UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETSKOPE, INC.,
Petitioner,

v.

FORTINET, INC.,
Patent Owner.

IPR2023-00030
Patent 10,826,941 B2

Before JAMES P. CALVE, THOMAS L. GIANNETTI, and CHRISTOPHER L. OGDEN, *Administrative Patent Judges.*

CALVE, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

Netskope, Inc. ("Petitioner") filed a petition requesting *inter partes* review of claims 1–22 (the "challenged claims") of U.S. Patent No. 10,826,941 B2 ("the '941 patent") (Ex. 1001). Paper 2 ("Pet."), 5. Fortinet, Inc. ("Patent Owner") filed a Preliminary Response. Paper 6. Applying the standard in 35 U.S.C. § 314(a), we instituted an *inter partes* review of all challenged claims on all grounds asserted in the Petition. Paper 9 ("Inst. Dec.").

After we instituted trial, Patent Owner filed a Patent Owner Response. Paper 16 ("PO Resp."). Petitioner filed a Reply to Patent Owner's Response. Paper 19 ("Reply"). Patent Owner filed a Sur-reply to Petitioner's Reply. Paper 24 ("Sur-reply").

An oral hearing was held on February 6, 2024, and a copy of the transcript was entered in the record. Paper 36 ("Tr.").

We have jurisdiction pursuant to 35 U.S.C. § 6. This Decision is a Final Written Decision under 35 U.S.C. § 318(a) (2018) and 37 C.F.R. § 42.73 (2020) as to the patentability of the claims on which we instituted trial. Petitioner bears the burden of proving unpatentability of the challenged claims. *Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015). To prevail, Petitioner must prove unpatentability by a preponderance of the evidence. *See* 35 U.S.C. § 316(e); 37 C.F.R. § 42.1(d).

For reasons that follow, we determine that Petitioner has shown by a preponderance of the evidence that claims 1–22 of the '941 patent are unpatentable.

II. BACKGROUND

A. Related Proceedings

The parties identify the following proceeding involving the ’941 patent: *Netskope, Inc. v. Fortinet, Inc.*, No. 3:22-cv-01852-JSC (N.D. Cal.). Pet. 5; Paper 4 (Patent Owner’s Mandatory Notices), 2.

B. Real Parties in Interest

Petitioner identifies Netskope, Inc. as the real party in interest. Pet. 5. Patent Owner identifies Fortinet, Inc. as the real party in interest. Paper 4, 2.

C. The ’941 Patent

The ’941 patent describes a cloud managed virtual security perimeter that protects enterprise networks as shown in Figure 1, reproduced below.

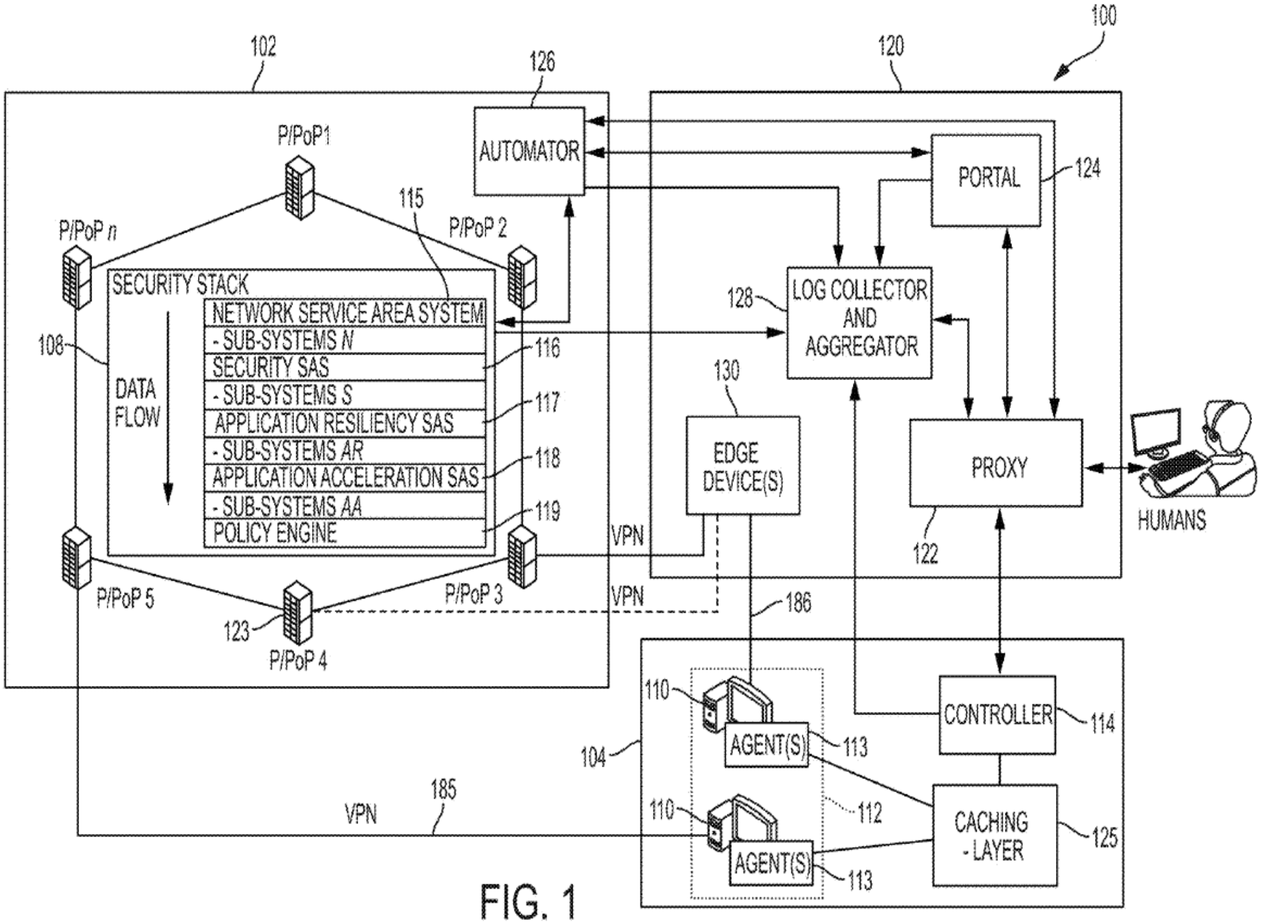


FIG. 1

Figure 1 depicts system 100 that manages cloud-based firewalls for network security. Ex. 1001, 6:25–28. Virtual perimeter 102 provides virtual *firewall* services for computing endpoints 110 (nodes) of enterprise network 112. *Id.* at 6:35–53. Perimeter Points of Presence (P/PoPs) 121[1] located in buildings, cities, regions, countries and continents connect to computing endpoints 110 via physical or virtual connections 185, 186. *Id.* at 6:53–7:6. Endpoints 110 access untrusted or unknown entities through P/PoPs 121. *Id.* at 7:6–14.

Computing endpoints 110 may be Application-as-a-Service platforms (AaaS), office computers, data centers, public or private cloud instances, mobile devices, remote users, and software-as-a-service (SaaS), and other endpoints distributed geographically or functionally. Ex. 1001, 6:60–67.

Each P/PoP 121 includes security stack 108 of selectable service area systems that can customize the virtual perimeter for an enterprise to process inbound and outbound data. Ex. 1001, 7:14–31. Policy engine 119 enables policies to be defined for each system and sub-system of P/PoPs including triggers, functions, actions, and event records. *Id.* at 7:32–36. A policy may apply uniformly for all P/PoPs or use different elements at disparate P/PoPs. *Id.* at 7:43–47. Policies changes are made via policy digest 123 at portal 124 as structured representations of configuration changes that add, remove, or change sites, policies, and rules of virtual perimeter 102. *Id.* at 11:30–39.

Network segmentation subsystem 104 adds software defined network segmentation at each endpoint 110 by adding network segmentation agents 113 to endpoints to control traffic happening behind the firewall, i.e., behind the virtualized network firewalls provided by P/PoPs. Ex. 1001, 7:55–61.

[1] The P/PoPs appear to be mis-labeled as item 123 in Figure 1.

Agents 113 connect with network segmentation controller 114 hosted in the cloud with virtual network firewall P/PoPs 121 to provide a security infrastructure that protects networks and endpoint hosts. *Id.* at 7:61–66, 8:21–23. Controller 114 provides instructions and rules to endpoint agents 113 to use to monitor and gate endpoint communications. *Id.* at 8:9–15.

When a connection request is received at endpoint 110, its network segmentation agent 113 checks the metadata against a local cache of rules. Ex. 1001, 8:60–62. If a cached rule applies, agent 113 applies that rule to allow or block the connection. *Id.* at 8:62–65. If no rules apply, agent 113 sends the metadata to network segmentation controller 114 in an escalation request to see if controller 114 approves the new connection based on a rule or policy cached in its caching-layer 125 while agent 113 holds the request for a connection pending a response from controller 114. *Id.* at 8:65–9:6.

D. Prosecution History of the '941 Patent

The '941 patent issued from Application No. 16/023,388, filed June 29, 2018. Ex. 1001, codes (21), (22). In the first office action, the Examiner issued a Notice of Allowability indicating that the prior art did not teach

> automatically generating a policy digest formatted according to a predefined format, the policy digest comprising the modifications, and storing the policy digest in the memory;
>
> retrieving the policy digest from the memory;
>
> generating one or more calls to one or more system components that control the communications to and from the enterprise network and the endpoint to endpoint connections based on the policy digest; and
>
> modifying control of the communications to and from the enterprise network and the endpoint to endpoint connections based on the one or more calls.

Ex. 1003, 147–148.

E. Challenged Claims

Petitioner challenges claims 1–22 of the ’941 patent. Pet. 5. Claims 1 and 12 are independent. Claims 2–11 depend from claim 1. Claims 13–22 depend from claim 12. Ex. 1001, 25:1–26:64 (the ’941 patent claims).

Claim 1 is illustrative of the claimed subject matter and is reproduced below with Petitioner’s annotations that identify each limitation:

> 1[pre] A method for protecting an enterprise network, the method comprising, at a system comprising one or more processors and memory that are remote from the enterprise network:
>
> 1[a] controlling communications to and from the enterprise network according to a set of security policies;
>
> 1[b] controlling endpoint to endpoint connections within the enterprise network according to the set of security policies;
>
> 1[c] receiving a request for modifications to one or more policies of the set of policies;
>
> 1[d] automatically generating a policy digest formatted according to a predefined format, the policy digest comprising the modifications, and
>
> 1[e] storing the policy digest in the memory; retrieving the policy digest from the memory;
>
> 1[f] generating one or more calls to one or more system components that control the communications to and from the enterprise network and the endpoint to endpoint connections based on the policy digest; and
>
> 1[g] modifying control of the communications to and from the enterprise network and the endpoint to endpoint connections based on the one or more calls.

Ex. 1001, 25:2–25; *see* Pet. 19–36 (Petitioner’s annotations of claim 1).

F. Asserted Grounds of Unpatentability

Petitioner asserts that the challenged claims are unpatentable on the following twelve grounds (Pet. 8):

Ground	Challenged Claims	35 U.S.C. §	Reference(s)
1	1, 2, 4, 5, 12, 13, 15, 16	103[2]	Wang[3]
2	3, 14	103	Wang, Pasdar[4]
3	6, 7, 17, 18	103	Wang, Sikka[5]
4	8, 19	103	Wang, Sikka, Botzer[6]
5	9, 20	103	Wang, Shafer[7]
6	10, 11, 21, 22	103	Wang, Terrill[8]
7	1, 2, 4, 5, 10–13, 15, 16, 21, 22	103	Chambers,[9] Terrill

[2] The Leahy-Smith America Invents Act ("AIA") included revisions to 35 U.S.C. § 103 that became effective on March 16, 2013. Changes made to 35 U.S.C. § 103 in the AIA do not apply to any application for patent filed before March 16, 2013. Because the '941 patent has an effective filing date after March 16, 2013, we refer to the AIA version of 35 U.S.C. § 103.

[3] US 2017/0250951 A1, published Aug. 31, 2017 (Ex. 1004, "Wang").

[4] US 2014/0366079 A1, published Dec. 11, 2014 (Ex. 1005, "Pasdar").

[5] US 2013/0298190 A1, published Nov. 7, 2013 (Ex. 1006, "Sikka").

[6] US 2016/0350145 A1, published Dec. 1, 2016 (Ex. 1009, "Botzer").

[7] US 7,376,719 B1, issued May 20, 2008 (Ex. 1010, "Shafer").

[8] US 2016/0323318 A1, published Nov. 3, 2016 (Ex. 1007, "Terrill").

[9] US 2014/0068705 A1, published Mar. 6, 2014 (Ex. 1008, "Chambers").

8	3, 14	103	Chambers, Terrill, Pasdar
9	6, 17	103	Chambers, Terrill, Litvin[10]
10	7, 18	103	Chambers, Terrill, Litvin, Wang
11	8, 19	103	Chambers, Terrill, Litvin, Wang, Botzer
12	9, 20	103	Chambers, Terrill, Shafer

Petitioner relies on Declarations of Dr. Wenke Lee. Exs. 1002, 1016. Patent Owner relies on Declarations of Dr. John Black Jr. Ex. 2003.

III. DISCUSSION

A. Level of Ordinary Skill in the Art

Petitioner asserts a person of ordinary skill in the art "would have had a B.S. in computer science, computer engineering, or electrical engineering, with at least two years' experience working on network security design and related applications." Pet. 16 (citing Ex. 1002 ¶ 28). Patent Owner asserts a person of ordinary skill in the art "would have had a Bachelor of Science in electrical engineering and/or computer science, and two 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 one year of work or research experience in related fields." PO Resp. 7 (citing Ex. 2003 ¶ 18). Patent Owner asserts that its positions in the Patent Owner Response would be the same under either party's proposal. *Id.*

[10] US 2009/0249470 A1, published Oct. 1, 2009 (Ex. 1011, "Litvin").

The parties substantially agree on the level of ordinary skill in the art. Consistent with their proposals, we adopt Petitioner's definition with Patent Owner's contention that a master's degree in electrical engineering and/or computer science and one year of relevant work or research experience also suffice. PO Resp. 7 (asserting that "Patent Owner's description of the level of ordinary skill in the art is essentially the same as that of Petitioner"). This level of ordinary skill is consistent with the description of the relevant field of invention and background art in the '941 patent (*see* Ex. 1001, 1:14–3:51) and the prior art. However, the outcome of our Decision would be the same under either party's proposal.

B. Claim Construction

We interpret claims "using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b)." 37 C.F.R. § 42.100(b). Under that standard, words of a claim are generally given their ordinary and customary meaning as understood by a person of ordinary skill in the art at the time of the invention. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc).

We construe the claims only to the extent necessary to reach our decision. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) ("[W]e need only construe terms 'that are in controversy, and only to the extent necessary to resolve the controversy.'") (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)). Petitioner asserts its belief that no claim constructions are needed. Pet. 16. Patent Owner argues that "controlling endpoint to endpoint connections within the enterprise network" in claims 1 and 12 requires interpretation. PO Resp. 8–9.

1. Patent Owner's contentions

Patent Owner argues that "[t]he specification plainly disavows control of 'endpoint to endpoint connections' through the use of legacy firewalls—*i.e.* controlling traffic to and from the network at a network perimeter, as opposed to controlling traffic between endpoints ***within*** a network." PO Resp. 9. Patent Owner argues that legacy firewalls control traffic from network to network and any traffic that goes in and out of the network goes through the firewall. *Id.* at 9–10. Patent Owner asserts that the '941 patent "specification repeatedly disparages legacy firewalls and their control of traffic between networks, noting that '***[t]raditional*** enterprise network security relies on using ***firewalls*** to provide security at ***network perimeters***' and [t]he phrase 'security at network perimeters' plainly means security ***between*** networks, not ***within*** networks." *Id.* at 10. Patent Owner argues that "legacy firewalls are able to control traffic ***between*** those subnetworks, but still could not control traffic ***within*** each subnetwork." *Id.* at 11.

