims obvious. Ground 2 asserts that the combination of Lee and Magdych renders the Challenged Claims obvious. Ground 3 asserts that the combination of Lee, Magdych, and Judge renders the Challenged Claims obvious. Ground 4 asserts that the combination of Fang—which is in the same family and shares the same specification as the ‘968 patent—and FortiGate renders the Challenged Claims obvious. Below are short summaries of these six references.

A. Jordan (Ex-1005)

Jordan discloses defending a computer network using a traffic filter. Jordan at Abstract; Black Decl., ¶38. A traffic filter can be used as a “perimeter device to control all communications crossing a network boundary.” Jordan at 5:28-30. *Id.* A traffic filter detects “any anomalies within received communications” and determines “how to handle those anomalies.” *Id.* at 5:36-39. Anomalous communications are routed to a virtual space engine, which approximates the request (e.g., to entice deployment of a malicious payload). *Id.* at Abstract, 16:7-21. Anomalous communications are also routed, from a traffic filter or from a virtual space engine, to an analytical engine, which “analyze[s] the received communication” and, based on the analysis, “can generate or update rules.” *Id.* at

16:21-23, 6:40-44, 9:33-38. The rules are then employed by the traffic filter against future received communications. *Id.* at 9:38-45, 16:25-29. A traffic filter, virtual space engine, and an analytical engine, which are ***all part of the network system 100***, are depicted in Fig. 1 below.



Jordan, Fig. 1, 9:33-50. Jordan discloses that the traffic filter and other components of the network system 100 can be “integrated into a single device instead of being distributed within the network system.” *Id.* at 10:45-56.

Jordan states that “the dynamic determination of filtering rules by the analytical engine [] exhibits some significant advantages over standard, slower adapting, rules-based systems, as the analytical engine [] is able to adapt based on the most recently received communications.” *Id.* at 9:45-50.

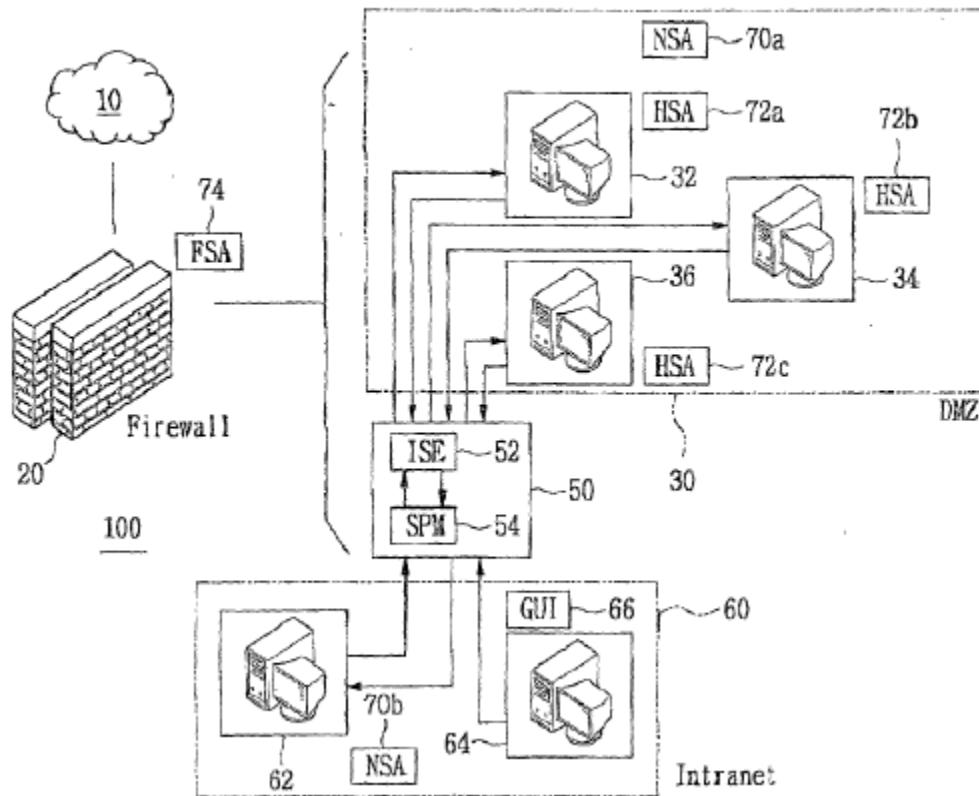
B. FortiGate (Ex-1008)

FortiGate is a user manual version 2.5 for the FortiGate-3600. Black Decl., ¶40. FortiGate discloses a FortiGate Network Intrusion Detection System (NIDS) for preventing suspicious network activity. FortiGate at 16. To identify attacks, a FortiGate unit uses antivirus and attack signatures received from the FortiResponse Distribution Network (FDN). *Id.* at 115. The updates can be pushed or released in scheduled updates (e.g., hourly, daily, or weekly). *Id.* at 115, 118-121. The FDN is a world-wide network of FortiResponse Distribution Servers (FDSs). When the FortiGate unit connects to the FDN, it connects to the nearest FDN. *Id.*

C. Lee (Ex-1009)

Lee discloses a security system with individual security agents. Lee, ¶2; Black Decl., ¶41. One “object” of Lee’s invention is “to implement a distributed security environment based on a number of independent security agents without degrading network performance.” Lee, ¶¶12, 14. Independent security agents include a network security agent (NSA) for analyzing suspicious traffic and providing a network security function, a host security agent (HSA) for reacting to threats associated with resources of a server within the network, and a firewall security agent (FSA) for adopting a security policy and causing the firewall to block a traffic from an attacker. *Id.*, ¶14. The security system also includes an intelligent security engine (ISE) for analyzing traffic information transferred from the

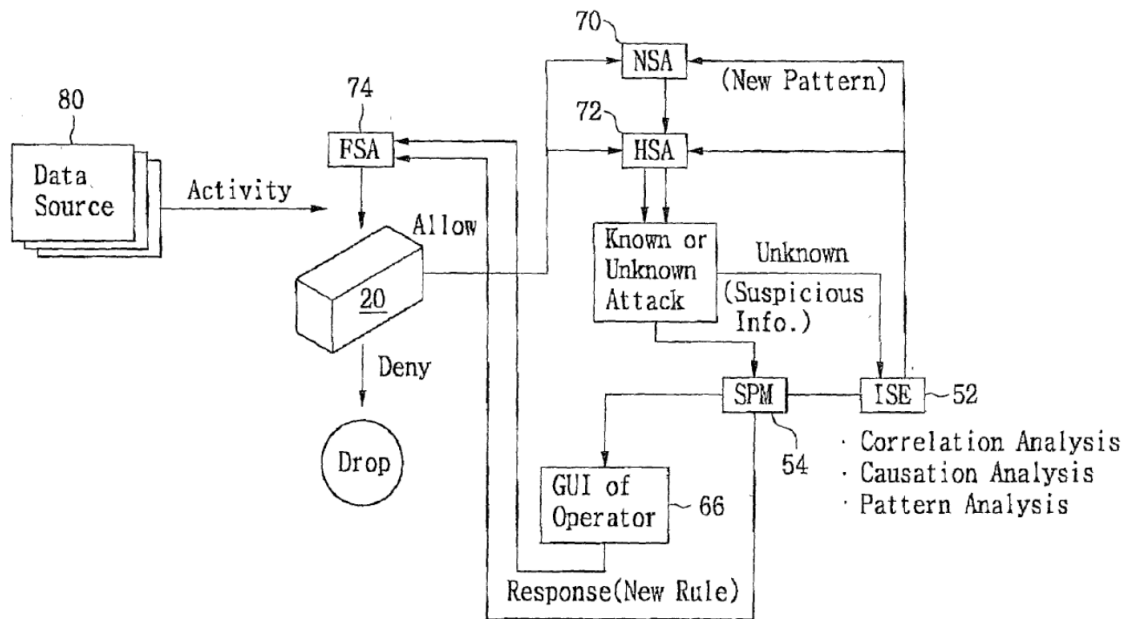
FIG 1



NSA analyzes traffic and, when suspicious traffic is detected, generates a report to ISE and a security policy manager (SPM). *Id.*, ¶51. ISE analyzes the suspicious traffic and, if the traffic is detected as an attack and the attack is an

unknown pattern, generates a new signature. *Id.*, ¶52. The generated signatures is transferred to the NSA and HSA so that future attacks of the same pattern are recognized. *Id.* When the new pattern of attacked is recognized, a new or modified rule is given to FSA through SPM so that traffic from the attacker can be blocked. *Id.* Fig. 2 below illustrates the operational flow. Importantly, because ISE, FSA, and NSA are all inside of a network secured by the firewall 20, the transfer of information among these security agents does not cross a network boundary.

FIG 2



Id., Fig. 2; Black Decl., ¶42.

Maintaining independence between the different security agents is key to Lee's disclosures. Black Decl., ¶43. According to Lee, "[b]ecause agents are independent of one another, the implementation is less cumbersome and preferably

requires less overall code space. Lee, ¶40. Furthermore, independence allows “different agents” to be “easily added, removed, or modified as necessary to fulfill the requirements of network security.” *Id.*

D. Magdych (Ex-1010)

Magdych discloses that firewalls “typically restrict access based only on address/port/protocol information” and “do not typically examine content of communications for security purposes.” Magdych at 2:28-29. “A port is a numerically designated element contained in the overhead of a packet,” “indicat[ing] the nature of a service associated with a packet.” *Id.* at 2:15-17, 4:29-31 (“[P]acket filtering involves the investigation of port or protocol information contained in a data packet”). As shown in Fig. 4 below, Magdych discloses incorporating an intrusion detection system 404 into the firewall device 210 and states that such incorporation allows the intrusion detection system to “analyz[e] all incoming data and identif[y] threats before hostile data reaches a switched or segmented network, i.e. VLAN.” *Id.* at 6:46-55.

