

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

UNIFIED PATENTS, LLC,
Petitioner,

v.

FIRENET TECHNOLOGIES, LLC,
Patent Owner.

IPR2020-00471
Patent 8,892,600 B2

Before KIMBERLY McGRAW, DANIEL J. GALLIGAN, and
MICHAEL T. CYGAN, *Administrative Patent Judges*.

GALLIGAN, *Administrative Patent Judge*.

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

I. INTRODUCTION

In this *inter partes* review, Unified Patents, LLC (“Petitioner”) challenges the patentability of claims 1–17 and 19–23 of U.S. Patent No. 8,892,600 B2 (“the ’600 patent,” Ex. 1001), which is assigned to Firenet Technologies, LLC (“Patent Owner”).

We have jurisdiction under 35 U.S.C. § 6. For the reasons discussed below, we determine that Petitioner has proven by a preponderance of the evidence that claims 1–17 and 19–23 of the ’600 patent are unpatentable. *See* 35 U.S.C. § 316(e) (“In an *inter partes* review instituted under this chapter, the petitioner shall have the burden of proving a proposition of unpatentability by a preponderance of the evidence.”).

A. Procedural History

On March 13, 2020, Petitioner requested *inter partes* review of claims 1–17 and 19–23 of the ’600 patent on the following grounds:

Claims Challenged	35 U.S.C. §	References/Basis
1–14, 16, 17, 19–22	103(a) ¹	Coley, ² Coss ³
15, 23	103(a)	Coley, Coss, Shand ⁴
1–14, 16, 17, 19–22	103(a)	Coss, Gelb ⁵
15, 23	103(a)	Coss, Gelb, Shand

Paper 1 (“Pet.”), 7. Patent Owner did not file a preliminary response. We instituted trial on all grounds of unpatentability. Paper 7, 12.

¹ The Leahy-Smith America Invents Act (“AIA”) included revisions to 35 U.S.C. § 103 that became effective after the filing of the application for the ’600 patent. Therefore, we apply the pre-AIA version of this section.

² Coley, US 5,826,014, filed Feb. 6, 1996, issued Oct. 20, 1998 (Ex. 1007).

³ Coss, US 6,098,172, filed Sept. 12, 1997, issued Aug. 1, 2000 (Ex. 1009).

⁴ Shand, US 6,147,976, filed June 24, 1996, issued Nov. 14, 2000 (Ex. 1010).

⁵ Gelb, US 5,550,984, issued Aug. 27, 1996 (Ex. 1008).

During the trial, Patent Owner did not file a response. During a call with the Board, the parties agreed that briefing in the matter was closed, and the parties stated that they would not seek oral argument. Paper 9.

Although Patent Owner did not file a response, the burden remains on Petitioner to prove unpatentability of the challenged claims. 35 U.S.C. § 316(e); *see also Dynamic Drinkware LLC, v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015).

B. Related Matters

As required by 37 C.F.R. § 42.8(b)(2), the parties identify various related matters. Pet. 5–6; Paper 4, 1.

C. Real Parties in Interest

The parties identify themselves as the real parties in interest. Pet. 5; Paper 4, 1.

D. The '600 Patent and Illustrative Claim

The '600 patent “relates to a management system for providing access to and security for data on network attached devices.” Ex. 1001, 1:21–23.

Claim 1 is illustrative and is reproduced below.

1. A system comprising:
 - a first computing device coupled to an internal network;
 - and
 - a second computing device in communication with the first computing device, wherein the second computing device has at least one attached device and the second computing device is isolated from the internal network;
 - wherein the first computing device comprises a memory having stored thereon instructions that, in response to execution on the first computing device, cause the first computing device to at least:

receive data packets over the internal network, wherein at least some of the data packets are sent to the internal network from an external network;

examine the data packets to determine whether the data packets contain an IP address associated with the at least one attached device;

filter data packets containing a valid IP address in a header of the data packet to determine whether to authorize data packets requesting access to the at least one attached device;

reformulate the data packets for communication to the second computing device; and

transmit the reformulated packets to the second computing device in response to determining that the request for access is authorized.

Ex. 1001, 9:56–10:15.

