

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.
Petitioner,

v.

UMBRA TECHNOLOGIES, LTD.
Patent Owner.

U.S. Patent No. 10,574,482
Issue Date: February 25, 2020
Title: MULTI-PERIMETER FIREWALL IN THE CLOUD

Inter Partes Review No.: IPR2024-00498

**PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO.
10,574,482 UNDER 35 U.S.C. §§ 311-319 and 37 C.F.R. §§ 42.1-.80, 42.100-
.107**

Mail Stop “PATENT BOARD”
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. OVERVIEW	1
III. GROUND FOR STANDING (37 C.F.R. § 42.104(A))	5
IV. REASONS FOR THE REQUESTED RELIEF	5
A. Summary of the '482 Patent.....	5
B. Prosecution History	11
C. Claim Construction.....	13
D. Priority Date of the Challenged Claims	14
E. Person of Ordinary Skill in the Art	14
F. State of the Art	15
V. IDENTIFICATION OF CHALLENGES	19
A. Challenged Claims	19
B. Statutory Grounds for Challenges	19
VI. IDENTIFICATION OF HOW THE CHALLENGED CLAIMS ARE UNPATENTABLE	20
A. Challenge 1: Claims 1-26.....	20
1. The Shieh Reference	20
2. The Potti Reference	28
3. Detailed Application of Shieh and Potti to the Challenged Claims	29
VIII. Mandatory Notices Under 37 C.F.R. §42.8.....	64
A. Real Party-in-Interest (37 C.F.R. § 42.8(b)(1)).....	64

B.	Related Matters (37 C.F.R. § 42.8(b)(2)).....	65
1.	Judicial Matters	65
2.	Administrative Matters	65
3.	Related Patents	65
C.	Lead/Back-up Counsel (37 C.F.R. § 42.8(b)(3)):	65
D.	Notice of Service Information (37 C.F.R. § 42.8(b)(4)):.....	66
E.	GROUND FOR STANDING (37 C.F.R. § 42.204(A))	66
IX.	CONCLUSION	67

TABLE OF AUTHORITIES

PAGE(S)

CASES

<i>Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH,</i> IPR2019-01469.....	58
<i>HP Inc. v. Slingshot Printing LLC,</i> IPR2020-01084.....	62
<i>Sotera Wireless, Inc. v. Masimo Corp.,</i> IPR2020-01019.....	63

Petitioner's Exhibit List

<i>Exhibit #</i>	<i>Description</i>
1001	U.S. Patent No. 10,574,482 (“the ’482”)
1002	Prosecution history of the ’482 (“’482 File History”)
1003	Declaration of Petitioner’s Expert Petitioners expert (Narasimha Reddy)
1004	U.S. Pat. No. 8,955,093 (“Shieh”)
1005	U.S. Pat. App. Pub. No. 2007/0156919 (“Potti”)
1006	Firewall Evolution- Deep Packet Inspection, Security Focus, Ido Dubrawsky (2003) accessed at https://web.archive.org/web/20031206194534/http://www.securityfocus.com/printable/infocus/1716 (Dec. 6, 2003).
1007	Cisco Router Firewall Security, Richard A. Deal, Cisco Press, 2005
1008	Cisco ASA, All-in-One Firewall, IPS, and VPN Adaptive Security Appliance, Jazib Frahim, Cisco Press, Second Edition, 2010
1009	A 10Gb/s Firewall System for Network Security in Photonic Era, IEICE Trans. Commun., Vol. E88-B, No. 5 May 2005
1010	Security as a Service for Hybrid Clouds, Markku Vajaranta, Master of Science Thesis, May 2014
1011	Exhibit 5, Infringement Contentions for ’482 Patent, UMBRA Technologies Inc. , v. Cisco Systems Inc., USDC WD Tex, Case 1:23-cv-00903 Document 1-5, Filed 8/02/23
1012	U.S. Pat. Publ. 2012/0210417
1013	Related Patents

I. INTRODUCTION

Pursuant to 35 U.S.C. §§ 311 *et seq.* and 37 C.F.R. §§ 42.1 *et seq.*, Cisco System, Inc. (“Petitioner”) hereby petitions for an *inter partes* review of U.S. Patent No. 10,574,482 (“the ’482 Patent”). Petitioner respectfully submits that Claims 1-26 (the “Challenged Claims”) of the ’482 Patent are unpatentable under 35 U.S.C. §103 in view of the prior art references discussed herein. This Petition demonstrates by a preponderance of the evidence that there is a reasonable likelihood that Petitioner will prevail with respect to at least one of these claims. Accordingly, it is respectfully requested that the Board institute an *inter partes* review of the ’482 Patent pursuant to 37 C.F.R. § 42.108.

II. OVERVIEW

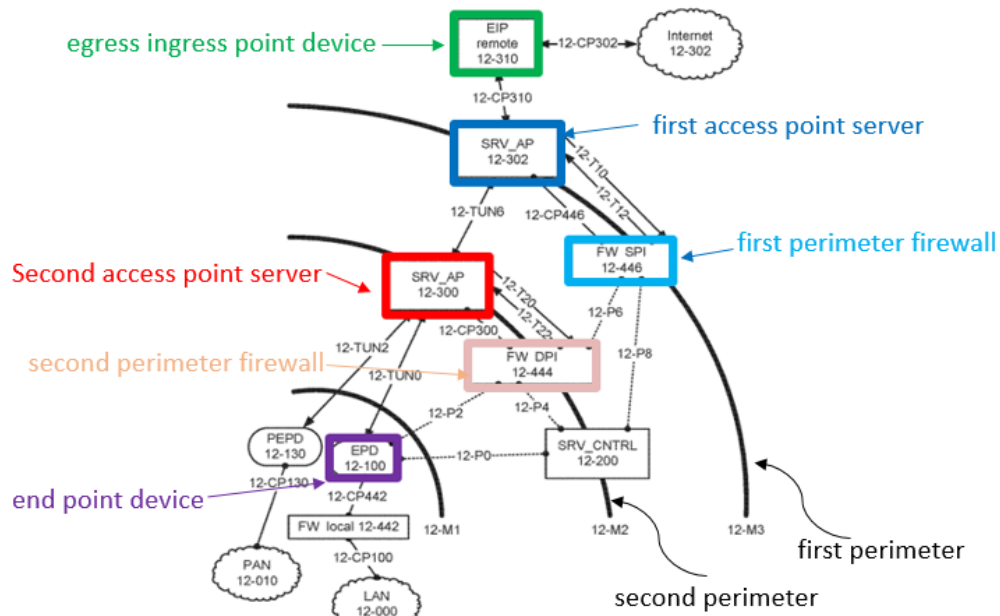
The Challenged Claims are unpatentable as obvious over the prior art. The claims are directed to a communication network having distributed firewall system in the cloud.

The distributed firewall system provides a layered defense by pairing a first access point server with a first perimeter firewall that performs stateful packet inspection, and then a second access point server with a second perimeter firewall that does deep packet inspection. Packets traversing the network are subject to stateful packet inspection at the first perimeter firewall, which prevents some traffic from passing to the second access point server. The second perimeter

firewall then performs deep packet inspection on the traffic that passed from the first access point server to the second access point server. The deep packet inspection is performed on a cloned copy of the traffic in order to avoid interrupting the flow of traffic through the network. This claimed architecture functionality already existed in the prior art. *EX-1003* ¶ 28.

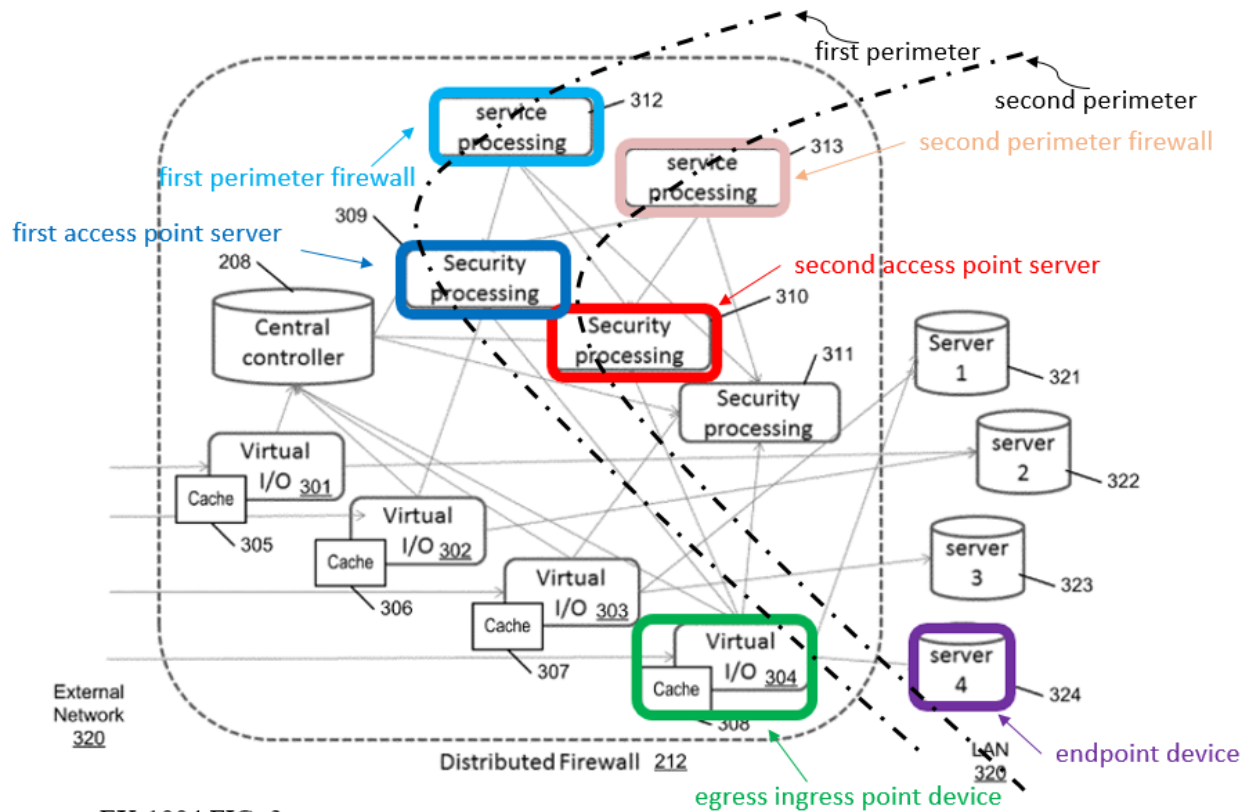
For example, the prior art Shieh reference is directed to a communication network having a distributed firewall system in the cloud. Shieh includes a parallel disclosure to that of the '482 Patent in that it is directed to the same problem and provided the same solution as the '482 Patent, the only difference being that Shieh uses different words to describe the identical concepts described and claimed in the '482 Patent. *EX-1003* ¶ 29.