2. Petitioner's contentions

Petitioner argues that the specification and prosecution history lack a clear and unmistakable disclaimer of legacy firewalls and none of the claims recite an exclusionary limitation for firewalls or legacy firewalls. Reply 1–2. Petitioner asserts that "the word 'legacy' is mentioned only once in the specification, in the discussion of *optionally* removing 'legacy hardware firewalls' in *some* embodiments . . . [b]ut this *optional* removal from *some* embodiments does not equate to a disavowal of *all* 'legacy firewalls.'" *Id.* at 2. Petitioner asserts that "legacy" is time dependent so its scope can shift with new technologies, and the meaning of "legacy firewalls" is subject to varying interpretations and is not defined in the '941 patent. *Id.* at 4–5.

3. Analysis

We determine that the ’941 patent does not clearly and unmistakably disavow legacy firewalls. In fact, the ’941 patent describes P/PoPs having features of legacy firewalls that Patent Owner argues are disavowed. In particular, the ’941 patent describes firewalls distributed geographically at a corporation’s main and satellite offices to form a network perimeter and provide security at network perimeters. Ex. 1001, 1:19–32.

The ’941 patent describes P/PoPs as *geographically distributed* across multiple buildings, cities, regions, countries, and continents to service an enterprise’s geographically distributed endpoint locations. Ex. 1001, 6:49–7:14. P/PoPs form a “virtual *perimeter*” at these distributed locations as illustrated in Figure 1 of the ’941 patent (reproduced above). A “P/PoP” is a “perimeter point of presence” that can connect virtually or physically and directly to distributed computing endpoints 110. *Id.* at 6:54, 6:49–7:14.

The ’941 patent also indicates that legacy firewalls can be moved “out of corporate offices and into the cloud.” Ex. 1001, 1:31–32. Such legacy firewalls provide a “*virtual* perimeter” just as the allegedly inventive P/PoPs form a “virtual perimeter” as “[v]irtualized, cloud-based network firewalls.” *Id.* at 1:56–65. Patent Owner does not assert that the ’941 patent disavows P/PoPs when they provide a virtual perimeter in the cloud or geographically-distributed perimeter points of presence at enterprise endpoints like prior art firewalls described in the background. *Id.* at 1:31–32, 6:25–60, 7:63–64.

The ’941 patent describes prior art firewalls controlling endpoint to endpoint connections that “hair-pin” when end users *within* the enterprise network communicate across the same link (firewall) forcing traffic to flow through the main office on its way between end users. Ex. 1001, 1:23–30.

The ’941 patent shows endpoint to endpoint connections hair-pinning at P/PoPs when endpoints 110, 110 communicate with one another through P/PoPs in Figure 1. Ex. 1001, 7:1–31, 9:7–23. Data from a bottom endpoint 110 passes by direct connection 185 to P/PoP5 and to P/PoP4 and to P/PoP3 before *hair-pinning* back to the upper endpoint 110 via edge device 130 and connection 186. *Id.* at 7:1–14. Patent Owner does not disavow P/PoPs when endpoint to endpoint connections hair-pin through them. The ’941 patent’s embodiments are *non-limiting* in any case. *Id.* at 24:48–57.

The ’941 patent describes prior art firewalls as “often used to provide *segmentation within internal networks* [to] help stop the spread of attacks” and provide “the ability to see *and control internal network traffic* [that] can be lost” when firewalls move to the cloud. Ex. 1001, 1:35–40 (emphasis added). Thus, prior art firewalls can control internal network traffic between endpoints within the network. Nor does the claim language exclude prior art firewalls from controlling endpoint to endpoint connections.

4. *Conclusion*

We determine that the ’941 patent does not clearly and unmistakably disavow legacy firewalls. The sole use of that term in the specification does not identify what features are disavowed (Ex. 1001, 4:52–67; Reply 2), and the ’941 patent describes prior art firewalls as having features and functions that P/PoPs perform (*id.* at 3–5) including segmenting internal networks and controlling internal network traffic. Ex. 1001, 1:35–40; *see* Tr. 12:18–15:1. Thus, we determine that “controlling endpoint to endpoint connections within the enterprise network” has its ordinary and customary meaning, which may include controlling endpoint to endpoint connections via firewalls. We discuss this limitation further in Section III.D.2.c. *infra*.

C. Principles of Law

A patent claim is unpatentable "if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains." 35 U.S.C. § 103. "The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007). Similarly, "if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill." *Id.* at 417.

The question of obviousness is resolved based on underlying factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) when in evidence, objective evidence of obviousness or non-obviousness. *Graham v. John Deere Co. of Kan. City*, 383 U.S. 1, 17–18 (1966). Neither party has presented objective evidence of obviousness or non-obviousness.

A party must show that a skilled artisan had a motivation to combine references and a reasonable expectation of success in meeting the limitations of the claimed invention. *Arctic Cat Inc. v. Bombardier Recreational Prods. Inc.*, 876 F.3d 1350, 1360–61 (Fed. Cir. 2017); *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1367 (Fed. Cir. 2016); *see Elekta Ltd. v. ZAP Surgical Sys., Inc.*, 81 F.4th 1368, 1376 (Fed. Cir. 2023) ("a finding of reasonable expectation of success can be implicit").

D. Ground 1: Alleged Obviousness Over Wang

Petitioner asserts that claims 1, 2, 4, 5, 12, 13, 15, and 16 are unpatentable under 35 U.S.C. § 103 over Wang. Pet. 16–39.

1. Wang

Wang discloses "a dynamic firewall controller for automatic firewall policy generation and configuration." Ex. 1004 ¶ 2. Firewall controller 102 dynamically and automatically configures and applies firewall policies in network 100 to control network data traffic to and from devices 104, 106, 108 in the network shown in Figure 1 of Wang, reproduced below. *Id.* ¶ 12.

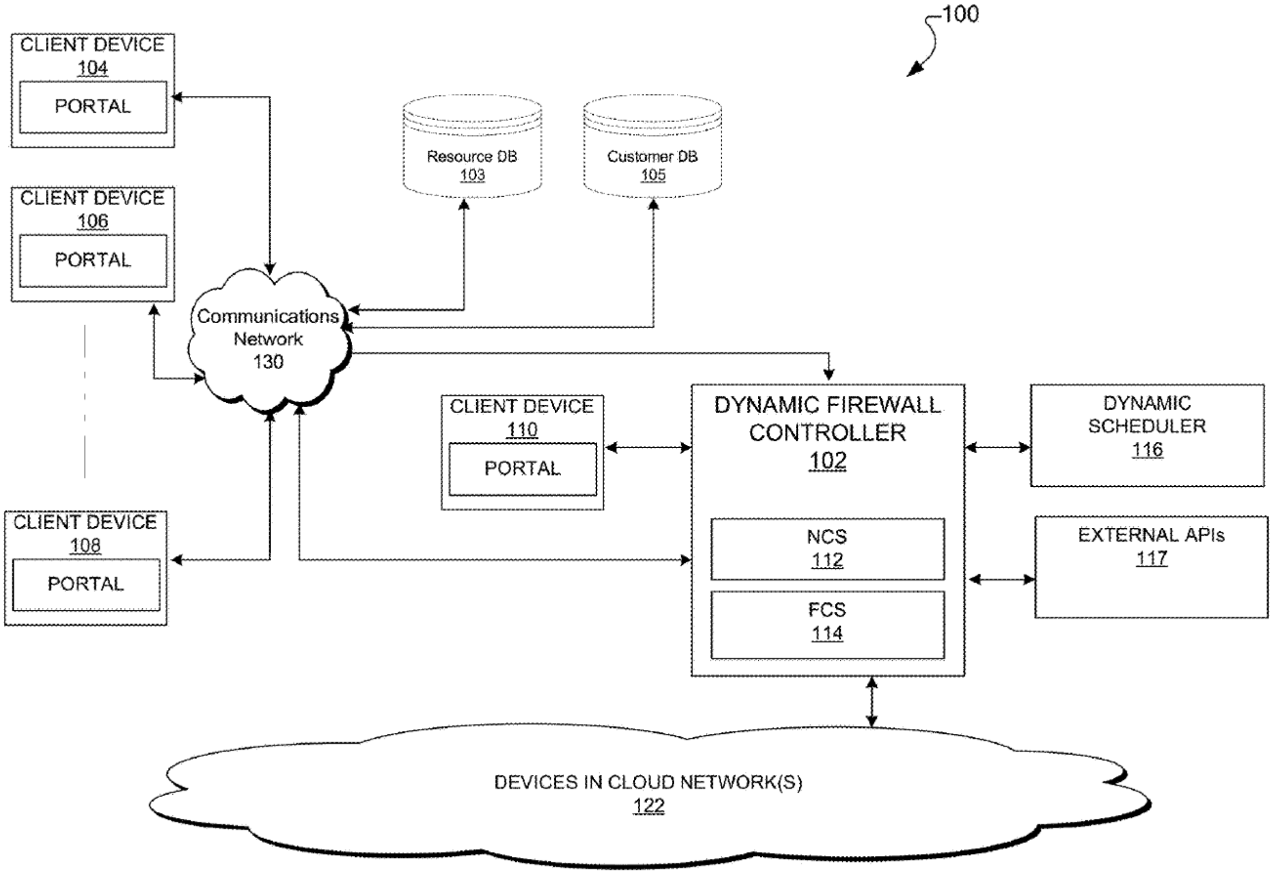


FIG. 1

Figure 1 illustrates network 100 with dynamic firewall controller 102 that connects client devices 104–110 within network 100. Ex. 1004 ¶ 15.

Controller 102 sends application programming interface (API) calls to network configuration system (NCS) 112 and firewall configuration system (FCS) 114 to configure policies, queue requests in scheduler 116, and push firewall policies to network elements. Ex. 1004 ¶¶ 18, 19, 25. Firewall policies relate to ports, communication protocols, source and destination IP addresses, and source and destination ports. *Id.* ¶ 23. NCS 112 may do a dry run to validate firewall policies in a virtual environment that emulates network elements. *Id.* ¶ 26. Resource database 103 stores firewall policies as database records with fields for configurations, which apply to subnets of computing devices illustrated in Figure 2, produced below. *Id.* ¶ 16.

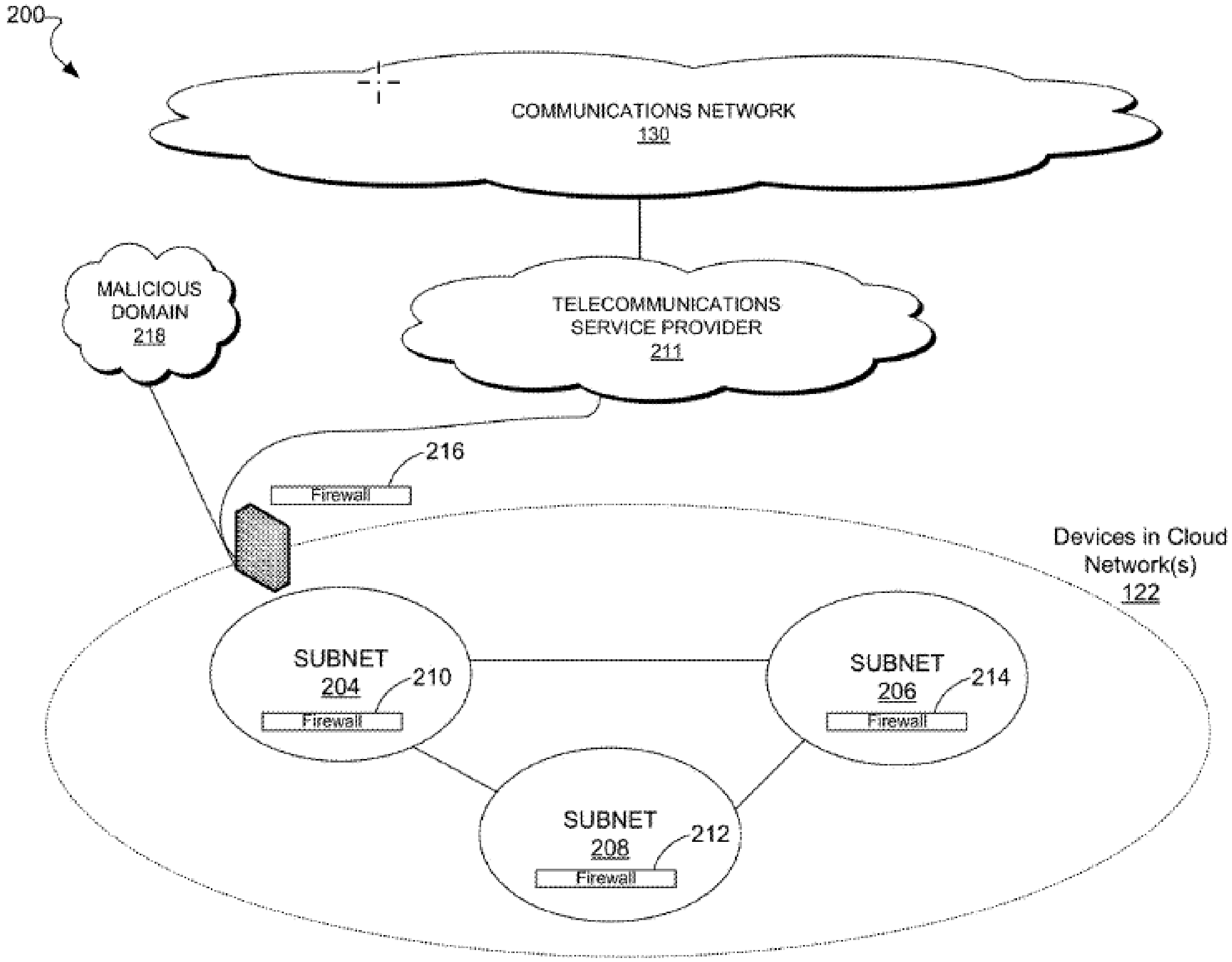


FIG. 2

Figure 2 shows subnets in cloud network 122. Ex. 1004 ¶ 20. The subnets include an entity's computing devices maintained in geographic locations or all the computing devices of an organization located in the same local area network (i.e., the subnet). *Id.* ¶ 17. Subnet 204 includes human resources computing systems (e.g., hardware and/or software). *Id.* ¶ 20. Subnet 206 includes engineering computing resources. *Id.* Subnet 208 includes sales data and management computing resource*s* of the enterprise. *Id.* Firewalls 210, 212, 214 control connections between computers in these subnets. *Id.*

Wang's firewall policies control network traffic between computing resources in subnets 204, 206, 208, i.e., endpoint to endpoint connections. Ex. 1004 ¶ 21. "[A] customer may want to implement a firewall policy that states that subnet 206 corresponding to the engineering office and related *computing systems* should not *access resources* of subnet 204 corresponding to the customer's human resources and *computing systems*." *Id.* A policy thus controls traffic between computing resources of subnets, i.e., endpoints.

Firewall policies control traffic between computing resources of each subnet 204–208 and threats or malicious activity for traffic coming from a domain external to the subnets, e.g., malicious domain 218. Ex. 1004 ¶ 21.

To manage firewall configurations, customers use client devices 104–110 to access a portal and provide firewall policy configurations to dynamic firewall controller 102. Ex. 1004 ¶ 21. "[A] customer may interact with the client devices 104–110 to implement configurations that automatically block traffic from the malicious domain." *Id.* Client devices 104–110 include a personal computer, handheld computer, mobile phone, digital assistant, smart phone, server, or application that may generate requests to configure firewalls and policies, or any combination of these devices. *Id.* ¶ 15.

2. Claims 1 and 12

a. *1[pre]: "A method for protecting an enterprise network, the method comprising, at a system comprising one or more processors and memory that are remote from the enterprise network"/12[pre]: "A system for protecting an enterprise network . . ."*

i. Petitioner's contentions

Petitioner contends that Wang discloses a method for protecting devices in cloud networks 122 of an enterprise network at controller 102, which is a system that is remote from the enterprise network system in elements 1[pre]/12[pre]. Pet. 19–25 (citing Ex. 1004 ¶¶ 17, 18, 19, 20, 21, 28–31, code (57), Figs. 1, 2, 4; Ex. 1002 ¶¶ 57, 59–62, 64).

ii. Patent Owner's arguments

Patent Owner does not contest Petitioner's assertions regarding elements 1[pre]/12[pre]. *See generally* PO Resp.; Sur-reply.

iii. Conclusion

Regardless of whether the preamble is limiting, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Wang discloses or suggests elements 1[pre]/12[pre].

b. *1[a]/12[a]: "controlling communications to and from the enterprise network according to a set of security policies"*

i. Petitioner's contentions

Petitioner asserts that Wang's controller 102 controls communications to and from devices in enterprise network 122 by configuring firewall 216 to control network traffic and communications to and from enterprise network 122, e.g., by blocking traffic from a malicious domain outside the network. Pet 25–26 (citing Ex. 1004 ¶¶ 12, 17, 18, 21, Fig. 2); Reply 9–11.