II. ANALYSIS

A. Level of Ordinary Skill in the Art

Petitioner asserts that a person of ordinary skill in the art “would have had at least a bachelor’s degree in Electrical Engineering, Computer Science, or an equivalent field, and at least two years of work experience involving networking, network security, and/or firewalls. More education can supplement practical experience and vice versa.” Pet. 9 (citing Ex. 1003 (Declaration of Tal Lavian, Ph.D.)) ¶¶ 18–19).

With the exception of the open-ended language “at least,” we adopt this formulation because it is consistent with the types of problems and solutions described in the ’600 patent and the cited prior art.

B. Claim Interpretation

We interpret claim terms 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) (2019).

For purposes of assessing patentability in this proceeding, we need not construe expressly any claim terms. *See, e.g., 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))).

C. Principles of Law

A patent claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of 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) any secondary considerations, if in evidence.⁶ *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

D. Obviousness over Coley and Coss (Claims 1–14, 16, 17, 19–22)

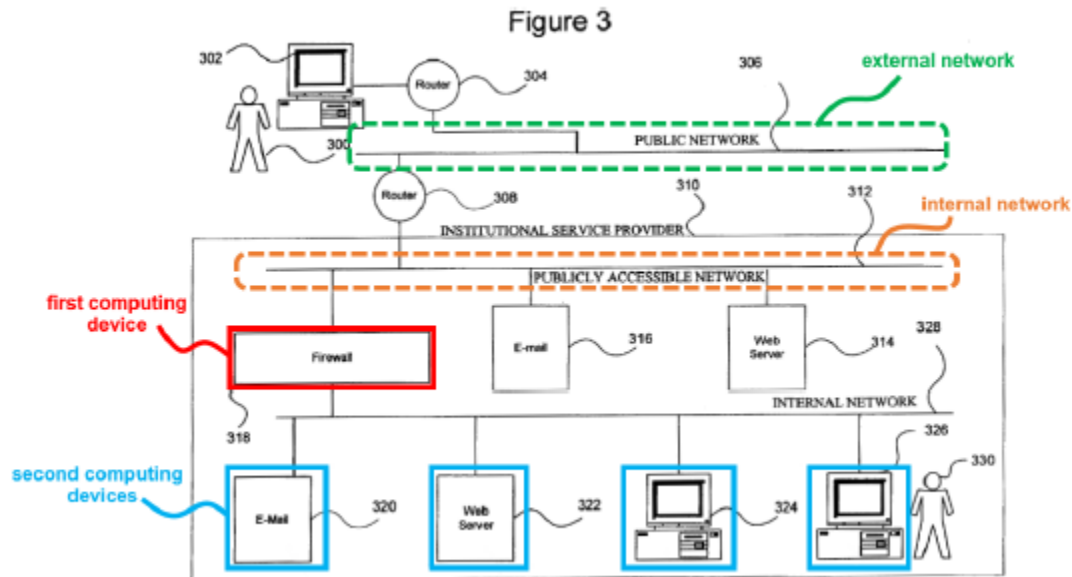
Petitioner asserts claims 1–14, 16, 17, and 19–22 of the ’600 patent are unpatentable under 35 U.S.C. § 103(a) as obvious over Coley and Coss. Pet. 14–54. Because the pertinent details of Coley and Coss are discussed in

⁶ As noted above, Patent Owner did not file a response and, therefore, did not present objective evidence of nonobviousness (i.e., secondary considerations).

the analysis of claim 1, we do not provide a separate overview of these references.

1. Independent Claim 1

In its contentions for claim 1, Petitioner presents the following annotated version of Coley's Figure 3:



Pet. 14. Coley's Figure 3 illustrates a computer network arrangement with a firewall. Ex. 1007, 6:58–59. In the annotated version of Coley's Figure 3, reproduced above, Petitioner maps certain depicted items to particular elements recited in claim 1 as follows: firewall 318 to “first computing device” (illustrated in red); publicly accessible network 312 to “internal network” (illustrated in orange); items 320, 322, 324, and 326 to “second computing device[s]” (illustrated in blue); and public network 306 to “external network” (illustrated in green). Pet. 14.

