

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

TREND MICRO INC.,
Petitioner,

v.

CUPP COMPUTING AS,
Patent Owner.

IPR2021-00813
Patent 10,621,344 B2

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

GIANNETTI, *Administrative Patent Judge*.

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

I. INTRODUCTION

A. Background

Trend Micro Inc. (“Petitioner”) filed a Petition requesting *inter partes* review of claims 1–20 (the “challenged claims”) of U.S. Patent No. 10,621,344 B2 (Ex. 1001, the “’344 patent”). Paper 1 (“Pet.”). CUPP Computing AS (“Patent Owner”) filed a Preliminary Response. Paper 6. 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 (“Institution Dec.”).

Following institution, Patent Owner filed a Response. Paper 12 (“PO Resp.”). Subsequently, Petitioner filed a Reply to Patent Owner’s Response (Paper 15, “Pet. Reply”), and Patent Owner filed a Sur-reply (Paper 16, “PO Sur-reply”).

On July 27, 2022, we held an oral hearing. A transcript of the hearing is included in the record. Paper 25 (“Hearing Tr.”).

We have jurisdiction under 35 U.S.C. § 6. This decision is a Final Written Decision, issued pursuant to 35 U.S.C. § 318(a). For the reasons we discuss below, we determine that Petitioner has proven by a preponderance of the evidence that all challenged claims of the ’344 patent are unpatentable.

B. Related Proceedings

The parties identify the following district court proceeding concerning the ’344 patent: *CUPP Cybersecurity LLC v. Trend Micro, Inc., et al.*, No. 3:20-cv-03206 (N.D. Tex.). Pet. 1; Paper 4.

A related patent, U.S. Patent No. 9,781,164 (the “’164 patent”),¹ was before the Board in IPR2019-00368 (the “’368 IPR”). A Final Written Decision in the ’368 IPR, finding all challenged claims of the ’164 patent unpatentable, was entered on May 28, 2020. Ex. 1005. Patent Owner’s request for rehearing by the Director of the USPTO was denied. ’368 IPR, Paper 30. The decision denying rehearing and the Board’s Final Written Decision were appealed to the Federal Circuit. ’368 IPR, Paper 31. On October 6, 2022, the Federal Circuit affirmed the Board’s Final Written Decision in the ’368 IPR. Ex. 3001.

C. Real Party-in-Interest

The Petition identifies Trend Micro as the real party-in-interest. Pet. 1. Patent Owner identifies CUPP Computing AS the real party-in-interest. Paper 4, 1.

D. The ’344 Patent

The ’344 patent describes a system and method for providing network security to mobile devices. Ex. 1001, 1:43–45. According to the patent, mobile devices are more vulnerable to attacks by malicious code when traveling outside an enterprise network. *Id.* at 2:6–10. The patent thus describes “a small piece of hardware [a ‘mobile security system’] that connects to a mobile device and filters out attacks and malicious code.” *Id.* at 2:56–60. The patent explains that “[u]sing the mobile security system, a mobile device can be protected by greater security and possibly by the same level of security offered by its associated corporation/enterprise.” *Id.* at 2:60–63.

¹ The ’344 patent is a continuation (through a chain of continuations) of the ’164 patent, and shares a common specification with the ’164 patent.

This system is illustrated in Figure 3 of the '344 patent, which follows:

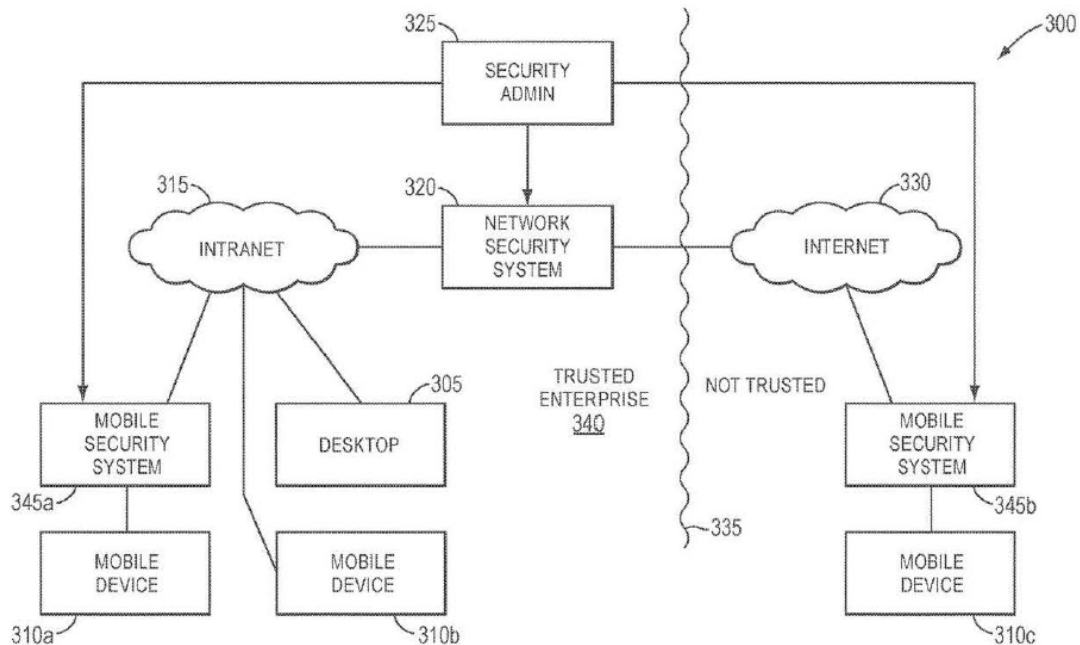


FIG. 3

Figure 3 of the '344 patent is a block diagram of a network system.

Ex. 1001, 4:12–13. Network system 300 includes desktop 305, first mobile device 310a, and second mobile device 310b. *Id.* at 4:57–60. First mobile device 310a is within trusted enterprise network 340 and is coupled to the enterprise’s intranet 315 via mobile security system 345a. *Id.* at 4:60–63.

Figure 3 further shows mobile device 310c that has travelled outside trusted enterprise network 340 and is coupled to untrusted internet 330 via mobile security system 345b. *Id.* at 5:27–30. This mobile device may be in use by an employee of trusted enterprise network 340 who is currently on travel.

Id. at 5:10–11. Security administrator 325 manages mobile security systems 345a and 345b and network security system 320 to assure that they include the most current security protection. *Id.* at 5:11–15.

The mobile security system includes “security engines,” “security policies,” and “security data.” *Id.* at Fig. 5, 7:33–40. The administrator can update the security policies, data, and engines implemented on the mobile security system. *Id.* at 5:46–50, 11:20–25. Security administrator 325 can centrally manage all enterprise devices, remotely or directly. *Id.* at 5:50–51. Further, security administrator 325 and mobile security systems 345 can interact to automatically translate enterprise security policies into mobile security policies and configure mobile security systems 345. *Id.* at 5:52–55.

