

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

**DECLARATION OF DR. JOHN BLACK JR. IN SUPPORT OF
PATENT OWNER'S PRELIMINARY RESPONSE**

TABLE OF CONTENTS

	<u>Page</u>
I. QUALIFICATIONS	1
II. LEVEL OF ORDINARY SKILL IN THE ART	5
III. LEGAL UNDERSTANDING	7
A. Obviousness.....	7
B. Claim Construction.....	8
C. Written description	9
IV. OVERVIEW OF THE '968 PATENT	10
V. OVERVIEW OF THE CITED ART	14
A. Jordan (Ex-1005).....	14
B. FortiGate (Ex-1008)	15
C. Lee (Ex-1009).....	16
D. Magdych (Ex-1010)	19
E. Judge (Ex-1011)	20
F. Fang (Ex-1012).....	20
VI. PRIORITY DATE	21
A. The Challenged Claims of the '968 Patent Are Entitled To The Priority Date of the '457 Provisional Application.	21
1. "configuration data"	22
2. "user identification"	23
3. "forwarding the network traffic to an analysis process"	24
4. "policy enforcement including user identification, content identification, and at least one of source verification and destination verification"	26
B. The '968 Patent Provides Written Description Support.....	27
1. "configuration data"	28
2. "user identification"	30
VII. GROUND 1: JORDAN AND FORTIGATE DO NOT RENDER ANY CLAIM OBVIOUS.....	32

A.	Jordan Does Not Qualify as Prior Art.	32
1.	Jordan Provisional Does Not Provide Support For Claim 1.	33
2.	Jordan Provisional Does Not Provide Support For The Subject Matter Relied Upon.....	34
B.	Even If Jordan is Deemed To Qualify as Prior Art, Jordan in View of FortiGate Does Not Render Any Claims Obvious.....	35
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.”	35
(a)	Network Interface Device.....	36
(b)	Indirectly From the Analysis Process Via an Update Station	40
2.	A POSITA Would Not Have Been Motivated To Combine Jordan With FortiGate.....	43
3.	Jordan Does Not Disclose “Wherein The Analysis Process Facilitates an Analysis That Includes Receiving Administrator Input.”	45
VIII.	GROUND 2 AND 3: LEE AND MAGDYCH DO NOT RENDER ANY CLAIM OBVIOUS.....	46
A.	There is No Motivation To Combine Lee And Magdych.....	46
B.	Magdych’s Port Does Not Constitute the Claimed “Configuration Data.”	50
C.	Lee Does Not Disclose or Render Obvious Enforcing “At Least One Policy That Defines a Suspicious Category of Network Traffic.”	51
D.	Lee Does Not Disclose or Render Obvious a “Network Gateway Device” or “Data Network Device” That Performs “User Identification.”	51
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.”	52

F. Lee Does Not Disclose or Render Obvious “Stor[ing] The
Additional Content Detection Data on The at Least One
Memory Device.” 57

IX. GROUND 4: FANG IS NOT PRIOR ART. 58

X. CONCLUSION.....58

EXHIBIT TABLE

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

1. I have been retained on behalf of Fortinet, Inc. (“Patent Owner”) in connection with the above-captioned *inter partes* review (IPR). I have been asked to provide my opinions regarding Fortinet’s Patent Owner Preliminary Response. I am being compensated for my time at the rate of \$625 per hour. I have no interest in the outcome of this proceeding.

2. In preparing this Declaration, I have reviewed and am familiar with the Patent Owner’s Petition submitted for IPR2023-00457, U.S. Patent No. 9,231,968 B2, (“the ‘968 patent”) and its file history, and all other materials cited and discussed in the Petition (including the declaration of Petitioner’s expert Dr. Wenke Lee), as well as the materials cited and discussed in this Declaration.

3. The statements made herein are based upon the cited documents as well as my own knowledge and experience in the field. This Declaration represents only the opinions I have formed to date. I may consider additional documents as they become available or other documents that are necessary to form my opinions. I reserve the right to revise, supplement, or amend my opinions based on new information and on my continuing analysis.

I. QUALIFICATIONS

4. My qualifications can be found in my Curriculum Vitae (see *infra* Ex. 2002), which includes my detailed employment background, professional experience, and list of technical publications and patents.

5. I am an Associate Professor of Computer Science at the University of Colorado, Boulder. I received a B.S. in Mathematics and Computer Science from the California State University at Hayward (now “California State University, East Bay”) in 1988. I received an M.S. in Computer Science in 1997, and a Ph.D. in Computer Science in 2000, both from the University of California at Davis.

6. I have taught more than 60 classes in computer science, on subjects including data structures, algorithms, networking, operating systems, software engineering, security, cryptography, discrete mathematics, and quantum computing. I have authored or coauthored more than 20 publications, primarily on issues relating to computer security. I have been involved with computers for over 40 years in both commercial and academic capacities.

7. My earliest interest was in networks and security. My first memories in this regard were around 1975 when a group of friends and I learned about the telephone network and its security. A few years later, personal computers became available and I spent most of my free time studying, programming, and modifying them. I worked extensively with various networking products throughout the 1980s, and developed an interest in cryptography soon thereafter. Although my undergraduate institution had no courses in cryptography or security in the 1980s, I decided to pursue self-study at the time, and opted to double major in Computer Science and Mathematics because cryptography is a blend of these two subject areas.

8. After earning my B.S. degree in 1988, I worked for six years at Ingres Corp as a software developer, writing and reviewing code written in C. My work primarily was directed at transaction logging, data type support, and security.

9. In 1995, I began my Ph.D. at UC Davis under cryptographer Phillip Rogaway. My area of focus was cryptography and security and my research involved encryption, authentication, hash functions, and network security.

10. After graduation I took a position as an Assistant Professor at the University of Nevada at Reno. In the Fall of 2001, I taught the networking class there, which included coverage of Ethernet, interior gateway protocols, exterior gateway protocols, ARP, DHCP/BOOTP, IP, UDP, TCP, HTTP, SMTP and other protocols. In 2001, a graduate student and I looked at the security of ARP and invented a new protocol “AuthARP” to add security to the protocol.

11. In 2002, I moved to the University of Colorado at Boulder where I am currently employed. In the Fall of 2002, I co-designed and co-taught a new course called “Foundations of Computer and Network Security,” which included descriptions of security issues around both wired and wireless security challenges, mostly for public-facing network services including the world-wide web. I have taught this class seven more times since then, including modern topics such as wireless networking, the Internet of Things, and so forth.

12. In my career at the University of Colorado, I have published several more papers in the area of cryptography and network security. I have taught more than 30 courses in network security and cryptography, and have graduated several PhD students in these areas.

13. I also have worked for a consulting company at times, writing software on contract basis. Although most projects are covered by NDAs, many involved networks and/or aspects of computer security.