Petitioner argues that firewall 18 teaches a “first computing device” as recited in claim 1 because Coley discloses “a firewall box comprising a stand alone computing platform.” Pet. 17 (quoting Ex. 1007, claim 1); *see*

Ex. 1007, 5:54–58 (“A firewall arrangement in accordance with the invention operates on a computing platform that is dedicated to the operation of the firewall. Such a dedicated firewall computing platform is referred to herein as a ‘firewall box.’”). Petitioner argues that publicly accessible network 312, to which firewall 318 is connected, teaches an “internal network.” Pet. 17 (citing Ex. 1007, 8:29–32). Coley describes network 312 as an “internal, publicly accessible, network.” Ex. 1007, 8:29–32. Based on Petitioner’s persuasive contentions and evidence, summarized above, we find that Coley teaches “a first computing device coupled to an internal network.”

Petitioner argues that each of network elements 320 (e-mail system), 322 (Web server), and 324 and 326 (internal computers) teaches “a second computing device” that is “in communication with the first computing device,” that “has at least one attached device,” and that “is isolated from the internal network,” as recited in claim 1. Pet. 18–22 (citing Ex. 1007, 2:57–3:4, 8:43–54, Fig. 3; Ex. 1003 ¶¶ 54–55). As shown in Coley’s Figure 3, each of network elements 320, 322, 324, and 326 is connected through internal network 328 to firewall 318. *See* Ex. 1007, Fig. 3. Coley states that “firewall 318 . . . physically separates the publicly accessible network 312 from the internal network 328” such that “all communications attempting to access the internal network 328, or any network elements attached thereto, must pass through the firewall 318.” Ex. 1007, 8:8:45–52.

Petitioner argues that each of network elements 320, 322, 324, and 326 has attached devices. Pet. 19. Petitioner asserts that servers 320 and 322, for example, have hard drives that are “attached device[s],” as claimed. Pet. 19 (citing Ex. 1003 ¶¶ 54–55; Ex. 1001, 1:18–39, 4:3–8); *see*

Ex. 1001, 1:28–34 (disclosing that “[a] network attached device (NAD) may be any type of hardware unit that is connected to a computer network,” including “hard disk drives” and “printers”).

Based on Petitioner’s persuasive contentions and evidence, summarized above, we find that Coley teaches “a second computing device in communication with the first computing device, wherein the second computing device has at least one attached device and the second computing device is isolated from the internal network.”

Claim 1 further recites “wherein the first computing device comprises a memory having stored thereon instructions that, in response to execution on the first computing device, cause the first computing device to at least” perform five operations recited in claim 1. Petitioner argues that Coley discloses that firewall 318 has memory that executes instructions. Pet. 22 (citing Ex. 1007, 7:27–30, 13:46–57); *see* Ex. 1007, 7:27–30 (“The processes, programs and applications running on the firewall computing platform are those involved with firewall processes, or their support (i.e., the computer’s operating system).”). Based on Petitioner’s persuasive contentions and evidence, we find that Coley teaches that “the first computing device comprises a memory having stored thereon instructions that, in response to execution on the first computing device, cause the first computing device to” perform certain operations, for which Petitioner relies on the teachings of Coley or the combination of Coley and Coss, as we discuss below. *See* Pet. 22–35.

Claim 1’s first recited operation for the first computing device is to “receive data packets over the internal network, wherein at least some of the data packets are sent to the internal network from an external network.”

Petitioner argues that Coley discloses that firewall 318 receives packets from network 306 (“external network”) through network 312 (“internal network”). Pet. 22–23 (citing Ex. 1007, 8:17–26, 8:43–54, 10:63–12:24, Fig. 3). We are persuaded by this contention because Coley discloses that “firewall 318 permits the internal network 328,” to which the “second computing device[s]” (network elements 320, 322, 324, and 326) are connected, “to be attached to the public network 306 (through the publicly accessible network 312) without rendering the secure network 328 open to public access.” Ex. 1007, 8:43–46. Coley further explains that “all communications attempting to access the internal network 328, or any network elements attached thereto, must pass through the firewall 318” (Ex. 1007, 8:49–52), and, therefore, packets from network 306 that are destined for network elements 320, 322, 324, and 326 go through network 312 to firewall 318. Thus, based on Petitioner’s persuasive contentions and evidence, we find that Coley teaches claim 1’s first recited operation of receiving data packets.

