

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

TREND MICRO INC.,
Petitioner,

v.

CUPP COMPUTING AS,
Patent Owner.

IPR2019-00561
Patent 8,365,272 B2

Before THOMAS L. GIANNETTI, GARTH D. BAER, and
SHARON FENICK, *Administrative Patent Judges*.

GIANNETTI, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision on Remand
Determining A Challenged Claim Unpatentable
35 U.S.C. §§ 144, 318

I. INTRODUCTION

A. Background

This case returns to the Board on remand from the United States Court of Appeals for the Federal Circuit. *Trend Micro Inc, v. CUPP Computing AS*, Nos. 2020-2236, 2020-2238 (Fed. Cir. Oct. 25, 2022) (vacating the Board’s Final Written Decision with respect to the appealed claims and remanding for further proceedings) (Paper 32, “Decision”).

We have jurisdiction under 35 U.S.C. § 6. We issue this Final Written Decision on Remand under 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73.

B. Procedural History

Trend Micro Inc. (“Petitioner”) filed a Petition requesting *inter partes* review of claims 1, 7, and 16 (the “challenged claims”) of U.S. Patent No. 8,365,272 B2 (Ex. 1001, the “’272 patent”). Paper 1 (“Pet.”). CUPP Computing AS (“Patent Owner”) filed a Preliminary Response. Paper 6.

After considering the arguments presented in Patent Owner’s Preliminary Response, pursuant to 35 U.S.C. § 314, we instituted this *inter partes* review as to all of the challenged claims and all grounds raised in the Petition. Paper 7.

Following institution, Patent Owner filed a Response. Paper 11 (“PO Resp.”), Petitioner filed a Reply (Paper 13, “Pet. Reply”), and Patent Owner filed a Sur-reply (Paper 20, “Sur-reply”).¹

¹ In addition, Patent Owner filed a Motion to Exclude. Paper 21. We denied that motion in a separate Order. Paper 28.

On April 20, 2020, we held a consolidated oral hearing with IPR2019-00641, involving related U.S. Patent No. 9,756,079, and a transcript of the hearing is included in the record. Paper 26 (“Hearing Tr.”).

On July 6, 2020, we entered a Final Written Decision in which we determined that Petitioner had demonstrated that claim 1 of the ’272 patent is unpatentable, but that Petitioner had not demonstrated that claims 7 and 16 are unpatentable. Paper 27 (“FWD”), 2–3. Petitioner appealed that Final Written Decision regarding claims 7 and 16 to the Federal Circuit.² Decision 2.

On October 25, 2022, the Federal Circuit vacated the Final Written Decisions entered by the Board in this case and in IPR2019-00641 with respect to each appealed claim and remanded both cases to the Board for further proceedings. Decision 2, 13.

For the reasons we identify below, we determine that Petitioner has demonstrated by a preponderance of the evidence that claim 16 of the ’272 patent is unpatentable. We further determine that Petitioner has not demonstrated that claim 7 is unpatentable.³

C. Related Proceedings

Petitioner identifies the following district court proceedings concerning the ’272 patent: *CUPP Cybersecurity LLC et al. v. Trend Micro, Inc., et al.*, No. 3:18-cv-01251 (N.D. Tex.); *CUPP Cybersecurity LLC v.*

² Patent Owner’s cross-appeal as to claim 1 (Paper 30) was voluntarily dismissed.

³ The Federal Circuit’s Decision does not discuss challenged claim 1 and vacated our Final Written Decision only with respect to the appealed claims, *i.e.*, claims 7 and 16. Decision 1, 13. We therefore do not address the patentability of claim 1 in this Final Written Decision on Remand.

Symantec Corp., No. 3:18-cv-01554 (N.D. Tex.); and *Symantec Corp. v. CUPP Cybersecurity LLC, et al.*, No. 3:18-cv-04720 (N.D. Cal.). Pet. 1. Patent Owner identifies the following additional action involving the '272 patent: *CUPP Cybersecurity LLC et al. v. Symantec Corp.*, 3:19-cv-00298 (N.D. Cal.). Paper 3, 1.

D. Real Party-in-Interest

The Petition identifies Trend Micro Inc. as the real party-in-interest. Pet. 1. Patent Owner identifies CUPP Computing AS as the real party-in-interest. Paper 3, 1.

E. Description of Relevant Internet Technology

The relevant technology is described in our Final Written Decision and the Federal Circuit's opinion. *See* FWD 3–5; Decision 3–4. We incorporate those descriptions into this Final Written Decision on Remand.

F. The '272 Patent

The '272 patent is titled “System and Method for Providing Network and Computer Firewall Protection with Dynamic Address Isolation to a Device.” Ex. 1001 (54). The patent relates generally to computer security, and more particularly, describes a system and method for providing data and device security between external and host devices on a computer network. *Id.* at 1:14–16.

According to the '272 patent, prior hardware-based firewalls made use of NAT (Network Address Translation) to translate the IP (Internet Protocol) addresses of the internal computers on a network into public IP addresses, “thus hiding the IP addresses of the internal computers.” *Id.* at 18:45–64,

Fig. 17. According to the '272 patent, hardware-based firewalls were an improvement over PC (personal computer) software-based firewalls running on internal computers. *Id.* at 18:65–19:3.

1. “Dynamic Isolation” Embodiment

The '272 patent describes an embodiment under the heading “Dynamic Isolation.” Ex. 1001, 18:45–21:31. The description of this embodiment begins with a discussion of Figure 18 of the '272 patent. Figure 18 shows a “prior art” network system having a software-based firewall. *Id.* at 19:4–5. Figure 18 follows:

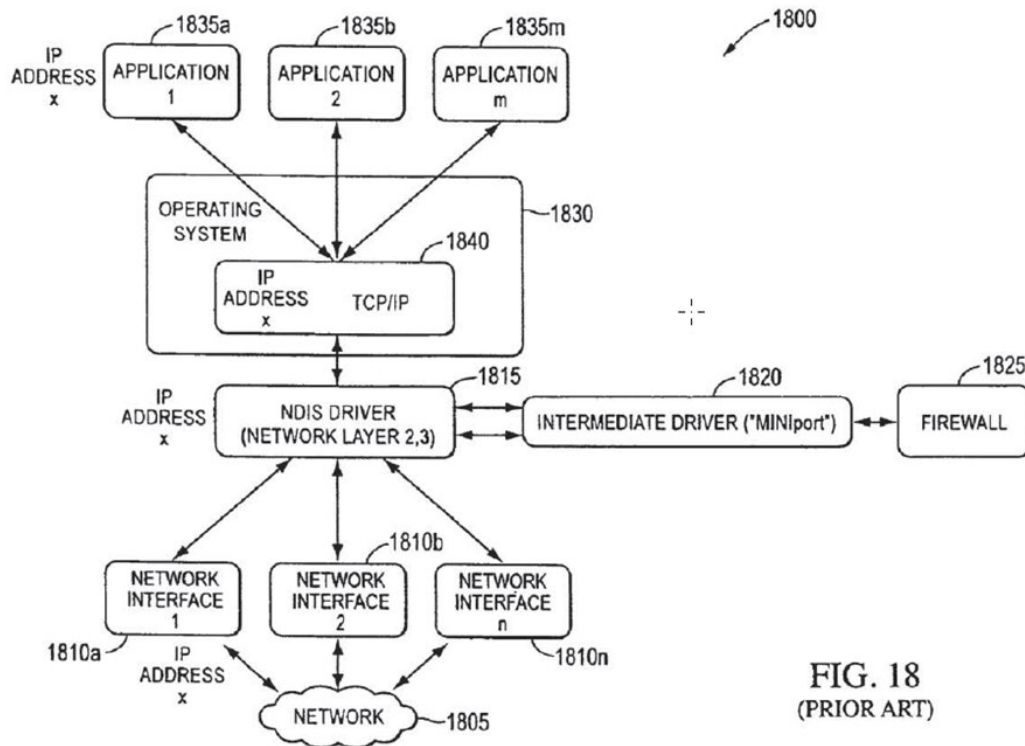


Figure 18 is a block diagram illustrating prior-art network system 1800 having software-based firewall 1825. *Id.* at 19:4–5. The network system includes external network 1805 (such as the Internet), one or more Network

Interface Cards (NICs) 1810 (denoted as 1810a, 1810b, . . . 1810n), and Network Driver Interface Specification (NDIS) driver 1815. *Id.* at 19:5–8.

As described in the patent, prior art software-based firewall networks such as that shown in Figure 18 include NDIS driver 1815 as an interface between Open Systems Interconnection (OSI) layer 2 (the data link layer) and OSI layer 3 (the network layer),⁴ as well as intermediate driver 1820, software-based firewall 1825, operating system 1830 containing the TCP/IP protocol suite, and one or more applications 1835. *Id.* at 19:7–15.