As illustrated below, the architecture shown in FIG. 12 of the '482 Patent is substantially identical to the architecture shown in FIG. 3 of Shieh with common elements being colored with the same color.



EX-1001 FIG. 12

FIG. 12



EX-1004 FIG. 3

FIG. 3

The first access point sever (blue) and first perimeter firewall (light blue) for performing stateful packet inspection in the '482 Patent (FIG. 12) are called the security processing module 309 (blue) and service processing module 312 (light blue), respectively, in Shieh (FIG. 3). The second access point server (red) and second perimeter firewall (pink) for performing deep packet inspection in the '482 Patent (FIG. 12) are called the security processing module 310 (red) and service processing module 313 (pink), respectively, in Shieh (FIG. 3). The egress ingress point device (green) and endpoint device (purple) of the '482 Patent are called virtual input/output module 304 (green) and server 324 (purple), respectively. *EX-1003* ¶ 31.

As described in more detail below, Sheih discloses in its cloud based distributed firewall system, a myriad of firewall functionality, including network address translation, stateful inspection and deep patent inspection. *EX-1004* 3:5-14; *EX-1003* ¶ 32.

The only feature recited in the Challenged Claims but not expressly disclosed in Sheih was the well-known concept of performing deep packet inspection *on a copy* of the packets traversing the network. Indeed, a POSITA understood that performing deep packet inspection on a copy of the packets traversing the network was a well-known method that avoided interrupting the flow of traffic through the network while the time and resource intensive deep

packet inspection was performed, as demonstrated by the prior art Potti reference.

EX-1003 ¶ 33.

Because there are no material differences between the architectures disclosed in the '482 Patent and the combination of Shieh and Potti, the Challenged Claims are unpatentable as obvious over Shieh and Potti. *EX-1003* ¶ 34.

III. GROUNDS FOR STANDING (37 C.F.R. § 42.104(A))

Petitioner certifies that the Patent for which review is sought is available for post grant review and that Petitioner is not barred or estopped from requesting a post grant review of the Challenged Claims on the grounds identified herein. 37 C.F.R. § 42.104(a). This Petition is filed pursuant to 37 C.F.R. § 42.106(a).

IV. REASONS FOR THE REQUESTED RELIEF

As explained in §§ II and VI-VIII of this Petition and in the attached Declaration of Petitioner's Expert, Petitioners expert (Narasimha Reddy), *EX-1003*, the distributed firewall system as described and claimed in the '482 Patent, is obvious over the prior art to a person of ordinary skill in the art ("POSITA") at the time of the invention.

A. Summary of the '482 Patent

The '482 Patent is directed to network security which protects the flow of traffic by the strategic positioning of distributed firewall devices placed at multiple perimeters in the cloud. *EX-1001* 1:15-19. The '482 Patent describes that it is an

improvement upon the standard use of firewalls through increasing their utility value by extending perimeters into the cloud. *EX-1001* 5:56-58; *EX-1003* ¶ 196.

The '482 Patent describes several advantages of a cloud based firewall systems. For example, locating a multi-perimeter firewall in the cloud allows identifying and isolating problem traffic at a point upstream from the location of a traditional firewall, and thus identifies problem traffic before it reaches the “last mile” connection network that tends to be slower than the backbone network. *EX-1001* 11:4-16. Further, cloud based firewalls are dynamically scalable via cloud firewall load balancing mechanisms that can bring more resources online as needed. *EX-1001* 11:20-22. In addition, the '482 Patent describes that a cloud based firewall offers the advantage of running different firewall mechanisms, such as stateful packet inspection and deep packet inspection, simultaneously. *EX-1001* 11:43-45; *EX-1003* ¶ 197.

FIG. 12 of the '482 Patent as annotated (Annotated FIG. 12) illustrates one embodiment of a multi-perimeter firewall in the cloud for protecting a flow of traffic through a network. *EX-1003* ¶ 198.

The '482 Patent describes that in one embodiment, the first firewall performs stateful packet inspection, and the second firewall performs deep packet inspection. *EX-1001* 2:59-61. The '482 Patent describes that when performing stateful packet inspection, the firewall examines the headers of packets to identify offending information while it ignores the payload of the packets. The '482 Patent explains that the advantages of stateful packet inspection over deep packet inspection are that it is fast and that it consumes lower processor, RAM and resources. The disadvantage is that the firewall does not look at the content within the payload of the packet(s). *EX-1001* 9:67-10:4; *EX-1003* ¶ 200.

On the other hand, deep packet inspection looks beyond and examines the content, e.g. payload of the packets. The advantages are that this examination is more comprehensive in providing visibility into content both within the payload of not just one packet but from a compilation payload from a series of multiple packets. The disadvantage of DPI is that it is significantly slower than stateful packet inspection and also that it consumes considerably more processor, RAM, and other resources than stateful packet inspection. *EX-1001* 10:5-15; *EX-1003* ¶ 201.

The '482 Patent describes that stateful packet inspection firewalls are devices through which the traffic flows, while deep packet inspection firewall devices can either be flow through or can analyze cloned copies of traffic offering

the option for deep packet inspection functionality as a trailing indicator. If harmful traffic is detected, it can be subsequently blocked once identified. A benefit of the communication between devices is that information about bad traffic sources identified by deep packet inspection firewalls can be messaged to stateful packet inspection firewalls to be blocked there. *EX-1001* 12:65-13:6. The '482 Patent describes the known benefit of analyzing cloned traffic as offering trailing results of time- and resources-expensive detection operations such as deep packet inspection without impeding the speed of the flow of traffic. *EX-1001* 13:24-27; *EX-1003* ¶ 202.

The '482 Patent describes that the distributed firewalls can be located at multiple boundaries in the cloud between a client location and their link to the internet. With reference to Annotated FIG. 12, the second perimeter 12-M2 (solid black line) is a boundary in the at a data center in close proximity to the second access point server (SRV_AP 12-300), and the first perimeter is another boundary at either the same data center as the second access point server (SRV_AP 12-300) or at another location in close proximity to the first access point server (SRV_AP 12-302), possibly in another region. *EX-1001* 13:64-14:4; *EX-1003* ¶ 203.

The '482 Patent describes that in one embodiment, an access point server may also perform firewall services. *EX-1001* 2:46-48; *EX-1003* ¶ 204.

The '482 Patent describes that in some embodiments, the first firewall and the second firewall share threat information including at least one of heuristic patterns, signatures of known threats, known malicious source IP addresses, or attack vectors. The threat information may be shared via a central control server. *EX-1001* 2:49-58; *EX-1003* ¶ 205.

The '482 Patent describes that in some embodiments, at least one of the firewalls includes a cloud firewall load balancer that can allocate cloud firewall resources on demand. *EX-1001* 2:65-67; *EX-1003* ¶ 206.

The '482 Patent includes 26 claims. Claims 1 and 13 are independent system claims directed to the embodiment illustrated in FIG 12 above. The remaining claims are dependent claims that ultimately depend from Claims 1 or 13. Claim 1 is representative:

1. A multi-perimeter firewall system located in a cloud and forming part of a global virtual network, comprising:
 - an egress ingress point device;
 - a first access point server in communication with the egress ingress point device;
 - a second access point server in communication with the first access point sever;
 - an endpoint device in communication with the second access point server;
 - a first perimeter firewall in communication with the first access point server, wherein the first perimeter firewall performs stateful

packet inspection to prevent at least some traffic from passing from the first access point server to the second access point server; and

a second perimeter firewall in communication with the second access point server, wherein the second perimeter firewall performs deep packet inspection to prevent at least some traffic from passing from the second access point server to the end point device,

wherein at least one of the egress ingress point device, the first access point server, the second access point server, the endpoint device, the first perimeter firewall, or the second perimeter firewall comprises hardware,

wherein the deep packet inspection is performed on a cloned copy of traffic that flows through the second perimeter firewall.

B. Prosecution History

During prosecution, all claims were rejected under 35 USC 101. In response, the Applicant argued that Claim 1 is directed to a multi-perimeter firewall system that employs at least two perimeter firewalls that prevent some traffic from passing among different locations. Applicant further argued that using two firewalls in series in the path of communications means that the amount of packets that need to be scanned by each individual firewall can be reduced. The applicant argued that this can correspondingly reduce the computational resources required to implement each individual perimeter firewall, which the applicant identified as an “an improvement in the technical area of the firewall system.” *EX-1002* p. 24.

In the next Office Action, the 101 rejection was maintained, with the examiner stating, “[T]he claim is considered to be directed towards software per se and is therefore, non-statutory. Applicant may overcome this rejection by specifically defining one or more of the devices, servers and firewalls as hardware.” Further, the independent claims were rejected as obvious over Uchida (U.S. Pub. No. 2002/0046253) in view of Feghali (U.S. Pub. No. 2015/0128246).

In response to the 101 rejection, the Applicant amended claim 1 to recite “hardware”, and in response to the 103 rejection the applicant amended claim 1 to recite that the first firewall performs stateful packet inspection and the second firewall performs deep packet inspection as follows:

1. (Currently amended) A multi-perimeter firewall system located in a cloud and forming part of a global virtual network, comprising:
 - an egress ingress point device;
 - a first access point server in communication with the egress ingress point device;
 - a second access point server in communication with the first access point sever;
 - an endpoint device in communication with the second access point server;
 - a first perimeter firewall in communication with the first access point server, wherein the first perimeter firewall performs stateful packet inspection to prevent[[s]] at least some traffic from passing from the first access point server to the second access point server; and
 - a second perimeter firewall in communication with the second access point server, wherein the second perimeter firewall performs deep packet inspection to prevent[[s]] at least some traffic from passing from the second access point server to the end point device,
 - wherein at least one of the egress ingress point device, the first access point server, the second access point server, the endpoint device, the first perimeter firewall, or the second perimeter firewall comprises hardware.

EX-1002 p. 62.

In response to the amendment, the examiner made an examiner's amendment to add to both independent claims the limitation "wherein the deep packet inspection is performed on a cloned copy of traffic that flows through the second perimeter firewall" and issued a Notice of Allowance. The examiner did not recite any specific reason for allowance (other than repeating the entire claim) but did note that "Applicant's amendments (and Examiner's amendments herein below) are sufficient to overcome the claim rejections under 35 U.S.C. 103 set forth in the previous Office Action." *EX-1002* p. 87.