Petitioner asserts that a skilled artisan would have understood that by configuring a firewall and/or policies that (1) control Internet Protocol (IP) data traffic to and from a network, (2) enable its subnets to allow the organization to access the Internet, and (3) automatically block traffic from outside the network, e.g., traffic from malicious domain 218, controller 102 controls network traffic and communications to and from the enterprise network by security policies as claimed. Pet. 26–27 (citing Ex. 1002 ¶ 67).

ii. Patent Owner's arguments

Patent Owner argues that Wang's subnet firewalls do not control communications to and from the enterprise network because resources in each subnet 204, 206, 208 may be equipped to detect threats from a domain external to the subnets such as malicious domain 218 using subnet firewalls to block traffic from the malicious domain, but Wang's subnet firewalls only control traffic to and from the respective subnet that it protects and cannot block traffic to and from devices within the enterprise network that are not within the subnets. PO Resp. 20–22.

iii. Analysis

Patent Owner's arguments do not address Petitioner's contentions that *Wang's controller 102* configures firewall 216 to control communications to and from enterprise network 122 and malicious domain 218. Pet. 25–26; Reply 9–11; Ex. 1002 ¶ 66; Ex. 1004 ¶¶ 18, 21. Wang's controller 102 uses firewall configuration systems engine (FCS) 114 to configure firewalls and define routines or protocols for firewalls of network 122 and subnet firewalls 210–216 to block network traffic coming from domain 218. *Id.* ¶¶ 18–22. Wang's firewall 216 also controls communications to and from the entire enterprise network 122 as Patent Owner agrees. Reply 10; PO Resp. 34.

Controller 102 also configures firewalls 210, 212, 214 of subnets 204, 206, 208 of enterprise network 122 to (1) manage communications between computing resources in the subnets *and* (2) control communications to and from the subnets and malicious domain 218 (Ex. 1004 ¶¶ 20–23; Reply 9–11; Pet. 25–27) just as P/PoPs 121 control traffic to and from an enterprise network that also comprises *subnets* (Ex. 1001, 7:1–14, 14:4–38). We agree with Dr. Lee that the subnets "constituted an enterprise network" (Ex. 1002 ¶¶ 57–59) and are part of the larger enterprise network 122 (Ex. 1004 ¶ 17).

iv. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Wang discloses or suggests elements 1[a]/12[a].

c. *1[b]/12[b]: "controlling endpoint to endpoint connections within the enterprise network according to the set of security policies"*

i. Petitioner's contentions

Petitioner asserts that Wang controls endpoint to endpoint connections between devices in subnets of enterprise network 122 using firewall policies that control network traffic between computing endpoints of subnets 204, 206, 208 such as a firewall policy that subnet 206 for the engineering office *and its computing systems* should not access *computing resources* of subnet 204. Pet. 27 (citing Ex. 1004 ¶ 21). Petitioner asserts that the "computing systems" in subnets 204 and 206 are endpoints within the enterprise network consistent with examples of "endpoint" devices in the '941 patent including office computers, data centers, and cloud instances. *Id.* at 27–28 (citing Ex. 1001, 6:60–64; Ex. 1002 ¶ 69).

ii. Patent Owner's arguments

Patent Owner argues, "Wang discloses legacy firewalls that control traffic ***between*** networks (or subnetwork[s])—control which the '941 patent disavowed from the scope of control of endpoint to endpoint connections." PO Resp. 16; *see* Sur-reply 6 ("Wang's subnet firewalls are precisely what the '941 patent disavows—physical legacy devices operating at the perimeter of subnets within a larger network."). Patent Owner asserts that Wang's firewalls do not control endpoint to endpoint connections ***within*** a network because they are legacy firewalls that control traffic ***between*** subnetworks using legacy firewalls that are outside the scope of the claims given the specification's disavowal of legacy firewalls. *Id.* at 17–18.

iii. Analysis

We disagree with Patent Owner because the '941 patent does not disavow firewalls that control endpoint to endpoint connections as discussed in Section III.B. *supra*. Wang's controller 102 configures policies for subnet firewalls 210, 214 to control connections between endpoints in subnet 206 (engineering office computing systems) and endpoints in subnet 204 (human resources office computing systems) as claimed. Ex. 1004 ¶¶ 18–21, Fig. 2.

We credit Dr. Lee's testimony that Wang's firewall policies control endpoint connections *within* enterprise network 122 such as a firewall policy controls connections of engineering office computing systems in subnet 206 to human resources computing systems in subnet 204. Ex. 1002 ¶ 69 (citing Ex. 1004 ¶ 21). Dr. Lee testifies that Wang's firewalls control connections between computing systems in subnets 204, 206, 208, and the systems are endpoints. *Id.* (asserting that "endpoints" are described as office computers, data centers, and cloud instances in Ex. 1001, 6:60–64); Tr. 11:4–16.

Dr. Black's testimony that Wang's firewalls provide security at the network perimeter (Ex. 2003 ¶¶ 39, 40; Sur-reply 6) and Patent Owner's arguments that Wang's firewalls control traffic between networks (PO Resp. 19) ignore Wang's teachings that firewalls 210–214 control connections between computing endpoints in subnets 204–206 *within* Wang's enterprise network 122. Ex. 1004 ¶¶ 18–22, Figs. 1–3; Reply 6–9. Endpoints include such subnet office computers and data centers. Ex. 1001, 6:60–64, 14:4–38.

Patent Owner also seeks to read "network segmentation agents" into elements 1[b]/12[b] by arguing that "the '941 patent's network segmentation agents can provide 'granular . . . control over all traffic happening "behind the firewall,"' . . . because 'each enterprise endpoint system has a firewall around itself'" and "Wang's firewalls do not provide such granular control." PO Resp. 19. We do not read such agents into the claims absent a disavowal or definition not present here. *See Liebel-Flarsheim Co. v. Medrad, Inc.*, 358 F.3d 898, 906 (Fed. Cir. 2004) ("Even when the specification describes only a single embodiment, the claims . . . will not be read restrictively unless the patentee has demonstrated a clear intention to limit the claim scope using 'words or expressions of manifest exclusion or restriction.'") (citation omitted); *SuperGuide Corp. v. DirecTV Enter., Inc.*, 358 F.3d 870, 875 (Fed. Cir. 2004) (a particular embodiment in the written description may not be read into a claim if the claim language is broader than the embodiment); *cf.* Ex. 1001, 1:31–40 (firewalls provide segmentation in internal networks).

iv. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Wang discloses or suggests elements 1[b]/12[b].

d. *1[c]/12[c]: "receiving a request for modifications to one or more policies of the set of policies"*

i. Petitioner's contentions

Petitioner contends that Wang's controller 102 receives a modification to the firewall policy when a user interacts with client devices 104–110 to initiate a request to dynamically configure the firewalls and its policies, and the user can use external APIs 117 provided by controller 102 to "trigger firewall policy change inputs" that would modify existing firewall policies. Pet. 28–29 (citing Ex. 1004 ¶¶ 15, 22, Fig. 3 (step 302); Ex. 1002 ¶ 72).

ii. Patent Owner's arguments

Patent Owner does not contest Petitioner's assertions regarding elements 1[c]/12[c]. *See generally* PO Resp.; Sur-reply.

iii. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Wang discloses or suggests elements 1[c]/12[c].

e. *1[d]/12[d]: "automatically generating a policy digest formatted according to a predefined format, the policy digest comprising the modifications, and storing the policy digest in memory"*

i. Petitioner's contentions

Petitioner asserts that Wang's controller is configured "for automatic firewall policy generation and configuration" to generate firewall policies that are stored as "database records having fields that reference specific firewall configurations" by receiving a modification to a firewall policy and automatically configuring aspects of the firewall and its policies. Pet. 30–31 (citing Ex. 1004 ¶¶ 2, 16, 18, Fig. 3 (step 304)).

Petitioner asserts that the ’941 patent describes a “policy digest” as a “structured representation of a set of user-requested changes to be made to the configuration,” and Wang’s firewall policies are “database records having fields that reference specific firewall configurations” based on a requested modification of a user. Pet. 31 (quoting Ex. 1001, 11:30–33 and Ex. 1004 ¶ 16). Petitioner asserts a skilled artisan would have recognized that Wang’s firewall policies are “policy digests” because they specify a configuration of ports, communication protocols, and services used to manage network traffic, and Wang’s fields match the policy digest fields in Figure 4C of the ’941 patent. Petitioner asserts that Wang’s fields have a predefined format because they are stored as “database records” with fields that reference specific firewall configurations and have a format defined by fields of the database records configuration. *Id.* at 31–33 (citing Ex. 1004 ¶¶ 16, 23, claim 6; Ex. 1001, 17:9–23, Fig. 4C; Ex. 1002 ¶ 75); Reply 12.

ii. Patent Owner’s arguments

Patent Owner argues that Wang does not describe its firewall configurations, and Petitioner’s obviousness theories fail to establish a predefined format such as a predefined syntax for firewall configurations. PO Resp. 22. Patent Owner asserts that Petitioner fails to identify any policy digest formatted in a predefined format, which is the syntax of the policy that is enforced and must be known to process the data because the format of the policy digest defines the specific files that the policy digest can support such as source address, destination address, port numbers, and protocol as illustrated in Figure 4C of the ’941 patent. *Id.* at 23–25. Patent Owner asserts that Wang does not disclose any such policy digest formatted in a predefined format. *Id.* at 25–26.

iii. Analysis

We find that Wang's firewall policies have predefined fields that are used to define policies at a Portal, and policies are stored as database records with "fields that reference specific firewall configurations." Ex. 1004 ¶ 16. The firewall policies predefine fields for "ports, communication protocols, or services" and "source IP addresses, destination IP addresses, source ports, destination ports, and/or protocols." *Id.* ¶ 23. Dr. Lee testifies that database records are a structured representation of changes to a configuration just as the '941 patent describes policy digests. Ex. 1002 ¶ 74; Ex. 1001, 11:30–32. Dr. Lee testifies that Wang's firewall policies prevent subnet computing devices from accessing one another within the enterprise network. Ex. 1002 ¶ 69. Dr. Black does not address this testimony. Ex. 2003 ¶¶ 51, 52.

Patent Owner asserts that "whether Wang's firewall configuration is formatted in a predefined format depends on whether it is formatted in the correct syntax, whether it uses fields appropriate for a firewall policy (such as *source address, destination address, port, protocol*)." PO Resp. 23 (emphasis added). We find that Wang's policy digest specifies source IP address, destination IP address, source port, destination port, and protocol syntax fields. Ex. 1004 ¶ 23; *see* PO Resp. 24 (a "correct syntax" has source and destination address, port, and protocol fields); Ex. 1001, Fig. 4C (policy digest specifies source and destination 1414, IP addresses 1402, 1404, ports 1406, 1410, protocols 1410). We find Wang's firewall policies use a syntax that allows firewalls to open specific ports that enable subnet computers to communicate with network services, block a port, adjust a protocol, apply security settings, and enable or disable a service. Ex. 1004 ¶ 23; Ex. 2003 ¶ 63 (a policy must use correct syntax for firewalls to be able to process it).

According to the ’941 patent, a policy digest may provide a uniform policy for all P/PoPs or different functions and elements at disparate P/PoPs. Ex. 1001, 7:43–47. Syntax formats vary. *Id.* at 17:4–8. Dr. Black testifies, “Figure 4C shows a lot of different policy digests in a predefined format.” Ex. 2003 ¶ 64. We find that Wang’s policy digests control endpoint to endpoint traffic, and traffic to and from the network, in formats that firewalls use for each connection, and Wang validates the syntax. Ex. 1004 ¶¶ 23–26.

iv. Conclusion

Based on the parties’ contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Wang discloses or suggests elements 1[d]/12[d].

f. *1[e]/12[e]: “storing the policy digest in the memory; retrieving the policy digest from the memory”*

i. Petitioner’s contentions

Petitioner asserts that controller 102 validates and implements firewall policy changes (policy digests) by retrieving policy changes from memory and checking and validating firewall policy changes against a set of known rules without actually changing the network elements, and a skilled artisan would have found it obvious that in order to validate the policy changes, controller 102 would store them in memory after they were generated and retrieve them from memory for validation using memory implemented with controller 102 so that validation could occur later to allow urgent operations to proceed. Pet. 33–34 (citing Ex. 1004 ¶¶ 26, 29–32; Ex. 1002 ¶¶ 76, 77).

ii. Patent Owner’s arguments

Patent Owner does not contest Petitioner’s assertions regarding elements 1[e]/12[e]. *See generally* PO Resp.; Sur-reply.

iii. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Wang discloses or suggests elements 1[e]/12[e].

g. *1[f]/12[f]: "generating one or more calls to one or more system components that control the communications to and from the enterprise network and the endpoint to endpoint connections based on the policy digest"*

i. Petitioner's contentions

Petitioner asserts that Wang's controller 102 generates API calls to network configuration systems engine (NCS) 112 or firewall configuration system engine (FCS) 114 that use logic to configure routers and switches in subnets and firewalls to control communications to and from devices in enterprise cloud network 122 and between devices in subnets (endpoint to endpoint connections) based on the policy changes. Petitioner asserts that a request to configure or update a firewall policy causes controller 102 to make API calls to NCS 112 and FCS 114 to define routines and protocols to configure the firewalls. Pet. 34–36 (citing elements 1[a]–1[b]/12[a]–12[b]; Ex. 1004 ¶¶ 18, 19, 24, 25, Fig. 1; Ex. 1002 ¶¶ 81, 82).

ii. Patent Owner's arguments

Patent Owner does not contest Petitioner's assertions regarding elements 1[f]/12[f]. *See generally* PO Resp.; Sur-reply.

iii. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Wang discloses or suggests elements 1[f]/12[f].

h. *1[g]/12[g]: "modifying control of the communications to and from the enterprise network and the endpoint to endpoint connections based on the one or more calls"*

i. Petitioner's contentions

Petitioner contends that Wang's controller 102 modifies control of network traffic to and from the enterprise network and between devices in subnets 204, 206, 208 by making API calls to NCS 112 and/or FCS 114 to implement updated firewall policies. Petitioner asserts that controller 102 automatically manages network traffic to and from subnets 204, 206, 208 to ensure network traffic complies with the updated firewall policy. Petitioner asserts that a skilled artisan would have recognized that managing network traffic to ensure that it complied with the updated firewall policy meant that controller 102 modified control of network traffic to and from the enterprise network and between devices in the enterprise network based on API calls. Pet. 36–37 (citing contentions for elements 1[a], 1[b]/12[a], 12[b], 1[f]/12[f]; Ex. 1004 ¶ 27, claim 6; Ex. 1002 ¶ 85).

ii. Patent Owner's arguments

Patent Owner does not contest Petitioner's assertions regarding elements 1[g]/12[g]. *See generally* PO Resp.; Sur-reply.

iii. Analysis

We find that Wang's validation of firewall policies changes before implementation teaches this element and policy syntax. Ex. 1004 ¶¶ 26, 27.

iv. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Wang discloses or suggests elements 1[g]/12[g].

i. *Conclusion*

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 1 and 12 are unpatentable over Wang.