14. In 2011, I began technical consulting for a local company called Cardinal Peak, which focuses primarily on video encoding and delivery systems. My work for Cardinal Peak has largely been directed to video encoding, transcoding, compression, encryption, and DRM, but also has included networking projects and embedded device work. For example, I designed the security system for the Pro1 smart thermostat, implemented the DRM for the Yonder Music App, worked on 802.1X code for smart dog collars, and helped design the cryptography used in Fitbit devices for wireless transfer of a Fitbit watch to a phone or laptop.

15. In 2016, I took a two-and-a-half year leave of absence from the University of Colorado to start a company named “SecureSet” in Denver, Colorado. The objective of SecureSet is to take reasonably proficient technical people and turn them into computer and network security specialists via five months of intensive training. SecureSet was sold to WeWork in 2019 and continues to offer computer

security classes today. In 2018 I returned to my position at the University where I remain employed to the present day.

II. LEVEL OF ORDINARY SKILL IN THE ART

16. I understand that a person of ordinary skill in the relevant art at the time of the invention (also referred to herein as “POSITA”) is presumed to be aware of all pertinent art, thinks along conventional wisdom in the art, and is a person of ordinary creativity-not an automaton.

17. I have been asked to consider the level of ordinary skill in the field that someone would have had at the time the claimed invention was made. In deciding the level of ordinary skill, I considered the following:

- the levels of education and experience of persons working in the field;
- the types of problems encountered in the field; and
- the sophistication of the technology.

18. A person of ordinary skill in the art 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.

19. I have reviewed the declaration of Dr. Lee, including his opinions regarding the Person of Ordinary Skill in the Art. My description of the level of ordinary skill in the art is essentially the same as that of the Dr. Lee except that Dr. Lee's description requires two years of work or research experience for someone with a Bachelor of Science degree (as compared to three years). Lee, ¶29. The opinions set forth in this Declaration would be the same under either my or Dr. Lee's proposal.

20. I am well-qualified to determine the level of ordinary skill in the art and am personally familiar with the technology of the '968 Patent. By 2000, I had obtained a PhD in Network and Computer Security and therefore I was a person of at least ordinary skill in the art at the time of the priority date of the '968 patent, regardless of whether the priority date is March 12 2004, which I believe to be the correct date, or some later date as Dr. Lee claims in his declaration. Regardless if I do not explicitly say that my statements below are based on a stated timeframe, all of my statements are to be understood as a POSITA would have understood something regardless of which date is adopted. If I believe a term has a different meaning depending on the priority date given to the '968 Patent, I will explicitly say so.

III. LEGAL UNDERSTANDING

21. I am not a lawyer and will not provide any legal opinions. Though I am not a lawyer, I have been advised that certain legal standards are to be applied by technical experts in forming opinions regarding the meaning and validity of patent claims.

A. Obviousness

22. I understand that to obtain a patent, a claimed invention must have, as of the priority date, been nonobvious in view of prior art in the field. I understand that an invention is obvious when the differences between the subject matter sought to be patented 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.

23. I understand that to prove that prior art, or a combination of prior art, renders a patent obvious, it is necessary to: (1) identify the particular references that singly, or in combination, make the patent obvious; (2) specifically identify which elements of the patent claim appear in each of the asserted references; and (3) explain how the prior art references could have been combined to create the inventions claimed in the asserted claim.

24. I understand that a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently,

known in the prior art, and that obviousness cannot be based on the hindsight combination of components selectively culled from the prior art to fit the parameters of the patented invention.

25. I also understand that a reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant. Even if a reference is not found to teach away, I understand its statements regarding preferences are relevant to a finding regarding whether a skilled artisan would be motivated to combine that reference with another reference.

B. Claim Construction

26. I have been informed that patent claims are construed from the viewpoint of a person of a POSITA and that patent claims generally should be understood consistent with their ordinary and customary meaning at the time of the invention. A review of the patent claim language, the patent specification, and its prosecution history are also necessary to determine the proper meaning and scope of the term at issue.

27. I understand that, 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.

28. I have further been informed that in the specification and prosecution history the patentee may define a claim term in a way that differs from the ordinary and customary meaning. I understand that during prosecution of the patent before the U.S. Patent and Trademark Office, the Applicant may make representations or provide definitions of terms that may affect the scope of the patent claims. In particular, the Applicant may, during the course of prosecution, limit the scope of the claims to overcome prior art and/or disavow claim coverage by making clear and unambiguous statements to that effect.

29. I have been informed that a POSITA may, among other things, consider dictionaries, publications, other patents, and treatises (*i.e.*, “extrinsic evidence”). I understand that extrinsic evidence may generally not be relied on if it contradicts the meaning of claim language provided by the intrinsic evidence, such as express definitions given for terms in the specification.

C. Written description

30. I understand that the written description must clearly allow a POSITA to recognize that the inventor invented what is claimed. I understand that the 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. I understand that the test requires an objective inquiry into the four corners of the specification from the perspective of a person of

ordinary skill in the art. I understand that the description requirement does not demand any particular form of disclosure. For example, I understand that the exact terms appearing in the claim need not be used verbatim in the specification.

IV. OVERVIEW OF THE '968 PATENT

31. The '968 Patent is entitled "Systems and Methods for Updating Content Detection Devices and Systems." It includes systems, methods, and software for "processing received network traffic content" using "detection data" and "configuration data" to either block, permit or "further evaluate" the content. '968 Patent at Abstract.

32. The '968 Patent Specification explains that at the time of the invention current content detection systems often used well-known virus signature detection methods but that new virus signatures were often not made available immediately after they were discovered unless a user manually downloads them. *Id.* at 1:50-56. It goes on to explain that other kinds of content may be undesirable for corporate environments such as spam, misuse of networks, etc., and that URL blacklisting was the most common method of preventing such content from entering the network. *Id.* at 1:57-59. But this URL blacklisting approach has the same problem as the virus signature method: a lack of updates may render the security system unable to block undesirable content.

33. The ‘968 Patent’s solution to the problems above is to use “processing stations” 104 to perform analysis on received network content and then generate “content detection data” which is provided to a “central station” 102. *Id.* at 6:12-45, Fig. 1. The central station then transmits content detection data to an update station 106 at a separate geographical location. *Id.* at 6:48-55. The specification describes in detail methods of balancing loads between various update stations and the failover methods used in various embodiments. *Id.* at 7:1-8:24. The specification is careful to state that each of the techniques described for managing updates, polling update stations, distribution of updates, etc., are for particular embodiments to illustrate the ideas behind the invention but that, of course, what is claimed by the patent is embodied in the claims.

34. Ultimately the invention allows content detection modules 108 to be updated by the update stations 106 and thereby respond quickly to emerging threats. *Id.* at 4:35-38, 6:40-62, 6:65-8:56, 8:59-9:5.