In operation, the intermediate driver directs traffic arriving to the software-based firewall. The firewall decides whether to allow, deny, or reject the traffic and permits only the allowed traffic to proceed to the operating system. *Id.* at 19:17–22. According to the patent, this prior art system is disadvantageous in that the IP internal addresses visible to the external network are the same IP addresses viewed and used by the applications, “(i.e., there is no address isolation between the applications 1835 and the external network 1805).” *Id.* at 19:25–29.

Figure 19 of the '272 patent shows a network system that “performs dynamic address isolation.” *Id.* at 19:30–32. Figure 19 (annotated by the Board) follows:

⁴ See Pet. 11–12 for a description of the OSI model.

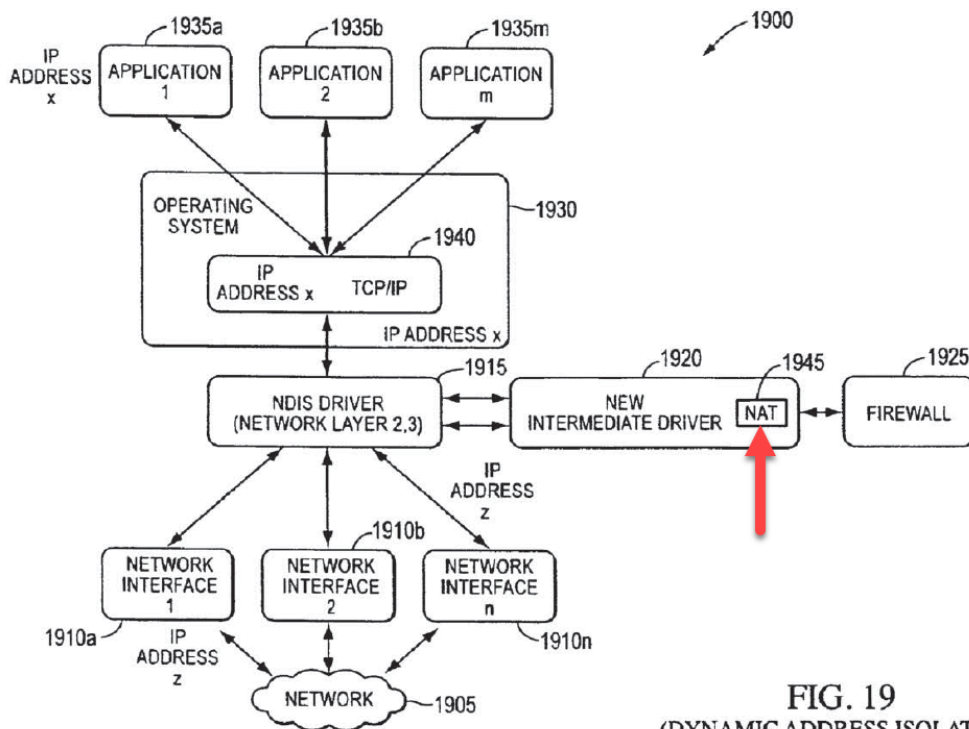


FIG. 19
(DYNAMIC ADDRESS ISOLATION)

Figure 19 is described as “a block diagram illustrating a network system that performs dynamic address isolation.” Ex. 1001, 4:29–30. The network shown in Figure 19 has the same general configuration as prior art network 1800 of Figure 18, reproduced *supra*. That is, Figure 19’s network system 1900 (like the network of Figure 18) includes external network 1905 (such as the Internet), one or more network interface devices (NICs) 1910a, 1910b, . . . 1910n, NDIS driver 1915 that acts as an interface between the OSI data link layer 2 and OSI network layer 3, intermediate driver 1920, software-based or hardware-based firewall 1925, operating system 1930, and one or more applications 1935a, 1935b, . . . 1935m. Further, as in Figure 18, operating system 1930 contains TCP/IP protocol suite 1940. *Id.* at 19:32–41.

In contrast to prior art Figure 18, however, in Figure 19, intermediate driver 1920 includes NAT engine 1945, indicated by the red arrow in the

annotated Figure, that contains a translations table for IP addresses. *Id.* at 19:41–43.

In operation, intermediate driver 1920 receives all data packets arriving from NICs 1910 and NDIS driver 1915 and routes each data packet to NAT engine 1945. NAT engine 1945 uses DHCP (Dynamic Host Configuration Protocol; *see* Exhibit 3001) to “dynamically isolate the IP addresses of the applications 1935 from the external network 1905.” *Id.* at 19:52–57. As shown in Figure 19, the dynamic NAT engine 1945 translates the IP address of the application 1935 (IP address x) to a different IP address (IP address z) while interfacing with the NIC, and translates the IP address z back to the IP address x when sending data to the operating system 1930. Thus, intermediate driver 1920 provides IP address z to external network 1905, while isolating IP address x from the external network. *Id.* at 19:57–65.

After NAT engine 1945 translates the IP address, intermediate driver 1920 directs each incoming data packet to firewall 1925. *Id.* at 20:4–6. Firewall 1925 decides whether to allow, deny, or reject the data packets it receives, and permits only allowed data packets to proceed to operating system 1930. *Id.* at 20:6–8. Intermediate driver 1920 receives each allowed data packet back from firewall 1925 and routes each allowed data packet to an application 1935. *Id.* at 20:9–11.

For outgoing data packets, intermediate driver 1920 receives each data packet from application 1935 and routes each data packet to NAT engine 1945. *Id.* at 20:12–14. NAT engine 1945 translates the IP address associated with the data packet as described above. Intermediate driver 1920 then receives each data packet containing the translated IP address

back from NAT engine 1945 and routes each data packet to external network 1905. *Id.* at 20:14–21.

2. “Hybrid Firewall” Embodiment

A separate embodiment of the ’272 patent is described under the heading “Hybrid Firewall.” Ex. 1001, 21:35–24:60. The description begins with a discussion of Figure 20 of the patent. *Id.* at 21:35–64. Figure 20 shows a “prior art” network system “having separate network and personal firewalls.” *Id.* at 21:35–36. Figure 20 follows:

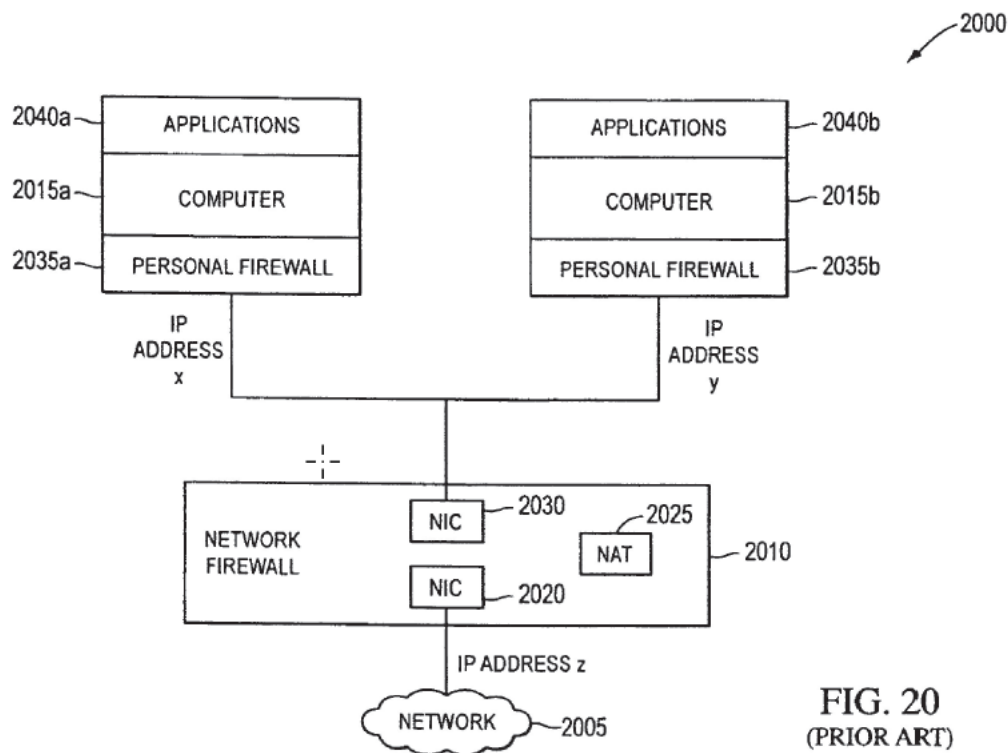


Figure 20 shows prior art network system 2000 having separate network and personal firewalls. *Id.* at 21:35–36. Network system 2000 includes external network 2005 (such as the Internet), network firewall 2010, and personal computers 2015 (denoted as 2015a, 2015b, etc.). *Id.* at 21:36–39. Each personal computer 2015 comprises personal firewall 2035

(denoted as 2035a, 2035b, etc.) and application 2040 (denoted as 2040a, 2040b, etc.). *Id.* at 21:42–44.