3. *Claims 2 and 13: ". . . wherein the request for modification is based on selections made by a user via a user interface"*

a. *Petitioner's contentions*

Petitioner asserts that Wang discloses that its controller 102 provided a user with access to "an initial set of network 'services' corresponding to a particular customer, via a web portal, interactive interface(s), graphical-user interface(s)," and the user may "interact with the Portal to initiate a request . . . defin[ing] and implement[ing] firewall policies." Petitioner also asserts that Wang discloses that the "graphical user-interface may provide various *components, buttons, menus* . . . allow[ing] the customer to provide input defining the firewall policy," and a skilled artisan would have understood that a user would initiate a request to modify a policy by selecting buttons and menus of Wang's graphical-user interface(s). Pet. 37–38 (quoting Ex. 1004 ¶¶ 13, 22 (emphasis added), 33) (citing Ex. 1002 ¶ 88).

b. *Patent Owner's arguments*

Patent Owner does not contest Petitioner's assertions regarding claims 2 and 13. *See generally* PO Resp.; Sur-reply.

c. *Analysis*

Wang's graphical user interface includes components, buttons, menus, and/or other functions that allow a user to identify configurations for various networks and communications services, to provide input defining a firewall policy, and to trigger firewall policy change inputs. Ex. 1004 ¶ 22.

Wang discloses that its dynamic firewall controller provides access to an initial set of network services for a customer via a web portal, interactive interface(s), and graphical-user interface(a), and users enter commands and information via a user interface or other input devices. Ex. 1004 ¶¶ 13, 33.

d. *Conclusion*

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 2 and 13 are unpatentable over Wang.

4. Claims 4 and 15: ". . . wherein the policy digest comprises one or more of an inbound network traffic policy modification, an outbound network traffic policy modification, and an internal network traffic policy modification"

a. *Petitioner's contentions*

Petitioner contends that Wang's controller 102 configured firewall policies that controlled inbound network traffic by blocking traffic from a malicious domain and controlling traffic to the enterprise network, Wang's controller controlled outbound network traffic by controlling IP traffic *from* a network and allowing the organization to access the Internet, and Wang's controller configured firewall policies that controlled internal traffic by blocking network traffic from subnet 206 to subnet 204 or limiting traffic to a specified set of connections. Petitioner asserts that a skilled artisan would have found it obvious that Wang's system generated and implemented policy changes (policy digests) for inbound, outbound, and internal network traffic policy modification to control communications to and from the network and between devices in the network. Pet. 38–39 (citing Ex. 1004 ¶¶ 12, 17, 21; Ex. 1002 ¶ 91).

b. *Patent Owner's arguments*

Patent Owner does not contest Petitioner's assertions regarding claims 4 and 15. *See generally* PO Resp.; Sur-reply.

c. *Conclusion*

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 4 and 15 are unpatentable over Wang.

5. *Claims 5 and 16: ". . . wherein the policy digest is retrieved according to a predefined schedule"*

a. *Petitioner's contentions*

Petitioner contends that Wang's controller 102 retrieves policy digests from memory, and dynamic scheduler 115 maintains requests received to define or configure a firewall policy in a queue for controller 102 and passes the requests to controller 102 "at the appropriate time for processing" so the firewall policy can be implemented at "a specific period of time (e.g., a *time window* during which the firewall policy is applicable)." Petitioner contends that a skilled artisan would have recognized that implementing a firewall policy at "a specific period of time" means controller 102 would retrieve and implement a policy on a predefined schedule in a "*time window* during which the firewall policy is applicable" for processing instead of requiring immediate application of a firewall policy. Pet. 39 (citing contentions for elements 1[e]/12[e]; Ex. 1004 ¶¶ 19, 23, claim 3; Ex. 1002 ¶ 95).

b. *Patent Owner's arguments*

Patent Owner argues that Petitioner relies on its contentions for elements 1[e]/12[e] where Petitioner asserted that controller 102 would retrieve a policy digest from memory *for validation*. PO Resp. 26.

Patent Owner argues that to prove that "the policy digest is retrieved according to a predefined schedule" Petitioner would have to show that Wang runs the policy validation on a predefined schedule, and Petitioner has not shown Wang's dynamic scheduler 116 validates policies in the specific time period that dynamic scheduler passes requests to controller 102 to implement at a specific time. PO Resp. 26–27. Patent Owner argues that a skilled artisan would not have understood Wang to use a dynamic scheduler for policy validation because validation is a highly complicated, time-consuming process that would be undesirable to schedule for a specific time window because it would delay implementation of the policy. *Id.* at 27–30.

c. *Analysis*

We agree with Petitioner that a skilled artisan would have found it obvious to use Wang's dynamic scheduler 116 to queue requests to define or otherwise configure a firewall policy *and* to schedule "dry runs" of such proposed firewall policies to check and validate a proposed firewall policy change "because Wang did not require immediate application of the firewall policy but instead described that the controller implemented the firewall policy in a 'time window during which the firewall policy is applicable' for processing." Pet. 39 (citing Ex. 1004 ¶¶ 19, 23). We agree with Petitioner that validating policies according to a predefined schedule, e.g., during off-peak hours, would minimize disruption to operations and allow control of testing for smoother deployment of policy changes. Reply 16 (citing Pet. 39). We agree with Petitioner that if Wang's validation is a complicated, time-consuming process, as Patent Owner argues, a predetermined schedule for validating such changes would minimize disruptions. *Id.* at 15–16.

We find that Wang validates firewall policy changes at network devices of a subnet using NCS 112 to execute the proposed firewall policy changes against replicated virtual devices to simulate changes in a virtual environment that uses the same network elements with emulated functions. Ex. 1004 ¶¶ 26, 27. We also find that Wang's validation process is linked to implementation because Wang validates policies before implementing them at network devices and elements. *Id.* We agree with Petitioner that it would have been obvious to schedule validation dry runs at off-peak hours to avoid disrupting other more urgent firewall operations. Reply 15–16.

Dr. Lee testifies that a skilled artisan would have recognized the benefits of storing policy changes in memory because "[t]his method enables deferred validation, allowing subsequent execution while giving precedence to urgent operations over the immediate implementation of policy changes." Ex. 1016 ¶ 1; *see* Ex. 1002 ¶ 95. "By storing policy changes in memory and validating them according to a predefined schedule, a [skilled artisan] would recognize the potential for optimizing network performance and stability" and "operational disruptions can be minimized, and a more controlled environment for testing and implementing policy changes can be achieved." Ex. 1016 ¶ 1. These contentions support Petitioner's proposal to use Wang's dynamic scheduler 116 to schedule validations of proposed policy digests. *DyStar Textilfarben GmbH & Co. Deutschland KG v. C.H. Patrick Co.*, 464 F.3d 1356, 1368 (Fed. Cir. 2006) (an implicit motivation to combine exists when an "improvement" makes a product stronger, cheaper, faster, lighter, smaller, more durable, or more efficient). Validations ultimately result in the implementation of the policies changes so that a validation supports the final implementation of a proposed policy change. Ex. 1004 ¶¶ 26, 27.

d. *Conclusion*

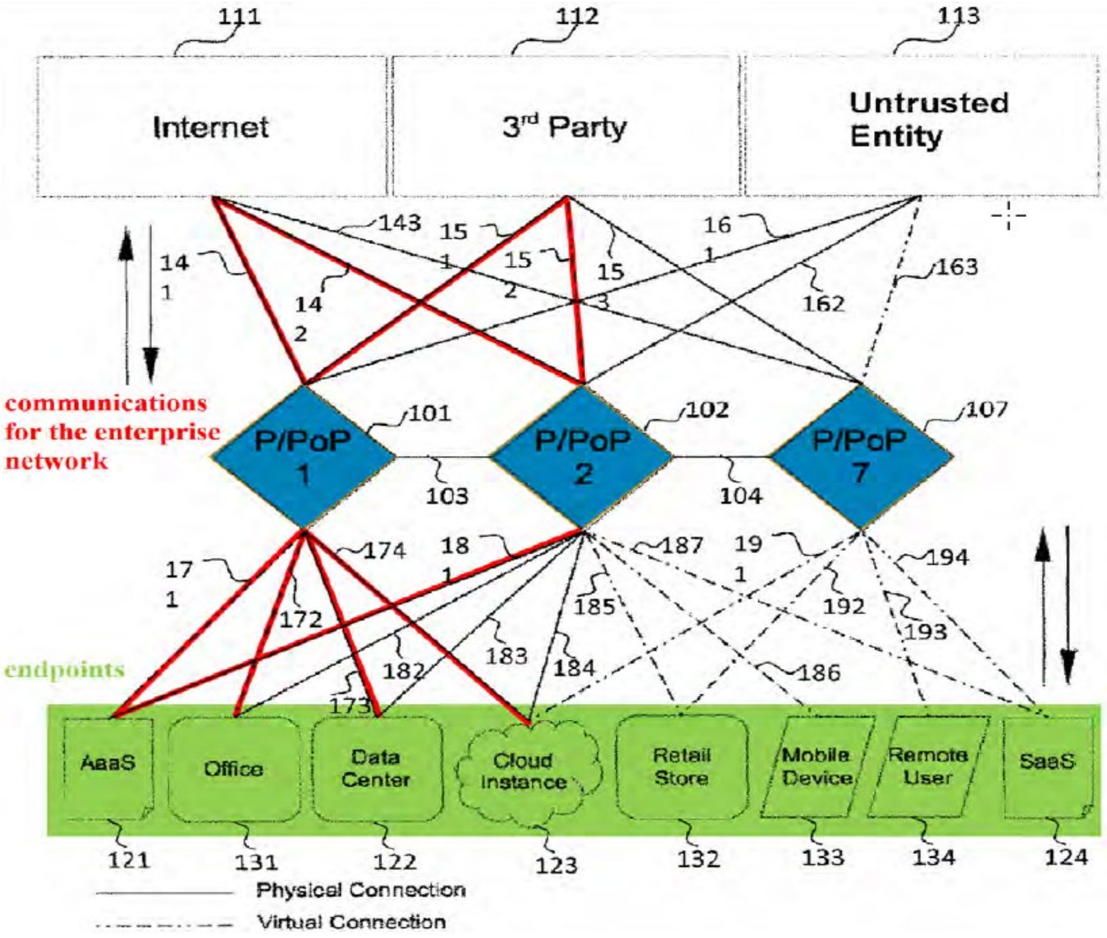
Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 5 and 16 are unpatentable over Wang.

E. Ground 2: Alleged Obviousness Over Wang and Pasdar

Petitioner asserts that claims 3 and 14 are unpatentable under 35 U.S.C. § 103 over Wang and Pasdar. Pet. 40–46.

1. Pasdar

Pasdar's network security system comprises P/PoPs (blue) shown in Figure 1, which is reproduced below with Petitioner's annotations (Pet. 41).



Pasdar, FIG. 1 (annotated)

Figure 1 of Pasdar depicts perimeter points of presence (P/PoPs) 101, 102, 107 that connect virtually or physically with computing nodes of AaaS 121, office 131, data centers 122, cloud instances 123, retail store 132, mobile device 133, remote user 134, and SaaS 124. Ex. 1005 ¶¶ 1, 49, 50. P/PoPs control inbound and outbound data to untrusted or unknown entities 111, 112, 113. *Id.* ¶¶ 51–53, 56, 57. P/PoPs include systems for processing data such as application resiliency system 202, security system 203, forensics system 204, DoS Protection System 205, and system Y 206. *Id.* ¶ 57. For example, P/PoP 101 virtually connects to AaaS 121 and Office 131 via virtual connections 171, 172 and physically connects with Data Center 122 and Cloud Instance 123 via physical connections 173, 174. Ex. 1005 ¶ 50.

2. *Petitioner's contentions*

Petitioner asserts that Pasdar routes communications of the enterprise network through P/PoPs that implement a security stack that is modifiable by calls as recited in claims 3 and 14. Pet. 40. Petitioner asserts that the P/PoPs deliver a virtual perimeter for an enterprise network and its multiple endpoints with a security stack of application resiliency system 202, security system 203, forensics system 204, DoS Protection System 205, and system Y 206 for routing inbound, outbound, and internal communications. *Id.* at 40–43 (citing Ex. 1005 ¶¶ 49, 52, 57, 94–96, Figs. 1, 2B). Petitioner asserts that Pasdar's P/PoP systems would have been recognized by a skilled artisan as the claimed "security stack" because application resiliency system 202, security system 203, forensics system 204, DoS system 205, and system Y 206 are identical to the systems of the security stack described in the '941 patent. Pet. 42 (citing Ex. 1005 ¶ 57, Fig. 2A; Ex. 1001, 7:14–31, Fig. 1; Ex. 1002 ¶ 100).

3. *Motivation to combine*

Petitioner contends that a skilled artisan would have included Pasdar's P/PoPs and security stack in Wang to provide a customized virtual perimeter of distributed devices that would manage disparate perimeters and augment and improve Wang's efficiency. Pet. 43–44 (citing Ex. 1004 ¶¶ 2, 4, 20; Ex. 1005 ¶ 5; Ex. 1002 ¶ 104). Petitioner asserts that providing modifiable security stacks in Wang would allow an enterprise to provide endpoints with data center and security services, privacy, and application resiliency and availability at each P/PoP as customized network services for Wang's growing network as both Wang and Pasdar desire to do. *Id.* at 44–46 (citing Ex. 1004 ¶¶ 13, 20; Ex. 1005 ¶¶ 5, 31, 117; Ex. 1002 ¶¶ 105–107).

4. *Patent Owner's arguments*

Patent Owner and Dr. Black assert that there is no motivation to combine Pasdar and Wang because "all of the purported motivations are already in Wang." PO Resp. 31 (citing Ex. 2003 ¶ 80); Ex. 2003 ¶ 80. Patent Owner asserts that Petitioner's assertion of reasonable expectation of success does not establish that Wang's calls are compatible with Pasdar's system for modifying security stacks of P/PoPs or that the P/PoPs can be updated by a remote system remote. PO Resp. 35–36.

5. *Analysis*

We find that Petitioner's asserted modifications with Pasdar would have improved Wang because Wang provided services at the firewall level, but Pasdar "implement[ed] these services at the P/PoP(s), offloading some tasks from individual firewalls and thus . . . enhancing performance." Reply 17 ("Patent Owner ignores other benefits, like the flexibility and granular customization, that Pasdar's P/PoP system would offer to Wang's system.").

We find that Pasdar's P/PoPs would customize Wang's initial settings to enhance security as the network expands and would have allowed Wang's distributed devices to leverage a single global perimeter policy for security, privacy, and application resiliency and availability as Pasdar teaches. Pet. 45 (quoting Ex. 1005 ¶ 31; citing Ex. 1002 ¶ 106); *id.* at 43–45; Reply 20.

We agree with Dr. Lee's testimony that a skilled artisan would have been motivated to add Pasdar's functionalities to route communications to a P/PoP and customize a P/PoP's security stack to Wang. Ex. 1002 ¶ 106. The upgrade would have improved Wang's similarly and would have had a reasonable expectation of success by using Wang's calls to modify a P/PoP's security stack to implement a policy, and combining these known prior art elements according to their known functions would have yielded predictable results as Dr. Lee testifies. *Id.* ¶ 107. *See KSR*, 550 U.S. at 416.

We find that Wang's configuration of network services at centralized resource database 103 (PO Resp. 34) would be improved by configuring P/PoPs to provide specific network services along Wang's varied enterprise network 122 that has different locations and needs (Ex. 1004 ¶¶ 17, 20, 21), just as Pasdar centrally controls P/PoPs (Ex. 1005 ¶ 115, Fig. 7A). We agree with Dr. Lee that Pasdar's customized P/PoP security stack would leverage a single global perimeter policy with security, privacy, application resilience, and application availability in Wang. Ex. 1002 ¶¶ 106, 107; Reply 18–19; Ex. 1016 ¶ 2 (coding software functions is routine and straightforward).

6. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 3 and 14 are unpatentable over Wang and Pasdar.

F. Ground 3: Alleged Obviousness Over Wang and Sikka

Petitioner asserts that claims 6, 7, 17, and 18 are unpatentable under 35 U.S.C. § 103 over Wang and Sikka. Pet. 46–52.

1. Sikka

Sikka's appliance 200 configures policies and settings based on data received from a user via daemon services 218 that run continuously and/or in the background to receive and forward service requests to other programs or processes and to perform continuous or periodic functions for network control as shown in Figure 2A reproduced below. Ex. 1006 ¶¶ 1, 116.