C. Claim Construction

Petitioner proposes that each claim term in the Challenged Claims be given its plain and ordinary meaning in this proceeding, and that no specific construction of any claim term is required because the prior art relied on in this Petition meets each of the claim terms under any reasonable construction.

It is noted that this interpretation is only applicable to the *inter partes* review sought herein and should not be construed as constituting, in whole or in part, the Petitioner's own interpretation of any claims for any other purposes, including any litigation. Accordingly, Petitioner expressly reserves the right to present an interpretation of a claim term in other proceedings, which is different, in whole or in part, from that presented in this Petition.

D. Priority Date of the Challenged Claims

The application that issued as the '482 Patent was filed September 29, 2017 claiming priority to provisional application No. 62/151,174 filed on April 22, 2015 and to provisional application No. 62/144,293 filed on April 7, 2015. Patent Owner bears the burden of establishing priority to the provisional applications.

The prior art cited below predates the earliest possible priority date, April 7, 2015, and thus for purposes of this Petition, this issue is moot.

E. Person of Ordinary Skill in the Art

With respect to the '482 Patent, a POSITA in April 2015 timeframe would have been familiar with communication networks having a distributed firewall system in the cloud. *EX-1003* ¶ 40. A POSITA would have a working knowledge of the function performed by firewalls including stateful inspection and deep packet inspection. *EX-1003* ¶ 40.

A POSITA would have gained knowledge of these concepts through a mixture of training and work experience, such as by having a Bachelor's degree in computer science and two years of experience; or by obtaining a Master's degree in computer science, but having only one year of experience; or by having no formal education but experience in computer network security of at least four years. *EX-1003* ¶ 40.

F. State of the Art

The following section describes the state of the art for distributed firewalls as of April 2015. The prior art references, and the discussions of what was known to a POSITA, provide the factual support for the general description of the state of the art at the time of the invention, and provide additional motivation to modify or combine the references. Accordingly, these references should be considered by the Board. *EX-1003* ¶ 42.

1. Firewalls

By April 2015, firewall technology was very well developed and decades old. Firewalls provided a variety of services to networks in terms of security. They provided for network address translation (NAT), they helped establish virtual private networks (VPN), and filtered traffic that did not conform to the network's stated security policy. *EX-1006* p. 1. *EX-1003* ¶ 43.

Firewalls control the flow of traffic to protect a communication network from security threats at defined boundary points, whether at the perimeter between a public and private network, or between different areas of a network. *EX-1007* pp. 42, 91.

A POSITA understood that a computer network security design typically uses a layered defense approach of multiple firewalls so that if one layer is

compromised the entire network is not exposed to the security threat. *EX-1007* pp. 83-84, *EX-1003* ¶ 45.

Known firewalls included stateful inspection firewalls and deep packet inspection firewalls. By the mid-to-late 1990s, stateful inspection had become an industry standard. *EX-1003* ¶ 46. Stateful inspection provided for the analysis of packets at the network layer as well other layers (typically the transport layer in the OSI model but the firewall looked at layers above that as well) in order to assess the overall packet. By combining information from various layers (transport, session, and network) the firewall was better able to understand the protocol it was inspecting. This also provided for the ability to create virtual sessions in order to track connectionless protocols such as UDP-based applications as well as RPC-based applications. *EX-1006* p. 2.

Stateful firewalls keep track of the state of a connection: whether the connection is in initiation, data transfer, or termination state. *EX-1007* p. 53-54. Stateful firewalls use a state table as a mechanism to keep track of the state of a connection. *EX-1007* p. 59.

Deep packet inspection (DPI) has also been around for over twenty years. *EX-1003* ¶ 48. Deep packet inspection looked within the application payload of a packet or traffic stream and made decisions on the significance of that data based on the content of that data. The engine that drives deep packet inspection typically

included a combination of signature-matching technology along with heuristic analysis of the data in order to determine the impact of that communication stream. *EX-1006* p. 2. Deep packet inspection could be used to detect and prevent cyberattacks, combat malware, optimize servers to reduce overhead, and analyze user behavior. Deep packet inspection could be inline, where a packet was inspected and if it satisfied the configured security policies the packet would be forwarded to its destination. *EX-1003* ¶ 49. Or the packet inspection could be offline, where a copy of the packet is sent for further analysis, while the original packet is forwarded to its destination. *EX-1008* pp. 617-618. Offline analysis permitted further analysis for traffic patterns and implementing advanced security functions without slowing down the original traffic, including IP logging, shunning (blocking packets) and anomaly detection. *EX-1008* pp. 650-669. For example, deep packet inspection could be used to identify malicious content, and then an IP address as the source of that malicious content, and then the IP address would be sent to other firewalls to block or drop packets from this IP address. *EX-1008* pp. 659-666. *EX-1003* ¶ 51.

The sharing of threat information between firewalls was also well-known and was sometimes referred to as “attack information advertising” and was critical to ensure that firewalls on the perimeter take countermeasures to prevent malicious packets from entering the network. *EX-1009* p. 1915. *EX-1003* ¶ 52.

It was well-known to use multiple layers of firewalls because it defended the network more efficiently and thus provided a safer environment. *EX-1003* ¶ 53.

For example, it was known to layer firewalls for network defense from the lightest to the heaviest solution. A packet filter firewall was placed on the perimeter of the network and the Internet, typically in a router which required little capacity and could handle large amounts of data. Stateful firewalls were then placed behind the packet filter to maintain the session tables and protected against attacks let through by the packet filter. Because some traffic was blocked by the stateless (packet filter) firewall, it lightened the load on the stateful firewall. Deep packet inspection firewalls, used to examine the content for undesired patterns or messages specified by the network administrator, were then placed in front of the servers requiring highest security. *EX-1010* p. 7. A POSITA understood that because some traffic was blocked by the stateful firewall, it lightened the load on the deep packet inspection firewall. *EX-1003* ¶ 53.

It was also known that deep packet inspection could be integrated with a stateful firewall with intrusion detection and prevention systems. *EX-1003* ¶ 54. The stateful firewall examined the received packet and the intrusion detection system would inspect the message carried. The DPI provided significant benefit when compared to a traditional stateful firewall system because the message is also inspected for fraud patterns. *EX-1010* p. 8.

2. Distributed Firewalls in the Cloud

Cloud computing generally refers to the on-demand availability of computer system resources, especially data storage and computing power. Large clouds often have functions distributed over multiple locations, and rely on sharing of resources to achieve coherence and typically use a pay-as-you-go model. *EX-1003*

¶ 55. For over a decade, as more computing resources were located in the cloud, firewall security services were also moved to the cloud, and the virtual firewall usually became the best choice because the cloud was meant to offer on-demand service for the user with the pay-as-you-go-model. *EX-1010* pp. 24-27.

V. IDENTIFICATION OF CHALLENGES

A. Challenged Claims

Claims 1-26 of the '482 Patent are challenged in this Petition.

B. Statutory Grounds for Challenges

The Challenges are set forth in detail below and summarized as follows:

Ground	Claims	Basis	Reference
1	1-26	§ 103	Shieh in view of Potti

Ground 1: Claims 1-26 of the '482 Patent are invalid as being obvious over Shieh in view of Potti.

U.S. Pat No. 8,955,093 titled “Cooperative Network Security Inspection” issued on February 10, 2015, from Application No. 13/860,408 filed on April 10,

2013 (“Shieh”) (*EX-1004*). Shieh qualifies as prior art under 102(a)(1)(AIA) and was not considered by the examiner during prosecution, nor was it previously considered by the Board.

U.S. Patent Publication No 2007/0156919 titled “Enforcing Network Service Level Agreements In A Network Element” published on July 5, 2007 from Application No. 11/473,298 filed on June 21, 2006. (Potti) (*EX-1005*). Potti qualifies as prior art under 102(a)(1)(AIA) and was not considered by the examiner during prosecution, nor was it previously considered by the Board.

VI. IDENTIFICATION OF HOW THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Challenge 1: Claims 1-26

1. The Shieh Reference

Shieh is directed to providing network security using distributed firewalls in the cloud. FIG. 1 is a block diagram illustrating an example of network configuration according to one embodiment of the invention. *EX-1004* 2:60-62.

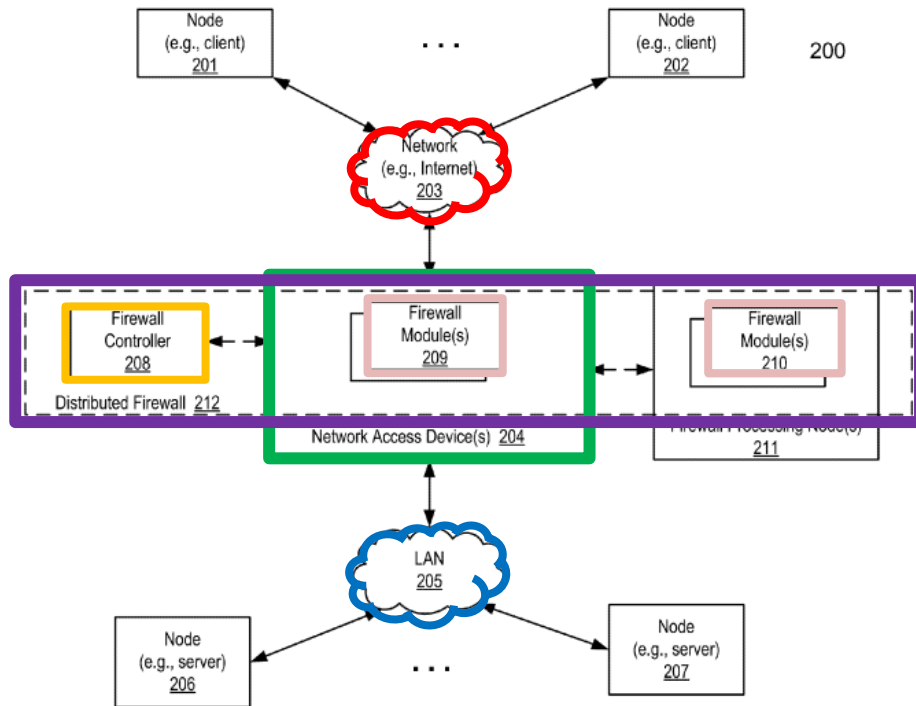


FIG. 1

Network access device 204 (green), which may be a router, gateway, switch access point, etc., provides an interface at the perimeter between a public network 203 (red) and private network 205 (blue). As shown in FIG. 1, network 203 may be an external network such as a wide area network or internet while network 205 represents a local area network (LAN). *EX-1004* 2:62-67; FIG. 1.