Network firewall 2010 comprises first NIC 2020, NAT gateway 2025, and second NIC 2030. *Id.* at 21:39–42. In operation, network firewall 2010 uses NAT gateway 2025 to translate the IP address of personal computer 2015a (denoted as IP address x) and the IP address of personal computer 2015b (denoted as IP address y) into public IP address z, and thus hiding the IP addresses of the personal computers. *Id.* at 21:45–50. Network firewall 2010 performs a similar translation on the MAC addresses⁵ of the personal computers 2015. *Id.* at 21:50–52.

According to the '272 patent, network firewall 2010 in Figure 20 performs security measures such as antivirus, anti-spyware, anti-adware, etc. “However, because the network firewall 2010 is application insensitive and at a lower layer of the information stack, its processes for malicious code detection are limited.” *Id.* at 21:52–59.

Further according to the '272 patent, personal firewall 2035 also performs security measures such as antivirus, anti-spyware, anti-adware, etc. “Because the personal firewall 2035 is application sensitive and at a higher layer of the information stack, its processes for malicious code detection can be more thorough and focused.” *Id.* at 21:60–64.

Figure 21 shows network system 2100 with a “hybrid fire wall.”
Ex. 1001, 21:65–66. Figure 21 follows:

⁵ The MAC (Media Access Control) address is an identifier assigned to a computer by its manufacturer. Ex. 1019, 42:6–8.

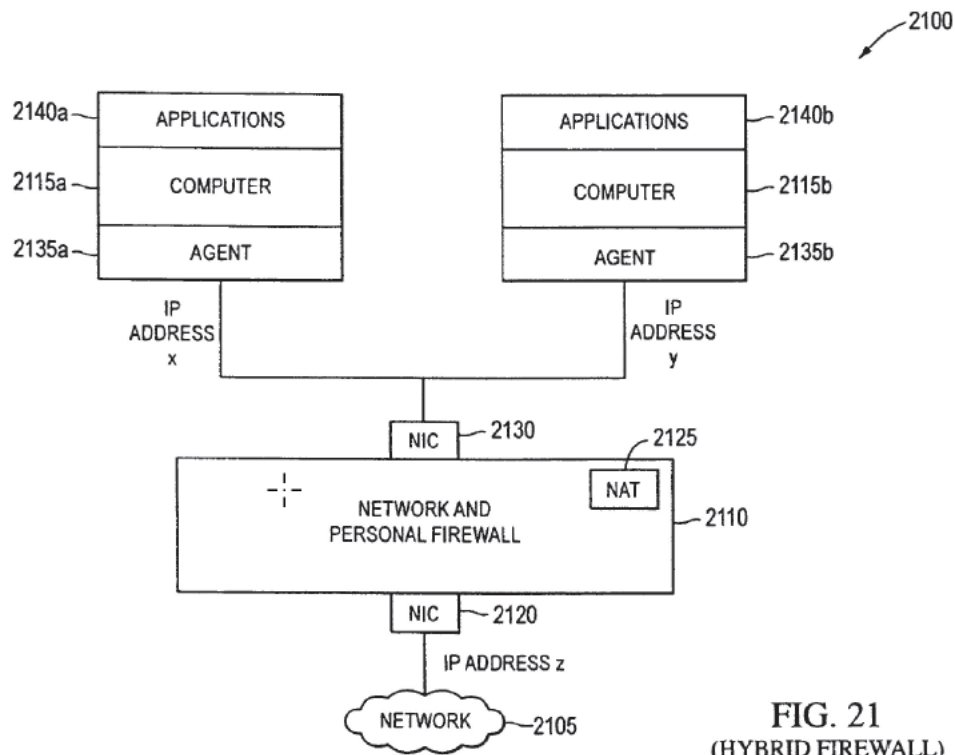


FIG. 21
(HYBRID FIREWALL)

Figure 21 shows network system 2100 comprising hybrid firewall 2110 in accordance with an embodiment of the '272 patent. *Id.* at 21:65–67. As in Figure 20, network system 2100 includes external network 2105 (such as the Internet) and personal computers 2115 (denoted as 2115a, 2115b, etc.). *Id.* at 21:67–22:3. In contrast to Figure 20, however, Figure 21 shows hybrid network/personal firewall 2110. The hybrid firewall 2110 comprises first NIC 2120, NAT engine 2125, and second NIC 2130. *Id.* at 22:7–8.

In this embodiment, each personal computer 2115 also comprises an agent 2135 (denoted as 2135a, 2135b, etc.) and one or more applications 2140 (denoted as 2140a, 2140b, etc.). *Id.* at 22:9–11. In operation, hybrid firewall 2110 uses NAT engine 2125, which contains a translations table for IP and MAC addresses, to translate the IP address of personal computer 2115a (denoted as IP address x) and the IP address of personal computer

2115b (denoted as IP address y) into public IP address z, thus hiding the IP addresses of the personal computers. *Id.* at 22:15–21. The network firewall 2110 performs a similar translation on the MAC addresses of the personal computers 2115. *Id.* at 22:21–23.

In contrast to the prior art firewall shown in Figure 20, however, hybrid firewall 2110 is capable of performing both the network firewall and personal firewall security measures. Because hybrid firewall 2110 is at the same level as traditional network firewall 2035 of Figure 20, it can stop malicious code before it enters the system 2100. *Id.* at 22:24–28. “Further, because the hybrid firewall 2110 is application sensitive, the hybrid firewall 2110 can perform the processes of the traditional personal firewall 2035.” *Id.* at 22:28–31.

To enable hybrid firewall 2110 to be “application sensitive,” agents 2135 send packets of data to hybrid firewall 2110, “each packet comprising data identifying the application 2140 associated with the packet.” *Id.* at 22:32–35. This enables hybrid firewall 2110 to “act as a personal firewall 2035 to handle application-level security.” *Id.* at 22:35–38.

G. Challenged Claims

Claims 7 and 16 of the '272 patent are independent claims, and are the only claims considered in the appeal and before us on remand. Pet. 3.

Claim 7 recites:⁶

7. A system, comprising:

[7.1] a network interface coupled to an external network;

⁶ Paragraph numbering in accordance with the Petition has been added to the claims.

[7.2] a firewall in communication with the network interface, the firewall configured to handle both network-level security and application-level security;

[7.3] a computer in communication with the firewall, the computer having one or more applications, each of the one or more applications associated with at least one application address, and the computer being configured to send to the firewall data packets identifying the one or more applications to the firewall; and

[7.4] a network address translation engine configured to translate the at least one application address of the one or more applications to a public address, thereby dynamically isolating the one or more applications from the external network;

[7.5] the firewall being configured to:

reject the data packets if the data packets include malicious content according to a mobile device security policy; and

[7.6] allow the data packets to pass to the one or more applications if the data packets do not include malicious content according to the mobile device security policy.

Ex. 1001, 25:34–56.

Claim 16 is a method claim. Claim 16 recites:

16. A method within a computer of processing outgoing data, the method comprising:

[16.1] receiving the outgoing data from an application, the application being associated with an internal address;

[16.2] translating, using a network address translation engine within the computer, the internal address into a public address;

[16.3] routing, using a driver within the computer, at least a subset of the outgoing data to an external network using the public address, thereby dynamically isolating the internal address from the external network; and

[16.4] providing, using a network interface within the computer, the subset of the outgoing data to the external network.

Id. at 26:37–48.

H. References and Other Evidence

Petitioner relies on the following references:

1. Intern. Pat. Appl. Pub. No. WO 2006/069041 A2 (Ex. 1004, “Sikdar”).
2. U.S. Patent Appl. Pub. No. 2005/0055578 A1 (Ex. 1006, “Wright”).

Pet. 3. In addition, Petitioner relies on admitted prior art (APA), specifically, Figure 18 of the ’272 patent, reproduced *supra*, and the accompanying description of that figure in the specification. *Id.* at 38–39.

Both parties rely on expert testimony. Petitioner submitted a Declaration of Dr. Markus Jakobsson (Ex. 1018, “Jakobsson Decl.”), and a Supplemental Declaration of Dr. Jakobsson (Ex. 1031, “Jakobsson Supp. Decl.”). Patent Owner submitted a Declaration of Nenad Medvidovic, Ph.D. (Ex. 2001, “Medvidovic Decl.”). In addition, the parties have submitted deposition transcripts for Dr. Jakobsson and Dr. Medvidovic.⁷

I. Asserted Grounds of Unpatentability

Petitioner asserted claims 7 and 16 are unpatentable on the following grounds:

Claim Challenged	Statutory Basis ⁸	References
7	35 U.S.C. § 103	Sikdar, Wright

⁷ Ex. 2002, “Jakobsson I Dep.”; Ex. 2009, “Jakobsson II Dep.”; Ex. 1019, “Medvidovic Dep.” In addition, Petitioner submitted Dr. Medvidovic’s declaration (Ex. 1026) and deposition testimony (Ex. 1028) from the district court action involving the ’272 patent.