35. The novelty in the ‘968 Patent over prior art is due to several improvements over the prior art. First, as the patent discusses at the outset, the process of requiring manual updates by users to keep content detection modules up-to-date (e.g., downloading virus signature updates or URL blacklist updates) is burdensome, error-prone, time-inefficient and creates a window of opportunity for bad actors to exploit the fact that manual updates often do not occur quickly after an

exploit is known. The automatic nature of the ‘968 patent’s invention improves every one of these aspects. *Id.* at 9:19-27. Further, the architecture described in the ‘968 Patent provides resiliency by load balancing and failover; in the case that an update station is unavailable or fails to work properly, another station nearby can provide content detection data to the content detection modules. *Id.* at 9:28-35. Further, update stations can be configured and customized to restrict Internet access or to serve only certain subsets of a company’s network, thereby allowing security administrators to have granular control over policy. *Id.* at 9:42-60.

36. I understand Petitioner challenges all 9 claims of the ‘968 patent: independent claims 1, 4, and 7, as well as dependent claims 2, 3, 5, 6, 8 and 9. Claim 1 recites:

1. A network gateway device comprising:

- at least one processor,
- at least one memory device;
- at least one network interface device;
- content detection and configuration data stored on the at least one memory device;
- and
- an instruction set, stored in the at least one memory device and executable by the at least one processor to:

receive network traffic via the at least one network interface device;

process the received network traffic in view of the content detection and configuration data stored in the at least one memory device 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, the policy enforcement performed to determine whether to allow the received network traffic to pass, the policy enforcement including user identification,

content identification, and at least one of source verification and destination verification, 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, 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;

receive, via the network interface device, the additional content detection data indirectly from the analysis process via an update station;

store the additional content detection data on the at least one memory device;

process subsequently received network traffic in view of the additional content detection data;

block network traffic determined to violate at least one policy; and

allow network traffic to pass that does not violate a policy.

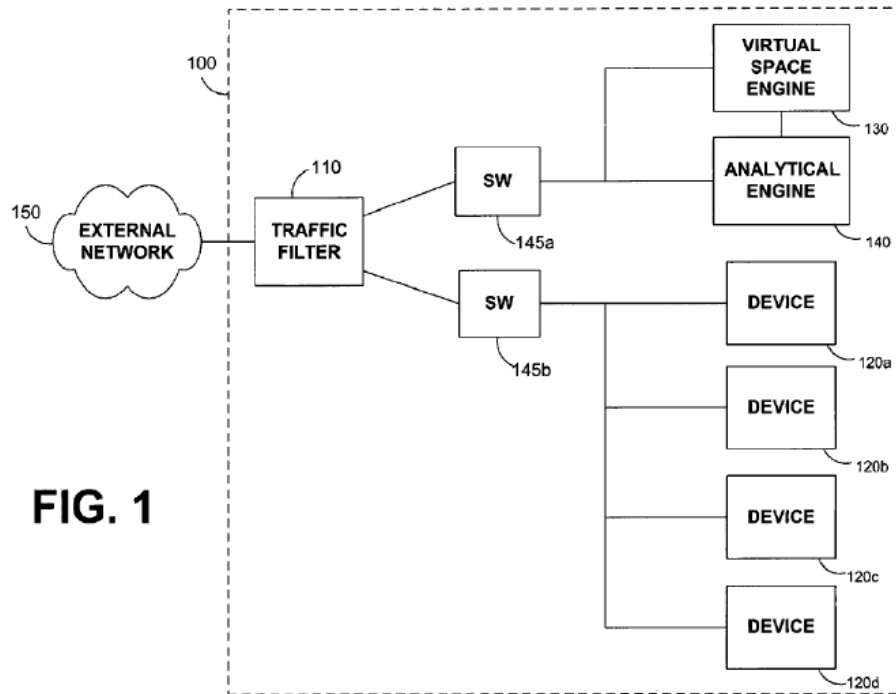
37. Claim 1 of the '968 patent is exemplary. The claim encompasses the ideas from the specification involving receiving network traffic at a device and processing that traffic to enforce security policies based on content detection and configuration data. A policy defines whether the network traffic is suspicious or not, and therefore whether it should be passed through or not; the policy includes items such as user identification, content identification and at least one of source verification or destination verification. If the network traffic fails the policy check, it is forwarded to an analysis process that determines whether the traffic contains a threat. The analysis process generates further content detection data, which is then received via an update station. Subsequent network traffic is then processed in view

of the new content detection data and traffic is blocked if it violates a security policy, otherwise it is allowed to pass through.

V. OVERVIEW OF THE CITED ART

A. Jordan (Ex-1005)

38. Jordan discloses defending a computer network using a traffic filter. Jordan at Abstract. 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.

39. 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)

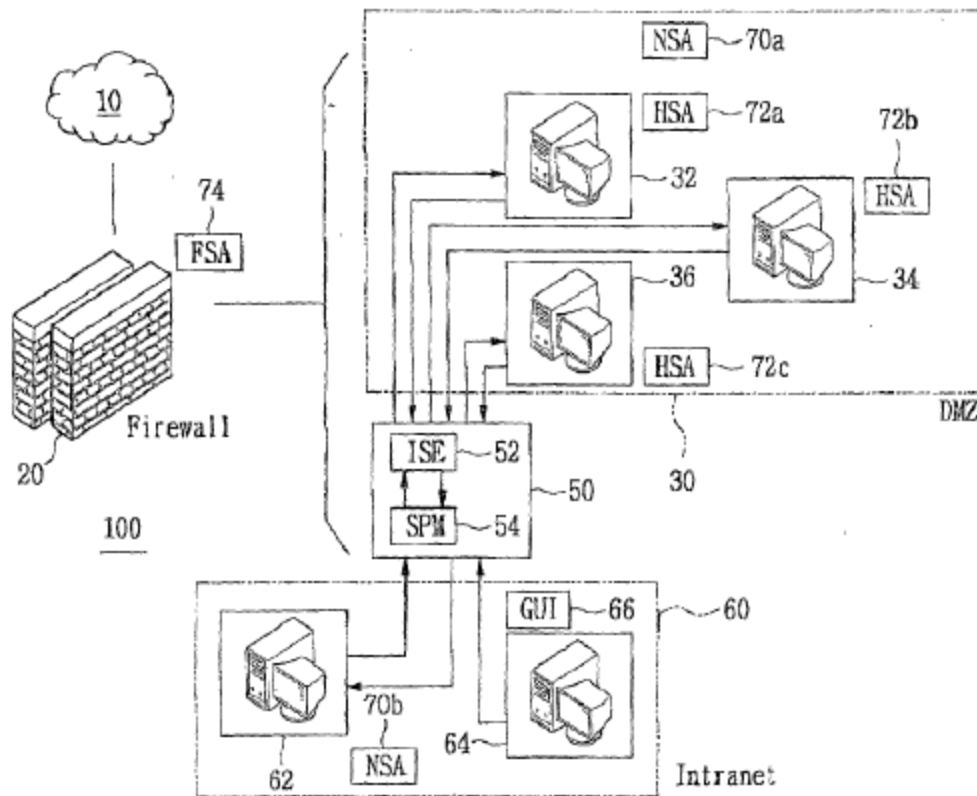
40. FortiGate is a user manual version 2.5 for the FortiGate-3600. FortiGate discloses a FortiGate Network Intrusion Detection System (NIDS) for preventing suspicious network activity. FortiGate at 16. To identify attacks, a