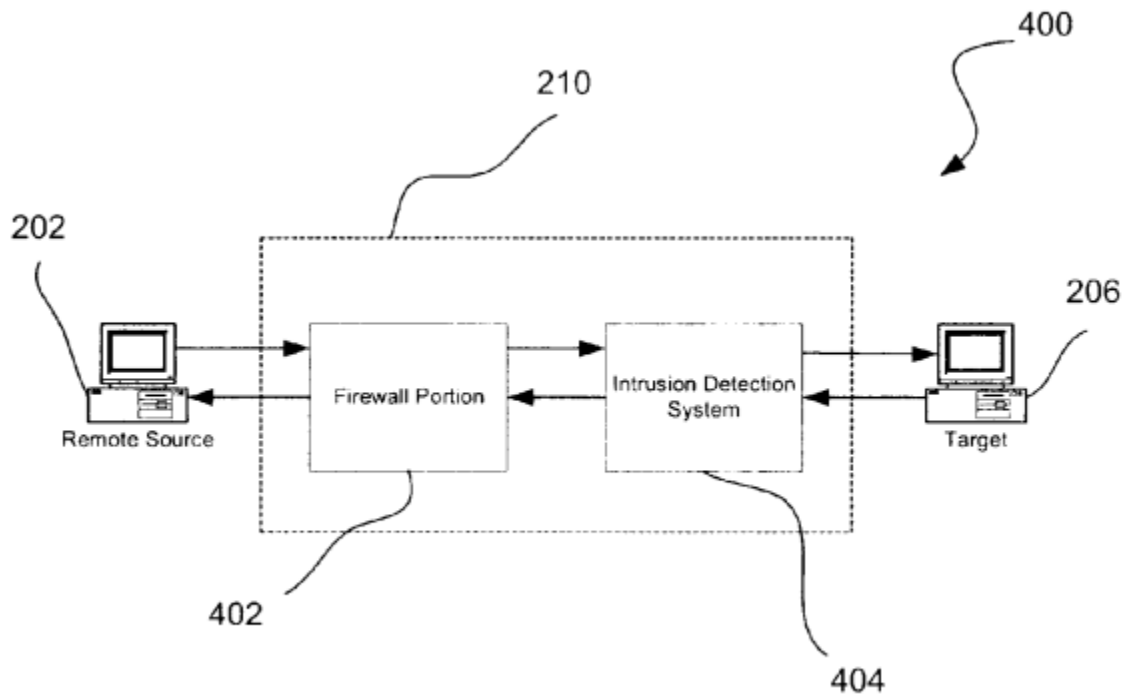


Figure 4

Id., Fig. 4.

E. Judge (Ex-1011)

Judge describes systems and methods for messaging threat protection. Judge, ¶40. When a communication is received, “[a] threat profile associated with the received communication is generated.” *Id.*, ¶44. “The threat profile is compared with configuration information.” *Id.* “Typically, configuration information can include threat types of interest and weights associated therewith.” *Id.*

F. Fang (Ex-1012)

Fang is in the same family as the ‘968 patent. The ‘968 patent issued as continuation of U.S. Pat. App. No. 13/795,407, which in turn is continuation of Fang.

As such, Fang and the '968 patent share the same specification and same named inventors.

IV. LEVEL OF ORDINARY SKILL IN THE ART

A person of ordinary skill in the art (“POSITA”) relevant to the '968 patent at the time of the invention 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. Black Decl., ¶18.

Patent Owner's description of the level of ordinary skill in the art is essentially the same as that of the Petitioner, except that Petitioner's description requires two years of work or research experience for someone with a Bachelor of Science degree (as compared to three years). *See* Pet., 20. The positions set forth in this preliminary response would be the same under either parties' proposal.

V. CLAIM CONSTRUCTION

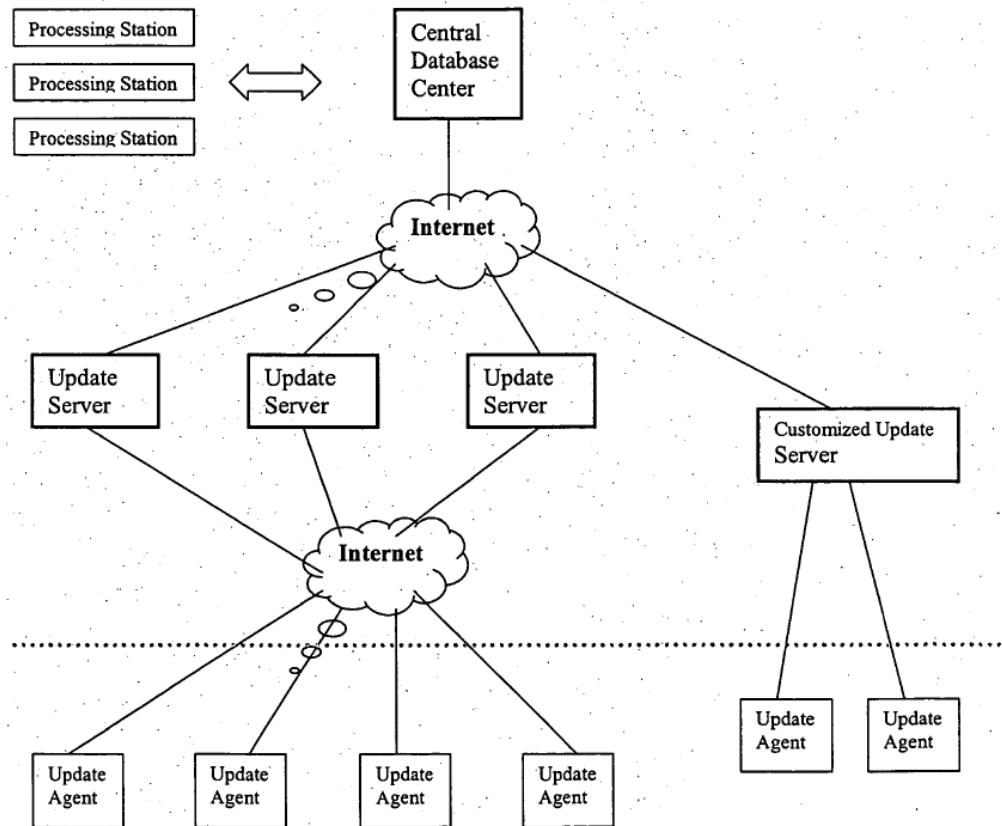
Claim terms in an IPR are “construed using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. §968(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by” a POSITA and in view of the prosecution history. 37 C.F.R. §42.100(b).

Patent Owner submits that no claim terms presently require construction to resolve any current dispute between the parties. Patent Owner reserves the right to proffer a construction for a claim term at a later point if it becomes pertinent to any particular dispute.

VI. PRIORITY DATE

A. The Challenged Claims of the ‘968 Patent Are Entitled To The Priority Date of the ‘457 Provisional Application.

The challenged claims of the ‘968 patent are entitled to the March 12, 2004 filing date of U.S. Provisional App. No. 60/552,457 (the “‘457 provisional”) (Ex. 1006). The ‘457 provisional discloses a network security system having substantially the same architecture as shown in Figure 1 of the ‘968 patent:



‘457 Provisional, §2. The security system includes an Update Agent, of which “main role is to inspect the traffic passing through it to ensure they are safe based on the latest update it gets from an Update Server.” *Id.* Update Servers are “geographically located around the world and responsible for delivering update data to update agents.” *Id.* An Update Server collects information from Update Agents and forwards it to the Central Database Centre. *Id.* The Central Database Centre maintains update data (e.g., virus signature) processed from the processing stations and distributes it to geographically located update servers. *Id.*

Petitioner argues that the ‘457 provisional does not provide written description support for four limitations, namely (1) “configuration data,” (2) “user

identification,” (3) “forwarding the network traffic to an analysis process,” and (4) “policy enforcement including user identification, content identification, and at least one of source verification and destination verification.” “[T]he test for sufficiency is whether the disclosure of the application relied upon reasonably conveys to those skilled in the art that the inventor had possession of the claimed subject matter as of the filing date.” *Ariad Pharms., Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010). “[T]he test requires an objective inquiry into the four corners of the specification from the perspective of a person of ordinary skill in the art.” *Id.* The description requirement does not demand any particular form of disclosure. *Ariad Pharms., Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1352 (Fed. Cir. 2010). For example, “the exact terms appearing in the claim need not be used *in haec verba*.” *Blue Calypso, LLC v. Groupon, Inc.*, 815 F.3d 1331, 1345 (Fed. Cir. 2016) (internal citation and quotation marks omitted).

As discussed below, the ‘457 provisional provides sufficient written description for each of these limitations.

1. “configuration data”

Petitioner does not explain why the ‘457 provisional allegedly lacks written description support for “configuration data.” Pet., 64-65. Contrary to Petitioner’s conclusory assertion, the ‘457 provisional describes at least two ways by which “configuration data” is used for the claimed network security system. The ‘457

provisional discloses that because some organizations restrict access to the Internet, Update Agents (which correspond to the claimed “content detection modules”) inside the Intranet of such organizations cannot access the Update Servers, which are available in the Internet. ‘457 Provisional, §3.3. In such an environment, a customer can “**configure** its own Customized Update Server to serve different Update Agents.” *Id.* The ‘457 provisional also discloses that, depending on “the health and load of each Update Server,” “an Update Server can be **added, removed**” at run-time to serve a certain geographical area. *Id.*, §3.4. In both disclosures, the information that customizes, adds, or removes an Update Server constitutes the claimed “configuration data.” Black Decl., ¶49. A policy is “defined at least in part by” such configuration data because the set of policies enforced by an Update Agent is determined “based on the latest update it gets from an Update Server.” *Id.*; see also Section VI.B.1, *infra*. And the configuration information would be stored in each Update Agent’s memory so the Update Agents can determine from which Update Servers to receive such updates. Black Decl., ¶49. Further, as Petitioner admits, “configuration data used in detection systems” was within “the knowledge of a POSITA.” Pet., 94. Based on the disclosures in the ‘457 provisional and knowledge in the field, a POSITA would have understood that the inventors possessed the idea of using “configuration data” as claimed.