⁸ Because the effective filing date of the application from which the ’272 patent issued was before March 16, 2013, the pre-AIA (“America Invents

Claim Challenged	Statutory Basis ⁸	References
16	35 U.S.C. § 103	Sikdar, APA
16	35 U.S.C. § 103	APA, Sikdar

Pet. 3

II. PRELIMINARY MATTERS

A. Level of Ordinary Skill

Petitioner contended “[a] person of ordinary skill in the art at the time of the alleged invention of the ’272 patent (i.e., May 30, 2007) . . . would have had a Bachelors’ degree in computer science, electrical engineering, or a comparable field of study, plus at least two years of professional experience with computer security systems and networks, or the equivalent.” Pet. 8 (citing Jakobsson Decl. ¶ 49). In our Final Written Decision, we adopted Petitioner’s description of the person of ordinary skill over an alternative formulation by Patent Owner’s expert, Dr. Medvidovic. FWD 17. However, we decided that we would reach the same result even under Dr. Medvidovic’s alternative formulation. *Id.*

The level of ordinary skill adopted by us has not been further disputed by the parties, nor is it discussed in the Federal Circuit’s Decision. We therefore apply the same formulation for the reasons given in our Final Written Decision.

Act”) version of 35 U.S.C. § 103 applies. Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284, 285–88 (2011).

B. Claim Construction

1. “dynamically isolating” (claims 7 and 16)

The construction of “dynamically isolating,” a term appearing in both claims 7 and 16, is central to resolving this dispute. As the Federal Circuit observed, “[t]he issue on appeal is whether, as the Board ultimately found, Sikdar fails to disclose what that construction requires.” Decision 7.

Relying on the specification and the claims, in our Final Written Decision, we construed “dynamically isolating” as including the use of DHCP or other source of addresses in connection with a NAT engine to translate IP addresses. FWD 23–24.

Before the Federal Circuit, the Board’s construction for this claim term was “accepted as correct by both parties.” Decision 7.

2. “the subset” (claim 16)

The construction of this term appearing in claim 16 is not discussed in the Petition or the Federal Circuit’s Decision, but it is addressed by Patent Owner’s Response in connection with claim 16. *See* PO Resp. 45–47, 49. The term “subset” appears twice in claim 16. The first occurrence refers to “routing . . . at least a subset of the outgoing data to an external network.” Ex. 1001, 26:44–45. The second occurrence refers to “providing . . . the subset of the outgoing data to the external network.” *Id.* at 26:48–49.

Patent Owner asserts that in Petitioner’s analysis of claim 16, “Petitioner reads out any distinctions between ‘at least a subset’ and ‘a subset.’” PO Resp. 45. Petitioner responds that “[t]he Board should reject Patent Owner’s argument that ‘the subset’ must be a ‘proper subset,’ *i.e.*, a set that is less than the full set of outgoing data.” Pet. Reply 5. Petitioner

cites dictionary definitions and other additional authorities to support this conclusion. Pet. Reply 5–6 (citing, e.g., Exs. 1022, 1023, 1024). For example, *A Dictionary of Computing* defines “subset” as “[a] set *T* whose members are all members of *S*,” and contrasts this with a “proper subset.” Ex. 1023, 3. Petitioner further points out that the antecedent basis of “at least a subset” for “the subset” in claim 16 supports its construction. Pet. Reply 6.

In our Final Written Decision, after considering Petitioner’s evidence and the language of the claim, we found that the references to “subset” in claim 16 should be construed broadly enough to read on providing any portion of the outgoing data, up to and including *all* the data, and not a proper subset. FWD 24–25. For the reasons summarized above and those given in our Final Written Decision, we find that the term “subset” in claim 16 does not limit the claim to a “proper subset,” i.e., the claimed subset may include all the members of the set.

C. Description of the Prior Art References

1. Sikdar

Sikdar discloses a Reconfigurable Semantic Processor (RSP) used for implementing a firewall capable of performing network address translation (NAT) and port address translation (PAT).⁹ Ex. 1004, 8, 49.¹⁰

⁹ The combination of PAT and NAT is sometimes referred to as Network Address Port Translation (NAPT). Jakobsson Decl. ¶ 61; Ex. 1010 (RFC 2663), 11.

¹⁰ Citations to Sikdar (Ex. 1004) refer to the original page numbers and not the page numbers added by Petitioner.

Figure 20 of Sikdar, which follows, illustrates this operation:

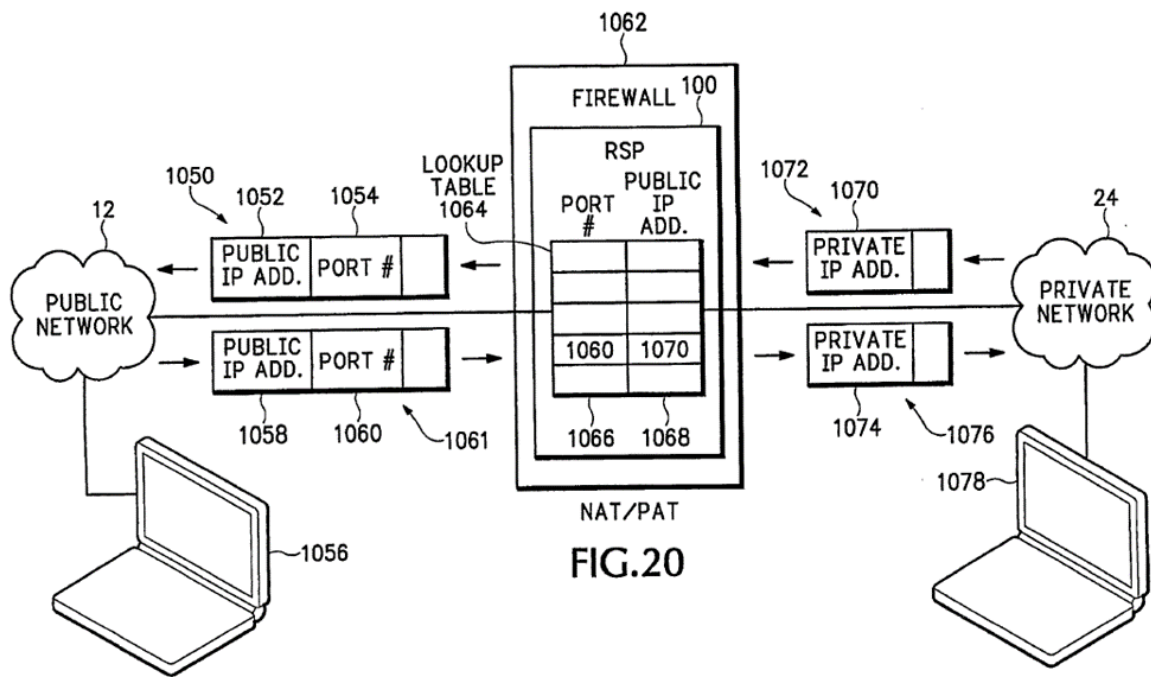


Figure 20 of Sikdar is a diagram showing how RSP 100 is used for NAT and PAT. *Id.* at 4. Figure 20 shows private network 24 and public network 12 separated by firewall 1062. *Id.* at 49. RSP 100 can be programmed for NAT/PAT operations that convert IP addresses and port numbers for packets traveling through firewall 1062 between public IP addresses that are used for transporting the packet over public network 12 and private IP addresses that are used for transporting the packet over the private network 24. *Id.* The private IP addresses and their corresponding port numbers are stored in lookup table 1064. *Id.* at 50.¹¹

¹¹ The parties agree that in Figure 20 of Sikdar, the heading for column 1068 in Lookup Table 1064, “Public IP Add[resses],” is incorrect and should be “Private IP Add[resses].” Hearing Tr. 10:13–18; Medvidovic Decl. ¶ 60 n.1.

Sikdar explains that typically there are multiple unique private IP addresses associated with different network processing devices operating in private network 24. “However, only one, or a few, public IP addresses may be used to represent the multiple private IP addresses.” *Id.* at 49.¹² This protects the identity of internal machines in private network 24 and reduces the number of public addresses required to map to multiple private addresses in private network 24. *Id.* at 49–50.

RSP 100 is configured to convert public IP address 1058 for an incoming packet 1061 into private IP address 1074. *Id.* at 50. Private IP address 1074 is then used to route internal packet 1076 to an associated network processing device 1078 in private network 24. RSP 100 also receives packet 1072 from local device 1078 in private network 24 that contains a private IP address 1070. *Id.* If packet 1072 is directed to endpoint 1056 in public network 12, RSP 100 converts private IP address 1070 into public IP address 1052 that is used to route packet 1050 over public network 12 to endpoint 1056. *Id.*

The details of NAT/PAT operation in Sikdar are shown in Figures 22 and 23. *Id.* at 4, 51. When packet 1072 is being sent, the RSP replaces private IP source address 1070 for the packet with public source IP address 1052 that includes associated port number 1054. *Id.* at 51. For incoming

¹² Several words in the sentence starting at the bottom of page 49 of Sikdar (Page 51 of Exhibit 1004) are illegible. The complete sentence, shown on Page 128 of Exhibit 1005, is: “This public-private address process protects the identity of internal machines in private network 24 and reduces the number of public addresses required to map to multiple private addresses in private network 24.”

packet 1061, the RSP replaces the public IP destination address 1058 for the packet with the identified private IP address 1074. *Id.* at 52.