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)

41. Lee discloses a security system with individual security agents. Lee, ¶2. 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.” *Id.*, ¶¶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 individual security agents. *Id.*, ¶13. An overall configuration of a Lee’s security system is illustrated in Fig 1:

FIG 1

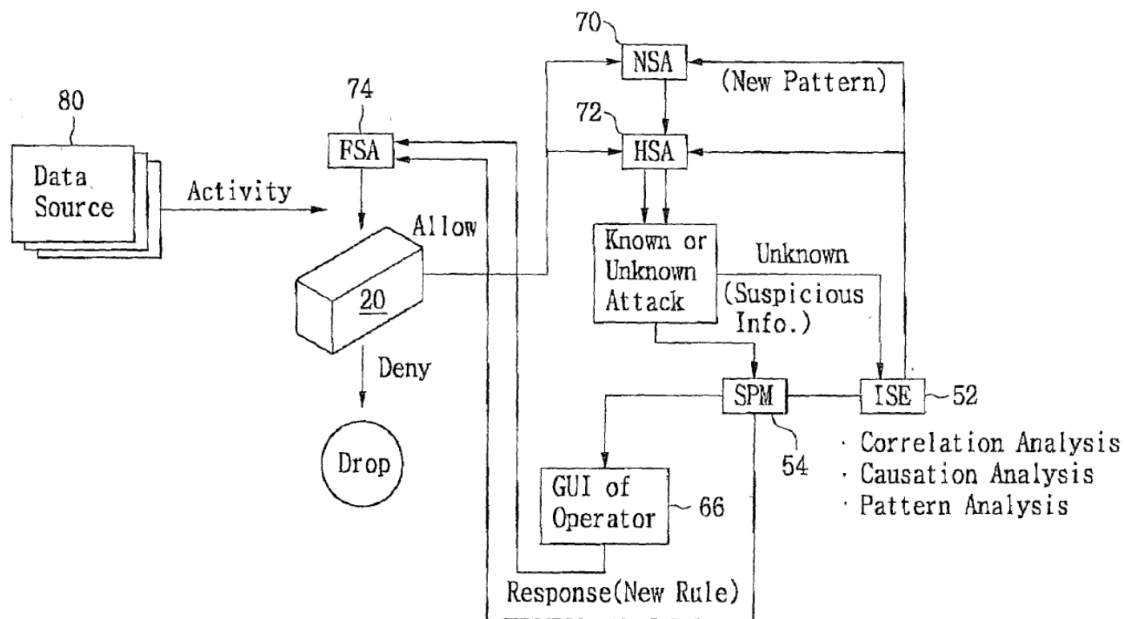


Id., Fig. 1. An FSA is provided for firewall 20, which protects internal network such as a DMZ 30 and Intranet 60 from outside network (e.g., public network 10). *Id.*, ¶¶34-35, 38. NSAs, on the other hand, are installed within the internal networks protected by the firewall. *Id.*, ¶¶37-38.

42. 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.

43. Maintaining independence between the different security agents is key to Lee’s disclosures. According to Lee, “[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.*

D. Magdych (Ex-1010)

44. 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.

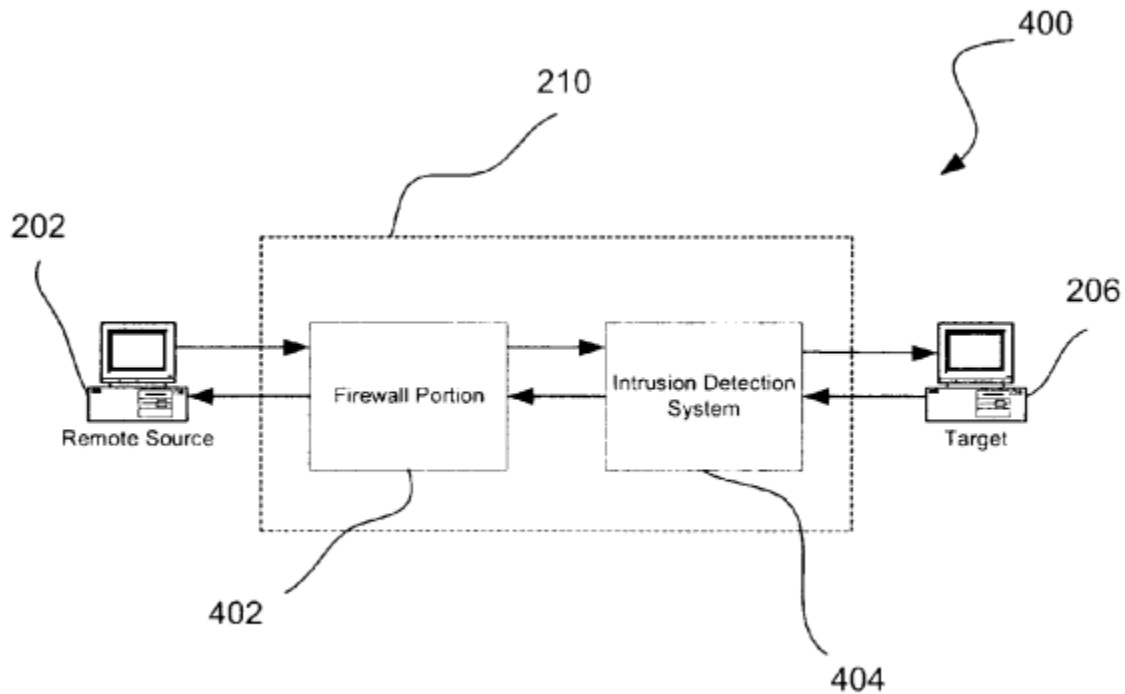


Figure 4

Id., Fig. 4.