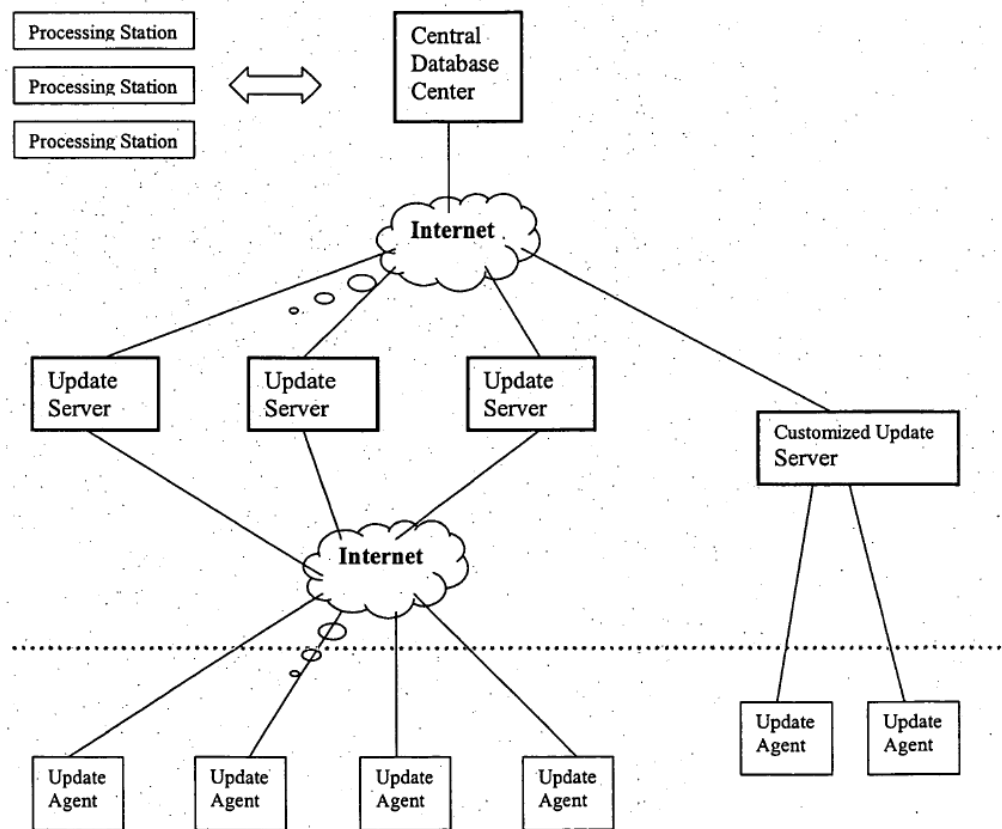
2. “user identification”

With respect to “user identification,” Petitioner’s argument is solely based on the fact that the terms “user,” “identification,” and “user identification” do not appear in the ‘457 provisional. Petitioner, however, ignores that update data, in view of which received traffic is processed, includes “spammer list.” ‘457 Provisional, § 2. To process received traffic in view of a spammer list, Update Agents must identify the user from whom the traffic originates. Black Decl., ¶50. For example, Update Agents would need to identify the user associated with the received traffic and compare the user to the spammer list. *Id.* The ‘457 provisional thus provides support for performing “user identification” to enforce policies.

Support for the “user identification” element is also found in the disclosure that “subscriber data” is part of the update data. ‘457 Provisional, § 3.1 (“There are two kinds of update data: security update data and subscriber data.”). A POSITA would have understood that the content detection module maintains subscriber data in part to confirm that received traffic is associated with a known subscriber and to control its access accordingly. Black Decl., ¶51. This is also supported by the disclosure that subscriber information is maintained in the Central Database Center: one of the primary reasons for maintaining subscriber information would be to match the user associated with the received traffic with the subscriber information. *Id.*

3. “forwarding the network traffic to an analysis process”

Petitioner contends that the ‘457 provisional does not disclose a network gate device (or data network device) “forwarding the network traffic to an analysis process.” Pet., 65. Petitioner claims that “[t]here is no communication between the processing stations and the update agents.” *Id.* This is not correct. As discussed above, the ‘457 provisional provides substantially the same figure as Figure 1 of the ‘968 patent, illustrating communications among different components, including the Processing Stations and Update Agents:



‘457 Provisional, §2. Contrary to Petitioner’s contention, Processing Station and Update Agent communicate with each other to allow analysis of suspicious traffic

and distribution of update data. The ‘457 provisional describes that “[a]n Update Server must handle requests from Update Agents and also collect Update Agents’ information and forward them to the Central Database Centre.” *Id.* A POSITA would understand that, as part of the “requests” sent to the Update Servers, Update Agents forward suspicious traffic so that additional update data (the claimed “additional content detection data”) can be generated. Black Decl., ¶52. Suspicious traffic can be forwarded to and analyzed by the Central Database Center and Processing Station, and newly generated virus signature is then distributed to Update Agents. *Id.*

This interpretation is further supported by the ‘457 provisional’s discussion of load balance and scalability. See ‘457 Provisional, §3.5. The ‘457 provisional discloses that an Update Server can be dynamically deployed (“added” or “removed” “at run-time”) to serve Update Agents in different geographical areas. *Id.* For example, “[i]f the whole system or the Update Servers for a certain geographical areas cannot keep up with the ever-increasing load, more Update Servers can be deployed.” *Id.* A POSITA would understand that the “load” on an Update Station primarily includes analyzing the traffic ***forwarded to it*** from the Update Agents. Black Decl. ¶53. If an Update Server receives, from the Update Agents, more traffic than what it can analyze, more Update Server will be deployed to distribute the load. *Id.*

Accordingly, the ‘457 provisional provides written description support for a “network gateway device” (claim 1) or “data network device” (claims 4 and 7) “forwarding the network traffic to an analysis process.”

4. “policy enforcement including user identification, content identification, and at least one of source verification and destination verification”

The ‘457 provisional sufficiently describes “policy enforcement including user identification, content identification, and at least one of source verification and destination verification.” First, the ‘457 provisional provides support for “user identification” for the reasons discussed above. See Section VI.A.2, *supra*.

Second, as Petitioner acknowledges, the ‘457 provisional discloses that an Update Agent inspects traffic to protect its network from “unsafe content” by using security update data such as a “virus definition” or “network intrusion detection definition” (NIDS). ‘457 Provisional, §§2, 3.1. This disclosure reflects the inventors’ possession of “content identification” because, to process traffic in view of a virus definition or NIDS, an Update Agent must identify the content of the traffic. Black Decl., ¶56.

Third, support for “at least one of source verification and destination verification” can similarly be found from the disclosures that the update data in view of which network traffic is inspected includes “spammer list,” NIDS, and “web filtering URL database.” ‘457 Provisional, §§ 1-2. For example, a POSITA would

have understood that, to inspect network traffic in view of “network intrusion detection definition” (*id.*, §2), an Update Agent verifies the source of the traffic or its intended destination. Web filtering also requires examining the URL destination and comparing it to “web filtering URL destination.” *Id.*; Black Decl., ¶57.

B. The ‘968 Patent Provides Written Description Support.

Petitioner asserts that the Challenged Claims are entitled to a priority date of no earlier than November 5, 2013, the date the ‘968 patent was filed. Pet., 14. Petitioner argues that the claims do not have written description support even in its immediate parent application because the specification allegedly does not disclose “configuration data” and “user identification.” Contrary to Petitioner’s arguments, the specification of the ‘968 patent provides sufficient support for these limitations.

1. “configuration data”

According to Petitioner, there is no written description support because the word “configuration” allegedly appears only in a different context. Pet., 15. But in blindly searching for the word “configuration,” Petitioner ignores the relevant disclosures. The specification of the ‘968 patent (and by extension the specification of all applications in the priority chain) describes at least three different embodiments of “configuration data.”

First, as discussed in connection with the ‘457 provisional above, the specification of the ‘968 patent discloses that configuration data can be used to

customize an update station from which contention detection module receives content detection data. See '968 patent at 9:42-43 (“[A]n update station can be customized to serve the need of certain organizations.”); Black Decl. ¶60. For example, when content detection modules are inside the Intranet of an organization and do not have access to the Internet, the customer can “**configure** an update station to serve its own content detection module(s).” *Id.* at 9:43-52. Because different content detection data may be received from different update stations, a policy is “defined” in part by the configuration data. Black Decl., ¶60. And the configuration information would be stored in the memory of each content detection module such that it can determine from which update station(s) to receive such updates. *Id.*

Second, the specification discloses that update stations can be “configured” to “serve one or more content detection module.” ‘968 patent at 7:27-8:58. Update stations can be “pre-assigned” or determined “during use, e.g., based on load demands and/or capacities of update stations.” *Id.* In either case, data that determines which update stations serve which content detection modules is “configuration data,” based on which policy is defined and stored in the memory of the content detection modules. Black Decl., ¶61.