2. *Wright*

Wright is titled “Administration of Protection of Data Accessible by a Mobile Device.” Ex. 1014, (54). Wright discloses protecting data on a client mobile computing device by a server computer within an enterprise network or on a separate mobile computing device. *Id.* at (57). Wright describes security tools that provide different security policies to be enforced, based on a location associated with a network environment in which a mobile device is operating. *Id.* Wright also describes methods for detecting the location of the mobile device. *Id.*

The security tools in Wright also provide for enforcing different policies based on security features such as the type of connection, wired or wireless, over which data is being transferred, the operation of anti-virus software, or the type of network adapter card. *Id.* The different security policies provide enforcement mechanisms that may be tailored based upon the detected location or active security features associated with the mobile device. *Id.*

Petitioner relies on Figure 2A of Wright, which follows:

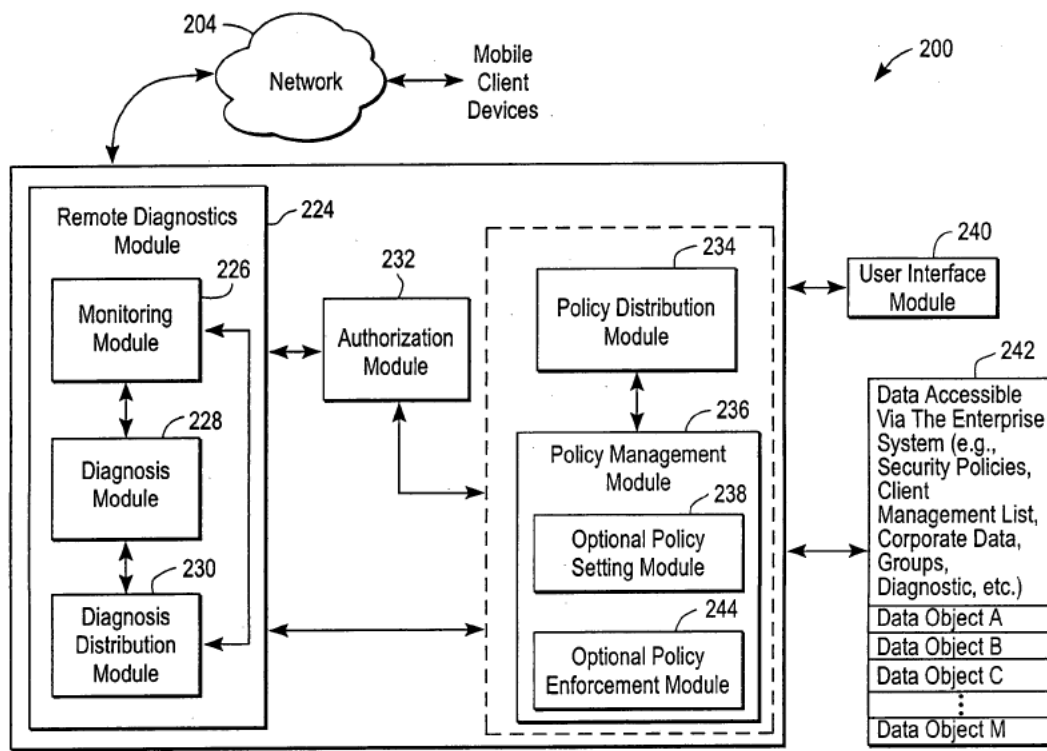


FIG. 2A

Pet. 16. Figure 2A shows server system 200 that includes memory 242. Ex. 1004 ¶¶ 53–54. The security system provides security services to remote mobile client devices. *Id.* ¶ 53. Memory 242 stores the security policies and other security information. *Id.* ¶ 110. The server includes policy management module 236, which manages security policies. *Id.* ¶ 55.

III. ANALYSIS OF CLAIMS 7 AND 16

Petitioner asserts unpatentability of claims 7 and 16 based on obviousness. Pet. 3.

A. Claim 7

Petitioner presents an element-by-element analysis, contending that each element of claim 7 is disclosed by Sikdar and Wright. Pet. 16–37.

Here, we address only the contested limitations. For the remaining claim limitations, we rely on and adopt the findings in our Final Written Decision. *See* FWD 30–36.

Petitioner summarizes its analysis of claim 7 as follows: “Sikdar discloses a ‘Reconfigurable Semantic Processor’ (‘RSP’) . . . that may perform network address translation (‘NAT’) and port address translation (‘PAT’), in addition to firewall functionality such as network-level security and application-level security.” Pet. 14. Further, “Wright discloses a security system 200 that provides security services to laptops and other mobile devices that may be in or out of a private enterprise network.” *Id.* at 15.

1. Dynamically Isolating

Claim element 7.4 requires “a network address translation engine configured to translate the at least one application address of the one or more applications to a public address, thereby *dynamically isolating* the one or more applications from the external network.” Ex. 1001, 26:24–29 (emphasis added). Petitioner contended that Sikdar’s description of “NAT/PAT operations” in connection with Figure 20 meets this limitation. Pet. 31–35. Petitioner explained that “Sikdar discloses that ‘the RSP 100 can be programmed for NAT/PAT operations that convert IP addresses [and] port numbers.’” *Id.* (citing Ex. 1004, 49, Fig. 20 (reproduced *supra*)). Further referring to Figure 20 of Sikdar, Petitioner asserted, “[t]he translated IP address and port number are used on the public network 12 and therefore are a public address. Such translation dynamically isolates the applications of laptops 1078 and 25C from public network 12 because it hides those

applications’ addresses from the public network as the packets pass through the RSP.” *Id.* (citations omitted).

Patent Owner responded that Sikdar does not teach “dynamically isolating” as recited in claim element 7.4. Prelim. Resp. 11–17. Patent Owner argued that “Sikdar does not dynamically isolate applications from the external network at least because Sikdar only converts the IP addresses of devices within a private network using conventional, static solutions.” *Id.* at 12 (emphasis omitted). Patent Owner explained further that “[l]ike the prior art system, Sikdar’s NAT technique simply converts the private IP address to the public address of the firewall, assigns the outgoing packet a port, and updates a lookup table.” *Id.* at 14.

In our Final Written Decision, we found that under our claim construction, Petitioner had failed to demonstrate that Sikdar discloses “dynamically isolating.” FWD 34–35. We reasoned that Sikdar differs from the ’272 patent’s disclosure of dynamic addressing because Sikdar discloses using the *same* IP address (the IP address of the firewall) for all packets traveling from the private network to the public network. *See* Ex. 1004, 50 (“The RSP 100 receives the packet 1072 and converts the private source IP address 1070 to the public IP address 1052 associated with firewall 1062.”). We, therefore, concluded that Petitioner had not demonstrated by a preponderance of the evidence that Sikdar discloses the translation of IP addresses “using DHCP or other source of addresses,” as our claim construction required. FWD 34.

The Federal Circuit disagreed with our analysis and concluded that “the Board’s finding is not supported by substantial evidence.” Decision 9. The Court continued, “[w]e do not see, and [Patent Owner] has not pointed

us to, any evidence that would permit a reasonable finding that Sikdar fails to teach ‘dynamically isolating’ under the agreed-on construction.” *Id.* In reaching this conclusion, the Court rejected the argument that Sikdar’s use of the firewall IP address for all outgoing packets indicated that it is not “dynamically isolating” the addresses of the packets. *Id.* at 10.

It is with this determination by the Federal Circuit, which is binding on this panel, that we evaluate on remand Petitioner’s contention that the “dynamically isolating” limitation is met by Sikdar. PO Resp. 20–27.

Quoting the Board’s construction of “dynamically isolating,” the Federal Circuit opinion specifically states that “Sikdar clearly discloses ‘the use of DHCP or other source of addresses in connection with a NAT engine to translate IP addresses.’” Decision 10. The Federal Circuit, therefore, held that Sikdar discloses “dynamically isolating” under the Board’s construction adopted by the parties:

This claim construction does not require the use of DHCP or a source that is, in some narrowing way, similar or comparable to DHCP. By its broad terms, this construction simply requires any source of addresses—“DHCP or other source of addresses.”

Id. The Federal Circuit further explained its holding that Sikdar teaches “dynamically isolating”:

Sikdar teaches this aspect of the claim construction in several ways: It discloses that the SPU “generates” the public IP address, says that this address is “usually” the address “assigned to” the firewall, and describes, in an alternative embodiment, a one-to-one mapping of private and public addresses. These disclosures teach a “source of addresses in connection with a NAT engine to translate IP addresses.”