Claim 1’s second recited operation for the first computing device is to “examine the data packets to determine whether the data packets contain an IP address associated with the at least one attached device.” Petitioner asserts that Coley’s firewall verifies that incoming Transmission Control Protocol/Internet Protocol (“TCP/IP”) packets seeking access to network elements attached to network 328 have permission to go to those devices. Pet. 23–24 (citing Ex. 1007, 1:21–36, 3:23–41, 6:4–11, 6:32–40, 7:47–57, 10:63–11:6; Ex. 1003 ¶¶ 56–58). Petitioner asserts that a person of ordinary skill in the art would have understood that TCP/IP packets include an Internet Protocol (“IP”) address of the destination network element. Pet. 24 (citing Ex. 1003 ¶¶ 56–58). Coley discloses that a firewall has “a variety of

access request validation programs referred to herein as ‘proxy agents,’” which “investigate incoming requests that seek to access network elements residing behind the firewall.” Ex. 1007, 7:35–39. Petitioner also argues that “the network elements to which the packets are sent in Coley include servers that provide access to attached devices (e.g., a hard drive or a printer),” thereby teaching “an IP address associated with the at least one attached device.” Pet. 24–25 (citing Ex. 1007, 7:24–63, 8:27–54, 10:63–12:24; Ex. 1003 ¶ 58). Based on Petitioner’s persuasive contentions and evidence, summarized above, we find that Coley teaches the second recited operation in claim 1.

In the alternative, Petitioner argues that Coss’s disclosure of inspecting and filtering packets at a firewall based on certain rules, which can be based on destination addresses, discloses examining data packets as the second recited operation in claim 1 requires. Pet. 24 (citing Ex. 1009, 1:12–24, 1:67–2:4, 5:41–7:52, Figs. 6, 8; Ex. 1003 ¶¶ 129–133). For example, Coss discloses that, “[a]t the firewall, packets are inspected and filtered, i.e., passed on or dropped depending on whether they conform to a set of predefined access rules,” and Coss discloses that “[t]he particular rule set that is applied for any packet can be determined based on information such as the incoming and outgoing network interfaces as well as the network source and destination addresses.” Ex. 1009, 1:20–24, 1:67–2:4.

Petitioner provides several articulated rationales for “incorporat[ing] Coss’s technique of examining a packet’s IP address into Coley’s network security system and proxy agents,” including that doing so “would have addressed and improved Coley’s goal of ‘protecting network elements connected to a public network’” and would have been combining prior art

elements in known ways to yield predictable results. Pet. 25–27 (citing Ex. 1003 ¶¶ 59–61).

As discussed above, we find that Coley alone teaches the second recited operation of examining packets. We also are persuaded by Petitioner’s contentions as to how the combination of Coley and Coss teaches this subject matter and by Petitioner’s rationale to combine the references. *See* Ex. 1003 ¶¶ 59–61.

Claim 1’s third recited operation for the first computing device is to “filter data packets containing a valid IP address in a header of the data packet to determine whether to authorize data packets requesting access to the at least one attached device.” Petitioner argues that Coley’s firewall permits packets that have a valid IP address to pass. Pet. 28 (citing Ex. 1007, 1:48–62, 3:5–10, 6:33–39, 8:27–41, 10:44–55, 10:63–12:24; Ex. 1003 ¶¶ 38, 39, 50, 54–58, 78). Petitioner explains that “a user may generate an access request for access to files stored on *an attached device* (e.g., a hard drive) that is connected to Web server 322 (*second computing device*),” in which case the firewall would determine whether to allow the packet based on whether it has a valid IP address. Pet. 28 (citing Ex. 1007, 1:48–62, 8:27–41, 10:63–12:24; Ex. 1003 ¶¶ 38, 39, 50, 54–58, 78).