Nodes 206-207 go through gateway device 204 (labeled “Network Access Device(s) 204” in FIG. 1 above) in order to reach nodes 201-202, or vice versa. Any of nodes 201-202 and 206-207 may be a client device (e.g., a desktop, laptop, smartphone, gaming device) or a server. *EX-1004* 2:67-3:4.

According to one embodiment, network access device 204 is associated with a distributed firewall 212 (purple) that includes various firewall processing modules (pink), for example, each being executed within a virtual machine (VM). In one embodiment, each firewall module is responsible for performing one or more firewall functions, but it does not include all of the firewall functions of a firewall. Examples of the firewall functions include, but are not limited to, network address translation (NAT), virtual private network (VPN), deep packet inspection (DPI), and/or anti-virus, etc. *EX-1004* 3:5-14.

In one embodiment, some of the firewall processing modules are located within network access device 204 (e.g., firewall modules 209) and some are located external to network access device 204 (e.g., firewall modules 210 maintained by firewall processing node(s) 211, which may be a dedicated firewall processing machine). All of the firewall modules 209-210 are managed by firewall controller 208 (orange), which may be located within network access device 204, or external to network access device 204. *EX-1004* 3:14-22. Shieh describes that each of the firewall modules may be implemented in a virtual machine, which may be located in the cloud. *EX-1004* 3:3:23-30; 9:12-15. Shieh describes that using such modules in a firewall cloud provides a security design that is best-fit for the emerging cloud computing, and provides great scalability and system availability. *EX-1004* 9:33-36.

Shieh describes a more detailed embodiment of the distributed firewall system in FIG. 3:

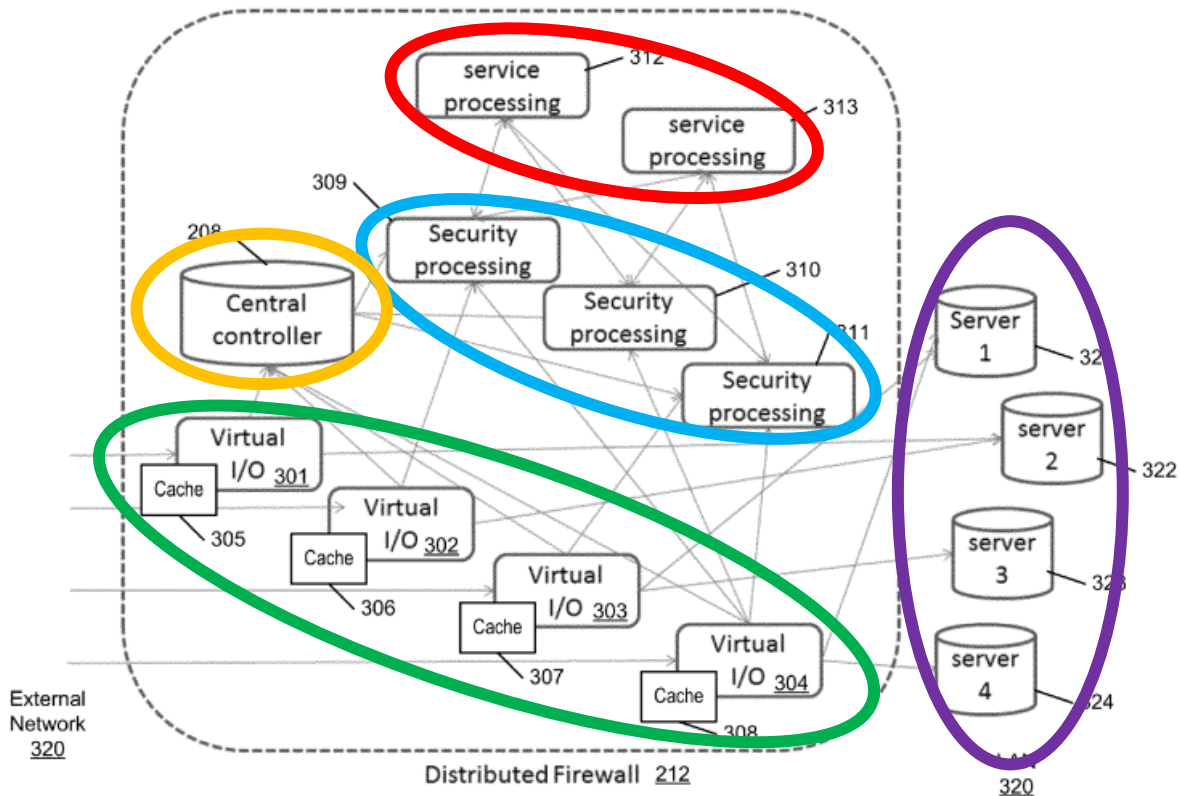


FIG. 3

Distributed firewall 212 includes, four different types of modules: virtual I/O modules 301-304 (green), security processing modules 309-311 (blue), service processing modules 312-313 (purple), and central controller 208 (orange). All modules can run on the same virtual machine, or on different virtual machines, or on same or different physical hosts. Some or all of modules 301-304 and 309-313 may be executed within a virtual machine. Dependent upon the specific

configuration, each of modules 301-304 and 309-313 may be executed by a respective virtual machine. In other configurations, multiple of modules 301-304 and 309-313 may be executed by the same virtual machine. *EX-1004* 7:11-30. Shieh describes that a virtual machine is software hosted on a server for performing the functions for the different types of modules. *EX-1004* 3:41-43; 11:33-36.

Shieh describes that the modules could be distributed in different networks, even on different locations, as long as the modules can reach the module that is next in terms of processing and the central controller. In one embodiment, virtual I/O modules and corresponding security processing modules are in a public cloud and the central controller is in a private cloud. This configuration may provide the flexibility to secure and control packets coming from the public cloud, and allow central controller to have an overall view of traffic from the Internet as well as from an internal network. *EX-1004* 9:9-18.

Each of virtual I/O modules 301-304 (green) receives packets from any of servers 321-324 of LAN 320 and sends packets to external network 315 outside of the firewall. In one embodiment, each of I/O modules 301-304 keeps a local cache (e.g., caches 305-308) storing location(s) of a security processing module(s) (e.g., security processing modules 309-311) for each connection session. A cache maintained by each I/O module contains a forwarding table mapping certain

connection sessions to any of security modules 309-311. Upon receiving a packet, an I/O module performs a packet classification to find out the associated connection and forwards the packet to the corresponding security processing module identified by the forwarding table. *EX-1004* 7:32-45.

In one embodiment, each of security processing modules 309-311 (blue) performs major security processing functions, such as, for example, network address translation (NAT), virtual private network (VPN), deep packet inspection (DPI), and/or anti-virus, etc. A security processing module receives packets and runs the packets through one or more various security functions in the module for security processing. There could be several security modules and each handles the same or different security functions. *EX-1003* ¶ 69. If the packets need to go through another security or service processing, the module sends the packets to the other modules. Optionally, it can run the packets through a load balancing mechanism to distribute the load to multiple modules. If a module is the last processing module in the chain to process the packets, it can forward the packets back to the virtual I/O module to send out, or send the packet out directly to its destination if it's configured to do so. *EX-1004* 7:53-67.

In one embodiment, each of service processing modules 312-313 (red) performs one or more of the functions of security processing module, such as, for example, NAT, VPN, DPI, and/or anti-virus, etc. However, the service processing

module is different from the security processing module in that it only receives and sends packets to the same security processing module. *EX-1003* ¶ 70. If the tasks cannot be done in a security processing module, for example, due to a resource limitation, system load, or the requirement of a different operation system, the packets can be forwarded to one or more of service processing modules 312-313 for further processing. The packets then are sent back to the same security processing module for the next security function processing. To further share the system load, any of security processing modules 309-311 can load balance the computational-intensive services using multiple service processing modules. *EX-1004* 8:1-16.

If a module is the last processing module in the chain to process the packets, it can forward the packets back to the virtual I/O module to send out, or send the packet out directly to its destination (purple) if it is configured to do so. *EX-1004* 7:64-67.

In one embodiment, central controller 208 (orange) is the central place to control forwarding of the packets amongst I/O modules 301-304, security processing modules 309-311, and service processing modules 312-313. When a virtual I/O module receives a packet, according to one embodiment, it forwards the packet to central controller 208 if it cannot find an existing connection in its local cache. When central controller 208 receives the packet, it decides which of

security processing modules 309-311 is able to process the packets, and then forwards the packets to the designated security processing module. It also instructs the virtual I/O module to create the local cache to store connection state information so the subsequent packets of the same connection session do not need to be forwarded to central controller 208: rather, they can be directly forwarded to the proper security processing module identified in the cache. *EX-1004* 8:17-33.

Shieh describes the following benefits and improvements of using a distributed firewall system in the cloud:

- By dividing a firewall into different modules, it allows putting virtual I/O and security processing functions at the best locations to protect the network entrance, while keeping the central control and monitoring functionality at the central controller. *EX-1004* 8:33-37.
- It enhances the scalability of the system since all modules can be expanded to multiple instances to share the system load. *EX-1004* 8:37-39.
- The distributed firewall can employ a significantly large amount of CPU and memory resources for service processing and protect the networks at multiple geometric locations. *EX-1004* 9:19-23.
- The central controller decides which security processing module is capable of processing particular connection, and is able to start a new

security processing at the place deemed best for packet processing. As a result, the location of the packet I/O is not limited on a single appliance. The I/O modules can be placed anywhere as virtual machines. *EX-1004* 9:24-30.

- The security processing power is significantly higher as packets and connections can be load balanced to any number of the security processing modules, and the modules could be added or deleted dynamically. *EX-1004* 9:30-33
- Using such modules in a firewall cloud provides a security design that is best-fit for the emerging cloud computing, and provides great scalability and system availability. *EX-1004* 9:33-36.

2. The Potti Reference

Potti is generally directed to enforcing service level agreements in a network infrastructure element, by giving some packets priority over other packets based on the contents of the packets. *EX-1005* Abstract, ¶ 0344. Potti discloses that to determine whether one or more conditions of a service level agreement are violated, deep packet inspection of packets is required. Because deep packet inspection can be time consuming and interrupt traffic flow, Potti discloses receiving packets in the network element, forwarding the packets to a next hop, and concurrently copying the packets without modification and without

interrupting the flow of traffic through the network element. The copied packets are subjected to deep packet inspection in which values of the IP header, TCP header and application-layer payload are examined. *EX-1005* ¶0345. Performing DPI on copied packets rather than packets in the traffic flow is consistent with the State of the Art section described above, that offline packet inspection allows further analysis without interrupting traffic flow. *EX-1003* ¶ 81.