E. Judge (Ex-1011)

45. 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)

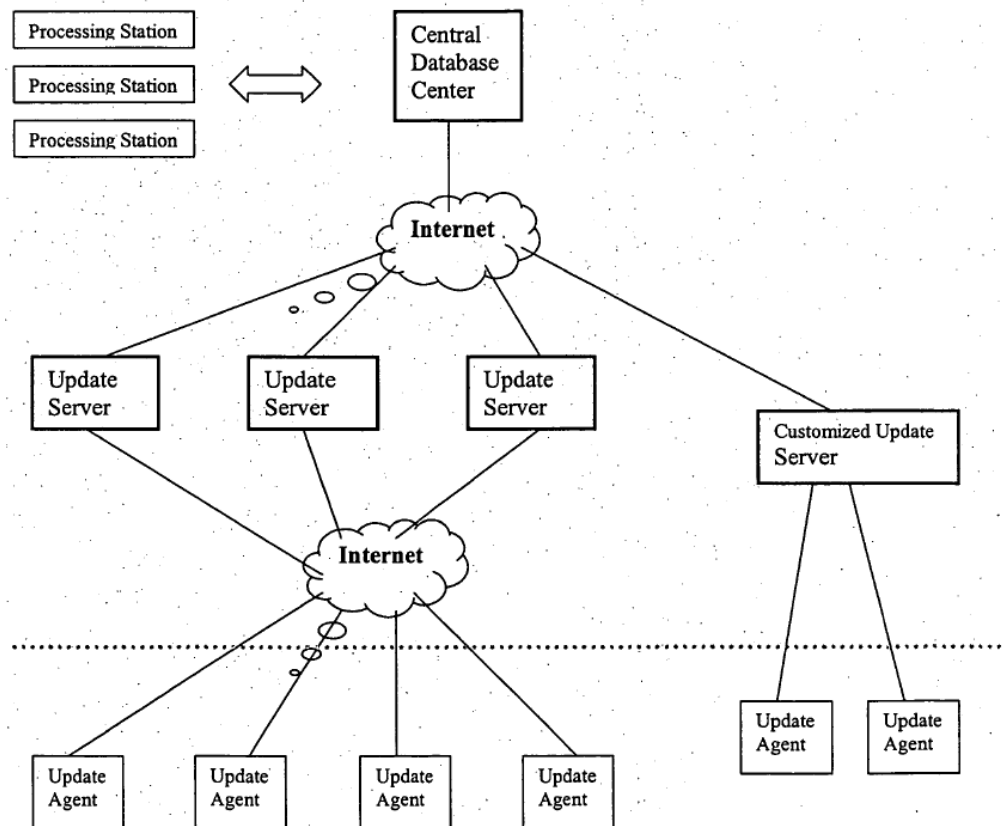
46. Fang is in the same family as the ‘968 patent. The ‘968 patent issued as continuation of U.S. Pat. App. No. 13/795,407, which in turn is continuation of

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

VI. PRIORITY DATE

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

47. In my opinion, 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.*

48. 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.” I disagree for the reasons discussed below.

1. “configuration data”

49. In my opinion, 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.” 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. 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”

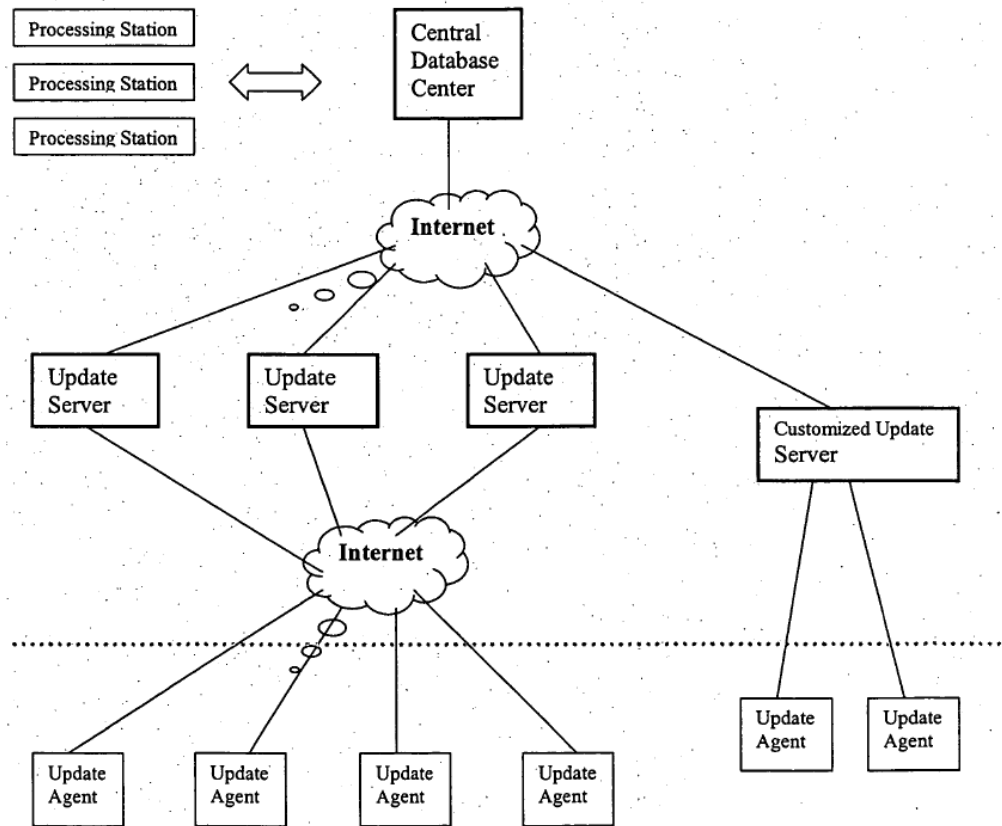
50. In my opinion, the ‘457 provisional discloses sufficient support for the “user identification” limitation. The ‘457 provisional discloses that update data, in view of which received traffic is processed, includes “spammer list.” ‘457 Provisional, § 2. To process received traffic in view of a spammer list, Update Agents must identify the user from whom the traffic originates. For example,

Update Agents would need to identify the user associated with the received traffic and compare the user to the spammer list. The ‘457 provisional thus provides support for performing “user identification” to enforce policies.

51. In my opinion, 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. 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.

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

52. I understand that 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.* I disagree. 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. The ‘457 provisional makes it clear that Processing Station and Update Agent communicate with each other to allow analysis of suspicious traffic and distribution of update data. Specifically, 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.* In my opinion, the “requests” each Update Agent forward to the Update Servers include suspicious traffic, which the Update Servers then forward to the Central Database Centre and Processing Station for analysis. In this manner, suspicious traffic can be forwarded to and analyzed by the Central Database Center and

Processing Station, and newly generated virus signature is distributed to Update Agents.

53. In my opinion, this interpretation is 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.* In this context, the “load” on an Update Station primarily includes analyzing the traffic ***forwarded to*** it from the Update Agents. 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.*

54. Therefore, it is my opinion 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”

55. In my opinion, 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*.

56. Second, 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.

57. 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.*

B. The ‘968 Patent Provides Written Description Support.

58. I understand that 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.” I disagree, for the reasons explained below.

1. “configuration data”

59. In my opinion, 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.”

60. 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.”). 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. 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.

61. 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.

62. 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.

63. Accordingly, in my opinion, the specification provides sufficient written description support for “configuration data.”