Third, the specification discloses that configuration data determines which content detection data is used to process received network traffic. There are different types of content detection data, such as virus signature, a spammer identification, a

URL, and the like. *Id.* at 4:24-25, 6:33-37. A content detection module can be configured to employ different content detection data depending on the configuration data. For example, it can be “configured to detect virus based on a virus signature received from update station.” *Id.* at 5:18-20; 8:62-65. In other cases, a content detection module may utilize “the spammer identification to detect and screen undesirable spam.” *Id.* at 8:65-8:2.

Accordingly, the specification provides sufficiently describes “configuration data.”

2. “user identification”

Petitioner is incorrect that the specification lacks written description support for the “user identification” term. The specification describes “user identification” in at least three ways.

First, as Petitioner acknowledges, the specification states that “the term ‘policy enforcement’ refers to a process or procedure” that includes “one or a combination of: source verification, destination verification, **user authentication**, virus scanning, content scanning ..., and intrusion detection” ‘968 patent at 5:23-31. Addressing this disclosure, Petitioner places undue weight on the fact that the word “authentication,” rather than “identification,” is used. It is black letter law that “the exact terms appearing in the claim need not be used *in haec verba*.” *Blue Calypso*, 815 F.3d at 1345. User identification and authentication are closely related

concepts that both involve receiving information about a user's identity and using that information to control a user's access to a resource. Black Decl. ¶65. Moreover, the specification describes "user authentication" in the same exact context as recited in the claims: "user authentication" is provided as one example, along with other processes such as source and destination verification, of "policy enforcement." '968 patent at 5:23-31. As such, although not the exact term is used, a POSITA would understand that the inventors possessed the idea of using "user identification" for policy enforcement. Black Decl., ¶65. As the Federal Circuit put it, "this is simply a case where the patentee used different words to express similar concepts." *Blue Calypso*, 815 F.3d at 1347.

Even assuming, as Petitioner contends, that user authentication is a "more complicated" process that takes a further step to determine if a user is who they claim to be (Pet., 17-18), user authentication would ***necessarily entail*** user identification because, to authenticate a user, one must first identify the user. Black Decl., ¶66. The disclosure of "user authentication" thus demonstrates that the inventors possessed *at least* "user identification." *Id.*

Second, support for "user identification" is found in the disclosure that the content detection module has "subscriber data" (*e.g.*, user identification). '968 patent at 4:60-5:4 ("[T]he update stations 106 also receives subscriber data, ***such as a user identification*** of a content detection module" "from content detection

module(s) and forward the subscriber data to central station 102 for processing.”), 4:38-42. Petitioner dismisses these disclosures, stating that user identification is not provided “to a content detection module/network gateway device” or “used in policy enforcement.” Pet., 17. But the claims do not require providing user identification to a network gateway device. Instead, the claims simply require policy enforcement performed by a network gateway device to include “user identification.” The specification discloses propagating subscriber data in a similar manner as suspicious network traffic, *i.e.*, from content detection module to the update stations and then to the central station for processing. ‘968 patent at 4:60-65. This disclosure supports that subscriber data (e.g., user identification) is used in policy enforcement, namely to determine whether received network traffic is associated with a known subscriber. Black Decl., ¶67.

Third, the disclosure of “spammer identification” provides support for user identification. See Section VI.A.4, *supra*. Similar to the ‘457 provisional, the specification of the ‘968 patent describes that content detection data, in view of which received traffic is processed, may include “spammer identification.” ‘968 patent at 6:33-38; *id.* at 2:5-6 (a spammer list is used to “eliminate unwanted email messages.”). To process received traffic in view of spammer identification, content detection modules must determine whether received traffic originates from a user that has been identified as a spammer. Black Decl., ¶68.

Accordingly, Petitioner has failed to establish that the specification of the ‘968 patent (and by extension the patents from which the ‘968 patent issued as continuation and share the same specification) lacks written description support.

VII. GROUND 1: JORDAN AND FORTIGATE DO NOT RENDER ANY CLAIM OBVIOUS.

A. Jordan Does Not Qualify as Prior Art.

As discussed in Section VI, *supra*, the challenged claims of the ‘968 patent are entitled to a priority date of March 12, 2004, *i.e.*, the filing date of the ‘457 provisional. Because Jordan was filed at a later date (November 30, 2004), for Jordan to qualify as prior art, Petitioner must establish that Jordan is entitled to the filing date (November 17, 2003) of U.S. Provisional Application No. 60/520,577 (the “Jordan provisional”) (Ex. 1007). Petitioner has failed to do so.

There are two separate requirements that Petitioner must meet to establish that Jordan is entitled to its provisional filing date. First, the provisional application must “provide[] support for the claims in the reference patent in compliance with § 112, ¶ 1.” *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1381 (Fed. Cir. 2015). Second, “the provisional application must provide written description support for the claimed invention.” *In re Giacomini*, 612 F.3d 1380, 1383 (Fed. Cir. 2010); *see also Ex Parte Robert A. Mann & Eric Colaviti*, No. APPEAL 2015-003571, 2016 WL 7487271, at *5 (P.T.A.B. Dec. 21, 2016) (“the provisional

application must *also* provide support for the subject matter relied upon in the rejection”) (emphasis in original). Petitioner failed to make either showing.

1. *Jordan Provisional Does Not Provide Support For Claim 1.*

Jordan Provisional does not provide support for Jordan’s claim 1, the only claim for which Petitioner attempts to identify support in Jordan Provisional. In particular, Jordan does not support the last limitation of Jordan’s claim 1, which recites a “first device” “performing a pattern recognition” and “generat[ing] new rules for pattern recognition activities.” Jordan, cl. 1.

Petitioner provides a cursory chart that purports to identify support for each limitation of Jordan’s claim 1 and cites paragraphs 16, 20, 32, 60, 61, and 64 of Jordan Provisional as supporting the “pattern recognition” limitation. Pet., 68. None of these paragraphs, however, mention the word “pattern” or any concept akin to “pattern matching.” Even if the analytical engine’s analysis of incoming packets (see Jordan Provisional, ¶64) was considered to support “pattern matching,” such an analysis is performed by the analytical engine, which cannot be the “first device” of Jordan’s claim 1. This is because Jordan’s claim 1 also requires the “first device” to “mangle” a communication received from within a network, but the only component that performs such a function in Jordan Provisional is the traffic filter, not the analytical engine. Jordan Provisional, ¶45 (“The difference between the initial handshake parameters can be mangled by the Traffic Filter ...”).

Accordingly, Petitioner has failed to show that Jordan Provisional provides sufficient support for Jordan's claim 1.

2. *Jordan Provisional Does Not Provide Support For The Subject Matter Relied Upon.*

Petitioner makes no attempt to establish that Jordan provisional provides written description support for the subject matter relied upon. For example, although Petitioner points to Jordan's switches as being the claimed update stations via which the traffic filter receives new rules from the analytical engine (Pet., 57), Petitioner does not identify any written description support for such switches in Jordan provisional. In fact, Jordan provisional is silent on the mechanism (switches or otherwise) by which filtering rules are transferred from an analytical engine to a traffic filter. Black Decl., ¶74. As another example, Jordan provisional does not include the disclosure (Jordan at 17:5-14) that Petitioner relies on for the "user identification" limitation. Nor does Jordan provisional disclose a "communication module" or "pattern matching" performed by a traffic filter. See Pet., 30, 32-33, 49. As such, even if Jordan's claim 1 is found to be supported by Jordan provisional, Jordan would still not be entitled to the filing date of Jordan provisional.

In sum, because Jordan is entitled only to its filing date (November 17, 2004), which post-dates the priority date (Mar 12, 2004) of the '968 patent, Jordan is not prior art.

B. Even If Jordan is Deemed To Qualify as Prior Art, Jordan in View of FortiGate Does Not Render Any Claims Obvious.

Even if Jordan is deemed to qualify as prior art—and to be clear, Jordan is not prior art, as explained above in Section VII.A—Jordan in view of FortiGate still does not render any claims of the ‘968 patent obvious.

1. *Jordan Does Not Disclose or Render Obvious “Receiv[ing], Via The Network Interface Device, The Additional Content Detection Data Indirectly From the Analysis Process Via an Update Station.”*

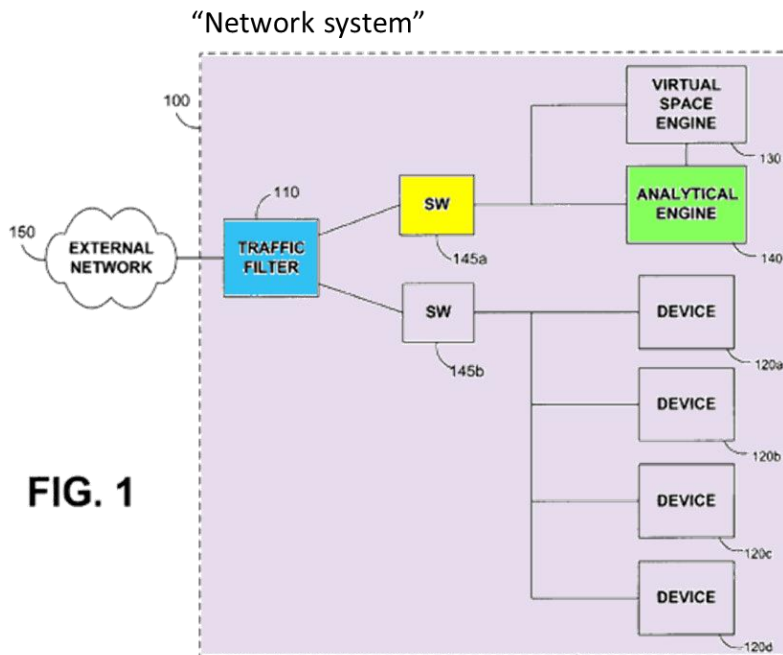
Jordan does not disclose or render obvious a “network gateway device” (claim 1) / “data network device” (claims 4 and 7) “receiv[ing], via the network interface device, the additional content detection indirectly from the analysis process via an update station.” Jordan discloses a fundamentally different 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. See ‘968 patent at 6:50-55, 6:63-8:58. Such a consideration, however, is wholly missing in Jordan. Black Decl., ¶77.

