Trials@uspto.gov
571-272-7822

Paper 12
Entered: November 24, 2021

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FORESCOUT TECHNOLOGIES, INC.,
Petitioner,

v.

FORTINET, INC.,
Patent Owner.

IPR2021-00913
Patent 9,369,299 B2

Before THOMAS L. GIANNETTI, KIMBERLY McGRAW, and CHRISTOPHER L. OGDEN, *Administrative Patent Judges*.

OGDEN, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

Petitioner Forescout Technologies, Inc. ("Forescout")[1] filed a Petition (Paper 2, "Pet.") under 35 U.S.C. §§ 311–319 requesting *inter partes* review of claims 11–16 and 18–21 of U.S. Patent No. 9,369,299 B2 (Ex. 1001, "the '299 patent"). Patent Owner Fortinet, Inc. ("Fortinet")[2] filed a Preliminary Response (Paper 10, "Prelim. Resp.").

Under the authority delegated to us by the Director under 37 C.F.R. § 42.4(a), we may only institute an *inter partes* review when "the information presented in the petition . . . and any response . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." 35 U.S.C. § 314(a); *see also* 37 C.F.R. § 42.108(c) (2020). Applying that standard, we do not institute an *inter partes* review, for the reasons explained below.

II. BACKGROUND

A. RELATED PROCEEDINGS

As a related matter, the parties identify *Fortinet, Inc. v. Forescout Technologies, Inc.*, No. 3:20-cv-03343-EMC (N.D. Cal. filed May 15, 2020) ("the parallel district court proceeding"). Pet. 64–65; Paper 4, 1. Also, IPR2021-00912 is another *inter partes* review proceeding involving the same parties and the same patent, but Forescout challenges a different set of claims. Pet. 1, 68–69; Prelim. Resp. 39–42.

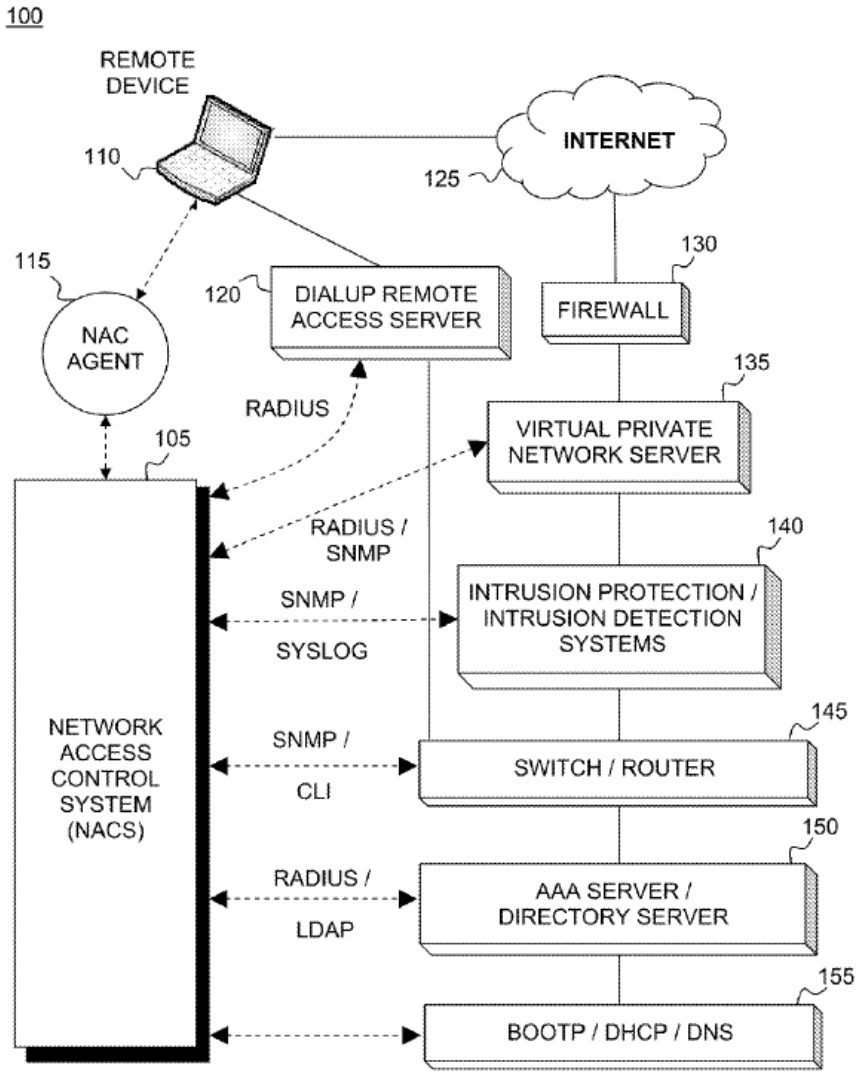
[1] Forescout identifies itself as the real party in interest. Pet. 64.