Id. (citation omitted) In reaching this conclusion, the Federal Circuit discussed and rejected the reasoning advanced by Patent Owner and the

Board, including the argument that Sikdar discloses using the same IP address (e.g., the public address of the firewall) for all outgoing packets:

But even if Sikdar were limited to using an unvarying public IP address (of the firewall), it still falls within the claim construction, which nowhere requires variability of the swapped-in public IP address from packet to packet.

Id. The Federal Circuit further held that Sikdar discloses address translation that occurs “when and as needed” as required by our construction of “dynamic”:

Sikdar discloses that translation (*i.e.*, the swapping of addresses) occurs when “a device 1078 operating in private network 24 . . . send[s] packet 1072 through firewall 1062 to a destination public network 12.” . . . This conversion of an address, described precisely as taking place when an outgoing packet is in transit, occurs “when and as needed”—as packets pass through the RSP and “if” the packet containing a private source IP address is destined for a public network.

Id. at 11 (first and second alterations in original).

We are constrained to follow the Federal Circuit’s determination, and we therefore find that given the Federal Circuit’s Decision, Petitioner’s arguments that Sikdar teaches or suggests “dynamically isolating” are persuasive. Therefore, for the reasons given by the Federal Circuit and Petitioner, we find that Petitioner has established that Sikdar meets the “dynamically isolating” limitation in claim 7.

2. *Hybrid Firewall Architecture*

Claim 7 is directed to the hybrid firewall embodiment of the ’272 patent. *See* PO Resp. 3–12. In this embodiment, the firewall is capable of performing both the network firewall and personal firewall security measures. *See supra*, Section I.F. Thus, claim element 7.2 recites “a

firewall in communication with the network interface, the firewall configured to handle *both network-level security and application-level security*” on incoming data packets. Ex. 1001, 25:37–39 (emphasis added).

Patent Owner contends that Sikdar (with or without Wright) fails to teach or suggest the claimed firewall architecture. PO Resp. 29–31. Because our Final Written Decision determined that Sikdar’s failure to meet the dynamically isolating claim limitation was dispositive, we did not address Patent Owner’s arguments based on the hybrid firewall features of the claim, nor were they considered in the Federal Circuit appeal.

To meet claim element 7.2 (“a firewall in communication with the network interface . . .”), Petitioner refers to Figure 20 of Sikdar and identifies firewall 1062 as the claimed firewall “in communication with the network interfaces . . . because it receives incoming packet 1061 from public network 12 via those interfaces.” Pet. 18 (internal quotation marks omitted) (citing Ex. 1004, 50).

Claim element 7.3 also is relevant to our analysis. That limitation calls for “a computer in communication with the firewall, the computer having one or more applications, each of the one or more applications associated with at least one application address, and the computer being configured to send to the firewall data packets identifying the one or more applications to the firewall.” Ex. 1001, 26:15–25. Again referring to Sikdar’s Figure 20, Petitioner identifies laptop computer 1078 as the claimed “computer in communication with the firewall” recited in this claim element. Pet. 21. Petitioner also identifies laptop 25C in Figure 1 of Sikdar as a computer in communication with a firewall as claimed. *Id.*

Petitioner contends the applications (e.g., email) on laptops 1078 and 25C meet the requirements of the claim for “one or more applications.” *Id.* at 23–24. According to Petitioner, the “application address” limitation is met by the “socket address” of each TCP/IP packet, consisting of an IP address (identifying the device) and TCP port number, which together identify the application address. Jakobsson Decl. ¶ 57; Pet. 9–10, 25. Alternatively, Petitioner contends that Wright discloses use of an “application identifier.” Pet. 27–28.

Patent Owner contends that Sikdar (alone or combined with Wright) fails to teach or suggest the computer and firewall architecture described in claim 7. PO Resp. 27–31. Patent Owner explains that “Sikdar does not disclose an architecture in which a computer sends data packets to a firewall and the firewall determines whether to allow those data packets to pass to one or more applications *on the computer*.” *Id.* at 28 (citing Medvidovic Decl. ¶ 85). Patent Owner explains that “Petitioner does not establish that Sikdar discloses that the data packets that are allegedly allowed to pass to the applications were the data packets received at the firewall *from the computer having the one or more applications*, as required by independent claim 7.” *Id.* at 28–29 (citing Medvidovic Decl. ¶ 87).

Patent Owner cites Figure 22 as an example from the '272 patent supporting its contention. *Id.* at 29. Figure 22 follows.

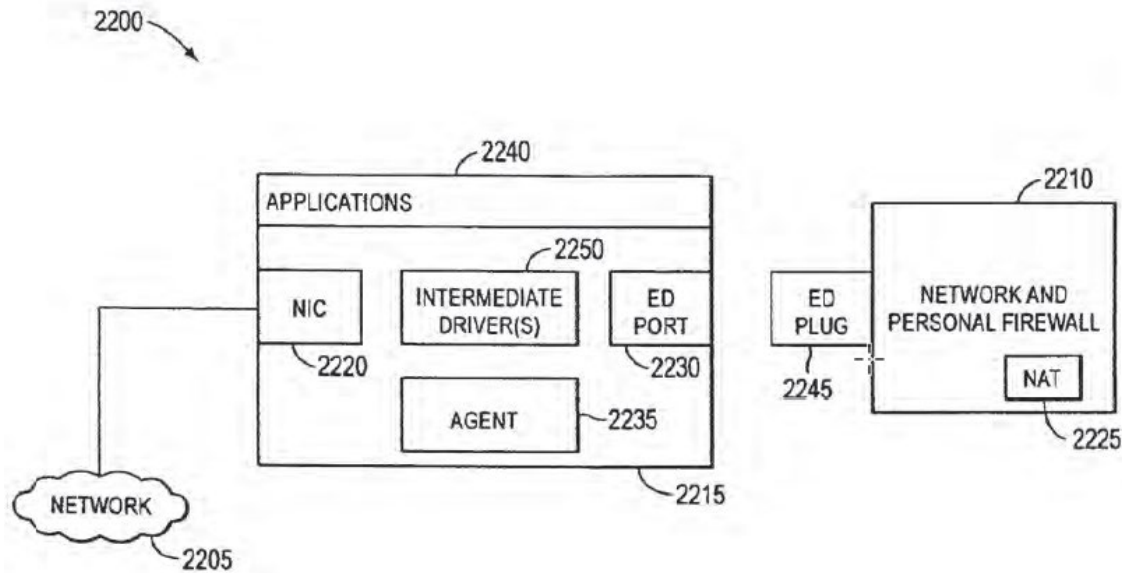


FIG. 22
(HYBRID FIREWALL EXAMPLE)

Figure 22 shows network system 2200. Network system 2200 includes external network 2205 (such as the Internet), hybrid network/personal firewall 2210, and mobile device 2215. Ex. 1001, 22:58–63. Mobile device 2215, in turn, comprises NIC 2220, ED port 2230, agent 2235, one or more applications 2240, and intermediate driver 2250. *Id.* at 23:7–10.

In operation, intermediate driver 2250 directs traffic arriving from the NIC 2220 from the network to hybrid firewall 2210 via the ED port 2230 and ED plug 2245. The hybrid firewall 2210 decides what to do with the traffic (allow, deny, or reject) and permits only the allowed traffic to proceed to applications 2240. *Id.* at 23:15–20.

As noted, claim element 7.2 recites “a firewall in communication with the network interface, the firewall configured to handle both network-level

security and application-level security.” Patent Owner identifies claim element 7.2 with network and personal firewall 2210 in Figure 22. PO Resp. 29. Claim element 7.3 recites “a computer in communication with the firewall, the computer having one or more applications, each of the one or more applications associated with at least one application address, and the computer being configured to send to the firewall data packets identifying the one or more applications to the firewall.” Patent Owner identifies the “computer” recited in claim element 7.3 with mobile device 2215 in Figure 22. *Id.*

Claim element 7.6 recites that the firewall is configured to “reject the data packets if the data packets include malicious content according to a mobile device security policy.” The antecedents for “the data packets” in claim element 7.6 are the “data packets” sent to the firewall by the computer in claim element 7.3. Thus, Patent Owner contends that in claim 7, as in Figure 22, the data packets received at the computer are sent to the firewall by the computer, and the firewall “determines whether to block those packets or allow them to proceed to an application (i.e., one of applications 2240) *on the computer.*” *Id.* at 29–30 (emphasis added).

In contrast to this description of the claimed hybrid firewall in claim 7, in Sikdar, the data packets that the firewall determines whether to block come from laptop 1056, and not from laptop 1078, identified by Petitioner as the “computer having one or more applications.” Thus, Petitioner does not establish that the data packets that are received by the firewall and allowed to pass to the applications are received *from the computer having the one or more applications*, as shown in Figure 22 and as claimed. PO Resp. 28–29.

In its Reply, Petitioner revises its analysis of how Sikdar allegedly meets this limitation. Pet. Reply 9–11. According to Petitioner’s new theory, “Petitioner’s contentions also encompass incoming packets (*i.e.*, packets going towards the laptop’s applications).” *Id.* at 10 (citing Pet. 33–35). We are not persuaded by this argument.