2. “user identification”

64. In my opinion, the specification describes “user identification” in at least three ways.

65. First, 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. In my opinion, 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. I also note that 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.

66. I understand that 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. Even if it were, user authentication would **necessarily entail** user identification because, to authenticate a user, one must first identify the user. As

such, in my opinion, the disclosure of “user authentication” demonstrates that the inventors possessed *at least* “user identification.”

67. 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. I understand that 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 in my opinion, 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.

68. 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.

69. Accordingly, in my opinion, the specification of the ‘968 patent (and by extension the patents from which the ‘968 patent issued as continuation and share the same specification) provides sufficient written description support.

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

A. Jordan Does Not Qualify as Prior Art.

70. As discussed in Section VI, *supra*, in my opinion, 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, I understand that 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). I understand that 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.

Second, the provisional application must provide written description support for the claimed invention. In my opinion, Petitioner failed to make either showing.

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

71. In my opinion, 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" on a "second network communication" and copying a portion of the second network communication "to generate new rules for pattern recognition activities." Jordan, cl. 1.

72. I have reviewed Petitioner's chart that purports to identify support for each limitation of Jordan's claim 1. Pet., 68. For the "pattern recognition" limitation, Petitioner cites paragraphs 16, 20, 32, 60, 61, and 64 of Jordan Provisional. *Id.* 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 ...”).

73. Accordingly, it is my opinion that 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.*

74. 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. 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.

75. 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.

76. In my opinion, even if Jordan is deemed to qualify as prior art, 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.”*

77. In my opinion, 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.

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

(a) Network Interface Device

79. 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. Under such an interpretation, the traffic filter must receive “additional content detection data” from the switch via a “network interface device.” Jordan’s system, however, does not include such a “network interface 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:”

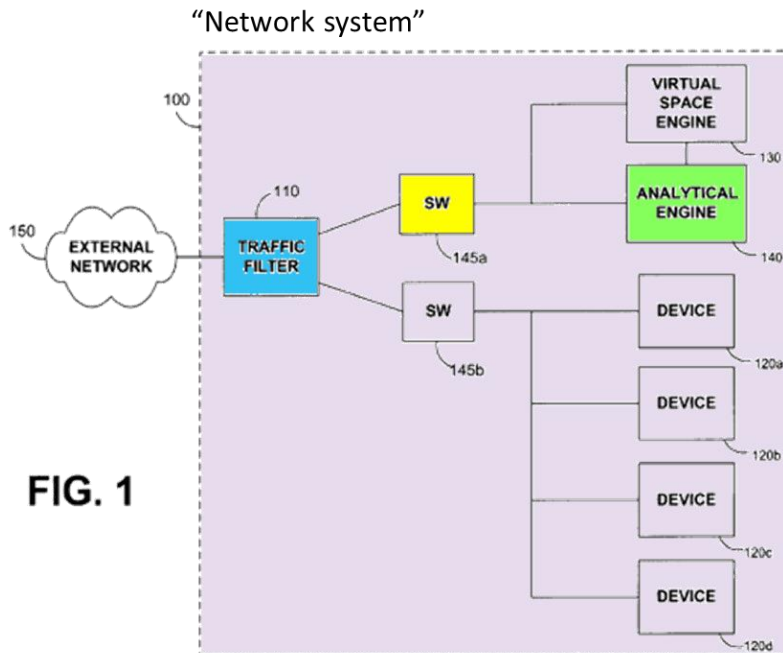


FIG. 1

Jordan, Fig. 1 (annotated).

80. 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. The transfer of data from the analytical engine to the switch and then to the traffic filter all occur internally (*i.e.*, in the network shaded in purple). 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. 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.

81. I understand that, 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.

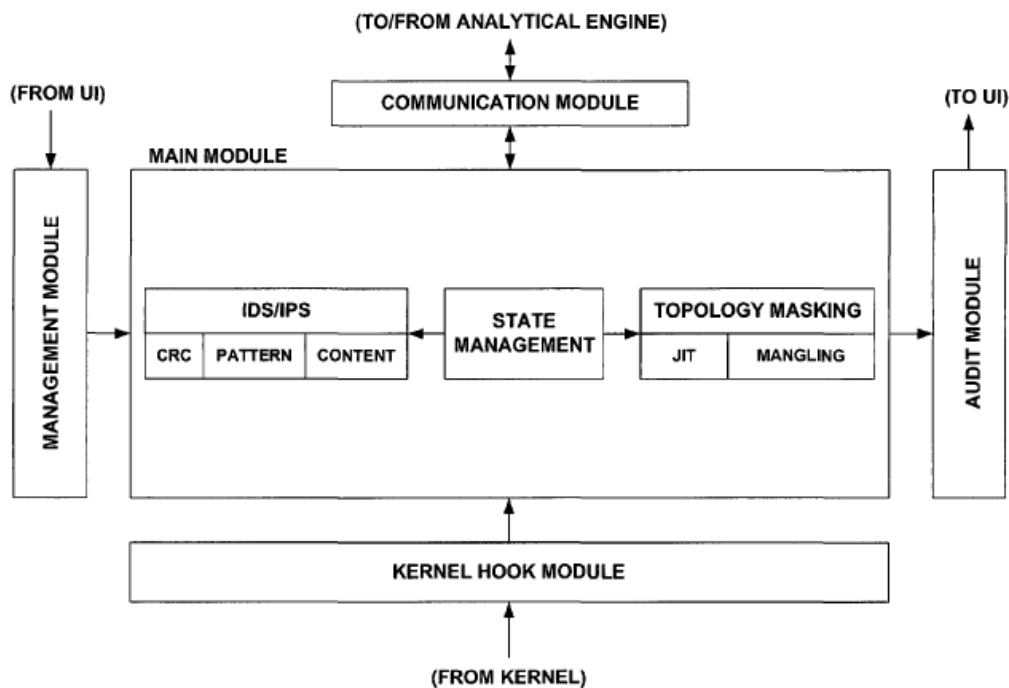


FIG. 11

Jordan, Fig. 11.

82. In my opinion, the communication module cannot be the “network interface device” via which the switch transfers additional content detection data to the traffic filter. 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.”

83. Further, while Jordan describes that the communication module is provided for communications to and from the analytical engine (*id.* 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.

84. 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.

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

85. 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. In my opinion, as discussed below, such a switch is not an “update station,” and receipt of data from such a switch is not “indirect.”

86. 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. The claims recite that a “network gateway device” (claim 1) / “data network device” (claims 4 and 7) 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. If an “update station” was simply another component in 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.” Rather, it would be through an internal router, a switch, or a communication bus.

87. The interpretation that an “update station” cannot be a component in the same network as the “network gateway device” / “data network device” is also supported by the claim requirement that content detection data be received “indirectly” from the analysis process. If having an update station as an intermediary

was all that was required for the receipt to be “indirect,” then the “indirect” limitation would be rendered superfluous because any system that includes an update station would meet that requirement. In my opinion, by reciting that the content detection data is received “indirectly,” the claims highlight that the content detection data is received through the Internet, *i.e.*, from the external network.