[2] Fortinet identifies itself as the real party in interest. Paper 4, 1.

B. THE ’299 PATENT (EX. 1001)

The ’299 patent describes a “method for network access control (NAC) of remotely connected devices.” Ex. 1001, code (57). According to the ’299 patent, existing NAC hardware solutions “often employ[ed] a network appliance inline with the network to provide NAC capabilities, sometimes in conjunction with access layer switches,” and relied “solely on user authentication to determine network access.” *Id.* at 1:28–30, 37–38. As an alleged improvement, the inventors describe a method with capabilities that “include user authentication, role-based authorization, endpoint compliance, alarms and alerts, audit logs, location-based rules, and policy enforcement.” *Id*. at code (57); *see also id.* at 1:43–46 (“What is needed is a network access control system that provides authentication, assessment, authorization, provisioning, and remediation, for a broad, user-centric, network-based, access control solution.”). The proposed “[e]mbodiments leverage security capabilities of existing network equipment along with authentication and authorization technologies to control network access down to the point of access.” *Id.* at 1:59–62.

The overall system of the ’299 patent is shown in Figure 1, reproduced below:



(NETWORK ACCESS CONTROL ARCHITECTURE)
FIG. 1

(VPN) server 135 (which connects to user 110 over the internet (125)). *Id.* at 5:34–36.

The '299 patent defines a "remote access device (RAD)" as "[a] network device that allows remote devices to connect to a network through one of its interfaces." Ex. 1001, 5:18–20. In disclosed embodiments, a RAD can also "authenticate[] the user to the NACS using RADIUS."[3] *Id.* at 10:8–9. Accordingly, in Figure 1, dialup and VPN servers 120 and 135 function as RADs by using RADIUS to authenticate user 110 to NACS 105. *See id.* at 5:44–45. The '299 patent states that its method has the benefit of being RAD-agnostic, or in other words, "a multi-vendor solution" that is "unaffected by the manufacturer of network devices being managed in the network." *Id.* at 4:36–37, 4:49–51; *see also id.* at 5:54–56 ("Embodiments of the remote access solution are designed to work with many different remote access devices and types.").

According to the '299 patent, it is also beneficial that its "authentication process is out of band,[4] and not involved in ongoing network traffic flow, whereby data throughput and remote access scalability are unimpeded." Ex. 1001, 3:31–33. In other words, while components of the system "are used during the authentication process for connecting remote access users, once a host is connected, it is not involved in the normal network traffic flow for that host. Therefore, it does not become a bottleneck

[3] The cited prior art references explain that "RADIUS" refers to a "Remote Access Dial-In User Service." Ex. 1005, 3:50–55; Ex. 1006, 3:63–65.

[4] The '299 patent defines "out of band" to mean "[u]sed to convey something that is not in the direct path of a process." Ex. 1001, 5:8–9.

for data throughput removing impact on remote access scalability." *Id.* at 9:14–17.

The RAD is also configured with a network access filter (NAF), which restricts a user device's access to the network. Ex. 1001, 2:64–65. Each user device can also include an agent (115), which is "[a] software application that executes on the remote device to provide the NACS with data describing that device," which "can also be used to enforce policy." *Id.* at 4:46–48. In operation, the NACS can instruct the RAD to modify the NAF to restrict network access if an agent's security scan shows that there is a failure of security compliance. *Id.* at 3:1, 3:13–19.