In the first place, this new theory is untimely. As the Federal Circuit stresses, “[i]t is of the utmost importance that petitioners in the IPR proceedings adhere to the requirement that the initial petition identify with particularity the evidence that supports the grounds for the challenge to each claim.” *Wasica Finance GmbH v. Continental Automotive Systems, Inc.*, 853 F.3d 1272, 1286–87 (Fed. Cir. 2017); *see* 35 U.S.C. § 312(a)(3) (The Petition must identify “with particularity . . . the evidence that supports the grounds for the challenge to each claim.”).

In addition, the new argument is not supported by evidence or expert testimony. The cited pages from the Petition (pages 33–35) relate to a claim element (element 7.5) not in dispute, and provide only a general description of Sikdar’s firewall. They do not describe a firewall like that in Figure 22 that screens packets received from the computer running the applications. Accordingly, for the reasons given we do not credit Petitioner’s new theory as meeting its burden on this issue.

We agree with Patent Owner’s analysis, and for the reasons given, find that these differences prevent Sikdar from meeting these limitations of claim 7, with or without Wright.¹³

¹³ Petitioner’s analysis does not rely on Wright for these features of claim 7.

3. *Conclusion – Claim 7*

Accordingly, for the reasons given, we are not persuaded that Petitioner has demonstrated that claim 7 would have been obvious over Sikdar and Wright.

B. Claim 16

Petitioner provides its element-by-element analysis of claim 16 in relation to Sikdar and the APA as two separate challenges. In the first (Ground 2), Sikdar is the primary reference. Pet. 47–52. In the second (Ground 3), APA is the primary reference. *Id.* at 64–67.

We focus on the challenge in which the APA is the primary reference (Ground 3). This is consistent with Petitioner’s presentation at the oral hearing. *See* Hearing Tr. 8:26–9:4.

We note that claim 16, unlike claim 7, is not directed to the dynamic firewall embodiment in which an “application sensitive” firewall is capable of performing both network and personal firewall security measures. *See* Ex. 1001, 22:28–31.

In the Ground 3 challenge to claim 16, with APA as the primary reference, Petitioner relies on the APA for claim elements 16.1 (“receiving the outgoing data from an application . . .”), 16.4 (“providing, using a network interface . . .”) and a portion of 16.3 (“routing, using a driver within the computer, at least a subset of the outgoing data to an external network using the public address . . .”). For claim element 16.2 (“translating, using a network address translation engine . . .”) and the “dynamically isolating” portion of claim element 16.3, Petitioner relies on Sikdar. Pet. 64–67. Here, we address only the contested limitations, which are those involving Sikdar.

For the remaining elements, we rely on and adopt the findings in our Final Written Decision. *See* FWD 45–47.

1. Dynamically Isolating

Claim 16 recites “routing, using a driver within the computer, at least a subset of the outgoing data to an external network using the public address, thereby *dynamically isolating* the internal address from the external network.” Ex. 1001, 26:44–47 (emphasis added). In both grounds, Petitioner relies on Sikdar to meet the “dynamically isolating” limitation. Pet. 48, 65. As we noted in discussing claim 7, the Federal Circuit has held that Sikdar meets the “dynamically isolating” limitation, which includes address translation by Sikdar’s RSP. Decision 10 (“Sikdar clearly discloses ‘the use of DHCP or other source of addresses in connection with a NAT engine to translate IP addresses.’”). For the reasons given previously in connection with claim 7, we find that Sikdar’s NAT engine also meets this limitation in claim 16. *See supra*, Section III.A.1.

2. Subset of outgoing data

Claim 16 recites, “routing, using a driver within the computer, at least a subset of the outgoing data to an external network using the public address.” Ex. 1001, 26:44–45. Patent Owner contends this element is not taught by the APA or Sikdar. PO Resp. 45–47, 49.

This argument is unavailing, as it is predicated on our acceptance of Patent Owner’s proposed construction of “subset” in claim 16 as a “proper subset.” *See* discussion in Section II.B.2 *supra*. As we have accepted Petitioner’s construction, in which the claimed “subset” would not exclude the entire set, and rejected Patent Owner’s proposed construction, we see no

merit in this argument. We find that this limitation is met by APA and Sikdar.

3. Motivation to Combine

Relying on testimony from Dr. Jakobsson, Petitioner argues that it would have been obvious to add the functionality of a network address translation engine, as taught by Sikdar, to the APA, represented by prior art software-based firewall in Figure 18. Pet. 55 (citing Jakobsson Decl. ¶ 165). Petitioner argues, “[m]otivation to do so arises from Sikdar, which discloses that NAT and PAT functionality can be integrated with a firewall.” *Id.* at 56. Petitioner argues further, “[a]dditional motivation arises from the ’272 patent’s Figures 17 and 20, both of which are admitted prior art and show network address translation occurring in a firewall.” *Id.* at 57.

Patent Owner contends that it “makes no sense” to incorporate Sikdar’s NAT engine in the APA. PO Resp. 48. Patent Owner asserts: “Petitioner’s argument that a [person of ordinary skill] would have modified the [APA] to include Sikdar’s alleged ‘network address translation engine’ fails for the same reason that it would not be implemented within Sikdar’s laptop 25C/1078.” *Id.* (citing Medvidovic Decl. ¶ 116). Patent Owner continues: “That is, traditional NAT/PAT devices like those disclosed in Sikdar and FIG. 17 of the ’272 Patent, operate by utilizing two NICs, one for interfacing with a public network and another for interfacing with a private network.” *Id.* Patent Owner concludes: “For at least these reasons, Petitioner’s argument that ‘a [person of ordinary skill] would have recognized that any address translation functionality implemented in hardware could readily be implemented in software’ is meritless.” *Id.* (quoting Jakobsson I Decl. ¶ 168).

In a recent decision, the Federal Circuit reminded us that “[t]he motivation-to-combine analysis is a flexible one. *Any* need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed.” *Intel Corp. v. PACT XPP Schweiz AG*, 61 F.4th 1373, 1379 (Fed. Cir. 2023) (citing *KSR Int’l Co. v. Teleflex*, 550 U.S. 398, 420 (2007) (alterations and internal quotation marks omitted)). The Federal Circuit further instructed that “a person of ordinary skill is also a person of ordinary creativity, not an automaton.” *Id.* (quoting *KSR*, 550 U.S. at 421 (alterations omitted.)).

Applying the Federal Circuit’s “flexible” standard, we find that for the reasons given that Petitioner demonstrates a motivation to combine Sikdar and the APA, as proposed by Petitioner, with a reasonable expectation of success. We disagree with Patent Owner’s arguments and find that a person of ordinary skill would have been motivated to add Sikdar’s NAT/PAT capability to the prior art network system of Figure 18, disclosing a software-based firewall. Pet. 55–58; Pet. Reply 23–25. As Petitioner points out, Sikdar’s RSP “does not include any NICs . . . , which are a separate hardware component.” Pet. Reply 24. We agree with Petitioner that Patent Owner’s argument is not convincing.

More importantly, however, Patent Owner’s argument fails because in Ground 3, Petitioner does not propose combining “any device containing two NICs with the APA.” *Id.* Petitioner proposes combining “the RSP’s NAT/PAT *functionality* with the APA.” *Id.* at 24–25 (citing Pet. 55–58) (emphasis added). “The test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the

primary reference Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art.” *In re Keller*, 642 F.2d 413, 425 (CCPA 1981); *see also In re Sneed*, 710 F.2d 1544, 1550 (Fed. Cir. 1983) (“[I]t is not necessary that the inventions of the references be physically combinable to render obvious the invention under review.”); *In re Nievelt*, 482 F.2d 965, 968 (CCPA 1973) (“Combining the *teachings* of references does not involve an ability to combine their specific structures.”).

Finally, Petitioner’s combination of the APA and Sikdar in Ground 3 also proposes making a software modification to the APA to provide NAT/PAT functionality, making it unnecessary to combine the RSP hardware with the APA. Pet. Reply 25 (citing Pet. 55–58; Jakobsson Supp. Decl. ¶ 65). We disagree with Patent Owner’s argument that a person of ordinary skill would not have been motivated to add NAT/PAT capability to the prior art network system software of Figure 18.

We are, instead, persuaded by Petitioner’s evidence of a strong motivation to modify the APA software to include NAT/PAT conversion. Jakobsson Decl. ¶¶ 164–170. We find that using NAT/PAT conversion for the purpose of protecting private IP addresses was well-known in the prior art to the ’272 patent, and in fact is described in the ’272 patent. Jakobsson Decl. ¶ 61; Ex. 1001, Fig. 17, 18:45–51. Similarly, we find the advantages of using NAT/PAT conversion to protect the identity of computers operating on a private network and reducing the number of external IP addresses required were well-known, supported by expert testimony and the RFCs. Ex. 1004, 49–50; Jakobsson Decl. ¶ 128; Exs. 1009, 1010. Also, we find the benefits of adding NAT/PAT translation to firewalls were well-known in

the prior art, and in fact acknowledged in the '272 patent. Jakobsson Decl. ¶ 126; Ex. 1001, 18:56–62; Ex. 1004, 49–50, Fig. 20.