88. In my opinion, 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:

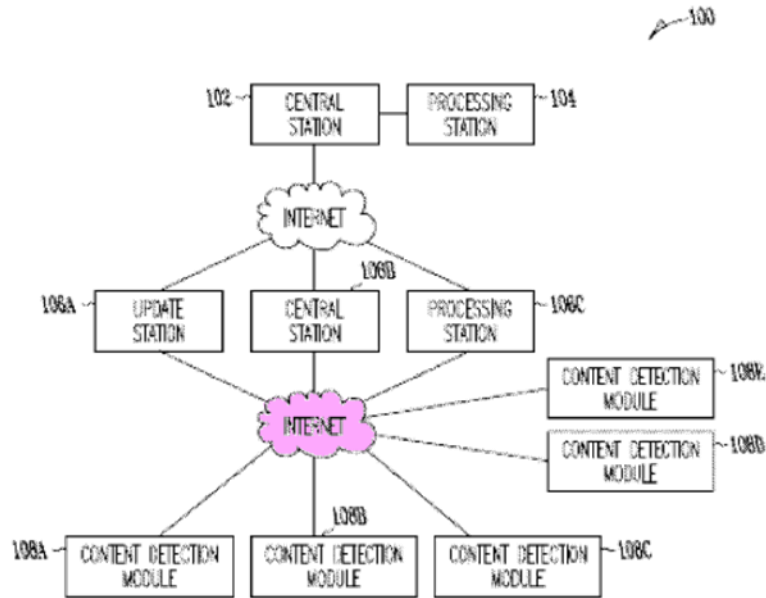


Fig. 1

89. 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. 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. As a result, an internal component such as Jordan’s switch would fail to provide the benefits of an update station.

90. In view of the claim language and the specification of the ‘968 patent, it is my opinion that 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.*

91. I understand that Petitioner attempts to combine Jordan with FortiGate on the basis that incorporating FortiGate’s FDSs (the alleged “update station”)—which push updates to the FortiGate firewalls—would “improve Jordan’s scalability.” *Id.* I disagree. A POSITA would not have been motivated to improve “scalability” of Jordan’s system. 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, adding an “update station” in the communication between the traffic filter and analytical engine would have been unnecessary. 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.

92. 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 ("The FDN is a world-wide network of FortiResponse Distribution Servers (FDSs). When your FortiGate unit connects to the FDN it actually connects to the nearest FDS."); *id.* at 117 ("You must configure your FortiGate unit and your network so that the FortiGate unit can connect to the Internet and to the FDN"). 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. 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.* In my opinion, 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.

93. Lastly, 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.

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

94. In my opinion, 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.

95. The disclosure of a “management module” also does not satisfy the claim requirement. A management module 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*.

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

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

96. In my opinion, Lee discloses a system that is fundamentally different from the invention of the ‘968 patent. Lee’s disclosures that the Petitioner points to are attributed to different “independent security agents,” not a single “network gateway device” (claim 1) or a “data network device” (claims 4 and 7) as required by the claims. In particular, the NSA monitors traffic and transfers suspicious traffic to the ISE so that a new signature is generated. Lee, ¶52. When the NSA recognizes a new attack based on the signature, “a new or modified rule” is given to FSA so

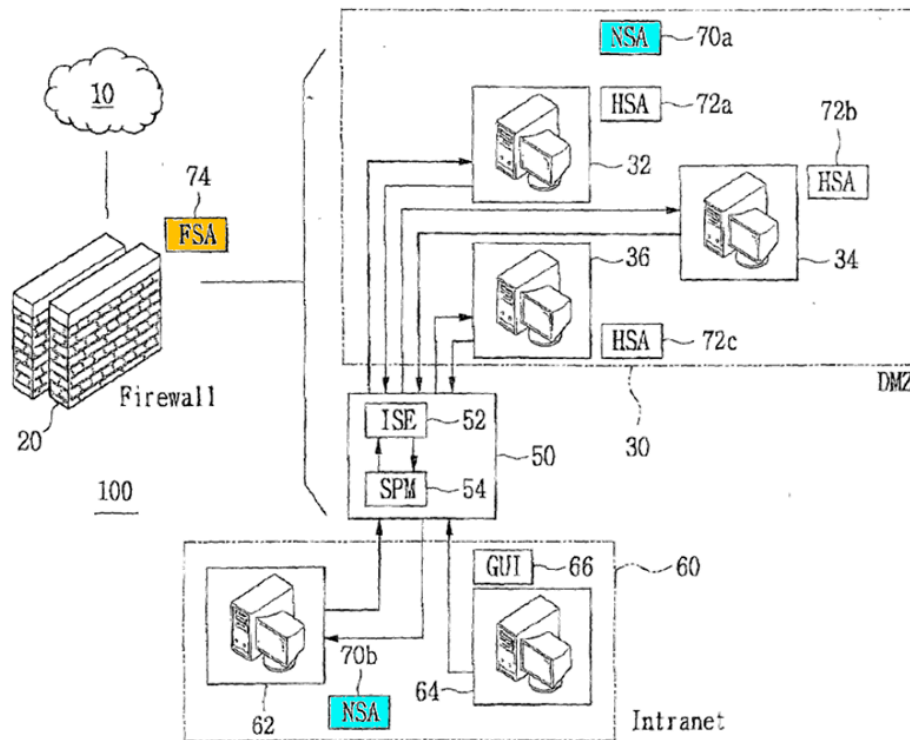
that traffic from the attacker can be blocked. *Id.*, ¶ 52. As such, Lee does not disclose a single device—“network gateway device” or “data network device”—that:

- 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. An NSA, however, does not enforce policies to determine whether to allow or block traffic; an FSA does.

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

FIG 1



Lee, Fig. 1.

98. 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 in my opinion, 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. Doing so would have been directly contrary to Lee’s stated objective and undermined the benefits of having independent security agents.

99. 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.” 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. Lee, ¶¶12, 40.

B. Magdych's Port Does Not Constitute the Claimed "Configuration Data."

100. I understand that Petitioner acknowledges 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.* I disagree that Magdych cures Lee's deficiency. 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.

101. 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.”). 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.

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

102. All Challenged Claims require a “network gateway device” / “data network device” enforcing a “policy that defines a suspicious category of network traffic.” See claim limitations 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.

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

103. In my opinion, 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. Indeed, Lee does not once mention FSA in connection with the disclosure that Petitioner relies on. *Id.* Petitioner’s assertion that FSA “could include user identification” thus lacks merit.