E. Illustrative Claims

The ’344 patent has twenty claims, all of which are challenged in the Petition. Claims 1, 10, 19, and 20 are independent. Claims 1 and 19 are representative of the claims. Claim 1 recites²:

1. A security system, comprising:

[1.1] security system memory; and

[1.2] a security system processor configured to:

[1.3] store in the security system memory at least a portion of security code, at least a portion of a security policy, and at least a portion of security data,

[1.4] the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data configured to provide security services to a mobile device coupled to the security system, the mobile device having at least one mobile device processor different than the security system processor of the security system,

[1.5.] the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data being managed by one or more information

² Paragraph numbering provided by Petitioner has been added.

technology (IT) administrators using an IT administrator system on a trusted enterprise network, the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data being configured based on one or more policies implemented by the one or more IT administrators on the trusted enterprise network, the mobile device being a first computer system, the security system being a second computer system, and the IT administrator system being a third computer system, the first computer system, the second computer system and the third computer system being separate computer systems;

[1.6] store in the security system memory at least a portion of remote management code configured to process an update command, the update command being an instruction to update at least one of the security code, the security policy, or the security data based on one or more revised policies implemented by the one or more IT administrators on the trusted enterprise network;

[1.7] receive a particular update command to update a particular one of the security code, the security policy, or the security data, the particular update command having originated from the IT administrator system and having been forwarded to the security system; and

[1.8] execute the update command using the remote management code to update the particular one of the security code, the security policy, or the security data.

Ex. 1001, 15:20–67.

Claim 19 recites:

19. A security system, comprising:

[19.1] security system memory; and

[19.2] a security system processor configured to:

[19.3] store in the security system memory at least a portion of security code, at least a portion of a security policy, and at least a portion of security data,

[19.4] the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data configured to be processed by the security system processor to implement security services for a mobile device coupled to the security system, the mobile device having at least one mobile device processor different than the security system processor of the security system,

[19.5] the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data being managed by one or more information technology (IT) administrators using an IT administrator system on a trusted enterprise network, the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data being configured based on one or more policies implemented by the one or more IT administrators on the trusted enterprise network, the mobile device being a first computer system, the security system being a second computer system, and the IT administrator system being a third computer system, the first computer system, the second computer system and the third computer system being separate computer systems;

[19.6] store in the security system memory at least a portion of remote management code configured to process an update command, the update command being an instruction to update at least one of the security code, the security policy, or the security data based on one or more revised policies implemented by the one or more IT administrators on the trusted enterprise network;

[19.7] receive a particular update command to update a particular one of the security code, the security policy, or the security data, the particular update command having originated from the IT administrator system and having been forwarded to the security system; and

[19.8] execute the update command using the remote management code to update the particular one of the security code, the security policy, or the security data.

Ex. 1001, 17:41–18:24.

Claims 10 and 20 are directed to computer-readable storage devices and are similar to claims 1 and 19, respectively.

F. References and Other Evidence

Petitioner relies on the following reference: U.S. Patent App. Pub. No. 2005/0260996 (Ex. 1003, “Groenendaal”).

Petitioner relies also on a Declaration of Dr. Markus Jakobsson (Ex. 1019, “Jakobsson Decl.”). Patent Owner relies on a Declaration of Michael T. Goodrich, Ph.D. (Ex. 2002, “Goodrich Decl.”). The parties have submitted deposition transcripts for those witnesses. Ex. 1020 (“Goodrich Dep.”); Ex. 2004 (“Jakobsson Dep.”). In addition, the parties have submitted several expert declarations and deposition transcripts from the ’368 IPR.³

G. Asserted Ground of Unpatentability

Petitioner asserts the challenged claims are unpatentable on the following ground (Pet. 3):

Claims Challenged	Basis (35 U.S.C.)⁴	Reference
1–20	§ 103(a)	Groenendaal

³ Patent Owner has submitted Dr. Jakobsson’s initial and supplemental declarations and deposition transcript from the ’368 IPR. Exs. 2003, 2005, 2006. In addition, the parties have submitted a declaration (Ex. 2007) and deposition transcript (Ex. 1011) of Nenad Medvidovic, Ph.D., from the ’368 IPR. Dr. Medvidovic testified for Patent Owner in the ’368 IPR.

⁴ Because the earliest application from which the ’344 patent issued was filed before March 16, 2013, the pre-AIA (“America Invents Act”) version of §103 applies. Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 285–88 (2011).

II. PRELIMINARY MATTERS

A. Level of Ordinary Skill

Petitioner contends “[a] person of ordinary skill in the art at the time of the alleged invention of the ’344 patent (i.e., December 13, 2005) . . . 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, or the equivalent.” Pet. 6 (citing Jakobsson Decl. ¶¶ 52–53).

Patent Owner does not provide a formulation of the person of ordinary skill. Dr. Goodrich, however, provides the following testimony: “In my opinion, a person of ordinary skill in the art in the field of the ’344 Patent as of its priority date would be someone with a bachelor’s degree in computer science or related field, and either (1) two or more years of industry experience and/or (2) an advanced degree in computer science or related field.” Goodrich Decl. ¶ 31. The two formulations differ only slightly. For example, Dr. Jakobsson is more specific in requiring “professional experience with computer security systems, or the equivalent.” Jakobsson Decl. ¶ 52.

Petitioner’s definition is supported by credible expert testimony and is more consistent with the prior art and the patent specification before us. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001) (prior art itself may reflect an appropriate level of skill). We, therefore, adopt Petitioner’s description, but without the qualifier “at least.”⁵ However, we would reach

⁵ Including “at least” suggests a broader and open-ended level of ordinary skill than that expressly stated by Petitioner. This change, however, does not affect the outcome of our analysis.

the same result under either the formulation proposed by Petitioner or that suggested by Dr. Goodrich.

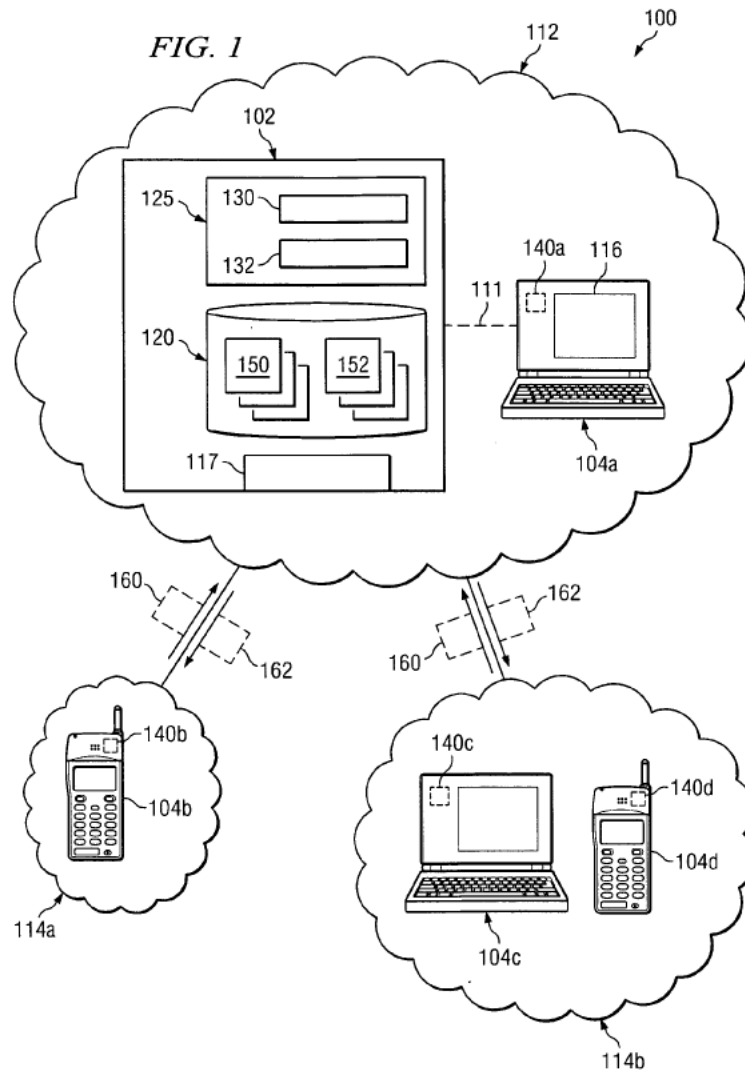
B. Description of the Groenendaal Reference

Groenendaal describes a wireless agent for a mobile device.