C. Challenged Claims and Asserted Grounds of Unpatentability

Claim 11, representative of the challenged claims, is as follows:

> 11. A method for out of band control for secure network access of a user device to a network comprising the steps of:
>
> [a] receiving a connect attempt to said network from said user device;
>
> [b] authenticating connecting user to a network access control server (NACS) by a remote access device (RAD) for out of band network control;
>
> [c] capturing RAD identification, location by said NACS;
>
> [d] providing out of band network enforcement comprising restricting access to said network by said user device with a network access filter (NAF) configured on said RAD; wherein said enforcement is out of band and is accomplished on said RAD, comprising communicating with said RAD to make real-time changes to its running configuration, whereby said enforcement is vendor-independent and said system is RAD-agnostic;

[e] directing said client device to an agent by said RAD;

[f] running said agent on said user device;

[g] identifying client to said NACS by said agent;

[h] modifying said NAF based on compliance;

[i] monitoring post-connection of successful connections.

Ex. 1001, 12:1–22 (Forescout's reference letters added).

Forescout argues two grounds for *inter partes* review, as summarized in the following table:

Claims Challenged	35 U.S.C. §	Reference(s)/Basis
11–16, 18–21	103(a)[5]	Palmer[6]
12, 15, 18	103(a)	Palmer, Gilde[7]

Pet. 14–15.

D. DECLARATORY TESTIMONY

For its Petition, Forescout relies on the declaration of Eric Cole, Ph.D. Ex. 1003. Patent Owner Fortinet does not challenge Dr. Cole's qualifications to provide expert testimony on the subject matter of his declaration, and does not submit rebuttal testimony at this stage.

[5] 35 U.S.C. § 103(a) (2006), *amended by* Leahy–Smith America Invents Act, Pub. L. No. 112-29 § 103, sec. (n)(1), 125 Stat. 284, 287, 293 (2011) (effective Mar. 16, 2013). This version of § 103 applies because the effective priority date of the '299 patent is before the effective date of the AIA amendments. *See supra* part II.B.

[6] Palmer, US 7,882,538 B1 (issued Feb. 1, 2011) (Ex. 1005). Forescout argues that Palmer is prior art under 35 U.S.C. § 102(e). Pet. 14.

[7] Gilde et al., US 8,520,512 B2 (issued Aug. 27, 2013) (Ex. 1006). Forescout argues that Gilde is prior art under 35 U.S.C. § 102(e). Pet. 14–15.

III. GROUNDS OF THE PETITION

For the reasons below, we determine that Forescout has not established that there is a reasonable likelihood of success in showing that at least one of the challenged claims of the '299 patent is unpatentable. Before analyzing those grounds in detail, we first address the level of ordinary skill in the art, and whether we need to construe any claim terms explicitly for our analysis.

A. LEVEL OF ORDINARY SKILL IN THE ART

The level of ordinary skill in the pertinent art at the time of the invention is relevant to how we construe the patent claims. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (en banc). It is also one of the factual considerations relevant to obviousness, *see Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

To assess the level of ordinary skill, we construct a hypothetical "person of ordinary skill in the art," from whose vantage point we assess obviousness and claim interpretation. *See In re Rouffet*, 149 F.3d 1350, 1357 (Fed. Cir. 1998). This legal construct "presumes that all prior art references in the field of the invention are available to this hypothetical skilled artisan." *Id.* (citing *In re Carlson*, 983 F.2d 1032, 1038 (Fed. Cir. 1993)).

Relying on Dr. Cole's testimony, Forescout argues that a person of ordinary skill in the art would have "a bachelor's degree in computer science, computer engineering, or electrical engineering and at least three years of experience in networking operating systems and cyber security," or alternatively, "a master's degree in one of the foregoing and at least two years of experience in the aforementioned fields." Pet. 9–10 (citing Ex. 1003

¶¶ 26–28). Forescout also argues that a person of ordinary skill in the art could be "[s]omeone with less or different technical education but more relevant practical experience, or more relevant education but less practical experience." *Id.* at 10 (citing Ex. 1003 ¶¶ 26–28).

In its Preliminary Response, Fortinet does not dispute Forescout's articulation of the level of ordinary skill in the art. Prelim. Resp. 12. Because it is supported by testimonial evidence and appears reasonable at this stage in light of the subject matter of the '299 patent, we adopt it for this decision.