We are persuaded by Petitioner’s contentions as to the third recited operation of filtering. In particular, Coley discloses that, when a user at computer 302 attempts to access web server 322, “the access request message is presented to the firewall 318,” on which a proxy agent is running that “analyze[s] a source address to determine whether the host computer 302 from which the message originated is authorized to access the secure Web server 322.” Ex. 1007, 10:63–11:25. Coley explains that “if the

source address is not authorized . . . , the access request is denied.”

Ex. 1007, 11:30–32. Otherwise, additional checks can be made before authorizing the connection. Ex. 1007, 11:41–12:9.

Claim 1’s fourth and fifth recited operations for the first computing device are to “reformulate the data packets for communication to the second computing device” and to “transmit the reformulated packets to the second computing device in response to determining that the request for access is authorized.” Petitioner argues that Coley’s disclosure of the firewall initiating a connection to the destination device after verification “to maintain anonymity on each side of the firewall” (Ex. 1007, 10:35–41) teaches this subject matter. Pet. 29–30 (citing Ex. 1007, 6:41–50, 10:36–43, 10:63–12:24; Ex. 1003 ¶¶ 62–67), 35. According to Petitioner, a person of ordinary skill in the art “would have understood this as generating new packets based on the incoming packets because this is how a new connection is created between the firewall and the server when the firewall acts as an intermediary.” Pet. 30 (citing Ex. 1003 ¶¶ 62–67). We are persuaded by Petitioner’s contentions for the fourth and fifth recited operations of reformulating and transmitting, and in particular, we credit Dr. Lavian’s testimony explaining how Coley’s disclosure of maintaining anonymity would have been understood by a person of ordinary skill in the art to teach reformulating the packets because, without some reformulation, such as an address translation, the device behind the firewall could determine the source address of the access request by examining the packets. *See* Ex. 1003 ¶¶ 62–67; Pet. 30.

Alternatively, Petitioner asserts that the subject matter recited in the fourth and fifth recited operations of reformulating and transmitting would

have been obvious based on the combined teachings of Coley and Coss. Pet. 31–35. Although we need not rely on Coss’s disclosure because we find that Coley alone teaches this subject matter, we have reviewed Petitioner’s contentions and evidence, and we are persuaded that this subject matter also would have been obvious based on the combined teachings of Coley and Coss. *See* Ex. 1003 ¶¶ 68–76.

Based on Petitioner’s persuasive contentions and evidence, discussed above, we find that Coley alone and together with Coss teaches the subject matter recited in claim 1, and we find that a person of ordinary skill in the art would have been motivated to combine the teachings of Coley and Coss as asserted with a reasonable expectation of success. We determine, therefore, that Petitioner has proven by a preponderance of the evidence that claim 1 is unpatentable under 35 U.S.C. § 103(a) as obvious over Coley and Coss.

2. Dependent Claims 2–7

Claim 2 recites the following:

The system of claim 1 wherein the instructions that, in response to execution on the first computing device, cause the first computing device to reformulate the data packets comprise instructions that, in response to execution on the first computing device, cause the first computing device to generate new packets based on information contained in the data packets received over the internal network.

Referring to its contentions for the fourth recited operation of reformulating in claim 1, Petitioner persuasively argues that “Coley’s proxy agents initiate a connection ‘on behalf’ of the access request and initiating such a connection would have involved, or at least would have been obvious to involve, generating new packets.” Pet. 36; *see also* Pet. 36 (citing

Ex. 1003 ¶¶ 80–84) (additionally arguing that the subject matter of claim 2 would have been obvious over the combined teachings of Coley and Coss).

Claim 3 recites, “The system of claim 1, further comprising a firewall coupled between the internal network and the external network, and wherein the firewall is configured to filter data packets transmitted over the external network and addressed to the internal network.”

Petitioner contends that router 308, which connects public network 306 (the recited “external network”) to network 312 (the recited “internal network”), teaches a firewall, as recited in claim 3, because Coley discloses that it can perform packet filtering, which is a firewall technique. Pet. 37–39 (Ex. 1007, 3:5–10, 8:17–26, 10:43–47, 10:63–11:7; Ex. 1003 ¶¶ 85–88). We are persuaded because Coley discloses that “[o]ne technique used by firewalls to protect network elements is known as ‘packet filtering,’” and Coley further discloses that router 308 can perform packet filtering. Ex. 1007, 3:5–6, 10:47–48. Petitioner also argues that the combination of Coley and Coss teaches the subject matter recited in claim 3. Pet. 38–41. Although we need not rely on this alternative argument because we are persuaded that Coley alone teaches this subject matter, we have reviewed Petitioner’s contentions based on the combination of Coley and Coss and find them persuasive.