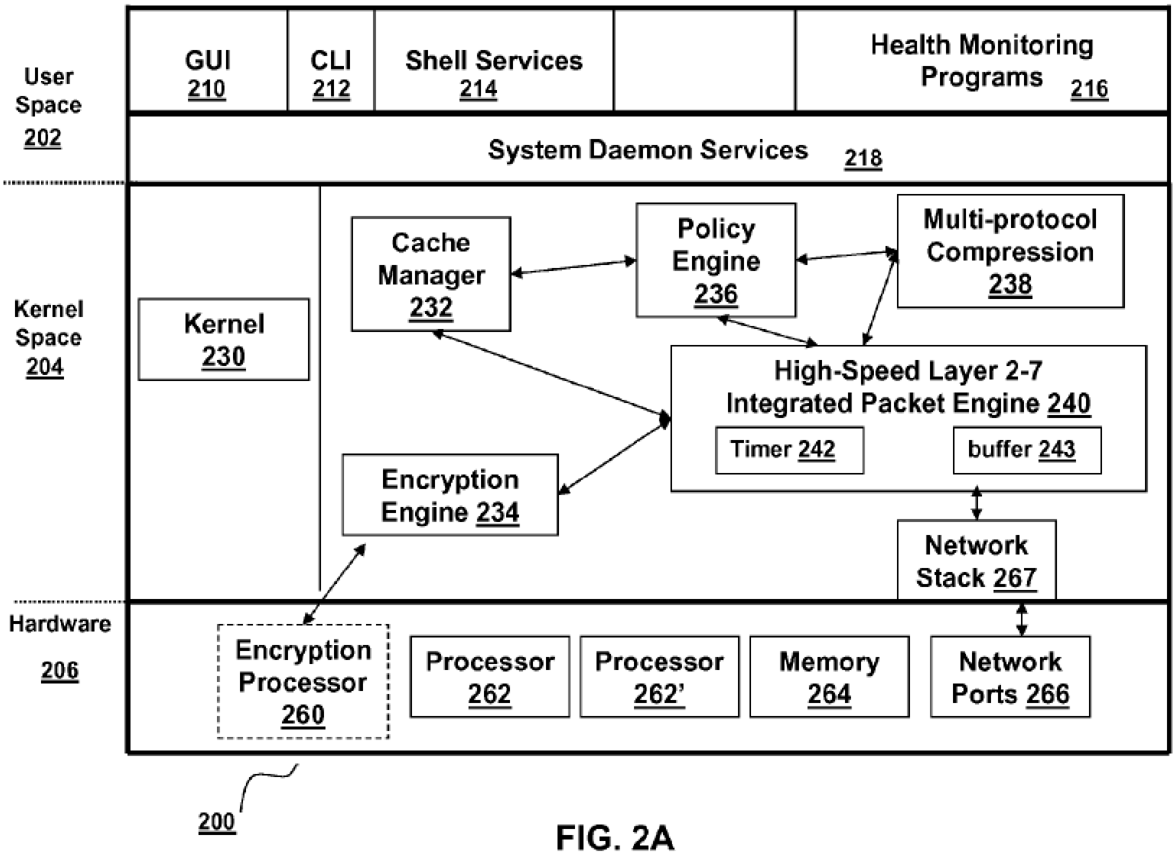


FIG. 2A

Figure 2A above depicts the architecture of appliance 200, which includes daemon services 218 that run continuously and/or in the background to handle service requests received by appliance 200. *Id.* ¶¶ 96, 116.

2. *Motivation to combine and expectation of success*

Petitioner contends that a skilled artisan would have added Sikka's daemon services to Wang's controller to improve data processing efficiency by performing system-wide functions continuously and/or periodically in the background to retrieve policy digests, generate calls to system components, and allow operations to run unattended as Wang desires to do. Pet. 49 (citing Ex. 1006 ¶ 116; Ex. 1004 ¶ 13; Ex. 1002 ¶ 113). Petitioner asserts that it would have been obvious to use the daemon service in the Wang-Sikka combination to initiate a connection to the portal process to retrieve and apply the policy digests automatically for a particular client device and customer. *Id.* at 52 (citing Ex. 1004 ¶¶ 16, 22, Fig. 1; Ex. 1002 ¶¶ 119, 120).

Petitioner asserts that a skilled artisan would have had a reasonable expectation of success in combining Wang and Sikka because a daemon service was a well-known feature and the combination would have produced expected results using systems disclosed in Wang and Sikka. Pet. 50 (citing Ex. 1006 ¶ 116; Ex. 1011 ¶¶ 104–106; Ex. 1002 ¶ 114).

3. *Petitioner's contentions*

Regarding claims 6 and 17, Petitioner contends that Wang's dynamic controller, which automatically applies, manages, and allocates firewalls in a network to make the system flexible and efficient, would have benefitted from adding Sikka's daemon service to run unattended in the background to handle and forward service requests to other programs and processes and to perform continuous or periodic system-wide functions including retrieving a policy digest and generating calls to system components as recited in claims 6 and 17. Pet. 46–49 (citing Ex. 1004 ¶¶ 12, 13, 15, 16; Ex. 1006 ¶¶ 1, 116, 197, Figs. 2A, 7B; Ex. 1002 ¶¶ 112–114; Ex. 1011 ¶¶ 104–106).

Regarding claims 7 and 18, Petitioner contends that Wang's resource database 103 provided a memory for storing updated firewall policies that are retrieved by a Portal process in a client device, so modifying controller 102 with Sikka's daemon service would enable the initiation of a connection with the client Portal to retrieve updated firewall policies stored in resource database 103. Petitioner also asserts that the Portal process in client devices 104, 106, 108 would define and implement firewall policies in Wang using a web portal and interactive interface to define firewall policies and configure firewalls as described in the '941 patent. Pet. 50–52 (citing Ex. 1004 ¶¶ 13, 15, 16, 21, 22, Fig. 1; Ex. 1002 ¶¶ 116, 118–120; Ex. 1001, 10:57–63).

4. Patent Owner's arguments

Patent Owner argues that Petitioner does not explain why a skilled artisan would have incorporated Sikka's teachings of a daemon service when Wang already discloses an automated, dynamic system that runs unattended to implement firewall changes periodically. PO Resp. 36–38. Patent Owner asserts that Wang's firewall controller does not connect to Portals to retrieve a firewall policy stored in a database because it connects to the database via network 130, and client device 110 does not connect to resource database 103. *Id.* at 39–40.

5. Analysis

We agree with Petitioner that adding Sikka's daemon service is not redundant because its advantages extend beyond the automation of Wang. We find that the daemon service operates in the background, as Dr. Black describes, without being connected to a terminal. As such, it would have enhanced security by running unattended and unimpeded from interference by users at Portals and terminals. Reply 21 (citing Ex. 1017, 45:8–21).

Petitioner cites Dr. Black's testimony that daemon services were used in network security, intrusion detection, and firewalls and their benefits and enhancements to network security were a well-known, prevalent industry practice. Reply 21. We find that Sikka's daemon services 218 run in user space 202 or kernel space 204 for more flexibility to implement functions as unattended, background operations. Ex. 1006 ¶ 116.

We find that using Sikka's daemon service to retrieve firewall policies from client portals would improve the flexibility and capabilities of Wang by automating retrieval of such policies as they are input by clients at a portal to send all or certain new policies or policy updates for validation before or in conjunction with storage of the policies in policy resource database 103 or to schedule all or some new policies or policy updates for implementation and processing at scheduled times via dynamic scheduler 116. Ex. 1004 ¶¶ 16–19, 26. Wang also uses APIs to push firewall policies to network elements and automatically invoke specific processes for specific network elements and devices in a subnet. *Id.* ¶ 25. Sikka's daemon service would add other capabilities that would enhance Wang's desired automation by processing new or updated policy requests and digests entered at portals and placing them into particular processes in the background without user interference or initiation thereby allowing validation, scheduling, and other processes to be initiated with respect to such policies when the policies are configured at a portal. *KSR*, 550 U.S. at 416–417; *DyStar*, 464 F.3d at 1368; Pet. 48–52.

6. *Conclusion*

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 6, 7, 17, and 18 are unpatentable over Wang and Sikka.

G. Ground 4: Alleged Obviousness Over Wang, Sikka, and Botzer

Petitioner asserts that claims 8 and 19 are unpatentable under 35 U.S.C. § 103 over Wang, Sikka, and Botzer. Pet. 52–55.

1. Botzer

Botzer applies lock 120 to virtual machine 101 to control inbound and outbound communications as shown in Figure 1, reproduced below.

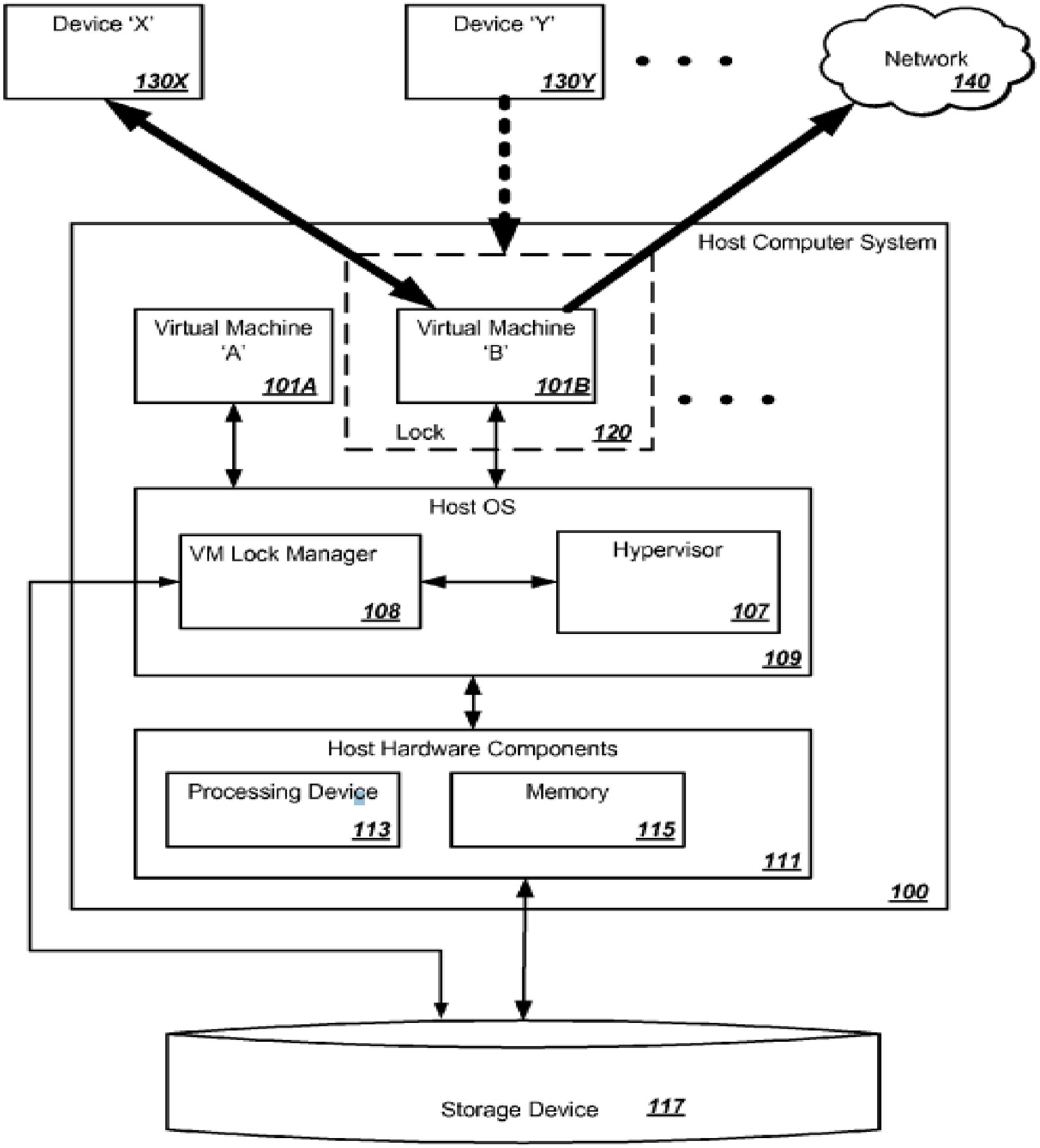


FIGURE 1

Figure 1 shows host computer system 100 having a virtual machine (VM) lock manager 108 and hypervisor 107 that apply lock 120 to virtual machine 101B to enable ongoing operation of VM 101B while selectively preventing inbound communications from certain devices 130Y and allowing inbound communications from other devices 130Y to VM 101B. Ex. 1009 ¶¶ 13, 14.

2. *Petitioner's contentions*

Petitioner contends that the Wang-Sikka combination does not use Sikka's daemon service to prevent Wang's portal process from initiating a connection as recited in claims 8 and 19. Pet. 52. Petitioner asserts that Botzer controls inbound and outbound communications of a virtual machine of host computer system 100 by applying lock 120 to virtual machine 101B to enable the ongoing execution or operation of the virtual machine while selectively preventing inbound communications from device 130Y, e.g., a desktop/laptop computer or terminal, thereby restricting a connection or access to a particular function of the virtual machine by a remote device, which could be Wang's client device 104 in the combination. *Id.* at 53–54 (citing Ex. 1009 ¶¶ 12, 14, 23, code (57), Fig. 1; Ex. 1002 ¶ 124).

3. *Motivation to combine and expectation of success*

Petitioner contends that a skilled artisan would have been motivated to use Botzer's lock to prevent initiating a connection to the daemon service in the Wang-Sikka combination by Wang's client device 104 via its Portal to block threats and other malicious activity from a particular external domain and prevent interference by users or external threats to automatic functions of the daemon service and block unwanted Portal connections that consume system resources. Pet. 54–55 (citing Ex. 1009 ¶¶ 8, 9, 14, 23; Ex. 1004 ¶ 21; Ex. 1012 ¶ 112; Ex. 1002 ¶¶ 124, 126, 127).

Petitioner asserts that a skilled artisan would have had a reasonable expectation of success in making the combination because blocking inbound connections from remote devices was a well-known functionality, and this functionality would have been compatible with Wang's controller as Dr. Lee testifies. Pet. 55 (citing Ex. 1002 ¶ 128; Ex. 1012 ¶ 112).

4. Patent Owner's arguments

Patent Owner argues that Petitioner did not establish that Wang and Sikka disclose or suggest a connection from the portal process to the daemon service so there is no benefit to using Botzer's teachings. PO Resp. 41–42. Patent Owner asserts that Botzer's lock would not prevent access by Wang's client device to the daemon service because the Wang-Sikka combination does not disclose that such access is attempted. *Id.* at 42–44.

5. Analysis

We find that Wang's system provides access by client devices 104, 106, 108, 110 to dynamic firewall controller 102 via Portals (portal process), and a skilled artisan would have been motivated to use Botzer's teachings to block client device access to the daemon service at controller 102 *selectively* to prevent interference by users with the automatic functions of the daemon service. Blocking access would have improved the daemon service, which is designed to run in the background without any interference by outside users, to enhance the security that the daemon service provides, prevent unwanted connections from Portals, and preemptively secure a network against threats and malicious activity. Pet. 49, 54–55; Reply 24–26; Ex. 1004 ¶¶ 15, 18, 19, 21, Fig. 1. We agree with Dr. Lee that Botzer's teachings would improve the Wang-Sikka combination in these ways. Ex. 1002 ¶¶ 124–127. His testimony supports Petitioner's contentions and the prior art's teachings.

Dr. Black testifies that access to the daemon service of the Wang-Sikka combination is never attempted from client devices or their Portals at controller 102 in the first place so there is no need to block such access with Botzer's lock. Ex. 2003 ¶¶ 104–107. We find his testimony is inconsistent with the teachings of Wang that client devices 104–110 initiate requests to firewall controller 102 to configure firewalls or policies via their Portals at one or more client devices 104–110. Ex. 1004 ¶ 15. We find that the Wang-Sikka combination places a daemon service at controller 102 where it might be accessed by client devices 104–110 via their Portals, and access to the daemon service by a client device and its Portal might occur legitimately by a client device authorized to configure the daemon service *or* illegitimately by an unwanted intruder, malicious party, hacker, or unauthorized user of a client device. Pet. 48–49. Thus, we agree with Petitioner that providing Botzer's lock on client devices or other external devices that might be used to access the daemon service without authority would prevent unwanted intrusions, improve network security, and preserve the integrity and background functionality of the daemon service. *Id.*; *id.* at 54–55; Reply 24–26. We disagree with Dr. Black's individual attacks on teachings of the references rather than the teachings as combined and asserted by Petitioner.

6. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 8 and 19 are unpatentable over Wang, Sikka, and Botzer.

H. Ground 5: Alleged Obviousness Over Wang and Shafer

Petitioner contends that claims 9 and 20 are unpatentable under 35 U.S.C. § 103 over Wang and Shafer. Pet. 55–57.

1. Petitioner's contentions

Petitioner asserts that Wang verifies policy changes before they are implemented but does not disclose explicitly checking for adherence to a predefined format. Pet. 55. Petitioner contends that Shafer checks policy changes for adherence to a predefined format using a management interface to check candidate configuration changes against syntactical and semantic rules of a standard as the '941 patent checks syntax of a policy digest. *Id.* at 55–56 (citing Ex. 1010, 1:48–67; Ex. 1001, 19:41–44; Ex. 1002 ¶ 131).

Petitioner asserts it would have been obvious to add Shafer's ability to check a policy change against a predefined format to Wang to avoid any erroneous policy changes and problems as Shafer and Wang warn. Pet. 56 (citing Ex. 1004 ¶¶ 18, 26; Ex. 1010, 2:1–11; Ex. 1002 ¶ 132). Petitioner asserts that a skilled artisan would have had a reasonable expectation of success because Wang verifies policy changes in a predefined format. *Id.* at 56–57 (citing limitations 1[d]/12[d] of Ground 1; Ex. 1002 ¶ 134).

2. Patent Owner's arguments

Patent Owner argues that Ground 5 relies on Ground 1 and fails for the reasons discussed in Section V. for Ground 1. PO Resp. 44.

3. Analysis

Patent Owner's arguments are not persuasive for reasons discussed in Section III.D. for Ground 1. Wang's validation emulates functions of subnet devices and thereby effectively checks policy change syntax. Ex. 1004 ¶ 26.

4. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 9 and 20 are unpatentable over Wang and Shafer.

I. Ground 6: Alleged Obviousness Over Wang and Terrill

Petitioner asserts that claims 10, 11, 21, and 22 are unpatentable under 35 U.S.C. § 103 over Wang and Terrill. Pet. 57–65.

1. Motivation to combine and expectation of success

Petitioner contends that Wang has endpoint to endpoint connections, and a skilled artisan would have added Terrill's additional features because both references automatically and dynamically configure and enforce endpoint to endpoint communications in an enterprise network, and Terrill's features would improve Wang's ability to provide real-time network services when no local policies apply by escalating requests to seek directives from the controller for greater flexibility in real-time. Pet. 59–61 (citing Ex. 1004 ¶¶ 4, 21, 22, Fig. 1; Ex. 1007 ¶¶ 54, 57, 81, 90, code (57), Fig. 1; Ex. 1002 ¶¶ 139–141). Petitioner contends that a skilled artisan would have had a reasonable expectation of success in combining these teachings because Wang's controller receives information for changes to endpoint devices being connected/disconnected, and Terrill's controller and endpoint agents are compatible with Wang's system and would yield predictable results. *Id.* at 61–62 (citing Ex. 1004 ¶ 24; Ex. 1007 ¶¶ 56, 88, Fig. 1; Ex. 1002 ¶ 144).

2. Petitioner's contentions

Petitioner contends that Terrill's controller 140 receives connection escalation requests from endpoint agent 130 of endpoint 110 and responds with a directive or rule instructing agent 130 how to handle the request such as Allow or Deny a request from endpoint 110C by blocking a connection by agent 130 based on controller 140 sending directives to agent 130 as recited in claims 10, 11, 21, and 21. Pet. 62–65 (citing Ex. 1007 ¶¶ 56, 70–72, 75–81, 88, 89, Fig. 1; Ex. 1002 ¶¶ 148, 152).

3. *Patent Owner's arguments*

Patent Owner argues that Ground 6 relies on Ground 1 and fails for the reasons discussed in Section V. for Ground 1. PO Resp. 44.

4. *Analysis*

We disagree with Patent Owner's arguments for the reasons discussed in Section III.D. *supra*, for Ground 1 and Wang.

5. *Conclusion*

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 10, 11, 21, and 22 are unpatentable over Wang and Terrill.

J. Ground 7: Alleged Obviousness Over Chambers and Terrill

Petitioner asserts unpatentability of claims 1, 2, 4, 5, 10–13, 15, 16, 21, and 22 under 35 U.S.C. § 103 over Chambers and Terrill. Pet. 65–92.

1. *Chambers*

Chambers' cloud-based management server 101 stores and manages access control policies (ACPs) 114 and access control rules (ACRs) 115 that network access devices (NADs) use to control communications of network client devices (NCDs) over network 104. Ex. 1008 ¶¶ 17–20. Management module 110 manages and configures NADs 102, 103, which control local area networks (LAN) 105, 106 that interface with wide area network (WAN) 104, e.g., the Internet. *Id.* ¶¶ 20–25. Access control policy (ACP) manager 113 manages and synchronizes centrally-located ACPs 114 and ACRs 115, including updates, with NADs, which enforce ACPs 117 and ACRs 118 to control the access of associated NCDs 108, 109 controlled by that NAD 102, 103 and provide network connectivity. *Id.* ¶¶ 18–23, 49. Figure 1 of Chambers is reproduced below to illustrate this configuration.

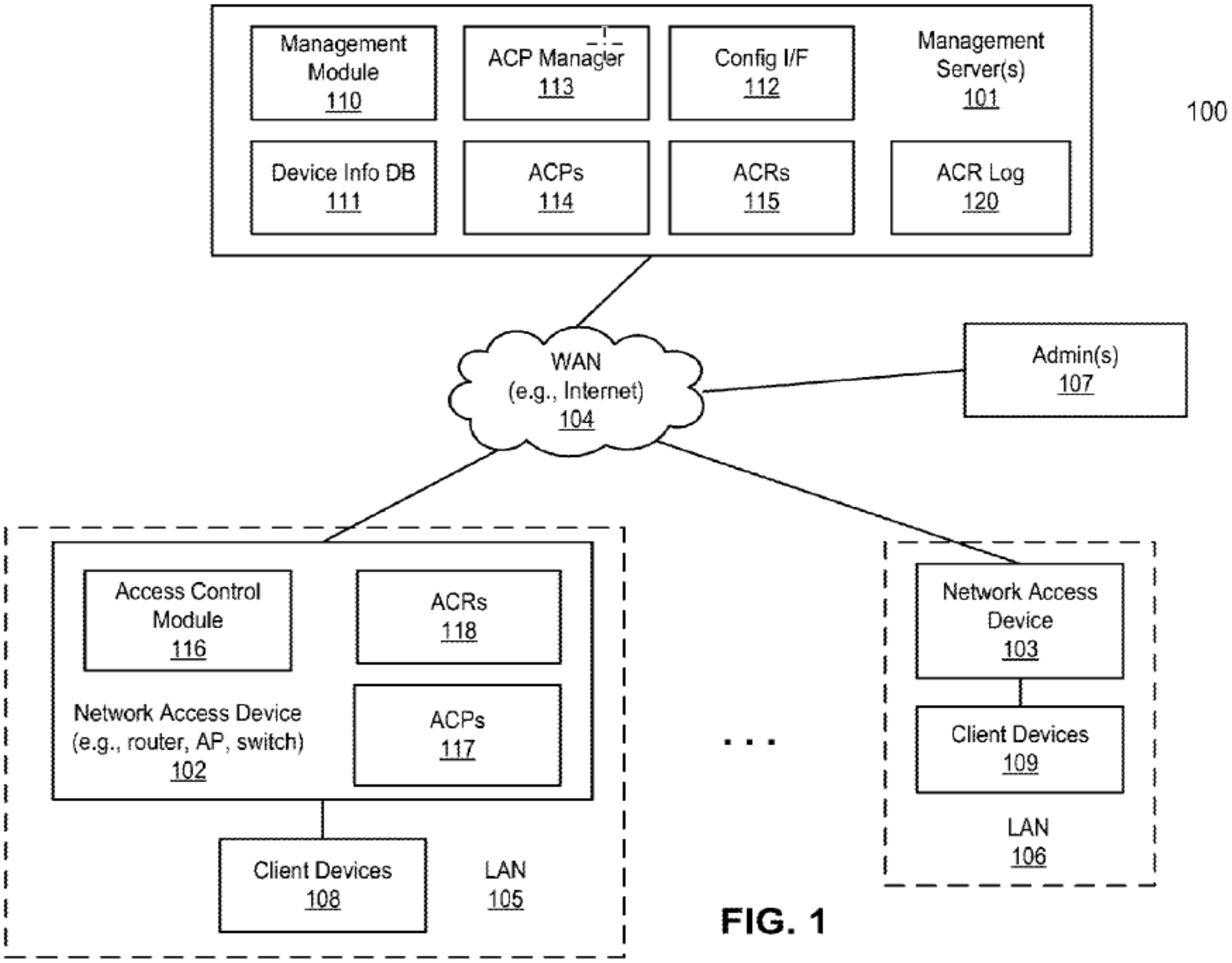


FIG. 1

Figure 1 depicts management server 101 with interface 112 for administrator 107 to configure NADs 102, 103. Ex. 1008 ¶¶ 20–22. ACPs 114 are access policies applied using ACRs 115 sent by ACP manager 113 to NADs 102, 103. *Id.* ¶ 23. Access control module 116 enforces ACPs 117 and ACRs 118 to control access by NCDs 108 (*id.* ¶ 24) and sends updates of ACPs and ACRs to management server 101 to broadcast to other NADs (*id.* ¶ 25). System 100 may implemented in a cloud managed system. *Id.* ¶ 52, Fig. 7A.

2. *Terrill*

Terrill controls communications between computers 110 over network 120 using endpoint agents 130 as shown in Figure 1, reproduced below.

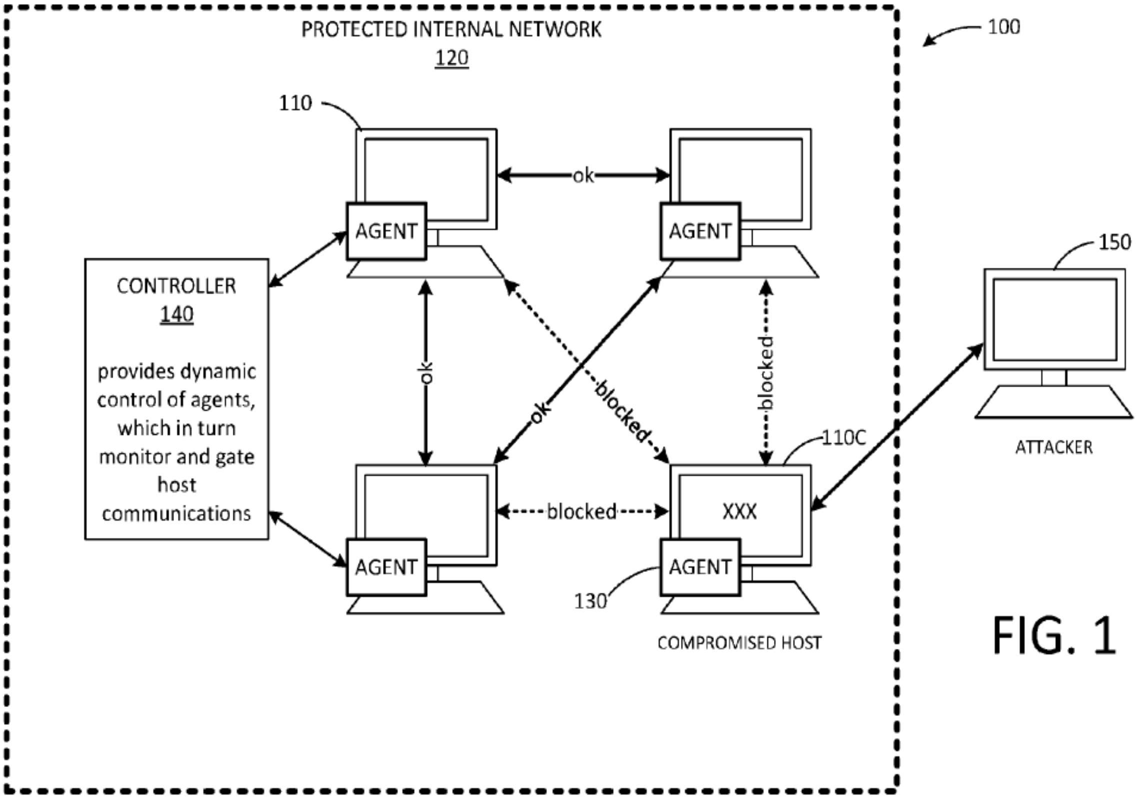

PROTECTED INTERNAL NETWORK
120
100
110
AGENT
ok
AGENT
CONTROLLER
140
provides dynamic control of agents, which in turn monitor and gate host communications
150
ok
ok
blocked
blocked
110C
ATTACKER
blocked
XXX
AGENT
AGENT
130
COMPROMISED HOST

FIG. 1

Figure 1 depicts agents 130 that analyze requests for connections between hosts 110. Ex. 1007 ¶¶ 52–54. Agents 130 check metadata for connections against a local cache of rules and send requests to controller 140 if no rule applies while holding the request. *Id.* ¶ 56. Controller 140 tells agent 130 how to handle a request and provides rules to cache for future use. *Id.*

3. *Motivation to combine and expectation of success*

Petitioner asserts a skilled artisan would have combined Chambers and Terrill because Chambers configures and synchronizes policies from a central server to manage network access devices and LANs in disparate locations, and Terrill uses a central controller to configure policy rules for a large number of hosts with complementary techniques that would improve Chambers' system. Pet. 68–69 (citing Ex. 1008 ¶ 5; Ex. 1007 ¶¶ 54, 144, code (57), Fig. 1; Ex. 1002 ¶ 159).

Petitioner asserts that adding Terrill's ability to control endpoint to endpoint connections would improve Chambers' security by preventing a compromised internal device running malicious code from attacking other internal devices, where both references restrict internal access to resources in their enterprise networks. Pet. 69 (citing Ex. 1008 ¶ 41; Ex. 1007 ¶¶ 3, 81; Ex. 1002 ¶¶ 160, 161). Petitioner asserts that a skilled artisan would have had a reasonable expectation of success in combining Chambers and Terrill because both use a central controller to control connections, and Terrill's agents would have been installed easily on Chambers' NCDs for predictable results using known techniques and systems. *Id.* at 69–70 (citing Ex. 1008 ¶ 20; Ex. 1007 ¶¶ 52, 56, 88; Ex. 1001, 6:60–64; Ex. 1002 ¶¶ 162–164).