Given the foundational difference, Jordan does not disclose or render obvious the limitations discussed below.

(a) Network Interface Device

All Challenged Claims require a “network gateway device” (claim 1) / “data network device” (claims 4 and 7) receiving, via a “network interface device,” “additional content detection data indirectly from the analysis process via an update station.” Petitioner reads the “network gateway device” on Jordan’s traffic filter and “update station” on Jordan’s switch. Pet., 57-58. But critically, Petitioner does not identify a “network interface device” via which the “additional content detection data” is received. On this basis alone, Ground 1 should be rejected.

Indeed, Jordan does not disclose the claimed “network interface device.” Under Petitioner’s interpretation, the traffic filter (the alleged network gateway device) must receive “additional content detection data” from the switch (the alleged update station) via a “network interface device.” Jordan’s system, however, does not include such a device because, as illustrated in Jordan’s Fig. 1 below, the switch (yellow) and the traffic filter (blue) are both part of the **same network** (network system 100, shaded in purple), and thus the communications between the two do not occur through a “network interface device:”



Jordan, Fig. 1 (annotated).

This makes sense because, in Jordan, the analytical engine (green) is also part of the same network as the switch and the traffic filter. See Jordan at 9:34-35 (“the traffic filter ... can communicate with an analysis engine 140, which is also **part of the network system 100.**”); Fig. 1. In the context of the invention of the ‘968 patent, a POSITA would have understood a “network interface device” to refer to a device that connects one network to another network. Black Decl., ¶180; Ex. 2003 (T. Dean, Guide to Telecommunications Technology) at 147-45 (a “network interface device” is “[t]he physical equivalent of the demarcation point,” *i.e.*, “location where one entity’s telephone or network facilities connect to another entity’s telephone or network facilities”). The claims of the ‘968 patent use term “network interface device” consistent with that understanding, reciting that “network traffic” is received

from an external network via the same “network interface device.” See claim limitation 1[e][i]/4[a]/7[a]. As such, a POSITA would have understood that the internal transfer of data between the switch and the traffic filter is not “via” a network interface device. Black Decl., ¶80.

Elsewhere in the petition (for a *different* limitation), Petitioner points to a “communication module,” shown in Fig. 11 below, as being a “network interface device.” Pet., 30-31.

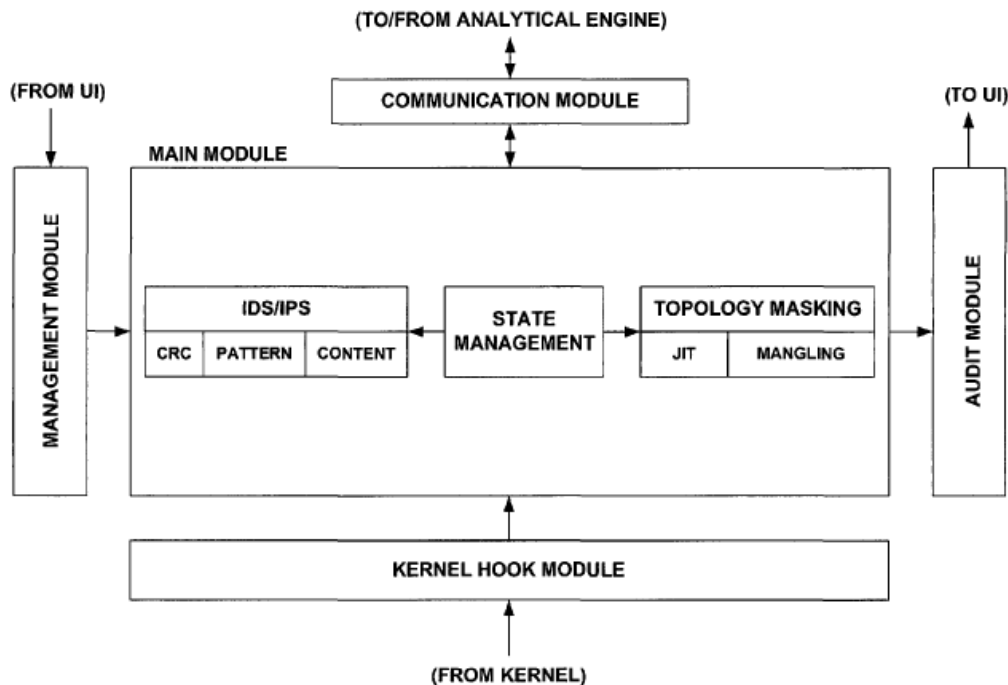


FIG. 11

Jordan, Fig. 11.

Although Petitioner does not allege that the communication module is the “network interface device” via which the traffic filter receives the “additional

content detection data” from the switch, such an allegation would be unavailing. Jordan represents the communication module as being one of the “code blocks” of a traffic filter (Jordan at 4:60-61), and the only examples of the communication module disclosed in Jordan are “application program interfaces (APIs).” Jordan at 25:45-49. In view of these disclosures, a POSITA would have understood the communication module to be a software module, not a “device.” Black Decl., ¶82.

Further, while Jordan describes that the communication module is provided for communications to and from the analytical engine (Jordan at 25:40-45), Jordan is silent on the communication module’s relationship vis-à-vis the switch (the alleged “update station”). In particular, Jordan does not disclose that the switch transfers data to the traffic filter via the communication module, as required by the Challenged Claims. Black Decl., ¶83.

Lastly, even if the “communication module” were deemed a “network interface device” in a vacuum, it cannot be “*the* network interface device,” *i.e.*, the same device via which “network traffic” is received from external network, as required by limitation 1[e][i]/4[a]/7[a]. Jordan discloses the communication module exclusively within the context of describing the traffic filter’s “communications to and from the analytical engine” and does not suggest that the communication module receives “network traffic” from external network. See Jordan at 25:40-49, Fig. 11; Black Decl., ¶84.

In sum, Petitioner’s failure to identify a “network interface device” via which “additional content detection data” is received is fatal to Ground 1. And Petitioner cannot cure that deficiency because Jordan discloses that the alleged “additional content detection data” is transferred internally within the same network, not via a “network interface device.”

(b) Indirectly From the Analysis Process Via an Update Station

As noted above, Petitioner reads an “update station” on Jordan’s switch. Pet., 57-58. But Jordan’s switch is an **internal** component, routing communications between the traffic filter and the analytical engine within the same network. Jordan at 10:31-40. For the reasons discussed below, such a switch is not an “update station,” and receipt of data from such a switch is not “indirect.”

The context in the claims makes clear that an “update station” is a station located outside of a network boundary, not a component internal to the network. “While certain terms may be at the center of the claim construction debate, the context of the surrounding words of the claim also must be considered in determining the ordinary and customary meaning of those terms.” *ACTV, Inc. v. Walt Disney Co.*, 346 F.3d 1082, 1088 (Fed. Cir. 2003). The claims recite that a network gateway device (or a data network device) receives data from an update station “via the network interface device.” A network interface device, as discussed above, is a device that connects one network to another. Black Decl., ¶86. If an

“update station” was simply another component within the same network as the network gateway device, the network gateway device’s receipt of data from the “update station” would not be “via the network interface device.” *Id.*

Patent Owner’s interpretation is also supported by the claim requirement that content detection data be received “indirectly” from the analysis process. A POSITA would understand the term “indirectly” in the context of the invention to require that data is received from the external network, across a network boundary. Black Decl., ¶87. Petitioner assumes that the “indirectly” limitation is met as long as data is received via an “update station.” Pet., 58 (“[T]he traffic filter received the data indirectly from the analytical engine because it went through the switch.”). But such an interpretation would render the term “indirectly” superfluous because the presence of an “update station” would ***always*** render the communication “indirect.” This cannot be correct. *See Bicon, Inc. v. Straumann Co.*, 441 F.3d 945, 950 (Fed. Cir. 2006) (“claims are interpreted with an eye toward giving effect to all terms in the claim.”). The communication must possess the characteristic of being “indirect” other than by virtue of having an update station in the chain. As discussed above, in view of the surrounding words of the claim, a POSITA would have understood the “indirectly” element to require that the communication be through the Internet, *i.e.*, from the external network.