Claim 4 recites, “The system of claim 1 wherein the second computing device further comprises operating system instructions that, in response to execution on the second computing device, cause the second computing device to process the reformulated data packets for communication with the at least one attached device over a communications interface.”

Petitioner persuasively explains how Coley's Web server 322 and e-mail system 320 ("second computing device[s]") receive requests for content and communicate those requests to attached devices such as hard drives over a physical port using a communication standard ("communication interface"), thereby teaching the subject matter of claim 4. Pet. 42–43 (citing Ex. 1007, 1:48–62, 8:27–54, 10:63–12:24; Ex. 1003 ¶¶ 94–101).

Claim 5 recites the following:

The system of claim 1 wherein the instructions that, in response to execution on the first computing device, cause the first computing device to filter data packets comprise instructions that, in response to execution on the first computing device, cause the first computing device to determine whether the data packets contain authorized port information.

Petitioner argues that Coley discloses that proxy agents are assigned to individual ports and that a proxy agent verifies access requests based on, for example, whether access is allowed on its port based on particular criteria, such as time of day, source and destination address, and user identity, thereby teaching the subject matter of claim 5. Pet. 44 (citing Ex. 1007, 6:4–20, 8:6–9, 8:62–9:46, 9:47–60, 9:61–10:10; Ex. 1003 ¶¶ 102–103). We are persuaded because Coley discloses that "individual proxy agents are assigned to designated ports to monitor, respond to and verify incoming access requests (i.e., incoming packets) received on the port" and that "[a]ccess request verification can include analysis of source host machine and source user information; destination host machine and destination user information; and/or time of day analysis." Ex. 1007, 6:5–8, 8:5–9.

Petitioner also argues that the combination of Coley and Coss teaches the subject matter recited in claim 5. Pet. 44–45. Although we need not rely on this alternative argument because we are persuaded that Coley alone teaches this subject matter, we have reviewed Petitioner’s contentions based on the combination of Coley and Coss and find them persuasive.

Claim 6 recites the following:

The system of claim 1 wherein the instructions that, in response to execution on the first computing device, cause the first computing device to filter data packets comprise instructions that, in response to execution on the first computing device, cause the first computing device to determine whether the data packets contain authorized source network card information.

Petitioner argues that “Coss discloses packet filtering rules based on incoming and outgoing network interfaces,” which may be a network interface card, and that the “rules need to be met in order for a packet not to be dropped thereby teaching determining *authorized source network card information*.” Pet. 45–46 (citing Ex. 1009, 1:67–2:4, 4:40–5:40, 6:58–61). Petitioner argues that, in the combination with Coss, “Coley’s proxy agents would determine if the requests for access are authorized using the rules of Coss.” Pet. 46. We are persuaded by these contentions because Coss discloses that “[t]he particular rule set that is applied for any packet can be determined based on information such as the incoming and outgoing network interfaces as well as the network source and destination addresses” and that “[t]he incoming or outgoing network interface may be in the form of a network interface card.” Ex. 1009, 1:67–2:4, 6:58–61.

Claim 7 recites, “The system of claim 1 wherein the instructions that, in response to execution on the first computing device, cause the first

computing device to filter data packets comprise application layer instructions.” Petitioner argues that Coley discloses application layer instructions such as prompting a user to enter a password to determine whether packets should not be filtered. Pet. 46–47 (citing Ex. 1008, 9:49–60, 10:11–27; Ex. 1003 ¶¶ 104–106); *see* Ex. 1008, 9:49–51 (disclosing the proxy agent prompting the user to enter a user name and password). We are persuaded by this contention, and in particular, we credit Dr. Lavian’s testimony that a person of ordinary skill in the art would have understood that prompting a user to enter a password occurs at the application layer. Ex. 1003 ¶ 104.