B. CLAIM CONSTRUCTION

In an *inter partes* review, we construe a patent claim "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) (2020). This includes "construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent." *Id.* The ordinary and customary meaning of a claim term "is its meaning to the ordinary artisan after reading the entire patent," and "as of the effective filing date of the patent application." *Phillips*, 415 F.3d at 1313, 1321. We also consider "[a]ny prior claim construction determination concerning a term of the claim in a civil action . . . that is timely made of record" in the proceeding. 37 C.F.R. § 42.100(b) (2020).

Forescout notes that in the parallel district court proceeding, the parties agree that the term "remote access device (RAD)" means "[a] network device that allows remote devices to connect to a network through one of its interfaces." Pet. 11 (alteration in original) (citing Ex. 1011, 3; Ex.

1001, 5:18–20). Forescout also states that in the parallel district court proceeding, the parties disagree on the meanings of "out of band" and "RAD-agnostic," and that Fortinet has proposed constructions for several other terms that Forescout does not believe require construction. *See* Pet. 9–14.

Fortinet "asserts that the claim terms be given their plain and ordinary meaning," and does not offer any explicit construction as to those meanings. *See* Prelim. Resp. 13.

Because the parties do not, at this stage, argue opposing meanings for any of the claim terms that would be material to our analysis below, we do not need to construe any terms explicitly for our decision. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) ("[W]e need only construe terms 'that are in controversy, and only to the extent necessary to resolve the controversy.'" (quoting *Vivid Techs., Inc. v. Am. Sci & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))). Nevertheless, the '299 patent specification, its prosecution history, and arguments made in the parallel district court proceeding inform our interpretation of a key aspect of limitation 11d, and we discuss that interpretation as part of our analysis below.

C. GROUND BASED ON PALMER (CLAIMS 11–16 AND 18–21)

For its first ground, Forescout alleges that claims 11–16 and 18–21 are unpatentable under § 103(a) as obvious over Palmer. Pet. 14.

A claim is unpatentable under § 103 for obviousness 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). For a combination of known elements that are not explicitly found together in the prior art, we consider "whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *Id.* at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)). A successful petition must "articulate specific reasoning, based on evidence of record, to support the legal conclusion of obviousness." *In re Magnum Oil Tools Int'l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016) (citing *KSR*, 550 U.S. at 418); *see also* 35 U.S.C. § 322(a)(3); 37 C.F.R. §§ 42.22(a)(2), 42.104(b)(4) (2020).

We base our obviousness inquiry on factual considerations 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) any objective indicia of obviousness or non-obviousness that may be in evidence.[8] *See Graham*, 383 U.S. at 17–18.

The deficiency in Forescout's challenge arises primarily in its comparison of limitation 11d with the teachings of Palmer, so we begin with an overview of Palmer, followed by a discussion of Forescout's arguments with respect to claim 11.

[8] At this stage, the parties do not identify any objective indicia of obviousness or non-obviousness. *See* Pet. 64 ("As far as Forescout is aware, Fortinet has never alleged any secondary considerations that would be relevant to an obvious determination of any claims of the '299 patent."). Such indicia do not factor into our decision not to institute an *inter partes* review.

1. Overview of Palmer

Palmer describes "techniques of locally caching endpoint security information." Ex. 1005, code (57). Based on this cached endpoint security information, the system controls access to an endpoint device within the system. *Id.* The device uses "an intermediate device" that includes a "local access module that controls access from local endpoint devices to one or more remote servers of the enterprise." *Id.* at 1:50–52. An overview of the system is shown, below, in Figure 1:

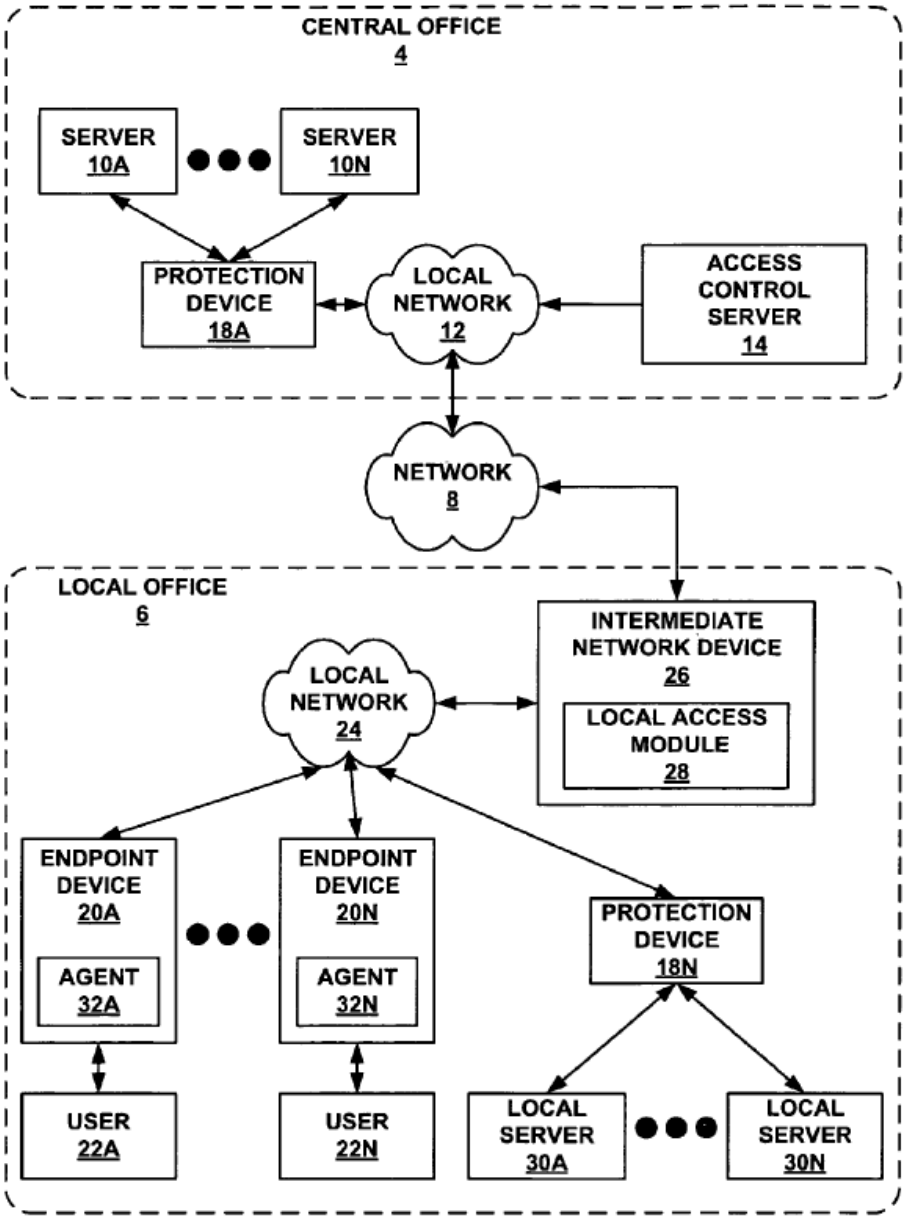


FIG. 1

Figure 1, above, is a block diagram showing central office 4 and local office 6, communicating with each other over inter-office network 8. Ex. 1005, 3:16–23. Central office 4 contains access control server 14, which "communicates with other devices in central office 4 through a local network 12." *Id.* at 4:17–19. Access control server 14 also "maintains a set of endpoint security information" that "instructs access control server 14

how to control access of an endpoint device to a network resource" based on the identity of the user and the security state of the device. *Id.* at 4:19–24.

Local office 6 contains several network devices, connected over local network 24, through which users 22 can communicate with central office 4 using endpoint devices 20, respectively. *Id.* at 3:24–30. Endpoint devices 20 may be, for example, "desktop or laptop computers, network-enabled mobile devices, network-based telephones, set-top boxes, cellular telephones, [or] network televisions." *Id.* at 3:31–33. The endpoint devices include defense agents 32, respectively, which collect authentication information about the user. *Id.* at 3:34–41. Also connected to local network 24 are protection devices 18 that "control access of endpoint devices 20 to servers 10 based on device-specific access rights." *Id.* at 4:2–4.

Local office 6 also includes intermediate network device 26, which provides an interconnection between local office network 24 and inter-office network 8. Ex. 1005, 3:42–44. Intermediate network device 26 includes local access module 28, which caches endpoint security information maintained by access control server 14, including the identity of the users of the endpoint devices and the security state. *Id.* at 3:50–55, 4:28–34.