Ex. 1003, (57). In one embodiment, the wireless agent is operable to dynamically determine an access point for wireless communications from a mobile device through a network. *Id.* The wireless agent is further operable to automatically select one of a plurality of security profiles associated with a mobile device based, at least in part, on the determined access point. *Id.*

Each security profile includes a plurality of security parameters for accessing a wireless network. The wireless agent then modifies at least one of a plurality of network configuration options of the mobile device based on the selected security profile, and automatically attempts to connect the mobile device to the access point using the network configuration options. *Id.*

Petitioner relies on Figure 1 of Groenendaal, which follows:



Pet. 17. Figure 1 of Groenendaal shows security management system 100 including server 102 and enterprise network 112. Ex. 1003 ¶ 16. The server includes security manager 130 and configuration manager 132. *Id.* ¶ 20. The server also includes memory 120 that stores security profiles 150 and configuration profiles 152. *Id.* ¶ 17.

The security system provides security services to mobile clients 104 (e.g., 104b, 104c, and 104d). *Id.* ¶ 14. For example, an administrator manages and updates the security profiles and configuration profiles using

GUI (graphical user interface) 116 on laptop 104a. *Id.* ¶¶ 27, 28. The configurable and updatable security policies relate to firewall settings, intrusion detection, file sharing, network authentication, and allowed and disallowed network access points, among other security services. *Id.* ¶¶ 57–60, Figs. 4–6.

C. Claim Construction

In an *inter partes* review, the claims of a patent shall be construed using the same claim construction standard that would be used to construe the claims in a civil action under 35 U.S.C. § 282(b), including construing the claims in accordance with the ordinary and customary meaning of such claims as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent. 37 C.F.R. § 42.100(b); *see also Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–14 (Fed. Cir. 2005). Under that standard, and absent any special definitions, we give claim terms their ordinary and customary meaning, as would be understood by one of ordinary skill in the art at the time of the invention. *See In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007).

Any special definitions for claim terms must be set forth with reasonable clarity, deliberateness, and precision. *See In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994). “In determining the meaning of the disputed claim limitation, we look principally to the intrinsic evidence of record, examining the claim language itself, the written description, and the prosecution history, if in evidence.” *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 469 F.3d 1005, 1014 (Fed. Cir. 2006) (citing *Phillips*, 415 F.3d at 1312–17). Extrinsic evidence is “less significant than the

intrinsic record in determining the legally operative meaning of claim language.” *Phillips*, 415 F.3d at 1317 (internal quotes and citation omitted).

We construe claim terms only as relevant to the parties’ contentions and only to the extent necessary to resolve the issues in dispute. *See Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999); *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017).

Both Petitioner and Patent Owner address claim construction and ask us to construe terms in the challenged claims. Pet. 6–15; PO Resp. 12–16.

1. “provide security services to a mobile device” (Claims 1, 10)

Independent claims 1 and 10 call for “a portion of the security data configured to provide security services to a mobile device coupled to the security system.” In our ’368 IPR Institution Decision, we determined that this phrase should be construed to encompass the distribution of security information to a mobile device, without more. Ex. 1004, 8–9.⁶ In our Final Written Decision in the ’368 IPR, after reviewing the evidence presented during the trial, we maintained that construction. Ex. 1005, 11–12.

Petitioner asks us to adopt the same construction in this proceeding. Pet. 6. Petitioner points out that “[p]roviding updated security information to the mobile device is a security service because doing so can, for example, protect the mobile device against newly identified threats, or configure it for securely connecting to new networks.” *Id.* (citing Jakobsson Decl. ¶ 57; Ex. 1001, 2:34–37). Petitioner relies also on dictionary definitions from *Merriam-Webster’s Collegiate Dictionary* (11th ed., 2007), defining

⁶ Unless otherwise specified, citations to exhibits use the page numbers assigned by the parties and not the original page numbers.

“service” as including “the occupation or function of serving,” “the work performed by one that serves,” and “HELP, USE, BENEFIT” (Ex. 1008, 3); *The Microsoft Internet & Networking Dictionary* (2003), defining “service” as including “a program or routine that provides support to other programs” (Ex. 1009, 3); and *Webster’s Collegiate Dictionary* (2002), defining “service” as “[t]he act or occupation of serving,” which would include serving information (Ex. 1010, 3). Pet. 7.

The term “security services” does not appear in the written description of the ’344 patent. However, in the Figure 3 embodiment, described *supra*, the mobile security device is described as effectively “a mobile internet gateway on behalf of the mobile device 310c.” Ex. 1001, 5:32–34. Furthermore, the specification of the ’344 patent describes how the security administrator manages the mobile device by providing updates to the mobile security system. *See, e.g.*, the following description of the Figure 3 embodiment from the ’344 patent:

In this embodiment, because the security administrator 325 is capable of remotely communicating with the mobile security system 345b, *IT can monitor and/or update the security policies/data/engines implemented on the mobile security system 345b*. The security administrator 325 can centrally manage all enterprise devices, remotely or directly. *Further, the security administrator 325 and mobile security systems 345 can interact to automatically translate enterprise security policies into mobile security policies and configure mobile security systems 345 accordingly*. Because the mobile security system 345 may be generated from the relevant security policies of the enterprise 340, the mobile device 310c currently traveling may have the same level of protection as the devices 305/310 within the trusted enterprise 340.

Ex. 1001, 5:46–60 (emphasis added). In this example from the specification, the security administrator provides security services to a mobile device by

monitoring and updating the security policies implemented on the mobile security system and by interacting with the mobile security system to automatically translate enterprise security policies into mobile security policies and configuring mobile security systems accordingly. The '344 patent explains also that the security administrator and the security system “can interact to automatically translate enterprise security policies into mobile security policies and configure mobile security systems . . . accordingly.” *Id.* at 5:52–55. Therefore, we agree with Petitioner and find that the proper construction of “provide security services to a mobile device” in claims 1 and 10 includes sending security information to the mobile device, as it is consistent with the description in the specification of the security administrator managing the security of the mobile devices.

Patent Owner does not address directly this proposed construction. *See generally* PO Resp. 12–26. However, in discussing *Groenendaal*, Patent Owner implicitly challenges this construction by making the argument that “*Groenendaal* teaches the well-known prior art technique of transferring security policies to a mobile device without any separate security system processing security information and implementing security services on its behalf.” *Id.* at 12; *see also id.* at 28 (“*Groenendaal* is directed to pushing security profiles from a server to a mobile device, where the mobile device itself implements any attendant security services.”).

We disagree with this argument by Patent Owner implicitly limiting the scope of “provid[ing] security services,” and, for the reasons given by Petitioner, we find that “[p]roviding updated security information to the mobile device is a security service because doing so can, for example, protect the mobile device against newly identified threats, or configure it for

securely connecting to new networks.” Pet. 6 (citing Jakobsson Decl. ¶ 57; Ex. 1001, 2:34–37).