3. Detailed Application of Shieh and Potti to the Challenged Claims

a. Claim 1

[1.0] A multi-perimeter firewall system located in a cloud and forming part of a global virtual network, comprising:

To the extent the preamble is limiting, Shieh discloses a distributed *firewall system located in a cloud* using virtual machines located at several perimeters. For example, Shieh discloses network access device 204 is associated with a distributed firewall 212 that includes various firewall processing modules, for example, each being executed within a virtual machine (VM). *EX-1004* 3:5-7. Further, Shieh discloses that all of the firewall modules 209-210 are managed by firewall controller 208, which may be located within network access device 204, or external to network access device 204, such as, for example, in a public cloud associated with network 203, or in a private cloud associated with network 205. Controller 208 and firewall processing modules 209-210 collectively are referred

to as distributed firewall 212. *EX-1004* 3:20-26. Shieh discloses that the security processing modules can be the endpoints of virtual private networks (*virtual network*) capable of performing firewall functionality such as VPN processing. *EX-1004* 3:5-14. Further, Shieh discloses that each of network access devices, including the firewall modules, maintains a persistent connection such as secure connections or tunnels with a controller or management entity. *EX-1004* 4:14-18. Shieh discloses in FIG. 3 that all of the firewall modules are located functionally at perimeters between an internal network an external network (*multi-perimeter firewall system*). See also FIG 2 (internal network 205 and external network 203). Shieh discloses that by dividing a firewall into different modules, and placing them at various geographic locations in the network, it increases security at the network entrance, while keeping the central control and monitoring functionality at the central controller, and enhances the scalability of the system. *EX-1004* 8:33-42; 9:9-18.

A POSITA understood that each of the four types of modules described by Shieh would be implemented in virtual machines distributed in the cloud at various geographic locations and would be considered part of a *global virtual network*. *EX-1003* ¶ 89. This is consistent with the '482 Patent's disclosure that the firewalls are virtualized in the cloud and the perimeters are located between the client and the internet at each firewall. *EX-1001* 11:17-25; 13:64-14:4. Shieh's disclosure is

also consistent with PO's infringement contentions, e.g., "By delivering security and network services together from the cloud, organizations will be able to securely connect any user or device to any application without having to install and maintain the network management and security infrastructure, i.e., a multi-perimeter firewall system located in a cloud and forming part of a global virtual network." *EX-1011* p. 3.

[1.1] an egress ingress point device

Shieh discloses this limitation. Any one of the virtual input/output (I/O) module (with cache) (green) of FIG. 3¹ can be the *egress ingress point device*:

¹ This annotated FIG. 3 will be used to illustrate each of the limitations of claim 1 ("Annotated FIG. 3").

and sends packets to external network 315 outside of the firewall. In one embodiment, each of I/O modules 301-304 keeps a local cache (e.g., caches 305-308) storing location(s) of a security processing module(s) (e.g., security processing modules 309-311) for each connection session. A cache maintained by each I/O module contains a forwarding table mapping certain connection sessions to any of security modules 309-311. *EX-1004* 7:31-41; FIG. 3. Shieh's disclosure is consistent with the '482 Patent's disclosure that the egress ingress point device can link to both the open internet or to an organizations cloud based assets. *EX-1001* 13:17-19.

[1.2] a first access point server in communication with the egress ingress point device;

Shieh discloses that any of the security processing modules 309-311 can be the *first access point server*. For example, with respect to Annotated FIG. 3, security processing module 309 (blue) can be the *first access point server* in communication with virtual I/O 304 (*egress ingress point device* (green)).³ *EX-*

³ As illustrated in FIG 3, Shieh discloses several different security processing modules in communication with several service processing modules, and also in communication with several virtual I/O modules. In the claims analysis of the Petition, specific examples are provided, but a POSITA understood that there are

1004 FIG. 6, 9:9-12 (“In one embodiment, firewall modules 300A-300B could be distributed in different networks, even on different locations, as long as the modules can reach the module that is next in terms of processing and the central controller.”) Shieh describes that the security processing module 309 may perform firewall services. *EX-1004* 7:53-67. Shieh describes that one of the advantages is that the distributed firewall can employ a significantly large amount of CPU and memory resources for service processing and protect the networks at multiple geometric locations. The central controller decides which security processing module is capable of processing particular connection. *EX-1004* 9:19-26. Shieh discloses that the security processing modules can perform VPN processing which a POSITA understood to be an endpoint of a secure connection or tunnel of a virtual network (*access point servers*). *EX-1003* ¶ 99, *EX-1004* 7:53-55; 7:64-67; 4:14-19. Shieh’s disclosure is consistent with the disclosure of the ’482 Patent which describes that the access point servers are endpoints of a virtual tunnel and may perform firewall services as well. *EX-1001* 2:46-48; 4:43-45; 5:9-13.

many other such examples that can be made from the various combinations of security processing modules, service processing modules and I/O modules. *EX-1003* fn. 3.

***[1.3] a second access point server in communication
with the first access point sever;***

Shieh discloses this limitation for the same reason as with respect to limitation [1.2]. For example, the *second access point* can be security processing module 310 (red). *EX-1003* ¶ 102. Although not shown in Annotated Figure 3, Shieh discloses that the security processing modules can send packets to another security processing module:

A security processing module receives packets and runs the packets through one or more various security functions in the modules for security processing. There could be several security modules and each handles the same or different security functions. If the packets need to go through another security or service processing, the module sends the packets to the other modules.

EX-1004 7:53-63.

***[1.4] an endpoint device in communication with the
second access point server;***

Shieh discloses this limitation. Shieh further discloses that destination nodes can be a destination server. *EX-1004* Abstract; 3:2-4. Shieh discloses that security processing module 310 (red) (*second access point*) can be in communication with a destination server 4 (purple) (*endpoint device*) directly, or through virtual I/O module 304 (green) (*ingress egress point device*):

If a module is the last processing module in the chain to process the packets, it can forward the packets back to the virtual I/O module to send out, or send the packet out directly to its destination if its configured to do so.

EX-1004 7:64-67.

For example, in Annotated FIG. 3, security processing module 310 (*second access point device*) can send the packet directly to the destination server 4 of LAN 320 (*endpoint device*). Shieh's disclosure is consistent with the '482 Patent's disclosure that an endpoint can be the destination host server. *EX-1001 4:53-55.*

[1.5] a first perimeter firewall in communication with the first access point server, wherein the first perimeter firewall performs stateful packet inspection to prevent at least some traffic from passing from the first access point server to the second access point server; and

Shieh discloses this limitation. Shieh discloses that service processing module 312 (light blue) (*first perimeter firewall*) performs one or more of the security functions for the security processing module 310 (red) (*first access point server*). *EX-1004 8:1-13.* As shown in Annotated FIG. 3, service processing module 312 is located functionally at a perimeter between an internal network 320 and an external network 315. *EX-1004 7:31-52.* Shieh discloses that that the distributed firewalls can be located at multiple boundaries in the cloud between a client location and their link to the internet. With reference to Annotated FIG. 3, a first perimeter (dashed black line) can be located in a cloud where the security

processing module 309 and the service processing module 312 are located in the same location, and a second perimeter (dashed black line) can be located in a cloud where the security processing module 310 and the service processing module 313 are located in a different location so long as the two security processing modules are in communication with each other. *EX-1004* 9:9-11. This is consistent with the '482 Patent's disclosure that the firewalls are virtualized in the cloud and the perimeters are located between the client and the internet at each firewall. *EX-1001* 11:17-25; 13:64-14:4.

As discussed in the State of the Art section, a well-known security function that had become an industry standard was stateful inspection. *EX-1006* p. 2. Stateful inspection provided for the analysis of packets at the network layer to identify packets belonging to the same flow or session. *Id.* Although, Shieh does not use the term stateful inspection, a POSITA understood that it would be included in Shieh's generic description that the firewall modules perform "firewall functions" because stateful inspection was an industry standard firewall function. *EX-1003* ¶ 111, *EX-1004* 3:11-14. Further, Shieh describes that security processing was done to packets belonging to a session that is stateful, and that information regarding each session including the state of the session was saved in a session table. *EX-1004* 4:63-5:3. Shieh further discloses that a security device would perform the security inspection on packets at the beginning of the flow or

session, and at a certain point, the security device decides that it no longer needs to inspect further packets of the same session. *EX-1004* 5:38-42. A POSITA understood that using a session table to make the decision to no longer inspect further packets would be as a result of the security inspection being a stateful inspection. *EX-1003* ¶ 113.

Shieh discloses that the security processing done at service processing module 312 is different from the security processing module 309 in that it only receives and sends packets to the same security processing module 309. After processing by service processing module 312 (*first perimeter firewall*), the packets then are sent back to the same security processing module 309 (*first access point server*) for the next security function processing. *EX-1004* 8:1-13. Thus, if service processing module 312 identified traffic that posed a security risk, it would prevent the traffic from passing from the security processing module 309 (*first access point server*) to the security processing module 310 (*second access point server*).

To the extent that PO asserts that Shieh does not expressly disclose stateful inspection, a POSITA would have found it obvious to modify the teachings of Shieh to include stateful packet inspection at the service processing module 312 (*first perimeter firewall*). *EX-1003* ¶ 115. For example, as discussed in the State of the Art section, it was well-known to use stateful packet inspection before deep packet inspection as part of a layered defense. *EX-1007* pp. 83-84. As discussed

below, the service processing module 313 (*second perimeter firewall*) performs deep packet inspection, and a POSITA would be motivated to include a stateful inspection at service processing module 312 prior to the deep packet inspection for several reasons. *EX-1003* ¶ 116. First, as explained in the State of the Art, stateful inspection provided for the analysis of packets at the network layer as well other layers in order to assess the overall packet. By combining information from various layers (transport, session, and network) the firewall was better able to understand the protocol it was inspecting. This also provided for the ability to create virtual sessions in order to track connectionless protocols such as UDP-based applications as well as RPC-based applications. *EX-1006* p. 2. Second, because some traffic is blocked by the stateful inspection, it lightens the load on the traffic subject to deep packet inspection. *EX-1010* p. 7. Third, stateful inspection had become an industry standard and would be simple to implement since Shieh already maintained a session table which identified the state of the connection, which is required for stateful inspection. Thus, a POSITA would be motivated to modify the teachings of Shieh to include stateful inspection in service processing module 312 prior to the deep packet inspection performed in security processing module 313 and would be confident of its success. *EX-1003* ¶ 120.