Central office 4 and local office 6 also include servers 10 (see also local servers 30), which provide network resources for endpoint devices 20. Ex. 1005, 3:56–61. When user 22 attempts to access one of servers 10, local access module 28 performs "an access right generation process," at the end of which it "generates device-specific access rights for the end-point device based on the endpoint security information, the identity of the user currently associated with the endpoint, and the security state for that particular endpoint device (referred to as the 'health information' of the endpoint)." *Id.*

at 4:62–5:4. "Subsequently, protection devices 18 may govern whether the particular endpoint device may communicate with a network resource based on the device-specific access rights generated for that particular endpoint device." *Id.* at 5:4–8.

2. Claim 11

Forescout provides an overview of Palmer and claim charts comparing the limitations of independent claim 11 (designated as 11pre–11i) with Palmer's teachings. Pet. 16–39. For the reasons below, we find Forescout's arguments insufficiently persuasive as to at least one aspect of limitation 11d, and consequently, Forescout fails to provide sufficient evidence that claim 11 would have been obvious over Palmer's teachings in light of the background knowledge of a person of ordinary skill in the art.

Limitation 11d recites, in relevant part, that when the NACS (recited in limitation 11b) enforces the network's usage policy, "said enforcement is out of band and is accomplished on said RAD, comprising communicating with said RAD to make real-time changes to *its* running configuration." Ex. 1001, 12:13–16 (emphasis added). In comparing claim 11 to Palmer, Forescout identifies the RAD as Palmer's access control server 14, and the NACS as intermediate network device 26. *See* Pet. 26.

According to Forescout, "Palmer . . . discloses that enforcement is done by the RAD communicating with intermediate network device 26, i.e., the NACS, to make real-time changes to the security configurations." Pet. 31 (citing Ex. 1003 ¶ 184). Forescout contends that this occurs when intermediate network device 26 caches local "authentication, user role policy, health policy, or protection device policy information from access control server 14" in local access module 28, either (1) when access control

server 14 pushes this information to local access module 28, or (2) when local access module 28 periodically requests endpoint security information from access control server 14. *Id.* at 31–32. In either case, according to Forescout, a person of ordinary skill in the art "would have understood that . . . real-time changes to the running configuration are being communicated between the access control server 14 and the intermediate network device 26." Pet. 32.

But as Patent Owner Fortinet points out, Forescout only identifies real-time changes made to the running configuration of local access module 28, which in Forescout's argument is part of the NACS, not the RAD. Prelim. Resp. 18. According to Fortinet, Forescout "has not demonstrated, nor even alleged, that these changes are made to the *access control server 14's*—what [Forescout] identifies as the RAD—running configuration." *Id.*

We agree. It is clear from the plain language of limitation 11d that the claimed system makes real-time changes to the running configuration of the RAD, not the NACS. Fortinet argues that Forescout agreed with Fortinet on this point in the parallel district court litigation. *See* Prelim. Resp. 19 n.4. In its Identification of Preliminary Proposed Constructions in the district court litigation, Forescout proposed that the term "communicating with said RAD to make real-time changes to its running configuration" should be construed to mean "communicating with said RAD to make real time changes to the particular hardware and/or software arrangement *of the RAD*." Ex. 1012, 4[9] (emphasis added) (citing Ex. 1001, 2:58–3:2, 3:26–47, 6:60–7:12, 7:42–48, 9:31–51, 10:13–29, 10:66–11:29, 12:1–22) ; *see also* Ex. 1011, 3 (Fortinet's

[9] We use the internal page numbering of the document, rather than the page numbers that Forescout added when it prepared the exhibit.

competing proposed construction in the parallel litigation, agreeing that what is changed is the configuration of the RAD).

This interpretation that it is the RAD's running configuration that changes is also consistent with the '299 patent specification, including the passages that Forescout cited as evidence in the parallel district court litigation. For example, the '299 patent discloses "restricting access to the network by the user device with a network access filter (NAF) configured on the RAD," and "modifying the NAF based on compliance" while the RAD is running. Ex. 1001, 2:64–3:1; *see also id.* at 3:37–39 ("restricting access to the network by the user device with a network access filter (NAF) configured on the RAD"); *id.* at 9:65–67 ("[The Campus Manager] instructs the RAD to remove NAF from the client connection and it is granted access to the unrestricted network."). It is also consistent with the applicant's arguments during prosecution of the '299 patent, where the applicant amended claim 11 to include limitation 11d. *See* Ex. 1002, 1242, 1246 (arguing that a prior art reference fails to teach limitation 11d because none of the reference's "enforcement methods communicates back to the RAD to make changes to affect the security state of a client").