2. “*implement security services for a mobile device*” (claims 19 and 20)

Consistent with its position on the “security services” recitation in claims 1 and 10, Petitioner contends the plain meaning of this limitation appearing in independent claims 19 and 20 “includes sending security information to a mobile device.” Pet. 8. Petitioner supports this construction with testimony from Dr. Jakobsson (Jakobsson Decl. ¶¶ 62–64) and a dictionary definition of “implement” as “CARRY OUT, ACCOMPLISH.” Pet. 8 (quoting Ex. 1012, 3). Based on this definition of “implement” from *Merriam-Webster’s Collegiate Dictionary*, (11th ed.), Petitioner contends “carrying out or accomplishing the act of providing security information to a mobile device is implementing that security service.” *Id.*

Patent Owner addresses this limitation in connection with its alternative construction of the “configured to be processed” limitation, discussed *infra* in Section II.C.4. For the reasons given by Petitioner and in our discussion, *infra*, of “configured to be processed,” we find that the proper construction for “implement security services for a mobile device” is “carrying out or accomplishing an action, such as providing security information to a mobile device.” Pet. 8; Jakobsson Decl. ¶¶ 62–64.

Patent Owner contends that the term “implement” means “put into effect.” PO Resp. 20. Despite Patent Owner’s treatment of this claim construction issue as dispositive, however, we agree with Petitioner that Groenendaal discloses this limitation even under Patent Owner’s construction, by providing (i.e., “putting into effect”) security services

beyond providing security profiles to the mobile device. *See* Pet. 24–27; Pet. Reply 17–21. This is further discussed *infra*, in Section III.B.5.

3. “*configured based on one or more policies implemented by the one or more IT administrators*” (claims 1, 10, 19, 20)

These independent claims recite “one or more policies implemented by the one or more IT administrators on the trusted enterprise network.” *See, e.g.*, claim elements 1.5, 19.5, *supra*. Petitioner contends that the “one or more policies” recited in these claims differ from the separately-recited stored “security policy” in claim limitations 1.3 and 19.3. Pet. 8–11. Petitioner contends that “the plain and ordinary meaning of ‘one or more policies’ does not require these policies be stored in computer memory.” *Id.* at 8–9. Petitioner explains that “the ‘one or more policies’ can include decisions made by the recited ‘one or more IT administrators.’” *Id.* at 9. Petitioner provides the following example: “[A] company may have a policy that employees may not access social media, which is different than the stored implementation in the form of a list of prohibited URLs.” *Id.* As Petitioner points out, this construction is consistent with our findings in the ’368 IPR. *Id.* at 9 (citing Ex. 1005, 32).

Patent Owner contends that the term “configured based on one or more policies implemented by the one or more IT administrators on the trusted enterprise network” should be accorded its “plain and ordinary meaning.” PO Resp. 20. Patent Owner asserts that the “one or more policies” do not encompass policies in the mind of the IT administrator. *Id.* at 21. As discussed *supra*, according to Patent Owner, the term “implemented” means “put into effect.” *Id.* at 20. Thus, Patent Owner asserts the claimed “security policy, security code, and security data” must

be “configured based on one or more policies *put into effect* by one or more IT administrators operating on the trusted enterprise network.” *Id.* (emphasis added). According to Patent Owner, this would exclude “the mental decisions of an IT administrator.” *Id.* at 21–25.

We do not agree with this limiting construction by Patent Owner. As we concluded in the ’368 IPR Final Written Decision, we find that the claims do not require that the security data be based on policies “put into effect.” Ex. 1005, 14–15. As we observed in the ’368 IPR, the claims require that the policies be “implemented.” *Id.* at 14. We construe this *supra* as “carrying out or accomplishing an action.” The claims themselves identify separately (1) the security code, security policy, and security data “being managed” by the IT administrators, and (2) the “policies implemented” by the IP administrators. *Compare* Ex. 1001, 15:33–38 with 15:41–43. The ’344 patent specification, likewise, distinguishes between the security code, security policy, and security data and the policies implemented by the administrators. Thus, the specification describes an embodiment where the security code, security policy, and security data are “based on” IT decisions or user preferences:

In an embodiment where the mobile security system 345 supports multiple mobile devices 310, the security engines 530, security policies 535 and security data 540 may be different for each mobile device 310 (*e.g., based on for example user preferences or IT decision*).

Ex. 1001, 10:41–45 (emphasis added).

For the reasons given by Petitioner and those summarized above, we adopt a construction of this limitation that includes “one or more policies” that are not necessarily “in computer memory.” Pet. 8–10. We find, as Petitioner contends, that “[t]he configuration of this limitation need be based

only on the policies; it does not also need to be based on the implementation of those policies.” *Id.* at 12.

We rely on the “plain meaning” of the claim language. As Petitioner explains, “in the claim language ‘configured based on one or more policies implemented by the one or more IT administrators,’ the clause ‘implemented by the one or more IT administrators’ simply indicates which policies may serve as the basis for the configuration.” *Id.* at 13.

We rely also on the ’344 patent specification, specifically, the above embodiment where the configuration of the security code, security policy, and security data are “based on” an IT decision. *Id.* at 13–14 (citing Ex. 1001, 10:41–47, 14:65). We reject Patent Owner’s belated attempt at the hearing to marginalize this disclosure as an “unclaimed embodiment.” Hearing Tr. 30:12–13. We have seen nothing in the intrinsic record that would support a disavowal of this embodiment by Patent Owner. “To disavow claim scope, the specification must contain ‘expressions of manifest exclusion or restriction, representing a clear disavowal of claim scope.’” *Retractable Techs., Inc. v. Becton, Dickinson & Co.*, 653 F.3d 1296, 1306 (Fed. Cir. 2011) (quoting *Epistar Corp. v. Int’l Trade Comm’n*, 566 F.3d 1321, 1335 (Fed. Cir. 2009)).

For the reasons given, we find that this limitation includes configurations that are not necessarily based on the implementations of policies, but are based on IT administrator decisions. Pet. 11–12. This is consistent with our findings in the ’368 IPR Final Written Decision. *See* Ex. 1005, 15.

As we also observed in that Final Written Decision, and for reasons discussed *infra*, this construction issue is not dispositive, as the Groenendaal

reference discloses this limitation, even under Patent Owner’s contentions regarding this limitation. *See* discussion *infra*, in Section III.B.6.

4. “*the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data configured to be processed by the security system processor to implement security services for a mobile device coupled to the security system*” (Claims 19 and 20)

Patent Owner proposes that the phrase “processed by the security system processor to implement security services for a mobile device,” from claim limitation 19.4 (but not present in claim element 1.4), be “accorded its plain and ordinary meaning.” PO Resp. 13. Drawing a distinction to claim element 1.4, Patent Owner continues, “[t]he plain language of claims 19 and 20 expressly requires security services be ‘implement[ed] . . . for’ a mobile device, rather than merely ‘provide security services to a mobile device’.” *Id.* at 14 (emphasis omitted; alterations in original).

Patent Owner argues that the Board should reject Petitioner’s construction of “implement security services for a mobile device” in claim 19 because it is “unsupported by the intrinsic record.” *Id.* at 16–18. Patent Owner repeats its argument that “[c]ontrary to Petitioner’s proposal, the plain and ordinary meaning of the term ‘configured to be processed by the security system processor to implement security services for a mobile device coupled to the security system’ does not encompass the mere distribution or sending of security information to a mobile device, without more.” *Id.* at 16.