[1.6] a second perimeter firewall in communication with the second access point server, wherein the second perimeter firewall performs deep packet

inspection to prevent at least some traffic from passing from the second access point server to the end point device,

Shieh discloses this limitation. Shieh discloses that service processing module 313 (pink) (*second perimeter firewall*) performs one or more of the security functions for the security processing module 310 (red) (*second access point server*). *EX-1004* 8:1-13. As discussed above with respect to limitation [1.5], and as shown in Annotated FIG. 3, service processing module 313 is located functionally at a second perimeter (dashed black line) between an internal network 320 and an external network 315. *EX-1004* 7:31-52. Shieh discloses that the security processing done at service processing module 313 is different from the security processing module 310 in that it only receives and sends packets to the same security processing module 310 (*in communication with the second access point server*). After processing by service processing module 313 (*second perimeter firewall*), the packets then are sent back to the same security processing module 310 (*second access point server*) for the next security function processing. *EX-1004* 8:1-13. Shieh discloses that service processing module 313 (*second perimeter firewall*) performs one or more firewall functions including deep packet inspection (DPI). After processing by service processing module 313 (*second perimeter firewall*), the packets then are sent back to the same security processing module 310 (*second access point server*) for the next security function processing.

EX-1004 8:1-13. Thus, if service processing module 313 identified traffic that posed a security risk, it would prevent the traffic from passing from the security processing module 310 (*second access point server*) to destination server 324 (*end point device*). EX-1003 ¶ 125.

[1.7] wherein at least one of the egress ingress point device, the first access point server, the second access point server, the endpoint device, the first perimeter firewall, or the second perimeter firewall comprises hardware,

Shieh discloses this limitation. FIG. 7 illustrates a method for performing firewall operations using the disclosed distributed firewall. EX-1004 1:55-57.

Shieh discloses that method 700 may be performed by processing logic that may include software, hardware, or a combination of both. EX-1004 9:39-41. Further, Shieh discloses that a virtual machine is software hosted on a server (*hardware*) for performing the functions for the different types of modules (e.g., *egress ingress point device, the first access point server, the second access point server, the endpoint device, the first perimeter firewall, or the second perimeter firewall*). EX-1004 3:41-43; 11:33-36.

[1.8] wherein the deep packet inspection is performed on a cloned copy of traffic that flows through the second perimeter firewall.

Shieh discloses deep packet inspection, but does not expressly state performing deep packet inspection on a cloned copy of traffic that flows through the service processing module 313 (*second perimeter firewall*). However, as discussed in the State of the Art section, a POSITA understood that deep packet inspection (DPI) could be performed inline or offline on a cloned copy of traffic that flows through the firewall. *EX-1003* ¶ 130. Thus, a POSITA understood Shieh's broad disclosure to include both inline and offline DPI. *EX-1003* ¶ 130.

To the extent that PO asserts that a POSITA would not understand Shieh to disclose performing DPI on a cloned copy of traffic, it would be obvious for a POSITA to modify the teachings of Shieh to include DPI on a cloned copy of traffic. *EX-1003* ¶ 131. As discussed in the State of the Art section, performing deep packet inspection on a cloned copy of traffic was well-known and provided several benefits. For example, Potti discloses that, because deep packet inspection can be time consuming and interrupt traffic flow, allowing packets to be forwarded to their destination while cloned copies are inspected allows traffic to flow without interrupting the flow of traffic through the network element. *EX-1005* ¶0345. This is particularly important to packets such as voice or streaming packets that require low latency. Shieh specifically identifies using rules to govern how packets are routed and that paths through the network can be set up to optimize for speed, fewest number of hops or reduced latency. *EX-1004* 4:38-44. A POSITA

understood that this speed and/or low latency requirement could be fulfilled by performing DPI on cloned copies. *EX-1003* ¶ 134. Second, using deep packet inspection of cloned copies of traffic allows further analysis of packets to discover trailing trends that may not have been identified using deep packet inspection on the traffic in real-time. Further, a POSITA understood that implementing a security processing function in Shieh that performed deep packet inspection of cloned traffic for traffic that required low latency as taught by Potti could be implemented successfully using well-known techniques. *EX-1003* ¶ 136.

b. Claim 2

[2] The multi-perimeter firewall system according to claim 1, wherein at least one of the access point servers is configured to perform firewall services.

Shieh discloses that security processing module 309 (*first access point server*) and security processing module 310 (*second access point server*) are configured to perform firewall functions, including “for example, NAT [network address translation], VPN [virtual private network], DPI [deep packet inspection], and/or anti-virus, etc.” *EX-1004* 7:53-63.

c. Claim 3

[3] The multi-perimeter firewall system according to claim 1, wherein the first perimeter firewall is in communication with the second perimeter firewall through a communication path.

Shieh discloses this limitation for the reasons discussed with respect to limitation [1.3], [1.5], [1.6]. Specifically, the service processing module 312 (*first perimeter firewall*) is in communication with security processing module 313 (*second perimeter firewall*) through a communication path through security processing module 309 (*first access point server*). *EX-1004* 7:53-63; 8:1-13.

Shieh further discloses that packets can be forwarded through the central controller 208 to the appropriate security processing modules. *EX-1004* 7:45-52. Shieh further discloses that the controller could set up paths through the network optimized for speed, fewest number of hops or reduced latency, among other characteristics. Using OpenFlow takes control of how traffic flows through the network out of the hands of the infrastructure, the switches and routers, and puts it in the hands of the network owner (such as a corporation), individual users or individual applications. *EX-1004* 4:44-48. Thus, Shieh also discloses a communication path between the service processing modules through the security processing modules and central controller.

d. **Claim 4**

[4] The multi-perimeter firewall system according to claim 3, wherein the communication path between the first perimeter firewall and the second perimeter firewall is a network path.

Shieh discloses this limitation in FIG. 2A which shows that firewall modules 209A-209C may be part of a distributed firewall connected through a network path

(solid lines). *EX-1003* ¶ 142. For example, when firewall module 209B receives a packet from node 206, it may forward the packet to firewall processing node 211A for content inspection using a network path. *EX-1004* 5:5-15. Further, Shieh discloses the service processing modules 312 and 313 (*first perimeter firewall and second perimeter firewall*) could be located in different networks and thus would communicate through a network path. *EX-1004* 9:9-18. Additionally, as discussed with limitation [3], Shieh discloses the employment of OpenFlow that allows paths to be set up between different entities on the network. *EX-1004* 4:44-48.

e. **Claim 5**

[5] The multi-perimeter firewall system according to claim 3, wherein the communication path between the first perimeter firewall and the second perimeter firewall is a network back channel.

The ‘482 Patent describes a back channel mechanism that offers a channel into devices which are not reachable from the open internet. *EX-1001* 6:8-11. Shieh discloses this limitation in FIG. 2A which shows that firewall modules 209A-209C may be part of a distributed firewall connected through a secured tunnel (*network back channel*) (dashed line). For example, when firewall module 209B receives a packet from node 206, it may forward the packet to firewall processing node 211A for content inspection and forwards the packet to controller 208 for routing information using secure tunnel 260. Each of the firewall processing nodes 211A-211B may further maintain a persistent connection or

tunnel with controller 208, for example, using the OpenFlow communication protocol. *EX-1004* 5:5-25. Thus, Shieh discloses a network back channel connecting the firewalls through the firewall controller. *EX-1003* ¶ 149.

f. **Claim 6**

[6] The multi-perimeter firewall system according to claim 3, wherein the first perimeter firewall and the second perimeter firewall share threat information including at least one of heuristic patterns, signatures of known threats, known malicious source IP addresses, or attack vectors.

Shieh discloses that the distributed firewalls exchange information and configuration, which a POSITA understood would include threat information such as a source IP address related to a malicious attack. *EX-1003* ¶ 150. For example, Shieh discloses that all of the firewall modules 209-210 are managed by firewall controller 208. *EX-1004* 3:20-26. For example, each of network access devices 204A-204C maintains a persistent connection such as secure connections or tunnels 260 with a controller or management entity 208 for exchanging management messages and configurations, or distributing routing information to network access devices 204A-204C, etc. *EX-1004* 4:14-32. Shieh discloses that an administrator 265 configures, for example, via a controller or a management entity 208, a network access device (e.g., network access devices 204A-204C) to set up a set of filtering rules concerning whether and/or what types of packets should be forwarded to a security device and which of the security devices (e.g., security

devices 211A-211B) for security inspection. Controller 208 is configured to manage multiple network access devices 204A-204C and/or multiple security devices 211A-211B. *EX-1004* 5:25-34.

As discussed in the State of the Art, one of the purposes for performing deep packet inspection is to identify malicious content, and the source IP address associated with a received IP packet or packets having malicious content. *EX-1003*

¶ 154. A POSITA understood that Shieh's teaching that a firewall controller exchanges management messages and configurations with firewall modules would include source IP address identified by a firewall performing deep packet inspection that would be sent to other firewall devices as part of the packet filtering rules. *EX-1003* ¶ 154, *EX-1009* pp. 659-666.

Shieh's disclosure of exchanging messages and configurations between security modules through a controller is consistent with the '482 Patent's disclosure that threat information is shared via a central control server. *EX-1001* 2:53-58.

To the extent that PO asserts that Shieh does not expressly state that the firewall modules share threat information, a POSITA would be motivated to modify the teachings of Shieh to include the well-known feature of "attack information advertising", as discuss in the State of the Art section, to ensure that firewalls on the perimeter take countermeasures to prevent malicious packets from

entering the network. *EX-1003* ¶ 156, *EX-1009* p. 1915. A POSITA understood that one of the purposes of a firewall performing deep packet inspection is to identify threats, such as the source IP address of a packet that contains malicious content. *EX-1003* ¶ 157. A POSITA would be motivated to modify the teachings of Shieh to share the identified source IP address with other firewalls as part of the filtering rules to be used to block or drop packet from the identified source IP address of malicious content in order to protect the network. *EX-1003* ¶ 157. This would result in the benefit of traffic being blocked at a more outer perimeter (e.g., as traffic enters from the external network) as part of a well-designed layered defense approach and defense in depth. A POSITA would be confident of the success of this modification as it would be implementing the layered defense that was discussed in the State of the Art section. *EX-1003* ¶ 157.

g. Claim 7

[7] The multi-perimeter firewall system according to claim 6, wherein the first perimeter firewall and the second perimeter firewall share threat information with a central control server.

Shieh discloses this for the same reason as discussed with respect to Claim 6.

h. Claim 8

[8] The multi-perimeter firewall system according to claim 1, wherein the deep packet inspection is performed on flow through traffic.