Based on Petitioner’s persuasive arguments and evidence, discussed above, we determine that Petitioner has proven by a preponderance of the evidence that claims 2–7 are unpatentable under 35 U.S.C. § 103(a) as obvious over Coley and Coss.

3. Claims 8–14, 16, 17, 19–22

Independent claim 8 is directed to a “computer-implemented method,” and it recites subject matter similar to that recited in claim 1. Petitioner shows how the limitations of claim 8 correspond to the limitations of claim 1 and argues that claim 8 is unpatentable for the same reasons. *See* Pet. 47–48. For claims 9 and 11, Petitioner refers to its contentions for claim 4, which recites similar subject matter. Pet. 49, 50.

Claim 10 recites:

The method of claim 8, further comprising:
filtering, by a firewall device coupled between the internal network and the external network, packets received by the firewall device over the external network; and

transmitting, by the firewall device, the filtered data packets from the external network that are addressed to the internal network.

For the filtering step of claim 10, Petitioner refers to its contentions for claim 3. Pet. 49. For the transmitting step, Petitioner argues that the packets allowed after filtering would be transmitted. Pet. 49–50 (citing Ex. 1007, 8:17–42, 10:44–11:7; Ex. 1003 ¶¶ 83–88).

For claims 12, 13, and 14, Petitioner refers to its contentions for claims 5, 6, and 7, respectively, which recite similar subject matter. Pet. 51.

Independent claim 16 is directed to “[a] non-transitory computer-readable storage medium comprising computer instructions that, in response to execution by a first computing device, cause the first computing device to” perform operations similar to those recited in claim 1 with slight differences. For example, while claim 1 recites “reformulate the data packets for communication to the second computing device,” claim 16 recites “generate new data packets, based at least in part on information contained within the data packets.” For this limitation of claim 16, Petitioner refers to its contentions for claim 2, which also recites generating new packets. Pet. 53. Moreover, for claim 16’s recitation that “the attached device is coupled to the second computing device by way of a communications interface,” Petitioner refers to its claim 9 contentions. Pet. 53. For the remaining limitations of claim 16, Petitioner refers its contentions for similar subject matter recited in claims 1 and 8. Pet. 51–52.

For claim 17, Petitioner refers to its contentions for claim 9, which recites similar subject matter, as well as claim 2, which recites “new” packets. Pet. 53. For claims 19, 20, 21, and 22, Petitioner refers to its

contentions for claims 4, 5, 6, and 7, respectively, which recite similar subject matter. Pet. 53.

We are persuaded by Petitioner’s showing that the subject matter recited in claims 8–14, 16, 17, and 19–22 would have been obvious for reasons discussed with respect to claims 1–7. Having considered the full record, we determine that Petitioner has proven by a preponderance of the evidence that claims 8–14, 16, 17, and 19–22 are unpatentable under 35 U.S.C. § 103(a) as obvious over Coley and Coss.

*E. Obviousness over Coley, Coss, and Shand
(Claims 15, 23)*

Petitioner also argues that claims 15 and 23 are unpatentable as obvious over Coley, Coss, and Shand. Pet. 54–59. Claim 15 recites, “The method of claim 8, further comprising: logging, by the first computing device, information regarding data packets that are rejected.” Claim 23 similarly recites, “The computer-readable storage medium of claim 16, further comprising computer instructions that, in response to execution by the first computing device, cause the first computing device to log information regarding data packets that are rejected.”

Petitioner first argues that Coley’s disclosure of a transaction log teaches or renders obvious the additional limitations of claims 15 and 23. Pet. 56 (citing Ex. 1007, 7:47–57, 11:21–32, 13:21–33). Coley discloses that “[a]n additional security feature that can be provided in the firewall system is a transaction log,” which “gathers information associated with any access request message seeking to connect to or inquire about network elements residing behind the firewall.” Ex. 1007, 13:21–25. Thus, because Coley discloses that its transaction log “gathers information associated with

any access request” (Ex. 1007, 13:22–25), which includes when “the access request is denied” (Ex. 1007, 11:30–32), we find that Coley’s disclosure of a transaction log teaches “logging, by the first computing device, information regarding data packets that are rejected,” as recited in claim 15, and similarly teaches the subject matter recited in claim 23.