Petitioner contends that the language added to claim 19, like claim limitation 1.4, “includes providing security services to a mobile device.” Pet. 26. But Petitioner contends that even under Patent Owner’s

construction, Groenendaal provides “additional security services” that involve processing by the server to implement security services for mobile devices. *Id.*; Pet. Reply 17–21. Petitioner argues that “[t]hese security services satisfy this limitation even under Patent Owner’s interpretation of this limitation because they go beyond merely providing security information to a mobile device.” Pet. Reply 17–18. One example is the description of Groenendaal’s server configuring a firewall policy for a given user on a wireless gateway when the user enters a particular access-zone. *Id.* at 19 (citing Ex. 1003 ¶ 14). Petitioner explains that in this example, “[t]he server’s doing so implements a security service because it accomplishes a security-related task that is helpful to the mobile device.” *Id.*

Patent Owner responds to this argument by imposing an additional, restriction on the term “implement.” PO Sur-reply 17–20. Patent Owner asserts, specifically referring to the firewall policy, that “this profile information is enforced onto an agent or by configuring another infrastructure entity, e.g., access point or gateway, to enforce security policies.” *Id.* at 20. Thus, Patent Owner argues,” [i]n Groenendaal, the server is never implementing security services for any other device. At best, it tells other devices what to do and the device does it itself.” Hearing Tr. 32:11–13.

We reject this implicit restriction, which would amount to a rewriting of the claim. Patent Owner’s restriction would require the security system processor *alone* to provide services to the mobile device, without the involvement of “another infrastructure entity” such as a gateway. *Id.*; *see also id.* at 34:18–19 (characterizing Groenendaal’s server 102 as “merely a conduit”), 56:10–56:24. Nothing in the claim requires the security system

processor *by itself* to “implement” security policies, without sending security information to an “infrastructure entity” such as a gateway to provide a service (such as a firewall) to the mobile device. Excluding such a firewall arrangement is inconsistent with Patent Owner’s description of the ’344 patent as providing “an additional line of defense for the mobile device.”

PO Resp. 8.

Furthermore, as will be discussed in greater detail in connection with our analysis of Groenendaal, *infra*, the processing of security information by a security system and implementing security services by providing security information to a mobile device (or to an entity such as a gateway for the benefit of the mobile device), are not mutually exclusive activities, as implied by Patent Owner’s proposed construction. Dr. Jakobsson testifies that Groenendaal discloses several examples of implementing security services for a mobile device that also involve the security server processing security information:

Groenendaal also discloses implementing security services for a mobile device beyond providing security information to the mobile device, as established for limitation 1.4 Each of these services is implemented by the security server processor by processing the stored security code, security policies, and security data, as established for limitation 1.4.

Jakobsson Decl. ¶ 105. Thus, while we agree with Petitioner’s construction, we also agree that Groenendaal meets this limitation under Patent Owner’s construction. *See infra*, Section III.B.5.

We have considered Patent Owner’s additional arguments and find them unavailing. For example, Patent Owner contrasts the recitation in claim 19 of “configured to be processed to implement security services for

the mobile device” with the recitation in claim 1 of “configured to provide security services to a mobile device.” PO Resp. 5–8. Based on this difference, Patent Owner asserts “the ’344 Patent’s additional claim limitation expressly requires security services be implemented for a mobile device, rather than merely “providing security services to a mobile device.” *Id.* at 8 (emphasis omitted). At the oral argument, Petitioner’s counsel acknowledged this difference in claim scope, but argued that “both limitations read on Groenendaal.” Hearing Tr. 45:16–21. We agree that Groenendaal meets both constructions, as is discussed *infra* in Section III.B.5.

For the reasons given, therefore, we do not adopt Patent Owner’s construction, including the proposed restriction of the term “configured to be processed by the security system processor to implement security services for a mobile device” as requiring the processor *alone* to provide the security services, without the involvement of other entities.

5. *Additional Terms*

To the extent necessary, we address the parties’ contentions regarding the term “configured to mirror,” found in claims 8 and 17, in Section III.D, *infra*. No other constructions are necessary to resolve the issues in dispute. *Vivid Techs., Inc.*, 200 F.3d at 803.

III. ANALYSIS OF THE CHALLENGED CLAIMS

The Petition challenges claims 1–20 of the ’344 patent. Petitioner asserts unpatentability of the claims based on obviousness. Pet. 3.

A. *Obviousness*

A 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 skill in the art; and (4) so-called “secondary considerations,” including commercial success, long-felt but unsolved needs, failure of others, and unexpected results. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966) (“the *Graham* factors”). Neither the Petition nor the Patent Owner has presented evidence on the fourth *Graham* factor. We therefore do not consider that factor in this decision.

Petitioner contends claims 1–20 would have been “obvious . . . in light of Groenendaal.” Pet. 15. As mentioned above, claims 1, 10, and 19, and 20 are independent. Petitioner combines its analysis of claim 1 with claim 19. We therefore address claim 1 and 19 together. *Id.* at 18–47.

B. Claims 1 and 19

Petitioner’s “limitation-by-limitation analysis” of claims 1 and 19 in relation to Groenendaal appears at pages 18–47 of the Petition. Petitioner supports its analysis with testimony from its expert, Dr. Jakobsson. Jakobsson Decl. ¶¶ 87–149. For the reasons that follow, we find that each limitation of claims 1 and 19 is disclosed or suggested by Groenendaal.

1. Preambles

The preambles of claims 1 and 19 each recite a “security system.” Petitioner contends this element is found in Groenendaal’s server 102. Pet. 18 (citing Ex. 1003, Fig. 1, ¶¶ 16, 20). Patent Owner does not challenge

this assertion. We find, based on the evidence presented by Petitioner, that Groenendaal teaches the preambles of claims 1 and 19.⁷

2. Elements 1.1, 19.1

Claim 1 and 19 both call for a “security system memory.” *See* claim elements 1.1, 19.1, *supra*. Petitioner contends that this element is met by memory 120 in server 102 of Groenendaal. Pet. 18 (citing Ex. 1003, Fig. 1, ¶¶ 16–17). Patent Owner does not challenge this assertion. We find, based on the evidence presented by Petitioner, that Groenendaal teaches claim elements 1.1 and 19.1.

3. Elements 1.2, 1.3, 19.2, 19.3

Claims 1 and 19 both call for “a security system processor configured to: store in the security system memory at least a portion of security code, at least a portion of a security policy, and at least a portion of security data.” *See* claim elements 1.2, 19.2, *supra*. Petitioner contends the “security system” limitation is met by Groenendaal’s server 102 and the “processor” limitation by processor 125 included in the server. Pet. 18 (citing Ex. 1003 ¶¶ 16, 20, Fig. 1). Petitioner explains that “because processor 125 executes the wireless manager, it is configured to perform the server functionality that satisfies the remaining limitations of this claim, described below” (referring to claim elements 1.3–1.8, *supra*, and citing Jakobsson Decl. ¶ 89).

Patent Owner does not challenge Petitioner’s identification of the processor in Groenendaal with the claimed security system processor. We find, based on the evidence presented by Petitioner, that Groenendaal teaches the security system processor of claim elements 1.2 and 19.2.

⁷ We do not express an opinion on whether these preambles are limiting.