4. *Claims 1 and 12*

a. *1[pre]/12[pre]*

i. *Petitioner's contentions*

Petitioner contends that Chambers' method protects an enterprise network (LANs 1005, 1006) using a server that managed ACRs of NADs that operate as gateways to the LANs and can be implemented using code and data stored on electronic devices. Pet. 70–73 (citing Ex. 1008 ¶¶ 4, 17, 18, 20, 49, 52, 69, 71, 72, code (57), Fig. 7B; Ex. 1002 ¶¶ 167, 169–171).

ii. *Patent Owner's arguments*

Patent Owner does not contest Petitioner's assertions regarding elements 1[pre]/12[pre]. *See generally* PO Resp.; Sur-reply.

iii. *Conclusion*

Regardless of whether the preamble is limiting, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Chambers discloses and/or suggests elements 1[pre]/12[pre].

b. *1[a]/12[a]*

i. Petitioner's contentions

Petitioner contends that Chambers' management server controls communications to and from an enterprise (LANs) using ACRs and ACPs at NADs to control access by NCDs 1002, 1003 associated with the LANs. Pet. 73–75 (citing Ex. 1008 ¶¶ 17, 18, 20, 22, 25, Fig. 7B; Ex. 1002 ¶ 175).

ii. Patent Owner's arguments

Patent Owner does not contest Petitioner's assertions regarding elements 1[a]/12[a]. *See generally* PO Resp.; Sur-reply.

iii. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Chambers discloses and/or suggests elements 1[a]/12[a].

c. *1[b]/12[b]*

i. Petitioner's contentions

Petitioner asserts that Terrill's controller 140 receives a connection escalation request from endpoint agents 130 to establish a connection with another endpoint 110 and provides a directive instructing the agent how to handle the connection (e.g., to allow or deny the request) and/or a rule that is applicable to the connection request. Petitioner asserts that a skilled artisan would have included this functionality of Terrill in Chambers' management server to improve Chambers' security features by preventing a compromised internal device running malicious code from attacking other internal devices via endpoint to endpoint connections. Pet. 75–76 (citing Ex. 1007 ¶¶ 3, 56, 70–72, 81; Ex. 1008 ¶ 41; Ex. 1002 ¶¶ 178–180; Pet. Ground 6, Claims 10/21; Pet. Ground 7, Section 1.b.).

ii. Patent Owner's arguments

Patent Owner does not contest Petitioner's assertions regarding elements 1[b]/12[b]. *See generally* PO Resp.; Sur-reply.

iii. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Chambers and Terrill disclose and/or suggest elements 1[b]/12[b].

d. *1[c]/12[c]*

i. Petitioner's contentions

Petitioner asserts that Chambers' management server 101 receives a request to modify ACPs 114/ACRs 115 stored there when administrator 107 updates ACPs 114/ACRs 115 via configuration interface 112. Pet. 76–77 (citing Ex. 1008 ¶¶ 23, 25, claims 2 and 5, Figs. 1, 2; Ex. 1002 ¶ 183).

ii. Patent Owner's arguments

Patent Owner does not contest Petitioner's assertions regarding elements 1[c]/12[c]. *See generally* PO Resp.; Sur-reply.

iii. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Chambers discloses and/or suggests elements 1[c]/12[c].

e. *1[d]/12[d]*

i. Petitioner's contentions

Petitioner contends that Chambers automatically generates a policy digest of ACP/ACR modifications, and management server 101 compiles the policies without administrator action. Pet. 77–80 (citing Ex. 1008 ¶¶ 19, 22, 26, 29–40, 48, 49, Fig. 2; Ex. 1001, Fig. 4C; Ex. 1002 ¶¶ 188, 189).

ii. Patent Owner's arguments

Patent Owner does not contest Petitioner's assertions regarding elements 1[d]/12[d]. *See generally* PO Resp.; Sur-reply.

iii. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Chambers discloses and/or suggests elements 1[d]/12[d].

f. *1[e]/12[e]*

i. Petitioner's contentions

Petitioner contends that Chambers stores updated ACPs 114/ACRs 115 as policy digests in memory (persistent storage) of management server 101. Petitioner asserts that Chambers' management server 101 periodically sends updated ACRs to NADs, and a skilled artisan would have recognized that to send such periodic policy updates, management server 101 would have to retrieve the updated ACRs from memory. Pet. 80 (citing Ex. 1008 ¶¶ 18, 19, 43, 49, 71, Fig. 1; Ex. 1002 ¶ 191).

ii. Patent Owner's arguments

Patent Owner does not contest Petitioner's assertions regarding elements 1[e]/12[e]. *See generally* PO Resp.; Sur-reply.

iii. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Chambers discloses and/or suggests elements 1[e]/12[e].

g. *1[f]/12[f]*

i. *Petitioner's contentions*

Petitioner asserts that Chambers generates calls to system components when management server 101 provides updated ACPs/ACRs to NADs that control communications to and from the enterprise network (LANs 1005, 1006) by NCDs 1008, 1009. Petitioner asserts that Chambers broadcasts updated ACRs to NADs and sends a command indicating which of the ACR entries are not invalid so NADs can remove invalid entries. Pet. 81–83 (citing Ex. 1008 ¶¶ 20, 25, 47–49, code (57), Fig. 7B; Ex. 1002 ¶ 195).

Petitioner contends that a skilled artisan would have found it obvious that by sending an updated ACR and/or a policy update command to NADs, management server 101 generated and sent a call to the NADs to cause the NADs to execute a particular function such as updating access control rules that control access or communications to or from the enterprise network. Pet. 83 (citing Ex. 1002 ¶¶ 195–196).

Petitioner contends that Chambers did not generate a call to control endpoint to endpoint connections between network client devices 1008 and 1009, but Terrill's controller 140 sent a directive and/or rule to agent 130 to "specify an action for handling" an endpoint to endpoint connection request, and a skilled artisan would have found it obvious that Terrill's controller 140 generated and sent a call when it sent a directive or rule to cause execution of a function that controlled endpoint to endpoint connections. Petitioner asserts that Terrill's functions would improve Chambers' security features to synchronize a global policy for communications to and from the enterprise network *and* endpoint to endpoint communications within the network. Pet. 83–84 (citing Ex. 1007 ¶¶ 57, 70–72; Ex. 1002 ¶¶ 197, 198; element 1[b]).

Petitioner contends that Chambers already controlled certain access functions for network client devices (endpoints) by limiting access to certain internal resources (e.g., the financial department) to certain people and their computers so that a skilled artisan would have been motivated to augment Chambers' system with Terrill's complementary features to generate calls to Chambers' NADs to control endpoint to endpoint connections and limit their access to internal resources that Chambers and Terrill aimed to protect. Pet. 84 (citing Ex. 1008 ¶¶ 20, 41; Ex. 1007 ¶ 81; Ex. 1002 ¶ 199). Petitioner asserts that a skilled artisan would have reasonably expected success in making this combination by using existing systems disclosed in Chambers and Terrill to produce expected results. *Id.* (citing Ex. 1002 ¶ 200).

ii. Patent Owner's arguments

Patent Owner argues that it is unclear which functionalities of Terrill are incorporated by Petitioner into Chambers, how the incorporation would be done, and how the combination "meets the claimed 'calls' for controlling endpoint-to-endpoint connection." PO Resp. 45. Patent Owner asserts that Petitioner's reliance on Terrill's directives/rules for calls to control endpoint to endpoint connections and Chambers' ACRs/ACPs for calls to control enterprise communications does not establish that Terrill's directives/rules are based on policy digests with a predefined format or that the calls control both communication to and from the enterprise network and endpoint to endpoint connections based on a single policy digest. *Id.* at 46–47. Patent Owner argues that a skilled artisan would not format the directives/rules of Terrill using Chambers' ACPs/ACRs format because it is unknown whether the formats are compatible. *Id.* at 48.

iii. Analysis

Patent Owner does not dispute that Chambers sends updated ACRs and ACPs as calls to system components to control traffic to and from the enterprise network, or that Terrill sends rules/directives as calls to system components to control endpoint to endpoint connections as claimed. PO Resp. 44–49; Reply 26–28, 31–32; Pet. 81–83. Patent Owner's arguments attack the references individually rather than as combined by Petitioner. *See In re Merck*, 800 F.2d 1091, 1097 (Fed. Cir. 1986); *see also In re Etter,* 756 F.2d 852, 859 (Fed.Cir.1985) (en banc) (a determination of obviousness does not require an actual, physical substitution of elements).

We agree with Petitioner that a skilled artisan would have wanted to improve Chambers' security by using Terrill's ability to control endpoint to endpoint connections in Chambers to enforce and synchronize a global communications policy for all traffic to and from, and within, the network as Petitioner asserts. Pet. 83–84; *id.* at 68–70. We find that Chambers' NADs can control access between NCD endpoints and internal finance department endpoints. Pet. 69, 84; Ex. 1008 ¶¶ 20–25, 29–41. Terrill's teachings would augment Chambers by generating calls to NADs to control other endpoint to endpoint connections. Pet. 83–84. Terrill's use of IP addresses, ports, and process name/ID to control endpoint connections (Ex. 1007 ¶¶ 60–69) would augment Chambers' similar use of MAC addresses/SSIDs of NCDs, ports, and policies to control endpoint connections to TCP port 80, internal finance department, and external WANs/Internets (Ex. 1008 ¶¶ 28–41). Chambers also translates MAC addresses to IP addresses for NCD endpoints (Ex. 1008 ¶¶ 20, 53, 58) facilitating endpoint to endpoint connections. Dr. Lee testifies that Chambers' format is similar to the '941 patent. Ex. 1002 ¶¶ 188–189.

As modified, Chambers' NADs would apply ACPs/ACRs with fields to control connections of NCD endpoints to and from the enterprise network *and* fields to control connections of those endpoints to other NCD endpoints within the enterprise network as a "global policy." Pet. 83–84; Reply 28–29; Ex. 1002 ¶¶ 198–199. Terrill's flexible rules control traffic based on a User ID and/or source or destination IP address. Ex. 1007 ¶¶ 60–74.

As modified, Chambers' ACRs/ACPs are a *single* policy digest. Pet. 83–84; *cf.* PO Resp. 47. Dr. Black's testimony that a skilled artisan would not know if Terrill's directives/rules are compatible with Chambers' policy digests ignores their similar formats. Ex. 2003 ¶¶ 118, 119; Ex. 1007 ¶¶ 60–72 (Terrill's fields use process/policy ID/Name, IP addresses, ports, and block connection fields); Ex. 1008 ¶¶ 20, 28–41, 53, 58 (Chambers' fields use MAC address, policy, block TCP port 80, policy_id 105, block access to finance, translate MAC to IP address), Fig. 2. Chambers blocks connections like Terrill. Ex. 1008 ¶ 36; Ex. 1007 ¶ 72; *cf.* Ex. 2003 ¶ 119. Chambers uses ACRs/ACPs to control connections between NCD endpoints based on MAC addresses (Ex. 1008 ¶¶ 28–41 (finance department), Fig. 2) and would control other endpoint to endpoint connections via Terrill's similar rules and directives using MAC and/or IP addresses as the references teach.

Because claims 1 and 12 do not recite agents running on endpoints as dependent claims 11 and 22 require, Chambers' NADs also generate calls to NCDs to control connections of NCD endpoints to other NCD endpoints within the enterprise network (e.g., NCDs in a finance department) by using MAC addresses that can be converted to IP addresses that Terrill uses. *See* Ex. 1008 ¶¶ 28–41; Pet. 83–84; Reply 31–32. No new theory is needed to determine that Chambers and Terrill teach and suggest elements 1[f]/12[f].

iv. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Chambers and Terrill disclose and/or suggest elements 1[f]/12[f].

h. *1[g]/12[g]*

i. Petitioner's contentions

Petitioner asserts that Chambers modifies control of communications to and from the enterprise network using calls from management server 101 to NADs to update ACRs that control access of NCDs to and from enterprise LANs 1005/1006. Pet. 84–85 (citing Ex. 1008 ¶ 26; Ex. 1002 ¶¶ 201, 202; elements 1[f]/12[f]). Petitioner asserts that Terrill modifies the control of endpoint to endpoint connections when controller 140 sends a directive/rule specifying an action to approve or deny an internal connection request, and the NADs of the Chambers-Terrill combination would receive such calls from management server 101 to implement updated access rules or policies that control communications to and from the enterprise network *and* control endpoint to endpoint connections with a reasonable expectation of success. *Id.* at 85–86 (citing Ex. 1007 ¶¶ 70–74; Ex. 1002 ¶¶ 203, 204; elements 1[b]/12[b], 1[f]/12[f]; Pet. § 1.b.).

ii. Patent Owner's arguments

Patent Owner does not contest Petitioner's assertions regarding elements 1[g]/12[g]. *See generally* PO Resp.; Sur-reply.

iii. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Chambers and Terrill disclose and/or suggest elements 1[g]/12[g].

i. *Conclusion*

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 1 and 12 are unpatentable over Chambers and Terrill.

5. Claims 2 and 13

a. *Petitioner's contentions*

Petitioner asserts that Chambers' management server 101 includes a configuration interface 112 that allows administrator 107 to configure NADs 102, 103 with parameters to change network access policies or rules (ACPs/ ACRs). Pet. 86–87 (citing Ex. 1008 ¶¶ 22, 55; Ex. 1002 ¶ 206; elements 1[c]/12[c]). Petitioner asserts that Terrill's controller 140 has an interface used for creating and enforcing policies, and its visualized, customizable configurations and graphical view would have improved Chambers' user interface to allow administrators to select hosts, groups, and users to create access control policies. *Id.* at 87 (citing Ex. 1007 ¶ 86; Ex. 1002 ¶ 208). Petitioner asserts that the addition would improve the ability of Chambers' interface to modify firewall rules and policies with a reasonable expectation of success. *Id.* (citing Ex. 1007 ¶ 86; Ex. 1008 ¶¶ 13, 22; Ex. 1002 ¶ 208).

b. *Patent Owner's arguments*

Patent Owner does not contest Petitioner's assertions regarding claims 2 and 13. *See generally* PO Resp.; Sur-reply.

c. *Conclusion*

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 2 and 13 are unpatentable over Chambers and Terrill.

6. *Claims 4 and 15*

a. *Petitioner's contentions*

Petitioner contends that Chambers uses ACPs/ACRs as policy digests that modify inbound and outbound network traffic by setting upload and download bandwidths, and Terrill's policy rules modify internal network traffic as recited in claims 4 and 15 by instructing system 100 to allow or deny traffic between hosts or modify a global policy. Pet. 87–88 (citing Ex. 1007 ¶¶ 57, 102; Ex. 1008 ¶¶ 18, 33–34; Ex. 1002 ¶ 211; elements 1[a]/12[a] and 1[d]/12[d]). Petitioner contends that it would have been obvious to add Terrill's policy digest to Chambers' policy digest for the reasons asserted for elements 1[b]/12[b], 1[f]/12[f], 1[g]/12[g], and Ground 7, Section 1.b of the Petition. *Id.* at 88 (citing Ex. 1002 ¶¶ 213, 214).

b. *Patent Owner's arguments*

Patent Owner does not contest Petitioner's assertions regarding claims 4 and 15. *See generally* PO Resp.; Sur-reply.

c. *Conclusion*

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 4 and 15 are unpatentable over Chambers and Terrill.

7. *Claims 5 and 16*

a. *Petitioner's contentions*

Petitioner asserts that Chambers' management server 101 retrieved a policy from memory and periodically sent updated ACRs and ACPs (policy digests) to NADs at regular intervals on a predefined schedule as claimed. Pet. 89 (citing Ex. 1008 ¶¶ 43, 49; Ex. 1002 ¶¶ 217, 219; Ex. 1014 (defining "periodic"); Ground 5, element 1[e]/12[e]).

b. *Patent Owner's arguments*

Patent Owner does not contest Petitioner's assertions regarding claims 5 and 16. *See generally* PO Resp.; Sur-reply.

c. *Conclusion*

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 5 and 16 are unpatentable over Chambers and Terrill.

8. Claims 10, 11, 21, and 22

a. *Petitioner's contentions*

Petitioner asserts that Terrill receives connection escalation requests from endpoint agents and responds with actions to handle connections based on policies (claims 10, 21), and requests from an endpoint agent running on a first endpoint are for approval to accept a connection of a second endpoint, and a response is an instruction to accept or deny the request (claims 11, 22). Petitioner asserts that it would have been obvious to add these functions to Chambers' management server to address attacks on the fly, in real-time if local policies are unavailable to control endpoint to endpoint connections. Pet. 89–92 (citing Ex. 1007 ¶¶ 54, 56, 57, 81, 88, 90; Ex. 1008 ¶¶ 22, 25, 26; Ex. 1002 ¶¶ 223–226; Ground 7, § 1.b.; Ground 1, claims 10, 11, 21, 22).

b. *Patent Owner's arguments*

Patent Owner does not contest Petitioner's assertions regarding claims 10, 11, 21, and 22. *See generally* PO Resp.; Sur-reply.

c. *Conclusion*

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 10, 11, 21, and 22 are unpatentable over Chambers and Terrill.

K. Ground 8: Alleged Obviousness Over Chambers, Terrill, and Pasdar

Petitioner asserts the unpatentability of claims 3 and 14 under 35 U.S.C. § 103 over Chambers, Terrill, and Pasdar. Pet. 92–94.