The specification of the ‘968 patent confirms this interpretation. The specification describes that an “update station” distributes content detection data to the content detection modules, *e.g.*, “through the Internet.” See ‘968 patent at 4:53-55 (“Update stations 106 receive the content detection data from central station 102, and send the content detection data to content detection modules 108 (e.g., through the Internet).”). The connection via the “Internet” (pink) is depicted in Fig. 1 of the ‘968 patent, reproduced below:

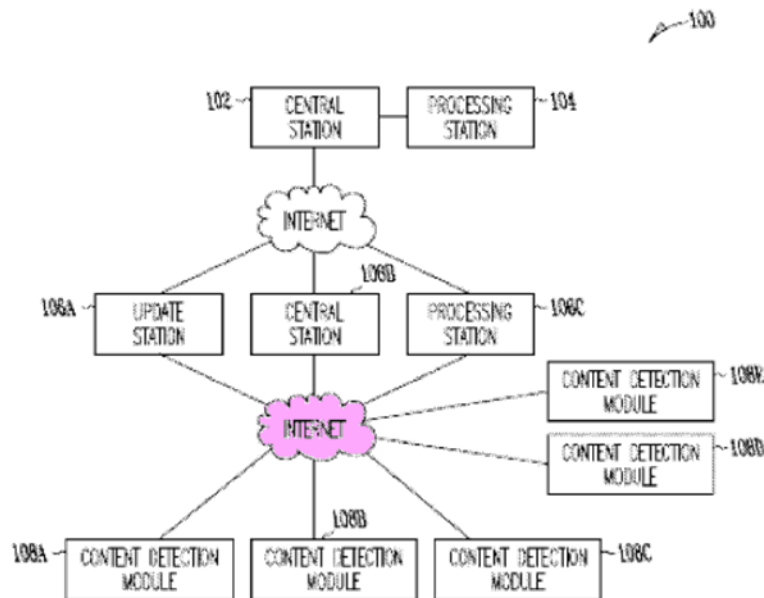


Fig. 1

Further, the specification describes that an update station may serve content detection modules in a “prescribed geographical area.” See ‘968 patent at 6:50-55; *see also* ‘457 provisional, §2 (update servers are “geographically located around the world and responsible for delivering update data to update agents”). And for each

content detection module, an update station can be pre-assigned or dynamically assigned based on a condition during use, *e.g.*, load demands and/or capacities of update stations, to increase the reliability of communication. *Id.* at 7:27-39. Such an assignment would not be possible if an update station was an internal component (*e.g.*, Jordan’s switches), routing data only within the same network. Black Decl., ¶89. Taking Jordan’s switch as an example, because it routes data between a traffic filter and its associated analytical engine all within the same network, the switch would not be able to transmit data to traffic filters outside the network, let alone serve any other traffic filters in a “prescribed geographic area” or be configurable to serve different traffic filters based on load demands or its capacities. *Id.* As a result, an internal component such as Jordan’s switch would fail to provide the benefits of an update station. *Id.*

In view of the claim language and the specification of the ‘968 patent, a POSITA would not consider Jordan’s switches an “update station,” and the traffic filters do not “indirectly” receive rules from the analytical engine.

2. *A POSITA Would Not Have Been Motivated To Combine Jordan With FortiGate.*

Petitioner asserts that “[i]f Jordan’s traffic filter is not an ‘update station,’ a POSITA would have found it obvious to incorporate that feature from FortiGate.” Pet., 58. Petitioner’s only argument for motivation to combine is that incorporating FortiGate’s FDSs (the alleged “update station”), which push updates to the FortiGate

firewalls, would “improve Jordan’s scalability.” *Id.* But Petitioner does not explain why one would have desired to improve Jordan’s “scalability.” Jordan’s traffic filter is served directly by its dedicated analytical engine, which is in the same network as the traffic filter. See Jordan at 9:34-35 (“the traffic filter ... can communicate with an analysis engine 140, which is also part of the network system 100.”); Fig. 1. As a result, contrary to Petitioner’s conclusory assertion, adding an “update station” in the communication between the traffic filter and analytical engine would have been unnecessary. Black Decl., ¶91. Indeed, the proposed modification would have been detrimental to the speed and reliability of Jordan’s security system because the transfer of data between the traffic filter and analytical engine would have to go through an extraneous layer (update station). Such a modification would undermine the “significant advantages” pursued by Jordan of quickly detecting and reacting to recently received communications. *Id.* at 9:40-50.

Petitioner does not explain why a POSITA would have had reasonable expectation of success. As discussed above, in Jordan, new rules are generated in the **internal network**. See Jordan at 9:34-35; Fig. 1. By contrast, in FortiGate, the alleged “update station” (*i.e.*, FDS) is in the **external, world-wide, network**. Fortigate at 116-117. Petitioner appears to assume that Jordan’s analytical engine, like Fortinet’s FDS, can simply be placed outside of the network. But if the communications between the traffic filter and the analytical engine were modified

to take place across a network boundary, they would take a substantial toll on the network bandwidth, leading to a slower and more expensive system. Black Decl., ¶92. And because such communications would be external (*i.e.*, received via the same network interface device via which external traffic is received), the modification would further necessitate protecting the communications with the analytical engine from threats and attacks. *Id.* The modification would have been extensive, and a POSITA would not have had reasonable expectation of success in maintaining the advantages pursued by Jordan (*e.g.*, quickly adapting based on the most recently received communications) while making such extensive modifications. *Id.*; Jordan at 9:45-50.

Lastly, contrary to Petitioner's assertion², FortiGate does not disclose a FortiGate firewall transferring suspicious traffic to the FDC. Rather, a FortiGate firewall simply receives rules from the FDC. FortiGate at 115, 118-121. Accordingly, the proposed modification would not result in a system where the traffic filter forwards suspicious traffic to the analytical engine. Black Decl., ¶93.

² Petitioner alleges that FortiResponse Distribution Center (FDC) received threats from Fortinet customer's and cites FortiGate at 335. Pet., 58-59. But that page does not exist in FortiGate.

3. *Jordan Does Not Disclose “Wherein The Analysis Process Facilitates an Analysis That Includes Receiving Administrator Input.”*

Jordan does not disclose “wherein the analysis process facilitates an analysis that includes receiving administrator input,” which is required by dependent claims 3, 6, and 9. Petitioner relies on Jordan’s disclosure of UI, in particular the statement that “the UI can access the rule generation capability of the analytical engine 140” Pet., 62 (quoting Jordan at 25:3-5). But that the UI can “access” the rule generation capability does not mean that the analytical engine (which allegedly performs the analysis process) receives “administrator input” in performing its analysis. Indeed, the functions performed on Jordan’s UI, such as categorizing, documenting, and monitoring, suggest that the UI is used to review information rather than to supply administrator input that facilitates the operation of the analytical engine. Black Decl., ¶94.

Petitioner also points to a “management module.” Pet., 62-63. A management module, however, provides an “interface between traffic filter 110 and a system administrator” and is not in communication with an analytical engine 140. As such, while the management module can “allow a system administrator to manage rules of the traffic filter 110, set system parameters, and/or read system logs” (Jordan at 25:50-53), Jordan does not disclose that the management module can be used to supply “administrator input” *to the analysis process*. Black Decl., ¶95.

VIII. GROUNDS 2 AND 3: LEE AND MAGDYCH DO NOT RENDER ANY CLAIM OBVIOUS.

A. There is No Motivation To Combine Lee And Magdych.

Petitioner appears to acknowledge a critical shortcoming of Lee, namely that there is not a single device that performs the recited functions. Petitioner’s argument that a POSITA would have been motivated to integrate the different functions into one device is contrary to Lee’s stated objective, which is to implement a *distributed* security environment based on a number of *independent* security agents.

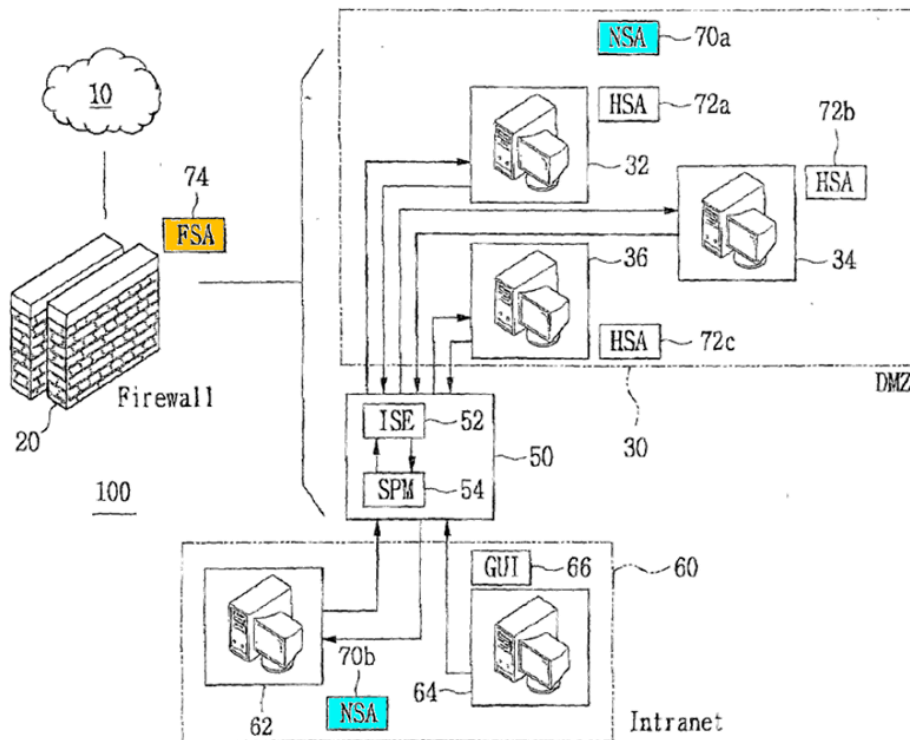
The disclosures Petitioner relies on are attributed to different “independent security agents.” In particular, NSA monitors traffic and transfers suspicious traffic to ISE so that a new signature is generated. *Id.*, ¶52. When the NSA recognizes a new attack based on the signature, “a new or modified rule” is given to FSA so that traffic from the attacker can be blocked. *Id.* As such, Lee does not disclose a single device—“network gateway device” (claim 1) or “data network device” (claims 4 and 7)—that:

- enforces “policies defined [] by the content detection and configuration data” and “at least one policy that defines a suspicious category of network traffic,”
- enforces policies to determine whether to allow traffic to pass,
- forwards suspicious network traffic to an analysis process,
- receives the additional content detection data from the analysis process, and
- blocks traffic determined to violate a policy.

For example, an FSA has nothing to do with identifying suspicious traffic or forwarding it to an ISE; an NSA performs those actions. Black Decl., ¶96. An NSA, however, does not enforce policies to determine whether to allow or block traffic; an FSA does.