As discussed with respect to limitation [1.6], Shieh discloses that service proceeding module performs deep packet inspection, and a POSITA understood there is no need to perform DPI on cloned traffic for traffic that is not speed and latency sensitive. Thus, a POSITA understood that the same firewall performs DPI on cloned traffic could perform DPI on flow through traffic. *EX-1003* ¶ 159.

i. **Claim 9**

[9] The multi-perimeter firewall system according to claim 1, wherein at least one of the firewalls includes a cloud firewall load balancer and wherein the cloud firewall load balancer can allocate cloud firewall resources on demand.

Shieh discloses that any of security processing modules 309-311 can load balance the computational-intensive services using multiple service processing modules. *EX-1004* 8:13-16; 7:62-64. Shieh discloses load balancing across any number of the security processing modules in the cloud, which provides a security design that is best-fit for the emerging cloud computing, and provides great scalability and system availability. *EX-1004* 9:28-36. Further, Shieh discloses that each of service processing modules 312-313 performs one or more of the functions of security processing module 309-311, which a POSITA understood would include load balancing. *EX-1004* 8:1-3, *EX-1003* ¶ 162. Shieh's disclosure is consistent with the '482 Patent's disclosure that cloud based firewalls are

dynamically scalable via cloud firewall load balancing mechanisms that can bring more resources online as needed. *EX-1001* 11:20-22.

j. Claim 10

[10] The multi-perimeter firewall system according to claim 1, wherein the egress ingress point device receives traffic directly from the Internet.

As shown in Annotated FIG. 3, Shieh discloses that virtual I/O module 304 (*egress ingress point device*) receives traffic directly from the external network 315, which a POSITA understood includes the Internet. *EX-1003* ¶ 164, *EX-1004* FIG. 3; 2:65-67.

k. Claim 11

[11] The multi-perimeter firewall system according to claim 1, wherein the first perimeter firewall is coupled to a multi-homed backbone.

Assuming Claim 11 is referring to a “multi-homed”, a POSITA understood it to mean that the connection to the internet is provided through at least two links for redundancy. *EX-1003* ¶ 165. Shieh does not provide the details of the connection to the internet but using a multi-homed backbone was common and well-known, and FIG. 3 shows that multiple virtual I/O modules, which communicate with each other, are each in communication with the internet, which a POSITA would consider to be a multi-homed backbone. *EX-1003* ¶ 166. Further a POSITA understood that cloud routinely multi-home their services and provide a

load balancer in front of the virtual I/O modules to ensure availability. *EX-1003* ¶ 167.

l. Claim 12

[12] The multi-perimeter firewall system according to claim 1, wherein the at least some traffic prevented from passing from the first access point server to the second access point server includes traffic with recognized malicious headers.

As described in the State of the Art section, filtering data according to a source IP address (*recognized malicious headers*) is a very well-known firewall function, which can be implemented as a filtering rule in service processing module 312 (*first perimeter firewall*) as described in limitation [1.5] to prevent traffic from passing from the first security processing module 309 (*first access point server*) to the second security processing module 310 (*second access point server*). Further, Shieh provides IP address based specific services with rules governing the traffic from a specific IP address. *EX-1004* 4:38-41. Thus a POSITA understood that packets known to be malicious from a source IP address would be subject to a rule to be dropped. *EX-1003* ¶ 169.

m. Claim 13

[13.0] A multi-perimeter firewall system located in a cloud and forming part of a global virtual network, comprising:

Shieh discloses this limitation for the same reasons as discussed with respect to limitation [1.0].

[13.1] an egress ingress point device;

Shieh discloses this limitation for the same reasons as discussed with respect to limitation [1.1].

[13.2] a first access point server in communication with the egress ingress point device;

Shieh discloses this limitation for the same reasons as discussed with respect to limitation [1.2].

[13.3] a second access point server in communication with the first access point sever;

Shieh discloses this limitation for the same reasons as discussed with respect to limitation [1.3].

[13.4] an endpoint device in communication with the second access point server;

Shieh discloses this limitation for the same reasons as discussed with respect to limitation [1.4].

[13.5] a first perimeter firewall in communication with the first access point server, wherein the first perimeter firewall performs stateful packet inspection to prevent at least some traffic from passing from the first access point server to the second access point server using a first firewall mechanism; and

Shieh discloses this limitation for the same reasons as discussed with respect to limitation [1.5]. The *first firewall mechanism* is the stateful packet inspection. During prosecution, the examiner rejected [issued claim 13] which recited that the first firewall used a first firewall mechanism and the second firewall used a second different, firewall mechanism. *EX-1002* p. 14 - 15. In response, the applicant amended [issued Claim 13] to include the limitation that the first firewall “performs stateful packet inspection” and the second firewall “performs deep packet inspection.” *EX-1002* p. 19. Thus, the *first firewall mechanism* is specifically recited to be stateful packet inspection, which is different from the *second firewall mechanism*, which is specifically recited to be deep packet inspection.

[13.6] a second perimeter firewall in communication with the second access point server, wherein the second perimeter firewall performs deep packet inspection to prevent at least some traffic from passing from the second access point server to the end point device using a second, different firewall mechanism,

Shieh discloses this limitation for the same reasons as discussed with respect to limitation [1.6] and [13.5]. The *second, different firewall mechanism* is deep packet inspection. *EX-1003* ¶ 180.

[13.7] wherein at least one of the egress ingress point device, the first access point server, the second access point server, the endpoint device, the first

perimeter firewall, or the second perimeter firewall comprises hardware,

Shieh discloses this limitation for the same reasons as discussed with respect to limitation [1.7].

[13.8] wherein the deep packet inspection is performed on a cloned copy of traffic that flows through the second perimeter firewall.

Shieh discloses this limitation for the same reasons as discussed with respect to limitation [1.8].

n. Claim 14

[14] The multi-perimeter firewall system according to claim 13, wherein at least one of the access point servers is configured to perform firewall services.

Shieh discloses this limitation for the same reasons as discussed with respect to Claim 2.

o. Claim 15

[15] The multi-perimeter firewall system according to claim 13, wherein the first perimeter firewall is in communication with the second perimeter firewall through a communication path.

Shieh discloses this limitation for the same reasons as discussed with respect to Claim 3.

p. Claim 16

[16] The multi-perimeter firewall system according to claim 15, wherein the communication path between

the first perimeter firewall and the second perimeter firewall is a network path.

Shieh discloses this limitation for the same reasons as discussed with respect to Claim 4.

q. Claim 17

[17] The multi-perimeter firewall system according to claim 15, wherein the communication path between the first perimeter firewall and the second perimeter firewall is a network back channel.

Shieh discloses this limitation for the same reasons as discussed with respect to Claim 5.

r. Claim 18

[18] The multi-perimeter firewall system according to claim 15, wherein the first perimeter firewall and the second perimeter firewall share threat information including at least one of heuristic patterns, signatures of known threats, known malicious source IP addresses, or attack vectors.

Shieh discloses this limitation for the same reasons as discussed with respect to Claim 6.

s. Claim 19

[19] The multi-perimeter firewall system according to claim 18, wherein the first perimeter firewall and the second perimeter firewall share threat information with a central control server.

Shieh discloses this limitation for the same reasons as discussed with respect to Claim 7.

t. **Claim 20**

[20] The multi-perimeter firewall system according to claim 13, wherein the deep packet inspection is performed on flow through traffic.

Shieh discloses this limitation for the same reasons as discussed with respect to Claim 8.

u. **Claim 21**

[21] The multi-perimeter firewall system according to claim 13, wherein at least one of the firewalls includes a cloud firewall load balancer and wherein the cloud firewall load balancer can allocate cloud firewall resources on demand.

Shieh discloses this limitation for the same reasons as discussed with respect to Claim 9.

v. **Claim 22**

[22] The multi-perimeter firewall system according to claim 13, wherein the second perimeter firewall is between the endpoint device and the second access point server.

Shieh discloses this limitation for the same reasons as discussed with respect to Claim [1.6]. Service processing module 313 (*second perimeter firewall*) performs DPI after receiving a packet from security processing module 310 (*second access point server*) and before it is forwarded to destination server 324 (*endpoint device*).

See Annotated FIG. 3. *EX-1003* ¶ 191

w. **Claim 23**

[23] The multi-perimeter firewall system according to claim 13, wherein the first perimeter firewall is between the first access point server and the second access point server.

Shieh discloses this limitation for the same reasons as discussed with respect to Claim [1.5]. Service processing module 312 (*first perimeter firewall*) performs SPI after receiving a packet from security processing module 309 (*first access point server*) and before it is forwarded to security processing module 310 (*second access point server*). See Annotated FIG. 3 ; *EX-1003* ¶ 192.

x. **Claim 24**

[24] The multi-perimeter firewall system according to claim 13, wherein the egress ingress point device receives traffic directly from the Internet.

Shieh discloses this limitation for the same reasons as discussed with respect to Claim 10.

y. **Claim 25**

[25] The multi-perimeter firewall system according to claim 13, wherein the first perimeter firewall is coupled to a multi-honed backbone.

Shieh discloses this limitation for the same reasons as discussed with respect to Claim 11.

z. **Claim 26**

[26] The multi-perimeter firewall system according to claim 13, wherein the at least some traffic prevented from passing from the first access point server to the second access point server includes traffic with

recognized malicious headers.

Shieh discloses this limitation for the same reasons as discussed with respect to Claim 12.

VII. THE BOARD SHOULD NOT EXERCISE ITS DISCRETION AND DENY INSTITUTION

A. The Board Should Not Deny Institution Under 35 U.S.C. § 325(d)

When determining whether to exercise discretion under § 325(d), “the Board uses the following two-part framework: (1) whether the same or substantially the same art previously was presented to the Office or whether the same or substantially the same arguments previously were presented to the Office; and (2) if either condition of first part of the framework is satisfied, whether the petitioner has demonstrated that the Office erred in a manner material to the patentability of the challenged claims.” *Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6, p. 8 (Feb. 13, 2020) (designated: March 24, 2020).

Denial under § 325(d) is not warranted because the challenges presented in this Petition are neither cumulative nor redundant to the prosecution of the ’482 Patent. None of the asserted prior art references were cited or considered by the Examiner during prosecution of the ’482 Patent. The references in this Petition were neither relied upon during prosecution nor are cumulative of art relied upon

during prosecution. Further, the '482 Patent has not been previously challenged in an IPR.