1. Petitioner's contentions

Petitioner asserts that Chambers and Terrill generate calls to system components to control network communications, and a skilled artisan would have routed endpoint communications to P/PoPs and modified their security stacks to manage and intercept traffic for geographically and functionally distributed devices and to provide centralized services that leverage a single global policy for privacy, security, and application resiliency and availability for endpoint communications in disparate perimeters, as Pasdar teaches, with a reasonable expectation of success. Pet. 92–94 (citing Ex. 1008 ¶¶ 5, 17, 18, Fig. 7B; Ex. 1007 ¶ 144, code (57), Fig. 1; Ex. 1005 ¶¶ 5, 31; Ex. 1002 ¶¶ 232–236; Ground 2, claims 3/14; Ground 7, elements 1[f]/12[f]).

2. Patent Owner's arguments

Patent Owner argues that Petitioner failed to establish any motivation that would improve the Chambers-Terrill combination. PO Resp. 49. Patent Owner asserts that having the same field of endeavor does not provide a motivation to combine. *Id.* at 49–51. Patent Owner argues that "running all traffic through a single P/PoP would be unnecessary in Chambers' network" because Chambers' system already services a large number of perimeter devices, and Petitioner does not establish that Chambers' ACRs/ACPs would be compatible for modifying the security stack of a P/PoP or how Pasdar's P/PoPs can be updated by a system remote from the enterprise network as Chambers does. *Id.* at 52–53.

3. Analysis

Patent Owner does not dispute that both references control network traffic of geographically and functionally distributed endpoints to enhance the security of internal and external network communications. Pet. 92–93; PO Resp. 49–50. Petitioner asserts that Pasdar's P/PoPs would improve this centralized control by using a customizable security P/PoP stack that would provide data center and secure internet services for Chambers' endpoint devices instead of providing servers at each device for improved efficiency. Pet. 44–45, 92–93; PO Resp. 50–51 (data center, secure internet services). These contentions are supported by Pasdar's teachings that P/PoPs provide customizable services with application resiliency, security, and forensics (Ex. 1005 ¶¶ 2, 5, 25, 31, 49, 54, 57; Reply 36–37) that enable Chambers' NADs to control finance department and other endpoints (Reply 34–35).

We find that Pasdar's distribution of network traffic across multiple P/PoPs enforces a cohesive security policy over a distributed network, and it would enable Chambers' distributed devices to operate in a unified security and policy framework of global enforcement policies that would adapt to unknown entities and various data types. PO Resp. 52; Reply 35–37 (citing Ex. 1005 ¶ 53; Ex. 1016 ¶ 6); Pet. 41–42. We agree with Dr. Lee that "Pasdar's P/PoP is not just a means to centralize traffic but a sophisticated method of enforcing global policies that can be adapted to unknown entities and various data types [and] Pasdar's architecture offered a scalable solution that can be customized to accommodate an array of devices, each potentially having different operational roles and security needs." Ex. 1016 ¶ 6 (Pasdar goes beyond the access control of Chambers). Dr. Lee explains how a single global perimeter policy would improve Chambers. *Id.*; *cf.* Ex. 2003 ¶ 127.

Dr. Black's testimony that "it is not clear to me how Chambers would benefit" (Ex. 2003 ¶ 126) does not address the data center, secure internet, and customizable application resiliency, security, and forensics services that Pasdar's P/PoPs provide, as discussed *supra*. Dr. Lee persuasively explains that routing communications through a P/PoP using calls is compatible with Chambers' system and would achieve predictable results. Ex. 1002 ¶ 236.

We disagree that Pasdar does not describe updating its P/PoPs by a system remote from the enterprise network or that the claims require the system to be remote from the enterprise network as Dr. Black testifies. Ex. 2003 ¶ 129. We also agree with Petitioner that Pasdar does not teach that its policy engine must be within the enterprise network. Reply 37 n.2.

Pasdar's P/PoPs are distributed geographically across buildings, cities, regions, and countries to provide a customized virtual perimeter for nodes, but the P/PoPs are controlled centrally by centralized policy engine 721 that defines policies for disparate P/PoPs and nodes located in different countries that have different restrictions and policies. *Id.* ¶¶ 49, 115–117, Fig. 7A; Ex. 2003 ¶ 129; PO Resp. 53. Chambers' NADs are distributed geographically but controlled centrally by management server 101 (Ex. 1008 ¶¶ 5, 25, 47), like Pasdar's P/PoPs and policy engine 721, and Chambers' devices would benefit from operating under a unified security policy framework but with tailored services and access control using Pasdar's P/PoP that provide the versatility to adapt to unknown entities and data types. Reply 36–37.

4. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 3 and 14 are unpatentable over Chambers, Terrill, and Pasdar.

L. Ground 9: Alleged Obviousness Over Chambers, Terrill, and Litvin

Petitioner asserts the unpatentability of claims 6 and 17 under 35 U.S.C. § 103 over Chambers, Terrill, and Litvin. Pet. 94–95.

1. Petitioner's contentions

Petitioner asserts that Chambers and Terrill retrieve a firewall policy and generate calls to system components to implement the policy, and Litvin runs a daemon in the background to perform functions of receiving policies from a firewall coordinator, providing policies to a packet filter on a host node, updating policies, and sending new policies similar to Chambers' management server 101, which compiles configuration data without direct administrator intervention and periodically sends updated ACRs to NADs. Pet. 94–95 (citing Ex. 1011 ¶¶ 91, 93, 96, 97, 105, code (57), Fig. 8; Ex. 1008 ¶¶ 23, 43, 48; Ground 7, elements 1[d]/12[d], 1[e]/12[e], 1[f]/12[f]).

Petitioner asserts it would have been obvious to add Litvin's daemon service to Chambers' server to improve efficiency by performing functions "in the background" to retrieve firewall policies and generate calls and to prevent unauthorized access by a client device to security policies stored in Chambers' server so the combined would not be accessed directly by the user, as Litvin teaches, with a reasonable expectation of success. *Id.* at 95 (citing Ex. 1011 ¶ 105; Ex. 1006 ¶ 116; Ex. 1002 ¶¶ 240–242).

2. Patent Owner's arguments

Patent Owner asserts that a skilled artisan would not use Litvin's daemon service in Chambers because Chambers' automated system already updates NADs in the background, and does not allow its management server to be accessed directly by users. PO Resp. 54–55.

3. Analysis

We find that using a daemon service to retrieve firewall policies and generate calls to system components would improve the efficiency of the Chambers-Terrill combination by allowing functions to be performed in the background without intervention of an administrator 107 such as receiving policies from a firewall coordinator, providing policies to a packet filter, updating policies, and sending policies while preventing users and others from interfering with such security policies and updates as Petitioner asserts and Litvin teaches. Pet. 94–95; Ex. 1011 ¶¶ 91, 93, 96, 97, 106; *see KSR*, 550 U.S. at 417; *DyStar*, 464 F.3d at 1368.

Patent Owner recognizes that Chambers restricts access to the security policy updating of management server 101 to administrator 107. PO Resp. 55 (citing Ex. 1008 ¶¶ 54, 55). We agree with Petitioner that Litvin's daemon service would improve Chambers' efficiency by retrieving firewall policies, generating calls, and sending security updates "in the background" run by a daemon service without administrator 107 intervention to perform or initiate such functions. Pet. 94–95; *see* Ex. 1002 ¶¶ 240, 241. We find that this modification would prevent potential unauthorized access by remote client devices to security policies that could not be accessed directly by the user. Pet. 95 (citing Ex. 1011 ¶ 105). We find that a skilled artisan would have been motivated to use Litvin's daemon services in Chambers' system for these reasons and would have done so with a reasonable expectation of success as Dr. Lee testifies. Ex. 1002 ¶ 242. We find that a daemon service would reduce the burden of security changes on Chambers' administrator 107 while limiting the ability of unauthorized parties to change the security policies. Reply 94–95; Ex. 1008 ¶ 48; *see* Ex. 2003 ¶ 133.

4. *Conclusion*

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 6 and 17 are unpatentable over Chambers, Terrill, and Litvin.

M. *Ground 10: Alleged Obviousness Over Chambers, Terrill, Litvin, and Wang*

Petitioner asserts the unpatentability of claims 7 and 18 under 35 U.S.C. § 103 over Chambers, Terrill, Litvin, and Wang. Pet. 95–99.

1. *Petitioner's contentions*

Petitioner asserts that Chambers-Terrill-Litvin teach a daemon service that retrieves policies, generates calls, and performs other functions, Wang connects to a portal process to retrieve a policy digest, and Chambers stores ACRs/ACPs (policy digests) in a memory of a management server and uses a portal process (interface 112) to retrieve ACPs/ACRs by administrators of different entities. Pet. 95–98 (citing Ex. 1008 ¶¶ 22, 49, 59, Fig. 1, 7A; Ex. 1002 ¶ 246; Grounds 3 and 9, claims 6/17; Ground 3, claims 7/18; Ground 7, element 1[e]/12[e]). Petitioner asserts that it would have been obvious to include Wang's functionality of initiating a connection to a portal process to retrieve policy changes into the daemon service of Chambers, Terrill, and Litvin because Chambers and Wang manage policies at central controllers, and Wang's multi-portal arrangement would prevent unauthorized access to an entity's policies via Chambers' single shared portal. *Id.* at 97–98 (citing Ex. 1008 ¶ 54, Fig. 7A; Ex. 1004 ¶ 16; Ex. 1002 ¶¶ 248, 249). Petitioner asserts that using a daemon service to retrieve policies from storage would have been implemented with a reasonable expectation of success. *Id.* at 98–99 (citing Ex. 1004 ¶ 16; Ex. 1008 ¶¶ 24, 25; Ex. 1002 ¶ 250).

2. *Patent Owner's arguments*

We disagree with Patent Owner's arguments based on Grounds 7 and 9 for the reasons discussed in Sections III.J. and III.L. *supra*. PO Resp. 55. Patent Owner also argues Wang does not disclose initiating a connection to the portal process or retrieving the policy digest as claimed. *Id.* at 56.

3. Analysis

Patent Owner's arguments do not address Petitioner's contentions that Wang's resource database 103 has a memory for storing updated firewall policies that would be retrieved by a client device Portal via controller 102 as modified with Litvin's daemon service that would connect with a client device Portal to retrieve updated firewall policies in resource database 103 to enable the Portal process in Wang's client devices to define and implement firewall policies. Pet. 50–52 (citing Ex. 1004 ¶¶ 13, 15, 16, 21, 22, Fig. 1; Ex. 1002 ¶¶ 116, 118–120; Ex. 1001, 10:57–63). We find that Petitioner's contentions are supported by record evidence cited above and in the Petition.

Petitioner applies Litvin's daemon process to Chambers' management server 101 to initiate a connection to a client portal to retrieve a policy digest as Wang teaches. Pet. 50–52, 95–96. We find that a daemon service would eliminate the need for a user at a client device portal to initiate a connection to retrieve a policy digest and thereby reduce the risk of tampering with the policies and processes from such a client portal to improve network security.

4. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 7 and 18 are unpatentable over Chambers, Terrill, Litvin, and Wang.

N. Ground 11: Alleged Obviousness Over Chambers, Terrill, Litvin, Wang, and Botzer

Petitioner asserts unpatentability of claims 8 and 19 under 35 U.S.C. § 103 over Chambers, Terrill, Litvin, Wang, and Botzer. Pet. 99–100.

1. Petitioner's contentions

Petitioner asserts that the Chambers-Terrill-Litvin-Wang combination did not prevent the portal process from initiating a connection to the daemon service. Pet. 99. Petitioner contends that a skilled artisan would have used Botzer's functionality to prevent such a connection, as discussed in Ground 3, to improve its efficiency and data security with a reasonable expectation of success. *Id.* at 99–100 (citing Ex. 1012 ¶ 112; Ex. 1002 ¶ 253).

2. Patent Owner's arguments

Patent Owner reasserts arguments presented for Grounds 7, 9, and 10. PO Resp. 56. Patent Owner also argues that a skilled artisan would not have combined Chambers-Terrill-Litvin-Wang with Botzer to prevent inbound traffic because Petitioner never established that the combination teaches a portal process that initiates a connection with a daemon service instead of a daemon process that initiates a connection to a portal process. *Id.* at 56–57.

3. *Analysis*

We disagree with Patent Owner's arguments from Grounds 7, 9, and 10 for reasons discussed in Sections III.J., III.L., and III.M. *supra*. We find Botzer would prevent Wang's portal process from connecting to a daemon service on Wang's or another controller. Reply 38–39; Pet. 98–99. Botzer would improve the combination by selectively preventing the portal process from accessing and interfering with a daemon service that was added to reduce user interference, as discussed in Sections III.L.3. and III.G. *supra*.

4. Conclusion

Based on the parties' contentions and record evidence, we determine Petitioner has demonstrated, by a preponderance of the evidence, that claims 8 and 19 are unpatentable over Chambers, Terrill, Litvin, Wang, and Botzer.

O. Ground 12: Alleged Obviousness Over Chambers, Terrill, and Shafer

Petitioner asserts the unpatentability of claims 9 and 20 under 35 U.S.C. § 103 over Chambers, Terrill, and Shafer. Pet. 100.

1. Petitioner's contentions

Petitioner asserts that a skilled artisan would have been motivated to add Shafer's function of checking a policy digest against a predefined format to Chambers' controller to avoid erroneous configuration changes based on an incorrect policy change before the erroneous change was made, as Shafer warns, with a reasonable expectation of success. Pet. 100 (citing Ex. 1010, 2:1–11; Ex. 1008 ¶ 26; Ex. 1002 ¶ 256; Ground 6; Ground 4, claims 9, 20).

2. Patent Owner's arguments

Patent Owner argues that Petitioner's Ground 12 relies on Ground 7 and fails for the same reason discussed in Section X. PO Resp. 58.

3. Analysis

We disagree with Patent Owner's arguments for the reasons discussed in Section III.J. *supra* for Ground 7.

4. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 9 and 20 are unpatentable over Chambers, Terrill, and Shafer.

IV. CONCLUSION

Petitioner has demonstrated by a preponderance of the evidence that claims 1–22 of the ’941 patent are unpatentable.

Claims	**35 U.S.C. §**	**Reference(s)/ Basis**	**Claims Shown Unpatentable**	**Claims Not Shown Unpatentable**
1, 2, 4, 5, 12, 13, 15, 16	103	Wang	1, 2, 4, 5, 12, 13, 15, 16	
3, 14	103	Wang, Pasdar	3, 14	
6, 7, 17, 18	103	Wang, Sikka	6, 7, 17, 18	
8, 19	103	Wang, Sikka, Botzer	8, 19	
9, 20	103	Wang, Shafer	9, 20	
10, 11, 21, 22	103	Wang, Terrill	10, 11, 21, 22	
1, 2, 4, 5, 10–13, 15, 16, 21, 22	103	Chambers, Terrill	1, 2, 4, 5, 10–13, 15, 16, 21, 22	
3, 14	103	Chambers, Terrill, Pasdar	3, 14	
6, 17	103	Chambers, Terrill, Litvin	6, 17	
7, 18	103	Chambers, Terrill, Litvin, Wang	7, 18	
8, 19	103	Chambers, Terrill, Litvin, Wang, Botzer	8, 19	
9, 20	103	Chambers, Terrill, Shafer	9, 20	
Overall Outcome			1–22	

V. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1–22 of the ’941 patent have been shown to be unpatentable; and

FURTHER ORDERED that because this is a Final Written Decision, parties to this proceeding seeking judicial review of this Decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.[11]

[11] Should Patent Owner wish to amend the challenged claims in a reissue or reexamination proceeding, we draw Patent Owner's attention to the *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. *See* 84 Fed. Reg. 16654 (Apr. 22, 2019). If Patent Owner files a reissue application or request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of such related matters in updated mandatory notices. *See* 37 C.F.R. § 42.8(a)(3), (b)(2).

PETITIONER:

Thomas Millikan
Wei Yuan
Babak Tehranchi
PERKINS COIE LLP
millikan-ptab@perkinscoie.com
yuan-ptab@perkinscoie.com
tehranchi-ptab@perkinscoie.com

PATENT OWNER:

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