The division between NSA and FSA is illustrated in Fig. 1 below. NSA is installed in the networks secured by the firewall, such as DMZ 30 and intranet 60 (see Lee, ¶35), whereas FSA is placed in the firewall 20, a different physical component. *Id.*, ¶38.

FIG 1



Lee, Fig. 1; Black Decl., ¶97.

Petitioner agrees that there is not a single device in Lee that performs the functions required of a network gateway device / data network device. Pet., 69 (an FSA “caused a firewall to block traffic from an attack data source” and an NSA “analyzed suspicious traffic”); *id.* at 71 (“Lee disclosed a system with separate agents performing separate functions.”). To overcome that deficiency, Petitioner argues that a POSITA would have been motivated to integrate Lee’s FSA and NSA into a single firewall unit in view of Magdych. Pet., 71. But this is contrary to Lee’s teachings. 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.* In view of such express disclosures in Lee, a POSITA would not have been motivated to integrate Lee’s FSA with NSA, as Petitioner proposes. Black Decl., ¶98. Doing so would have been directly contrary to Lee’s stated objective and undermined the benefits of having independent security agents. *Id.*

None of the reasons offered by Petitioner compel a different conclusion. Pet., 72. Moving an NSA to the firewall would simply shift the component from one

place in the internal network to another place in the internal network and thus would not save any “rack space.” Black Decl., ¶¶99. The purported feasibility and improvement in efficiency and security also do not justify modifying Lee in a way that directly undercuts Lee’s stated objective (“distributed security environment based on a number of independent security agents”) and the benefits Lee seeks to achieve (*e.g.*, “less cumbersome” implementation, “less overall code space,” ease of modification, etc.) as discussed above. *Id.*; Lee, ¶¶12, 40.

B. Magdych’s Port Does Not Constitute the Claimed “Configuration Data.”

Petitioner admits that Lee does not disclose “configuration data” but attempts to bridge that gap with Magdych. Pet., 77-78. Specifically, Petitioner contends that Magdych disclosed processing traffic based on a “port,” which according to Petitioner “indicated the nature of a service associated with the [configuration] data (*e.g.*, HTTP, Telnet, etc.) and caused the policy to restrict access based on the port number that was selected.” *Id.* Petitioner’s combination arguments are in vain. As a threshold matter, as discussed above, a POSITA would not have been motivated to modify Lee in view of Magdych. Petitioner also does not explain *how* Lee could have been modified to use a port to process network traffic.

Furthermore, the combination would still have been deficient because Magdych’s port is not “configuration data.” The Challenged Claims require three conditions with respect to “configuration data:” (1) it must be stored on a “memory

device,” (2) the received network must be processed “in view of” configuration data, and (3) policies must be defined in part by the configuration data. Magdych’s port does not meet any of these requirements. Magdych makes clear that a port is “information **contained in** a data packet” and not stored a memory device of a firewall that receives such a data packet. Magdych at 4:29-33; *see also id.* at 2:15-23 (“A port is numerically designated element contained in the overhead of a packet.”); Black Decl., ¶101. A port also does not meet the other two requirements: because a port is part of a received data packet, it is not “configuration data” in view of which the received network traffic is processed, and it does not define a policy. *Id.*

C. Lee Does Not Disclose or Render Obvious Enforcing “At Least One Policy That Defines a Suspicious Category of Network Traffic.”

All Challenged Claims require a “network gateway device” / “data network device” enforcing a “policy that defines a suspicious category of network traffic.” *See* claim limitation 1[e][iii]/4[b][ii]/7[b][ii]. Petitioner does not even attempt to show how Lee discloses such a policy. Instead, Petitioner’s arguments for these limitations are **entirely** about how Lee and Magdych purportedly disclose enforcing “policies defined ... by the content detection data and configuration data,” which is a distinct requirement. Pet., 81-82. Ground 2 fails for this reason alone.

D. Lee Does Not Disclose or Render Obvious a “Network Gateway Device” or “Data Network Device” That Performs “User Identification.”

Lee does not disclose or render obvious a “network gateway device” / “data network device” performing “user identification.” Petitioner reads a “network gateway device” / “data network device” on Lee’s firewall 20. Pet., 72 (“Lee disclosed a network gateway that included firewall (20).”); *id.* at 74. Petitioner alleges that FSA “could” include user identification because “[t]he system could detect and react to [a scenario where an attacker created a user ID] by determining if the attacker was a root user.” *Id.* at 84. But the alleged user identification is performed by ISE (intelligent security engine), not FSA. Lee, ¶84; Black Decl., ¶103. Indeed, Lee does not once mention FSA in connection with the disclosure that Petitioner relies on. Black Decl., ¶103. Petitioner’s assertion that FSA “could include user identification” thus lacks merit.

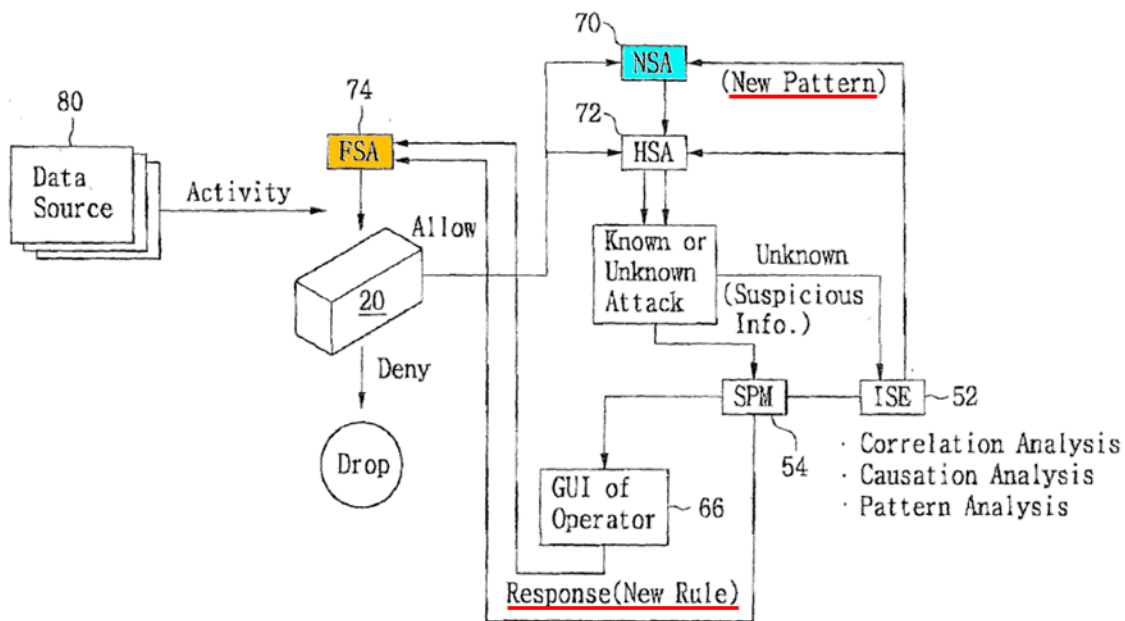
E. Lee Does Not Disclose or Render Obvious “Receiv[ing], Via The Network Interface Device, The Additional Content Detection Data Indirectly From The Analysis Process Via an Update Station.”

Lee does not disclose or render obvious a “network gateway device” / “data network device” “receiv[ing], via the network interface device, the additional content detection data indirectly from the analysis process via an update station.” Petitioner reads this claim limitation on functions performed by different security agents and thus failed to show that there is a single “network gateway device” or

“data network device” that satisfies the claim limitations. Moreover, Petitioner overlooks that, similar to Jordan, the transfer of the content detection data from the ISE (which allegedly performs the claimed “analysis process”) takes place inside of a network protected by the firewall. These deficiencies are discussed in detail below.

First, the alleged network gateway device in Lee (*i.e.*, the firewall) does not receive “the additional content detection data.” Petitioner reads “the additional content detection” data on “a generated signature” and states that “a generated signature from the ISE was transferred to the NSA (70) **and FSA (74) in firewall (20).**” Pet., 88. But Lee only discloses that a generated signature is transferred to NSA, **not to FSA**. Lee, ¶52 (“the generated signature is transferred to NSA 70 ...”); Black Decl., ¶105. Lee’s Fig. 2 also demonstrates that “new pattern” is sent only to NSA (cyan), not FSA (orange).