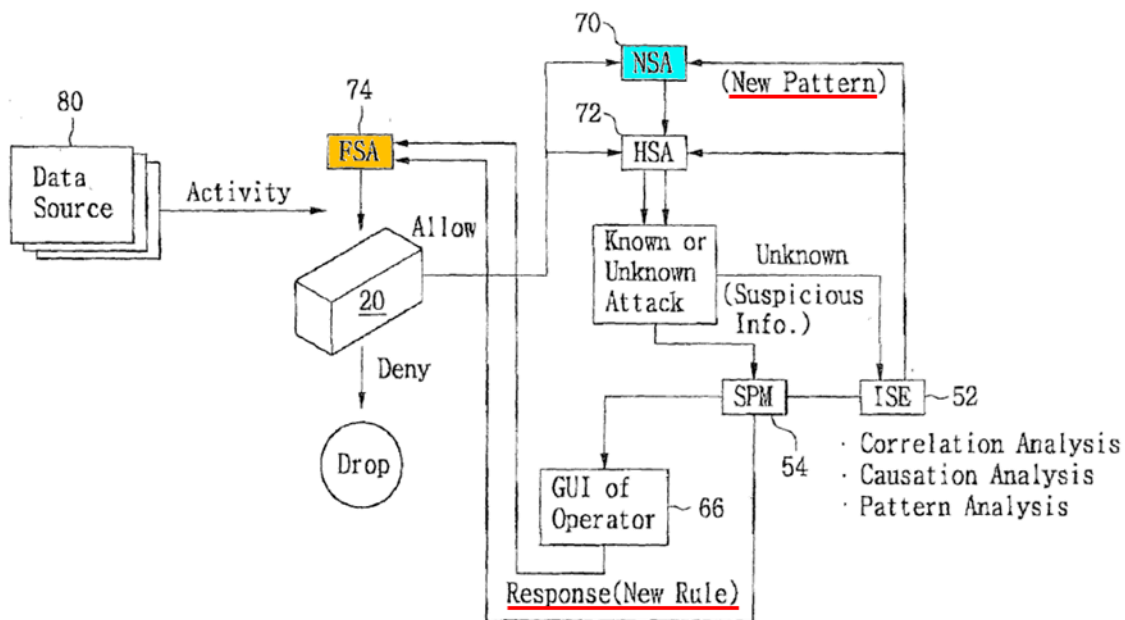
E. Lee Does Not Disclose or Render Obvious “Receiv[ing], Via The Network Interface Device, The Additional Content Detection Data Indirectly From The Analysis Process Via an Update Station.”

104. In my opinion, 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.

105. 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 ...”). Lee’s Fig. 2 also demonstrates that “new pattern” is sent only to NSA (cyan), not FSA (orange).

FIG 2



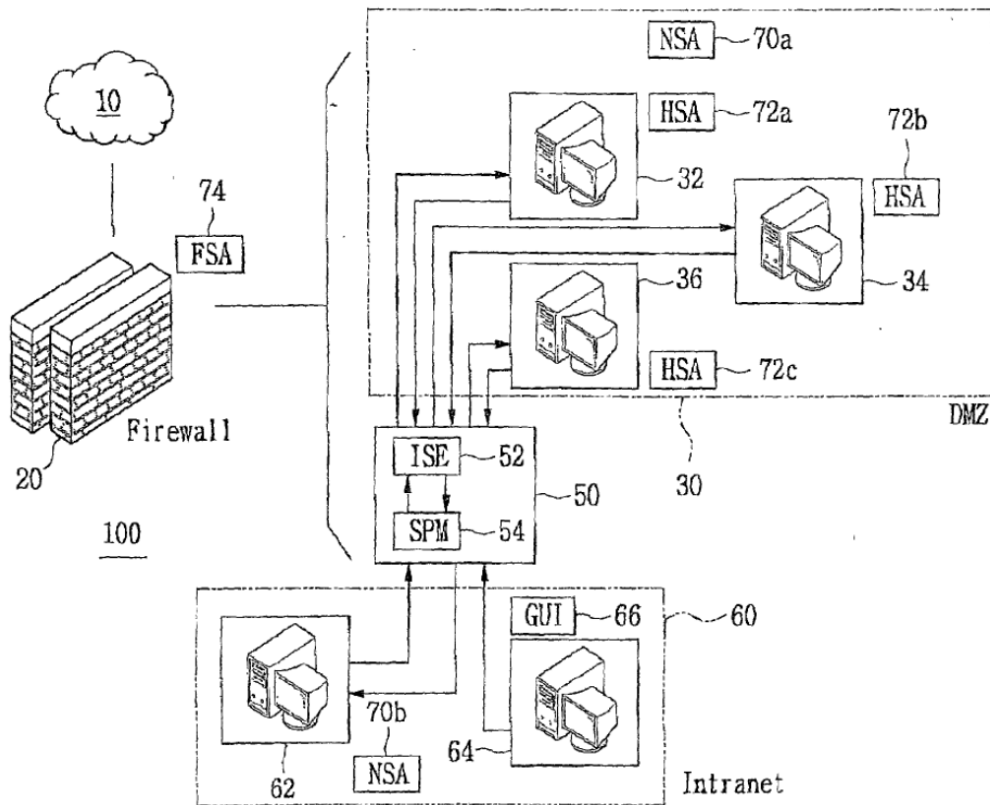
Lee, Fig. 2. Moreover, contrary to Petitioner’s assertion, an NSA is not “*in*” a firewall (the alleged network gateway device). Rather, an NSA is installed in a network secured by the firewall (*e.g.*, DMZ 30 or intranet 60). Lee, ¶37; Fig. 1. As a result, an NSA is not a “network gateway device,” and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

106. Although Lee discloses that an FSA receives from the ISE a “rule” (as opposed to a “signature”), a “rule” is not “content detection data” based on which a policy is defined. 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.” 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”).

107. 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. I disagree. 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. See Section VII.B.1(b), *supra*.

108. Third, Lee does not render obvious an FSA receiving a new rule “via the network interface device.” Lee discloses 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.” 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. These interfaces are two distinct devices, not a single “network interface device.”

109. For these reasons, it is my opinion that 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.”

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

110. 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.”

111. 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 I disagree that a “rule” can be lumped with a “signature” and treated collectively as “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.”

112. Accordingly, in my opinion, 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.

IX. GROUND 4: FANG IS NOT PRIOR ART.

113. Fang is the publication of the application No. 13/546,915, which the ‘968 patent claims priority to by a series of continuation applications. I understand that Petitioner argues that Fang is prior art because the Challenged Claims lack written description support under §112. But this is incorrect for the reasons I discussed in Section VI.B, *supra*. As a result, I understand that the ‘968 patent is entitled to the filing date of Fang, disqualifying Fang as prior art.

X. CONCLUSION

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on the information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Executed: June 20, 2023

A handwritten signature in black ink, appearing to read 'John Black Jr.', written over a horizontal line.

John Black Jr., Ph.D.