Petitioner contends that the “store” limitation of claim elements 1.3 and 19.3 (“store in the security system memory . . .”) is met by Groenendaal’s disclosure of memory 120 storing security profiles 150 and configuration profiles 152. Pet. 19 (citing Ex. 1003 ¶¶ 21, 23). Petitioner explains that “[s]ecurity profile 150 includes any parameters, variables, policies, algorithms, instructions, or rules for securing clients 104, and configuration profile 152 includes any parameters, variables, policies, algorithms, instructions, settings, or rules, including security settings, for wirelessly connecting clients 104.” *Id.* (citing Ex. 1003 ¶¶ 18–19) (internal quotation marks omitted). Also, “[a]n administrator may create and update these stored profiles, including their security code, security policies, and security data, using the graphical user interface (‘GUI’) shown in Figs. 7A–E, 8A–K, 9A–B.” *Id.* (citing Ex. 1003 ¶¶ 20, 28, 58–60).

Patent Owner does not challenge the assertion that Groenendaal stores policies, although Patent Owner disputes Petitioner’s identification of the stored policies. *See* discussion of “one or more policies” in Section II.C.3, *supra*.

Petitioner contends that the stored policies in claim elements 1.3/19.3 are not the same as the “one or more policies” recited in claim elements 1.5/19.5. Pet. 8. Petitioner contends that the “one or more policies” in 1.5/19.5 do not have to be stored in computer memory. *Id.* at 8–9; Pet. Reply 6. For the reasons given by Petitioner, we agree. Pet. 18–22; Pet. Reply 8–11. As discussed in Section II.B.3, *supra*, and in our Final Written Decision in the ’368 IPR, “[c]onsistent with this claim language, we find that there is a distinction between policies implemented by the IP administrators and the ‘security code, security policy, and security data’

described in the claim as ‘stored in the memory of the computer system.’” Ex. 1005, 33. We further find, based on our construction of “one or more policies” and the above reasons presented by Petitioner, that Groenendaal teaches claim elements claims 1.3 and 19.3. Jakobsson Decl. ¶¶ 90–96.

4. Element 1.4

Claim 1 further calls for “the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data configured to provide security services to a mobile device coupled to the security system, the mobile device having at least one mobile device processor different than the security system processor of the security system.” See claim element 1.4, *supra*. Petitioner contends the “different processors” limitation (“the mobile device having at least one mobile device processor different than the security system processor of the security system”) is met by Groenendaal: “Mobile devices 104 have ‘one or more processors’ different than the processor of server 102 (security system). [Ex. 1003] ¶¶ 27, 20, Fig. 1 (showing mobile devices 104 as separate from the server 102).” Pet. 22. The contention that the “different processors” limitation is met by Groenendaal is not disputed by Patent Owner. We find that Groenendaal meets this limitation for the reasons given by Petitioner. Jakobsson Decl. ¶ 97.

Petitioner further explains that Groenendaal meets the “configured to provide” limitation: “Groenendaal also discloses that the security code, security policy, and security data described above are configured to provide security services to mobile clients 104.” Pet. 22. Petitioner gives examples, such as Groenendaal’s description of security profiles 150 as including “any parameters, variables, policies, algorithms, instructions, or rules for securing

clients 104,’ (a security service).” *Id.* (citing Ex. 1003 ¶ 18); *see also id.* at 22–24 (further examples include an administrator “dynamically manag[ing] network security features of clients 104,” “server 102’s ‘wireless manager,’” and “distributed” security profiles 150). We find that Patent Owner’s response, that Groenendaal does not provide security services because it is directed to “pushing security profiles from a server to a mobile device,” is unavailing because it is contrary to our claim construction. *See supra*, Section II.C.1. Accordingly, we find that under our claim construction Petitioner demonstrates that Groenendaal meets this limitation. Jakobsson Decl. ¶¶ 98–100.

Anticipating Patent Owner’s argument that sending security information to a mobile device is not providing security services (*see supra*, Section II.C.1), Petitioner demonstrates also that Groenendaal also discloses that the stored security code, policy, and data provide security services to the mobile devices *other* than by sending security profiles 150. Pet. 24–26; Pet. Reply 17–22. For example, Petitioner demonstrates that Groenendaal discloses that security manager 130 may command client 104 “to perform an action such as shut down wireless access, block port, disable Internet sharing, and lose other privileges.” Pet. 24 (citing Ex. 1003 ¶ 21). Petitioner’s expert, Dr. Jakobsson, provides other examples of similar disclosures in Groenendaal. Jakobsson Decl. ¶¶ 101–103. He testifies that Groenendaal’s server may configure “infrastructure entities” to enforce the security policies. *Id.* ¶ 101 (emphasis omitted). For example, the server can configure or implement a firewall policy for a given user on a wireless gateway. *Id.* (citing Ex. 1003 ¶ 14). Petitioner contends that these “additional security services” meet this limitation even under Patent

Owner's claim construction. Pet. 24–26; Pet. Reply 17–18 (“These security services satisfy this limitation even under Patent Owner's interpretation of this limitation because they go beyond merely providing security information to a mobile device.”).

Patent Owner responds that Groenendaal “is directed to pushing security profiles from a server to a mobile device, where the mobile device itself implements any attendant security services.” PO Resp. 28 (citing Goodrich Decl. ¶ 87). As to Dr. Jakobsson's examples of the stored security code, policy, and data in Groenendaal providing security services to the mobile devices other than by sending security profiles, Patent Owner contends these do not meet the claim limitation because they are “implemented by the mobile device.” *Id.* at 31. Specifically, as to the firewall example, Patent Owner contends “the enabled profile is implemented on and by the mobile device, not the server.” *Id.*

We do not agree that these arguments by Patent Owner distinguish Groenendaal's disclosures from the challenged claims. For the reasons presented *supra*, we construe “provide security services to a mobile device” as including providing security information to the mobile device. *See supra*, Section II.C.1. We find that under this construction, Groenendaal meets this claim limitation, for example, by providing updated security information to the mobile devices. Pet. 6 (citing Jakobsson Decl. ¶ 57; Ex. 1001, 2:34–37).

But even if we had adopted a more restrictive construction for this limitation that would exclude sending security information to a mobile device, we find that Petitioner's example of configuring or implementing firewall protection for the mobile devices would meet the limitation. Pet. 24; Pet. Reply 20; Jakobsson Decl. ¶ 101. Patent Owner's attempt to

distinguish the firewall example by arguing that Groenendaal’s firewall is not implemented on the server because a gateway is involved is unavailing. *See, e.g.*, Hearing Tr. 55:23–56:2; *see also* discussion of “additional security services” in Section II.C.4, *supra*. As discussed in that Section, we do not agree with Patent Owner’s contention that due to the presence of the gateway, the server does not provide the claimed security services to the mobile device.

We find that for the reasons given by Petitioner, summarized *supra*, these additional services, and particularly processing on the server to set up the firewall for the mobile device in Groenendaal, meet this claim limitation. Jakobsson Decl. ¶¶ 101–103. As Dr Jakobsson testifies, “[e]ach of these services is implemented by the security server processor by processing the stored security code, security policies, and security data, as established for limitation 1.4.” *Id.* ¶ 105.

We find, based on the evidence presented by Petitioner, that Groenendaal teaches claim element 1.4.

5. *Element 19.4*

Claim element 19.4, similar (but not identical to) claim element 1.4, calls for “the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data *configured to be processed by the security system processor to implement security services* for a mobile device coupled to the security system.” Ex. 1001, 17:47–52 (emphasis added). As noted by Patent Owner, the language italicized above in claim element 19.4 above differs from element 1.4. PO Resp. 7. However, we declined to adopt Patent Owner’s proposed construction of the “configured to be processed” limitation in claim 19. *See*

Section II.C.4, *supra*. We observed, however, that “while we agree with Petitioner’s construction, we also agree that Groenendaal meets this limitation under Patent Owner’s construction.” *Id.*

For this claim element, Petitioner relies on its analysis of similar claim element 1.4. Pet. 26. For the reasons set forth in connection with claim element 1.4, *supra*, we find that Petitioner demonstrates that Groenendaal meets the common limitation “implement security services for a mobile device” under the construction we have adopted. *See* Section II.C.4, *infra*.