FIG 2



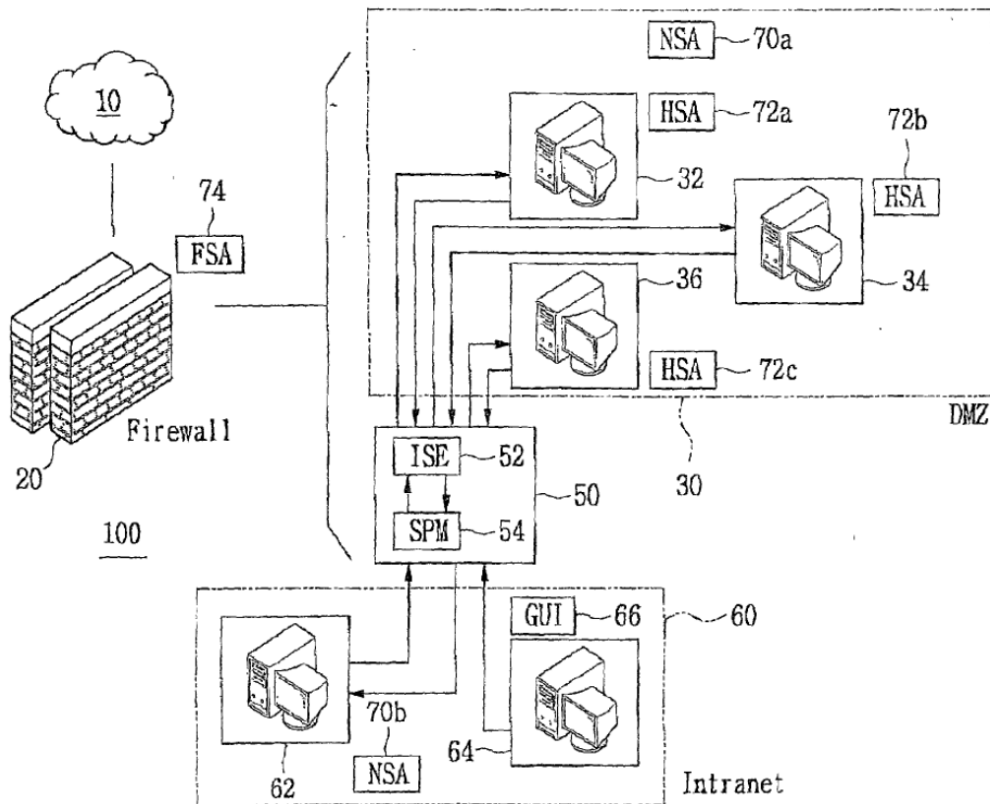
Lee, Fig. 2. Moreover, contrary to Petitioner’s assertion, an NSA is not “*in*” a firewall (the alleged network gateway device). Rather, an NSA is installed in a network secured by the firewall (*e.g.*, DMZ 30 or intranet 60). Lee, ¶37; Fig. 1. As a result, an NSA is not a “network gateway device,” and its receipt of a “generated signature” or “new pattern” does not constitute a “network gateway device” receiving the “additional content detection data.” Black Decl., ¶105.

Although Lee discloses that an FSA receives a “rule” (as opposed to a “signature”), a “rule” is not “content detection data” based on which a policy is defined. Black Decl., ¶106. Lee discloses that a signature is transferred to NSA “so that more rapid confrontation in response to future attacks of the same pattern is made possible” and that “when the new pattern of attack is recognized, a new or

modified rule is given to FSA ... so that traffic from the attacker [] can be blocked.” Lee, ¶52. A POSITA would have understood that, while a “signature” may be used (by NSA) to analyze traffic, a “rule” is used (by FSA) to allow or block traffic determined to contain a threat based on such analysis and therefore does not constitute the claimed “content detection data.” Black Decl., ¶106. Tellingly, elsewhere in the petition, Petitioner acknowledges the distinction, reading “policies” on Lee’s “rules” (received by FSA) and “content detection data” on Lee’s “pattern or signature” (received by NSA). *See* Pet., 81 (“The policies were defined by content detection and configuration data. For content detection data, for example, Lee disclosed that the policies/rules included a pattern or signature for detecting malicious data.”); *see also id.*, 76-77 (pointing to a pattern or signature, not the rule, as being the “content detection data”).

Second, even if Lee’s “rule” transferred to the FSA was considered “content detection data,” the FSA does not receive a rule “indirectly from the analysis process via an update station.” Petitioner states 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.” Pet., 88. But this assertion fails for the similar reasons as does Petitioner’s reliance on Jordan: as illustrated in Fig. 1 below, ISE and SPM cannot be an “analysis process” and “update station” because both are **internal** components, placed in the internal network secured by the firewall 20.

FIG 1



Lee, Fig. 1; *id.*, ¶38 (“The intelligent security management module 50 comprises ISE [] 52 and SPM [] 54”), ¶49 (describing that ISE and SPM are “installed integrally with the firewall 20”). A POSITA therefore would not consider Lee’s SPM to be a station via which updates are indirectly distributed, e.g., through the Internet. Black Decl., ¶107; see Section VII.B.1(b), *supra*.

Third, Lee does not render obvious an FSA receiving a new rule “via the network interface device.” Petitioner acknowledges that Lee does not disclose the “via the network interface device” element but asserts that “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. But Petitioner ignores Lee’s disclosure that an SPM is “installed integrally” with the firewall. Lee, ¶49. A POSITA would have expected the SPM–firewall communication to occur through a non-networked interface (*e.g.*, a switch, bus, etc.), not through a “*network* interface device.” Black Decl., ¶108. Even if the communication was over a network interface device, such a device cannot constitute “*the* network interface device,” *i.e.*, the same network interface via which “network traffic” is received per limitation 1[e][i]. In fact, for “network interface device” of limitation 1[e][i], Petitioner points to “a network interface that went to an unsecured external network,” which is distinct from the alleged “network interface for the internal part of the network” that Petitioner points to for this limitation. *Compare* Pet., 79 *with id.*, 89. Petitioner does not even attempt to explain why the different devices can be considered a single “network interface device.”

For these reasons, Petitioner has failed to show that Lee discloses or renders obvious a “network gateway device” / “data network device” “receiv[ing], via the network interface device, the additional content detection data indirectly from the analysis process via an update station.”

F. Lee Does Not Disclose or Render Obvious “Stor[ing] The Additional Content Detection Data on The at Least One Memory Device.”

As discussed above, the FSA does not receive, let alone store, the additional content detection data. *See* Section VIII.E, *supra*. Rather, it is the NSA that receives the alleged additional content detection data (*i.e.*, the “generated signatures”), and the FSA simply adopts a new “rule” to block traffic. As such, Lee does not disclose or render obvious a “network gateway device” / “data network device” “stor[ing] the additional content detection data on the at least one memory device.”

Petitioner states that “generated signatures were given to NSA (70) and a new or modified rule is given to the FSA (74)” and that “a POSITA would have understood that the FSA and NSA would store the updated rules or signatures, such as content detection data, in order to use it and apply it to future traffic.” Pet., 89-90. But Petitioner has no basis to lump together a “rule” and a “signature,” which are two distinct elements, and collectively treat them as being “content detection data.” As discussed above, Lee’s “rule” is used simply to allow or block traffic determined to contain a threat based on analysis performed by the NSA and thus does not constitute “content detection data.” Black Decl., ¶111.

Accordingly, contrary to Petitioner’s theory, a POSITA would not have understood the FSA (which only receives a rule) to store in memory a signature, which it does not even receive. *Id.*, ¶112.

IX. GROUND 4: FANG IS NOT PRIOR ART.

Fang is the publication of the application No. 13/546,915, which the ‘968 patent claims priority to by a series of continuation applications. Petitioner’s argument that Fang is prior art is premised on the false assumption that the Challenged Claims lack written description support under §112.

A patent application that has §112 support in a previously filed application (and meets other requirements that are not at dispute here, including naming an inventor in the previously filed application) is entitled to the filing date of the prior application. *See* 35 U.S.C.A. § 120. The ‘968 patent claims priority to Fang by an unbroken chain of continuation applications and shares the same specification with Fang.³ There is no dispute that Patent Owner maintained the “continuity of disclosure.” *See Lockwood v. Am. Airlines, Inc.*, 107 F.3d 1565, 1571 (Fed. Cir. 1997). As such, the ‘968 patent is presumptively entitled to the filing date of Fang, disqualifying Fang as prior art.

To overcome the presumption, Petitioner must establish that the ‘968 patent lacks written description support. *See Hynix Semiconductor Inc. v. Rambus Inc.*, 645 F.3d 1336, 1351 (Fed. Cir. 2011) (“To overcome the presumption of validity of

³ There are no continuation-in-part application in the chain extending from Fang to the ‘968 patent.

patents, the accused must show that the claims lack a written description by clear and convincing evidence.”). Petitioner failed to do so because, as discussed in Section VI.B, *supra*, the specification provides sufficient support for the two limitations (*i.e.*, “configuration data” and “user identification”) challenged by Petitioner.

Accordingly, Fang cannot qualify as prior art.

X. CONCLUSION

For the foregoing reasons, Patent Owner respectfully requests that the Petition be denied.

Date: June 20, 2023

Respectfully submitted,

By: /s/ James Glass

James M. Glass (Reg. No. 46,729)

QUINN EMANUEL URQUHART &

SULLIVAN, LLP

51 Madison Avenue, 22nd Floor

New York, NY 10010

Tel: (212) 849-7000

Fax: (212) 849-7100

Email: jimglass@quinnemanuel.com

*Counsel for Patent Owner –
Fortinet, Inc.*

CERTIFICATE OF COMPLIANCE

I hereby certify that this paper complies with the type-volume limitation of 37 C.F.R. § 42.24 because it contains 10,924 words, excluding the parts of the paper exempted by 37 C.F.R. § 42.24(b).

/s/ James Glass

James M. Glass
Registration No. 46,729

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. § 42.6(e), the undersigned hereby certify that PATENT OWNER'S PRELIMINARY RESPONSE, and all exhibits and other documents filed together with the preliminary response, were served on June 20, 2023 by e-mailing copies to:

Lead Counsel	Back-Up Counsel
Thomas N. Millikan Reg. No. 72,316 Perkins Coie LLP 11452 El Camino Real, Suite 300 San Diego, California, 92130 Phone: 858-720-5700 Fax: 858-720-5799 Netskope- FortinetIPRTeam@perkinscoie.com	Babak Tehrani Reg. No. 55,937 Andrew N. Klein <i>Pro Hac Vice Forthcoming</i> Perkins Coie LLP 11452 El Camino Real, Suite 300 San Diego, California, 92130 Phone: 858-720-5700 Fax: 858-720-5799 Netskope- FortinetIPRTeam@perkinscoie.com

Date: June 20, 2023

Respectfully submitted,

By: /s/ James Glass

James M. Glass (Reg. No. 46,729)

QUINN EMANUEL URQUHART &

SULLIVAN, LLP

51 Madison Avenue, 22nd Floor

New York, NY 10010

Tel: (212) 849-7000

Fax: (212) 849-7100

Email: jimglass@quinnemanuel.com

*Counsel for Patent Owner –
Fortinet, Inc.*