We find, therefore, that adding Sikdar's NAT/PAT conversion to protect private IP addresses, as described in Sikdar, to the computer system software shown in Figure 18 of the '272 patent would have amounted to application of a known technique to a known system to achieve predictable results. Jakobsson Decl. ¶ 175. "[I]f 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 that person's skill." *KSR Int'l Co.*, 550 U.S. at 401.

Furthermore, we find that a person of ordinary skill would have had a reasonable expectation of success in making these modifications to the APA, as the '272 patent itself suggests by describing prior art firewalls with NAT capability. *See* Ex. 1001, Fig. 17. We credit Dr. Jakobsson's testimony on this issue. Jakobsson Decl. ¶ 168 ("Although firewall 1715 in Figure 17 is 'hardware-based,' this would not discourage a [person of ordinary skill] from implementing NAT and PAT in the [APA's] 'software-based' firewall because a [person of ordinary skill] would have recognized that any address translation functionality implemented in hardware could readily be implemented in software.").

We find further support for this conclusion in the relatively high level of skill in the relevant art, namely, "a Bachelors' degree in computer science, electrical engineering, or a comparable field of study, plus at least two years of professional experience with computer security systems and networks, or the equivalent." *See supra*, Section II.A. We find that making

this modification would have been within the skill level of such an individual. Jakobsson Supp. Decl. ¶ 65 (“My opinions in this regard do not require combining the RSP hardware into the APA (although a [person of ordinary skill] could do so) because I also propose incorporating the RSP’s NAT/PAT functionality into the APA as software.”).

4. Address Translation Engine

Patent Owner’s response contends further that the APA (whether or not combined with Sikdar) “fails to disclose ‘a network address translation engine configured to translate between the application address and a public address.’” PO Resp. 48. Patent Owner’s asserted distinction between the APA and the challenged claims is that prior art conventional firewalls, including the APA, are “completely agnostic as to the applications that are on a particular computer. They don’t care.” Hearing Tr. 43:15–17. We are not persuaded by this argument.

As Petitioner pointed out at the hearing, nothing in the language of claim 16 requires that the claimed computer be “application sensitive,” or have knowledge of the applications. Hearing Tr. 79:14–16. Contrast the lack of any recitation indicating application sensitivity in claim 16 with claim 7, directed to the “hybrid firewall” embodiment, which the ’272 patent specifically describes as “application sensitive.” Ex. 1001, 22:28–31. Thus, claim 7 includes a hybrid firewall limitation not present in claim 16, specifically, “a firewall . . . configured to handle both network-level security and application-level security.”

5. *Application Addresses*

Claim 16 of the '272 patent does recite translating “internal address[es]” associated with “application address[es].” At the hearing, Patent Owner’s counsel identified an IP address in the '272 patent as an example of an “application address”:

[THE BOARD]: . . . An “application address” would be what? What would be an example of an application address?

[COUNSEL]: Well, the patent provides an example saying that it’s an IP address of the application.

Hearing Tr. 65:15–18. As discussed *supra*, IP addresses direct packets of data to specific computers, while TCP port numbers identify specific applications. Jakobsson Decl. ¶¶ 56–57; *see also* Ex. 1019, 20:23–21:6 (Dr. Medvidovic’s testifies: “A computer is like an apartment building, so an IP address is the address for the apartment building. An application is a particular apartment in that building. So in order to actually get the data to the application it is not enough just to get to the building, you also need to know in this particular context what port it is communicating through so once you get it to the computer you can also get it to the appropriate application.”).

Thus, in the context of the '272 patent, we find that the “application address” in claim 16 refers to the IP address of the computer on which the application is running. This is illustrated in Figures 18 and 19, reproduced *supra* in Section I.F, showing applications 1835 and 1935, respectively, having the same IP address x, indicating the applications are running on a computer with IP address x. And it is consistent with counsel’s statement at the hearing, quoted *supra*, and with the description of Figure 19 in the specification, which states: “In this way, the network system 1900 is able to

isolate the IP and MAC addresses of internal *computers/applications* from the external network 1905.” Ex. 1001, 20:22–24 (emphasis added).

Expressed in terms of Dr. Medvidovic’s analogy, the applications in the ’272 patent share the same apartment building, but not the same apartment, and therefore have the same IP address.

Thus, we are unconvinced of any material difference between the address translation described in Sikdar and that recited in claim 16. In both cases, internal IP addresses are translated into an external IP address to provide address isolation. Therefore, we see no basis for distinguishing the application addresses of claim 16 from the private IP addresses translated into a public IP address in Sikdar. Nor do we find that the firewall described in Sikdar is any more or less “application sensitive” than the firewalls shown in Figures 18 or 19 of the ’272 patent and described in the specification.

In any case, Petitioner points to numerous applications disclosed in Sikdar that would have IP addresses, as well as TCP addresses or port numbers. Pet. 21–23; Jakobsson Decl. ¶¶ 88–91. These include email, AV software, Command Line Interface software, and Windows applications such as Internet Explorer. Pet. 22–23; Jakobsson Decl. ¶¶ 89–90. Petitioner contends each of these applications would “necessarily and inherently” have had associated application addresses or otherwise incoming packets would have no way of reaching them. Pet. 25 (citing Jakobsson Decl. ¶ 95). For this additional reason, we find that the APA-Sikdar combination discloses the claimed translation of application addresses.

6. Objective Indicia of Non-obviousness

Patent Owner asserts that the patentability of the challenged claims is supported by “objective indicia” (also called “secondary considerations”) of

non-obviousness, including long-felt need, failure of others, and skepticism by experts in the industry. PO Resp. 50–52. *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). Before reaching a decision on obviousness of claim 16, we must weigh these secondary considerations. *In re Cyclobenzaprine Hydrochloride Extended-Release Capsule Patent Litig.*, 676 F.3d 1063, 1075–76 (Fed. Cir. 2012). “The patentee bears the burden of showing that a nexus exists.” *WMS Gaming Inc. v. Int’l Game Tech.*, 184 F.3d 1339, 1359 (Fed. Cir. 1999). To determine whether the patentee has met that burden, we consider the correspondence between the objective evidence and the claim scope. *Fox Factory, Inc. v. SRAM, LLC*, 944 F.3d 1366, 1373 (Fed. Cir. 2019) (citation omitted).

We concluded, in our Final Written Decision, that Patent Owner had failed to meet its burden. FWD 47–50. We agreed with Petitioner that Patent Owner had failed to establish the required nexus to its claims. *Id.* at 49. We agreed also that Patent Owner had not provided convincing evidence supporting the existence of such objective indicia. *Id.*

We find that, for the reasons given in our Final Written Decision, which we adopt for this Final Written Decision on Remand, Patent Owner’s evidence of secondary factors is insubstantial and unconvincing, and we therefore give it minimal weight in considering the obviousness of the challenged claims.

7. Conclusion – Claim 16

In sum, for the reasons given, we find that the combination of APA and Sikdar as described in Ground 3 of the Petition teaches or suggests each element of claim 16, and that a person of ordinary skill would have been motivated to combine the relevant teachings of those references with a

reasonable expectation of success. We therefore determine Petitioner has demonstrated that claim 16 would have been obvious and is unpatentable.

Because Ground 3 is dispositive of the obviousness challenges to this claim, we do not address further the challenge in which Sikdar is the primary reference (“Ground 2”).

IV. CONCLUSION

Based on the arguments and evidence presented during trial, Petitioner has not demonstrated by a preponderance of the evidence that claim 7 of the ’272 patent is unpatentable under 35 U.S.C. §103. Petitioner has demonstrated by a preponderance of the evidence that claim 16 is unpatentable under § 103.

A summary of our conclusions is set forth in the table reproduced below.

Claim(s)	35 U.S.C. §	Reference(s)	Claim(s) Shown Unpatentable	Claim(s) Not Shown Unpatentable
7	103	Sikdar, Wright		7
16	103	Sikdar, APA		
16	103	APA, Sikdar	16	
Overall Outcome			16	7

V. ORDER

Upon consideration of the record before us, it is:

ORDERED that claim 7 of the ’272 patent *is not* determined to be *unpatentable*;

FURTHER ORDERED that claim 16 of the '272 patent *is* determined to be *unpatentable*; and

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

IPR2019-00561
Patent 8,365,272 B2

For PETITIONER:

Robert Buergi
James Heintz
DLA PIPER LLP
robert.buergi@dlapiper.com
jim.heintz@dlapiper.com

For PATENT OWNER:

James Hannah
Jeffrey Price
Michael Lee
KRAMER LEVIN NAFTALIS & FRANKEL LLP
jhannah@kramerlevin.com
jprice@kramerlevin.com
mhlee@kramerlevin.com