Responding to Patent Owner’s construction of this limitation, Petitioner demonstrates that even under Patent Owner’s construction, “Groenendaal discloses implementing security services for a mobile device beyond providing security information to the mobile device.” Pet. 26–27. We find that these additional security services meet the claim construction proposed by Patent Owner for the reasons given by Petitioner. *Id.* Petitioner cites Groenendaal’s “firewall policy for a given user” as an example of “implementing security services for a mobile device” as well as the other examples cited in its analysis of element 1.4. *Id.* at 27.

Dr. Jakobsson provides testimony supporting this analysis. Jakobsson Decl. ¶¶ 104–106. Dr. Jakobsson testifies that the “processed by the security system processor to implement” limitation of claim element 19.4 is met by Groenendaal: “Each of these services is implemented by the security server processor *by processing the stored security code, security policies, and security data, as established for limitation 1.4.*” *Id.* ¶ 105 (emphasis added).

Patent Owner raises additional arguments to distinguish Groenendaal from this claim. PO Resp. 27–34. For example, Patent Owner describes the invention claimed in the ’344 patent as providing the mobile device with

“two lines of defense, one implemented by a security system and one implemented by the mobile device itself.” *Id.* at 28. According to Patent Owner, “[c]onsistent with this goal,” claims 19 and 20 of the ’344 patent require the security system to store “security information,” that is “configured to be processed by the security system’s processor to implement security services for the mobile device.” *Id.* Further, according to Patent Owner, this technique “is fundamentally different from the security system of *Groenendaal* Instead, *Groenendaal* is directed to pushing security profiles from a server to a mobile device, where the mobile device itself implements any attendant security services.” *Id.* at 28.

We do not agree with these arguments. First, as with claim element 1.4, we do not agree with Patent Owner’s claim construction that would require the security system to provide security information to the mobile units by itself. *See supra*, Sections II.C.1 & II.C.2. Furthermore, we find that Petitioner provides persuasive evidence, including expert testimony, that *Groenendaal* meets the “configured to be processed” limitation even under Patent Owner’s proposed construction. Pet. 26–27; Jakobsson Decl. ¶¶ 104–106. Petitioner demonstrates, and we find, that *Groenendaal* discloses that the security code, policy, and data provide security services to the mobile device “other than by sending a security profile.” Pet. 24–26; Pet. Reply 17–21. As Petitioner demonstrates, other examples from *Groenendaal* show the provision of “security services, *i.e.*, firewall protection, to a mobile device other than by sending it a security profile.” Pet. 24; Pet. Reply 20.

Our finding is supported by Dr. Jakobsson’s testimony that the “configured to be processed” limitation is met by *Groenendaal*. Jakobsson Decl. ¶¶ 104–106. Dr. Jakobsson testifies that in *Groenendaal*, certain

security services are provided beyond those provided by sending security information to the mobile device, and “[e]ach of these services is implemented by the security server processor by processing the stored security code, security policies, and security data.” *Id.* ¶ 105.

Patent Owner contends that Dr. Jakobsson’s examples, including the firewall, do not meet the claim limitation because they are “implemented by the mobile device.” PO Resp 31. Specifically, as to the firewall example, Patent Owner contends “the enabled profile is implemented on and by the mobile device, not the server.” *Id.*

We do not agree that these arguments distinguish Groenendaal from the challenged claims. For the reasons presented *supra*, we construe “implement security services for a mobile device” in claim element 19.4 as including providing security information to the mobile device. *See supra*, Section II.C.2. We find that under this construction, Groenendaal meets this claim element, for example, by providing updated security information to the mobile devices. Pet. 6 (citing Jakobsson Decl. ¶ 57; Ex. 1001, 2:34–37). But even if we had adopted Patent Owner’s proposed construction for “implement security services for the mobile device,” we would find that Groenendaal meets this claim element, for example, in configuring or implementing firewalls for the mobile devices.

Patent Owner’s attempt to distinguish the firewall example by arguing that Groenendaal’s firewall is not implemented on the server because a gateway is involved is unavailing. *See* discussion of “additional security services” in Section II.C.4, *supra*. As discussed there, we do not agree with Patent Owner’s contention that due to the presence of the gateway, the server does not provide the claimed security services to the mobile device.

See, e.g., Hearing Tr. 55:23–56:2. We find that the processing on the server to set up the firewall for the mobile device meets the claim limitation.

Jakobsson Decl. ¶ 101. As Dr Jakobsson testifies, “[e]ach of these services is implemented by the security server processor by processing the stored security code, security policies, and security data, as established for limitation 1.4.” *Id.* ¶ 105.

We therefore do not give weight to Patent Owner’s arguments or the testimony of its expert, Dr. Goodrich (Goodrich Decl. ¶¶ 82–107) attempting to rebut Dr. Jakobsson’s testimony or to distinguish Groenendaal.

Dr. Goodrich’s testimony tracks closely the arguments in Patent Owner’s responses that we find unavailing. Those arguments are based on claim constructions and other restrictions that we have rejected as not supported by the intrinsic record in Section II.C. *supra*.

We find, based on the evidence presented by Petitioner, that Groenendaal teaches claim element 19.4. Jakobsson Decl. ¶¶ 104–107.

6. Elements 1.5, 19.5

Claims 1 and 19 also require:

the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data being managed by one or more information technology (IT) administrators using an IT administrator system on a trusted enterprise network, the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data being configured based on one or more policies implemented by the one or more IT administrators on the trusted enterprise network.

Claim 19 recites, in addition,

the mobile device being a first computer system, the security system being a second computer system, and the IT administrator system being a third computer system, the first computer system,

the second computer system and the third computer system being separate computer systems,

See claim elements 1.5, 19.5, *supra*. Petitioner shows these elements are met by Groenendaal’s disclosure of an IT administrator using GUI 116 to manage the system’s connection, security, and firewall profiles. Pet. 28–29. Petitioner further contends, “Groenendaal also discloses the administrator manages the security manager (security code) by managing the security profiles that define its behavior, using the administrator system GUI.” *Id.* at 29–30 (citing Ex. 1003 ¶ 21). We agree with this analysis, and therefore find that the “one or more policies” referred to in the claim “can include the decisions made by the recited ‘one or more IT administrators.’” *Id.* at 30. This contention is consistent with Petitioner’s proposed claim construction which we have adopted here and in the ’368 IPR. *See supra*, Section II.C.3. Furthermore, we find, as Petitioner contends, that “Groenendaal discloses that the stored security policy, data, and code described for limitation 1.3 all are configured using input received from the IT administrator at GUI 116, which input reflects the ‘one or more policies’ in the mind of the IT administrator. The security policies, data, and code therefore are configured based on those ‘one or more policies.’” Pet. 31. We find, also, as Petitioner contends, that “Groenendaal discloses that its IT administrator implements the one or more policies discussed above.” *Id.* at 32. Thus, “the Groenendaal administrator also provides input to GUI 116 to create security profile 150 and configuration profile 152 based on the ‘one or more policies,’ as established above.” *Id.*

Finally, we find that Groenendaal discloses the “three separate computer systems” recited in claim 19: “Groenendaal’s computer 104a with GUI 116 (an ‘IT administrator system’) is a computer separate from client

computers 104b-d (mobile devices). And each of computer 104a and the mobile devices are computers separate from server 102 (security system).” *Id.* at 34 (citing Ex. 1003, Fig. 1, ¶¶ 16, 27).