Thus, we agree with Fortinet that Forescout's analysis fails to show that Palmer discloses or teaches the part of limitation 11d requiring that policy enforcement includes making real-time changes to the RAD's running configuration. Because of this shortcoming, we determine that Forescout is not reasonably likely to prevail in showing that claim 11 is unpatentable as obvious over Palmer.

3. Claims 12–16 and 18–21

Claims 12–16 and 18–21 depend, directly or indirectly, from claim 11, and thus incorporate limitation 11d and its requirement that "[policy] enforcement is out of band and is accomplished on said RAD, comprising communicating with said RAD to make real-time changes to its running configuration." *See* Ex. 1001, 12:12–16, 12:23–37, 12:42–57. Forescout's analysis of these claims addresses only the added limitations of each dependent claim and does not provide further argument that would remedy the deficiency in Forescout's analysis comparing claim 11 to Palmer. *See* Pet. 39–52.

For example, claim 13 depends from claim 11 and further recites "wherein said NACS instructs said RAD to reject user and network connection is disallowed when authentication fails." Ex. 1001, 12:26–28. In its Petition, Forescout argues that Palmer's intermediate device 26 (which Forescout identifies as the NACS) communicates with access control server 14 (which Forescout identifies as the RAD) during authentication. *See* Pet. 40–41. However, Forescout does not explain if, or how, this communication would constitute out-of-band policy enforcement or result in real-time changes in the running configuration of access control server 14. *See id.*

Thus, for the same reasons given above as to claim 11, we determine that Forescout has not demonstrated a reasonable likelihood of success in showing that claims 12–16 and 18–21 are unpatentable as obvious over Palmer. *See In re Fine*, 837 F.2d 1071, 1076 (Fed. Cir. 1988) ("Dependent claims are nonobvious under section 103 if the independent claims from which they depend are nonobvious.").

D. GROUND BASED ON PALMER AND GILDE (CLAIMS 12, 15, AND 18)

For its second ground, Forescout alleges that claims 12, 15, and 18 are unpatentable as obvious over Palmer in view of Gilde. Pet. 14–15. These claims depend from claim 11. *See* Ex. 1001, 12:23–25, 11:32–34, 11:42–44.

Gilde describes "managing dynamic network access control" by providing "services and controlled network access that includes quarantining nodes so that they may be identified, audited, and provided an opportunity to be brought into compliance with a security policy." Ex. 1006, 4:5–11.

Forescout's second ground relies on the same arguments Forescout makes for its first ground, but relies on Gilde for further teachings regarding the added limitations in claims 12, 15, and 18. *See* Pet. 53–64. But Forescout does not rely on Gilde to remedy Palmer's failure to disclose or teach "communicating with said RAD to make real-time changes to its running configuration" according to limitation 11d. *See id.*

Thus, for the same reasons as were given for claim 11, we determine that Forescout has not shown that there is a reasonable likelihood that it would prevail on its second ground challenging claims 12, 15, and 18.

IV. CONCLUSION

After considering the evidence and arguments on the preliminary record, we determine that Forescout has not demonstrated a reasonable likelihood of success in showing that at least one challenged claim of the '299 patent is unpatentable. Therefore, we deny the Petition.

V. ORDER

In consideration of the foregoing, it is

ORDERED that the Petition is *denied*, and no trial is instituted.

For PETITIONER:

Katherine A. Vidal
Louis L. Campbell
WINSTON & STRAWN LLP
kvidal@winston.com
llcampbell@winston.com

For PATENT OWNER:

Patrick D. McPherson
Christopher Tyson
D. Joseph English
Patrick C. Muldoon
Tairan Wang
Paul H. Belnap
DUANE MORRIS LLP
pdmcpherson@duanemorris.com
cjtyson@duanemorris.com
djenglish@duanemorris.com
pcmuldoon@duanemorris.com
twang@duanemorris.com
phbelnap@duanemorris.com