During prosecution of the '482 Patent, the examiner cited U.S. Pat. Publ. 2012/0210417 (“Shieh 2”) (EX-1012). Shieh 2 was owned by the same entity as Shieh, but has a different set of inventors, a different specification and claims a different priority date. The examiner cited Shieh 2 for disclosing a single claim limitation, “a cloud firewall load balancer” recited in Claims 9 and 21 (issued claims). The Patent Owner disagreed that Shieh 2 disclosed “a cloud firewall load balancer” and, focused on whether Shieh 2 disclosed the first perimeter firewall performing stateful inspection, and argued that Shieh 2 does not disclose firewalls that perform both stateful packet inspection and deep packet inspection:

The Office Action relies on Shieh to teach limitations related to a “cloud firewall load balancer.” (Office Action, p. 25). Applicant disagrees that Shieh teaches these limitations. However, even assuming *arguendo* that Shieh teaches a “cloud firewall load balancer,” Shieh does not further teach or suggest a “first perimeter firewall [that] performs stateful packet inspection” and a “second perimeter firewall [that] performs deep packet inspection,” as recited by amended claim 1. To the extent that Shieh may generally refer to the process of deep packet inspection, Shieh is silent regarding stateful packet inspection, and the Office Action does not cite Shieh for this claimed feature. Therefore, Shieh does not teach or suggest arrangements of firewalls that perform both stateful packet inspection and deep packet inspection, much less the claimed arrangement recited by amended claim 1. Accordingly, Shieh fails to teach or suggest “the first perimeter firewall performs stateful packet inspection to prevent at least some traffic from passing from the first access point server to the second access point server; and... the second perimeter firewall performs deep packet inspection to prevent at least some traffic from passing from the second access point server to the end point device,” as recited by amended claim 1.

EX-1002 p. 77.

In response to this argument, the examiner allowed the claims. EX-1002 p. 87.

Shieh is not the same or substantially the same art as Shieh 2 that previously was presented to the Office. Further, the arguments made by the examiner regarding Shieh 2 were not the same or substantially the same as the arguments presented in the Petition regarding Shieh.

In addition, the Patent Owner’s arguments regarding Shieh 2’s failure to disclose stateful packet inspection does not apply to Shieh, which includes a description of stateful session flows that was not in Shieh 2. Shieh discloses:

An established communication session may involve more than one message in each direction. A session is typically, but not always,

stateful, meaning that at least one of the communicating entities needs to save information about the session history in order to be able to communicate, as opposed to stateless communication, where the communication consists of independent requests with responses. Flow tables 251A-251C may be implemented as a combination of a flow table and a session table.

EX-1004 4:63-5:4.

Further Shieh includes a description of stateful packet inspection that was not in Shieh 2:

A security device may perform the security inspection on packets at the beginning of the flow or session, and at a certain point, the security device decides that it no longer needs to inspect further packets of the same session.

EX-1004 5:37-42.

Thus, Shieh is not the same or substantially the same as Shieh 2.

Further, the examiner cited Shieh 2 for disclosing only the claim limitation, “a cloud firewall load balancer.” *EX-1002* p. 14-15. Shieh is cited in the present Petition for disclosing most of the claim limitations of Claim 1.

Even if Shieh 2 is substantially the same, the examiner made a mistake by accepting Patent Owner’s argument that Shieh 2 does not disclose stateful packet inspection since Shieh 2 discloses that its distributed firewalls perform firewall functions, and as described in the State of the Art section, stateful inspection had

become an industry standard such that a POSITA would understand Shieh 2 to be referring to stateful inspection as one of the firewall functions.

Thus, the Board should not deny institution under § 325(d).

B. The Board Should Not Deny Institution Under 35 U.S.C. § 314(a)

The PTAB has discretion to deny institution under 35 U.S.C. § 314(a).

Related to the Director's June 2022 interim guidance regarding application of the *Fintiv* factors⁴, (1) the Petition is particularly strong in the underlying merits, and (2) the Petitioner adopts the identical stipulation from *Sotera*, namely, that if the IPR is instituted, Petitioner will not pursue in the Related Litigation any ground raised or that could have been reasonably raised in an IPR for the challenged patent. Thus, under the Interim Guidance, the Board should not deny institution.

Nevertheless, the Board's decision in *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 (Dec. 1, 2020) instructs that a holistic view of the remaining *Fintiv* factors also weighs in favor of institution.

Factor 1 is neutral because no request for stay has been filed.

⁴ Interim Procedure For Discretionary Denials In AIA Post Grant Proceedings With Parallel District Court Litigation, PTO Director's Memorandum (June 21, 2022).

Under factor 2, no trial date has been set, nor has a judge been assigned. According to the most recent statistics on median time-to-trial for civil actions (<https://www.uscourts.gov/statistics/table/t-3/federal-judicial-caseload-statistics/2023/03/31>), the median time from filing to trial was 32 months in the Western District of Texas. The Related Litigation was filed on August 2, 2023 and thus would be expected to go to trial April 2026 according to the median time to trial statistics. A Final Written Decision is expected in the present matter in July 2025, 9 months before trial in the Related Litigation. Thus, this factor weighs against discretionary denial.

Factor 3 favors institution. The co-pending litigation is in its early stages, and the investment in it has been minimal. No Scheduling Order has been entered. Thus, this factor weighs against discretionary denial.

Under factor 4, in addition to the *Sotera* stipulation that Petitioner issued to PO, PO has only identified in the Complaint a subset of the claims that are being challenged in the present Petition. Thus, it is unlikely the district court will be addressing the validity of all of the claims challenged by this Petition.

Under factor 5, Petitioner is a defendant in the Related Litigation. Nothing within *Fintiv* suggests that the same party between the proceedings weighs in favor of discretionary denial. *See HP Inc. v. Slingshot Printing LLC*, IPR2020-01084,

Paper 13 at 9 (having the “same parties as parallel proceeding” makes factor 5 “neutral”)).

Under factor 6, other circumstances weigh in favor of institution. Here, the merits of the Petition are particularly strong. For example, Shieh is a parallel disclosure to the '482 Patent, meaning that it is directed at the same problem and proposes the same solution as the '482 Patent, and discloses identical architecture and the identical concepts disclosed in the '482 Patent, but uses some different words, thus demonstrating that the Petition is particularly strong in the underlying merits. The evidence presented, if unrebutted in trial, would plainly lead to a conclusion that one or more claims are unpatentable by a preponderance of the evidence.

When viewed holistically, the timing of the present Petition is reasonable, there has been relatively limited investment in the Related Litigation, and there is minimal overlap between the present IPR and the Related Litigation. Further, coupling these *Fintiv* considerations with compelling evidence of unpatentability presented in the Petition, the efficiency and integrity of the IPR process is best served by instituting review.

VIII. Mandatory Notices Under 37 C.F.R. §42.8

A. Real Party-in-Interest (37 C.F.R. § 42.8(b)(1))

The real party-in-interest in this Petition is Cisco Systems, Inc.

B. Related Matters (37 C.F.R. § 42.8(b)(2))

1. Judicial Matters

As of the filing date of this Petition and to the best knowledge of Petitioner, the '482 Patent is involved in the following litigations:

UMBRA Technologies Ltd. (UK) et al v. Cisco Systems, Inc., Case No. 1:23-cv-00903-DII (W.D. Tex.) (filed Aug. 2, 2023) (ongoing)

UMBRA Technologies Ltd. (UK) et al v. VMware, Inc., Case No. 1:23-cv-00904-DII (W.D. Tex.) (filed Aug. 2, 2023) (ongoing).

2. Administrative Matters

As of the filing date of this Petition and to the best knowledge of Cisco Systems, the '482 Patent was subject to the following *inter partes* reviews which were not instituted:

3. Related Patents

See Exhibit 1013.

C. Lead/Back-up Counsel (37 C.F.R. § 42.8(b)(3)):

Lead Counsel:

Patrick D. McPherson, USPTO Reg. No. 46,255
DUANE MORRIS LLP, 901 New York Avenue N.W., Suite 700 East
Washington, DC 20001
P: (202) 776-7800 (202) 776-7801; PDMcPherson@duanemorris.com

Back-Up Counsel: Patrick Muldoon, USPTO Reg. No. 47,343

DUANE MORRIS LLP, 901 New York Avenue N.W., Suite 700 East
Washington, DC 20001

P: (202) 776-7840; F: (202) 776-7801; PCMuldoon@duanemorris.com

Joseph Powers, USPTO Reg. No. 47,006

DUANE MORRIS LLP, 30 South 17th Street, Philadelphia, PA 19103-4196

P: (215) 979-1842; F: (215) 689-3797; JAPowers@duanemorris.com

D. Notice of Service Information (37 C.F.R. § 42.8(b)(4)):

Please direct all correspondence to lead and back-up counsel at the above addresses. Petitioner consents to electronic service at the email addresses above.

E. GROUNDS FOR STANDING (37 C.F.R. § 42.204(A))

Petitioner certifies that the Patent for which review is sought is available for post grant review and that Petitioner is not barred or estopped from requesting a post grant review of the Challenged Claims on the grounds identified herein. 37 C.F.R. § 42.204(a). This Petition is filed pursuant to 37 C.F.R. § 42.206(a).

IX. CONCLUSION

For the reasons set forth above, Petitioner has established a reasonable likelihood of prevailing with respect to all Challenged Claims of the '482 Patent and requests the Board institute *inter partes* review and then cancel all claims as unpatentable.

Date: January 29, 2024

/Patrick D. McPherson/

Patrick D. McPherson, Reg. No. 46,255
901 New York Ave., N.W., Suite 700-East

P: (202) 776-7800

F: (202) 776-7801

PDMcPherson@duanemorris.com

ATTORNEY FOR PETITIONER

CERTIFICATION OF SERVICE ON PATENT OWNER

Pursuant to 37 C.F.R. §§ 42.6(e), 42.8(b)(4) and 42.105, the undersigned certifies that on the 29th of January 2024, a complete and entire copy of this Petition for *Inter Partes* Review of U.S. Patent No. 10,574,482 and all supporting exhibits were served via Federal Express, postage prepaid, to the Patent Owner by serving the correspondence address of record for the '482 Patent:

Wilmerhale
60 State Street
Boston, MA 02109
United States

/Patrick D. McPherson/
Patrick D. McPherson, Reg. No. 46,255
901 New York Ave., N.W., Suite 700-East
P: (202) 776-7800
F: (202) 776-7801
PDMcPherson@duanemorris.com

ATTORNEY FOR PETITIONER

CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. § 42.24 *et seq.*, the undersigned certifies that this document complies with the type-volume limitations. This document contains 12,837 words as calculated by the “Word Count” feature of Microsoft Word 2010, the word processing program used to create it.

Dated: January 29, 2024

/Patrick D. McPherson/
Patrick D. McPherson, Reg. No. 46,255
Duane Morris LLP
901 New York Ave., N.W., Suite 700-East
Washington D.C., 20001
P: (202) 776-7800
F: (202) 776-7801
PDMcPherson@duanemorris.com

ATTORNEY FOR PETITIONER