Dr. Jakobsson’s testimony supports our finding that Groenendaal discloses this limitation. Jakobsson Decl. ¶¶ 106–134. Dr. Jakobsson testifies that even under Patent Owner’s claim construction analysis, Groenendaal meets this claim limitation. *Id.* ¶¶ 124–134. He testifies that the firewall and other services result from policies implemented by the administrator using the GUI. *Id.* ¶ 125 (“In particular, the GUI 116 receives and stores settings such as whether to enable a firewall, whether to enable network file sharing, and which network authentication protocol to use. The administrator finalizes and gives effect to these settings by pressing the ‘Finish’ button.”) (citations omitted). He concludes that “[t]he settings in GUI 116 therefore are an implementation of the ‘one or more policies’ described above because they become the operative policies (i.e., the policies in effect).” *Id.* at ¶ 126.

Patent Owner contends that the “one or more policies” do not encompass “mental decisions” of the IT administrator. PO Resp. 35. As we discuss *supra* in Section II.C.3, we do not agree with that contention for the reasons given there.

Patent Owner also contests Petitioner’s argument that even under Patent Owner’s construction, Groenendaal meets this limitation. PO Resp. 35. According to Patent Owner, these settings are “temporarily stored” and therefore not “put into effect” until the user presses a “Finish” or “Save” button. *Id.* We disagree with these arguments for the reasons given by Petitioner. Pet. Reply 22–23 (“[T]he settings stored in GUI 116 are an

implementation of policies because they are concrete expression of policies and are stored (at least temporarily) in the memory of laptop 104a.”).

Patent Owner acknowledges that once the settings are entered by the IP administrator, they are stored (even if temporarily) in the memory of the laptop computer. PO Resp. 35 (referring to “temporarily stored” settings in the GUI); Hearing Tr. 50:16–23. As Dr. Jakobsson testifies: “The settings in GUI 116 therefore are an implementation of the ‘one or more policies’ described above because they become the operative policies (*i.e.*, the policies in effect).” Jakobsson Decl. ¶ 126.

We find, therefore, based on the evidence presented by Petitioner, that Groenendaal teaches claim element 19.5 under either Petitioner’s or Patent Owner’s claim construction.

7. Elements 1.6, 1.7, 1.8, 19.6, 19.7, 19.8

Petitioner provides similar element-by-element analyses for the remaining limitations of claim 1 and claim 19. Pet. 38–47. Patent Owner does not challenge this analysis. We find, based on the evidence presented by Petitioner, that Groenendaal teaches claim elements 1.6–1.8 and 19.6–19.8. Jakobsson Decl. ¶¶ 135–149.

8. Summary Claims 1 and 19

We have considered the entire record including Petitioner’s analysis of claims 1 and 19 in relation to Groenendaal and the arguments presented by Patent Owner. Considering the evidence presented in the Petition and Patent Owner’s responses, we determine that Petitioner has demonstrated by a preponderance of the evidence that claims 1 and 19 would have been obvious in light of Groenendaal.

C. Claims 10 and 20

Petitioner’s analysis of claims 10 and 20 tracks its analysis of claims 1 and 19. Pet. 53–55. Patent Owner does not specifically address claim 10 or distinguish between claims 19 and 20 in its response. PO Resp. 28–36. Accordingly, for the reasons given above for claims 1 and 19, we determine that Petitioner has demonstrated by a preponderance of the evidence that claims 10 and 20 would have been obvious in light of Groenendaal. Jakobsson Decl. ¶¶ 160–167.

D. Claims 2–9 and 11–18

Claims 2–9 depend directly from claim 1. Claims 11–18 depend directly from claim 10. The two sets of dependent claims are parallel, and each set provides the same additional features to the claims from which they depend. Claim 2, for example, specifies that the security system is “on a separate appliance removably coupled to the mobile device.” Ex. 1001, 16:1–3. Claim 11 requires “coupling the security system to the mobile device.” *Id.* at 17:10–12. Petitioner provides an element-by-element analysis of each dependent claim in relation to Groenendaal. Pet. 47–52, 55–56.

Patent Owner does not respond further to Petitioner’s analysis of these dependent claims with the exception of claims 8 and 17. PO Resp. 37–39; PO Sur-reply 22–24. Those claims each recite that “the security code, the security policy, and the security data are *configured to mirror* security policies of a gateway on the trusted enterprise network.” Ex. 1001, 16:20–23, 17:32–35 (emphases added).

Patent Owner contends that Groenendaal “does not teach or suggest this feature of the Challenged Claims.” PO Resp. 38 (citing Goodrich Decl.

¶¶ 108–117); PO Sur-reply 22. As explained by Patent Owner, “[t]he specification [of the ’344 patent] explains that the enterprise’s gateway (which is on the *enterprise[’]s network security system*) pushes security policies and data onto the claimed *security system* In this manner, the security system is ‘configured to mirror security policies of a gateway.’” PO Sur-reply 22. Patent Owner continues, “Groenendaal does just the opposite: at best, policies of a remote gateway are configured to mirror those of server 102.” *Id.* at 23.

We do not agree with this argument by Patent Owner attempting to distinguish Groenendaal because the argument is not supported by the language of the claims. We find, as Petitioner explains, that claims 8 and 17 do not impose an order of operations:

Groenendaal discloses that policies are pushed from the Groenendaal server to the Groenendaal gateway. Patent Owner argues that that disclosure doesn’t satisfy this limitation because the policies have to be on the gateway first and are copied to the server, not vice versa. But *the claim language doesn’t require an order of operations. The claim language includes the state of being mirrored.*

Hearing Tr. 22:20–23 (emphasis added). Petitioner relies on the inclusion in the claims of the term “configured”: “After one has configured a server and a gateway to have the same policies they are configured to mirror each other. They do mirror each other.” *Id.* at 23:1–3. We agree with Petitioner’s reasoning that the claims do not impose an order, and we therefore find that Groenendaal teaches the “configured to mirror” limitation of claims 8 and 17. We further determine for the reasons given by Petitioner that claims 2–9 and 11–18 would have been obvious over Groenendaal. Jakobsson Decl. ¶¶ 150–159, 168–175.

IV. CONCLUSION

For the foregoing reasons, we determine Petitioner has demonstrated by a preponderance of the evidence that all challenged claims of the '344 patent would have been obvious and are, therefore, unpatentable. Our conclusions are summarized in the following table.

Claims	35 U.S.C. §	Reference(s)/ Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1–20	103(a)	Groenendaal	1–20	
Overall Outcome			1–20	

V. ORDER

For the foregoing reasons, it is
ORDERED that claims 1–20 of the '344 patent are unpatentable; and
FURTHER 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. § 90.2.⁸

⁸ Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner's attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. See 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. See 37 C.F.R. § 42.8(a)(3), (b)(2).

IPR2021-00813
Patent 10,621,344 B2

PETITIONER:

Robert Buergi
James Heintz
DLA Piper LLR (US)
robert.buergi@dlapiper.com
jim.heintz@dlapiper.com

PATENT OWNER:

James Hannah
Jeffrey Price
Jenna Fuller
KRAMER LEVIN NAFTALIS &
FRANKEL LLP
jhannah@kramerlevin.com
jprice@kramerlevin.com
jfuller@kramerlevin.com