Petitioner also contends that, “[t]o the extent Coley does not disclose this limitation, Shand discloses it or at least renders it obvious.” Pet. 56. Petitioner relies on Shand’s disclosure of logging when packets are rejected. Pet. 56 (citing Ex. 1010, 17:48–65, 18:32–35). Shand discloses that, “[w]hen an event such as the filtering or dropping of a received packet . . . occurs, the occurrence of the event is recorded by the Packet Filtering Code in a log file.” Ex. 1010, 17:48–54. Shand discloses two-bit codes that are used to log an event, including “01” for “reject and log.” Ex. 1010, 17:58–65.

Petitioner argues that a person of ordinary skill in the art “would have been motivated to modify Coley’s firewall device in view of Shand because the addition of Shand’s logging would further Coley’s objective of network security and preventing unauthorized communications, by allowing Coley’s system to specifically identify unauthorized data packets that were rejected.” Pet. 57. Petitioner also asserts that, “at the time of the earliest priority date of the ’600 patent, the concept and advantages of logging rejected packets in a packet filtering scheme were exceedingly well known and widely used.” Pet. 57 (citing Ex. 1014, 154; Ex. 1003 ¶¶ 107–109). Petitioner further argues that a person of ordinary skill in the art “would have had a reasonable expectation of success in combining Coley and Shand because Shand’s conventional technique of logging rejected packets could be applied in the

same way in Coley’s firewall to accomplish the same results.” Pet. 58; *see also* Pet. 58–59 (citing Ex. 1007, 7:47–57, 13:21–33; Ex. 1010, 17:48–65, 18:32–35; Ex. 1003 ¶ 110).

We are persuaded by Petitioner’s contentions and evidence, summarized above, and we find that Coley alone and together with Coss and Shand teaches the subject matter recited in claims 15 and 23 and that a person of ordinary skill in the art would have been motivated to combine the teachings of Coley, Coss, and Shand with a reasonable expectation of success. Thus, Petitioner has proven by a preponderance of the evidence that claims 15 and 23 are unpatentable under 35 U.S.C. § 103(a) as obvious over Coley, Coss, and Shand.

F. Remaining Obviousness Contentions

In view of our determination that claims 1–17 and 19–23 are unpatentable as discussed above, we need not address Petitioner’s additional arguments of unpatentability based on the combination of Coss and Gelb and the combination of Coss, Gelb, and Shand. 35 U.S.C. § 318(a) (“If an inter partes review is instituted and not dismissed under this chapter, the Patent Trial and Appeal Board shall issue a final written decision with respect to the patentability of any patent claim challenged by the petitioner and any new claim added under section 316(d).”).

III. CONCLUSION

For the reasons discussed above, we determine Petitioner has proven, by a preponderance of the evidence, that the challenged claims of the '600 patent are unpatentable, as summarized in the following table:

Claims	35 U.S.C. §	References/Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1–14, 16, 17, 19–22	103(a)	Coley, Coss	1–14, 16, 17, 19–22	
15, 23	103(a)	Coley, Coss, Shand	15, 23	
1–14, 16, 17, 19–22	103(a)	Coss, Gelb ⁷		
15, 23	103(a)	Coss, Gelb, Shand		
Overall Outcome			1–17, 19–23	

IV. ORDER

Accordingly, it is:

ORDERED that claims 1–17 and 19–23 of the '600 patent have been shown to be unpatentable; and

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

⁷ As explained above, because we determine that the challenged claims are unpatentable on other grounds, we decline to address this ground and the ground based on Coss, Gelb, and Shand.

IPR2020-00471
Patent 8,892,600 B2

PETITIONER:

David Seastrunk
Roshan Mansinghani
UNIFIED PATENT, LLC
david@unifiedpatents.com
roshan@unifiedpatents.com

PATENT OWNER:

Gregory Carlin
Lawrence Aaronson
MEUNIER CARLIN & CURFMAN LLC
gcarlin@mcciplaw.com
laaronson@mcciplaw.com