

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETSKOPE, INC.,

Petitioner,

v.

FORTINET, INC.,

Patent Owner.

PTAB Case No. IPR2027-00011

U.S. Patent No. 11,916,902

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 11,916,902**

TABLE OF CONTENTS

EXHIBIT LIST	v
CLAIM LISTING	vii
I. INTRODUCTION	1
II. MANDATORY NOTICES	1
A. Real Party-in-Interest	1
B. Related Matters.....	2
C. Counsel and Service Information.....	2
D. Fees.....	2
III. IPR REQUIREMENTS	3
A. Standing.....	3
B. Challenged Claims: 1-18.....	3
C. Grounds	3
D. Discretionary Denial Is Unwarranted.....	3
IV. BACKGROUND	5
A. Remote Network Access	5
B. Network Access Control	6
C. Insecure IoT Devices.....	6
D. Virtual Private Networks.....	7
V. '902 PATENT.....	7
A. Alleged Invention	7

B.	Prosecution History	9
VI.	LEVEL OF ORDINARY SKILL	11
VII.	CLAIM CONSTRUCTION	11
A.	“processing device”/“processing resource”	11
B.	“providing a message to a user of the processing device requesting the user to access the known network via another remote network”	13
VIII.	SPECIFIC GROUNDS.....	14
A.	Ground 1: Loza with Bansal, Dupont, and Bareket Renders Claims 1-4, 6, 8-9, 11-14, and 16-18 Obvious.....	14
1.	Loza.....	15
2.	Bansal.....	16
3.	Dupont.....	18
4.	Bareket	20
5.	Combining Loza with Bansal, Dupont, and Bareket	21
6.	Element-by-Element Analysis	24
B.	Ground 2: Loza with Bansal, Dupont, Bareket, and Sahay Renders Claims 5, 7, 10, and 15 Obvious.....	38
1.	Sahay	38
2.	Combining Loza, Bansal, Dupont, and Bareket with Sahay	40
3.	Element-by-Element Analysis	42
C.	Ground 3: Mishaev with Schwartz Renders Claims 1-18 Obvious.....	45
1.	Mishaev	45

2.	Schwartz.....	50
3.	Combining Mishaev with Schwartz.....	54
4.	Element-by-Element Analysis	63
D.	Ground 4: Mishaev-Schwartz-Durbin Renders Claims 1-18 Obvious.....	81
1.	Durbin	81
2.	Combining Mishaev-Schwartz and Durbin	82
3.	Analysis.....	83
IX.	CONCLUSION.....	84

EXHIBIT LIST

Exhibit	Shorthand	Description
1001	'902 patent	U.S. Pat. No. 11,916,902
1002	'902 FH	File History of the '902 patent
1003	Franz	Declaration of Dr. Michael Franz
1004	Franz CV	Curriculum Vitae of Dr. Michael Franz
1005	Loza	U.S. Pat. App. Pub. No. 2005/0278777
1006	Bansal	U.S. Pat. App. Pub. No. 2020/0067949
1007	Dupont	U.S. Pat. App. Pub. No. 2009/0307753
1008	Sahay	U.S. Pat. No. 8,707,395
1009	Mishaev	U.S. Pat. App. Pub. No. 2020/0244646
1010	Schwartz	U.S. Pat. No. 10,498,758
1011	Durbin	U.S. Pat. App. Pub. No. 2015/0365381
1012	RESERVED	
1013	Ganesan	U.S. Pat. App. Pub. No. 2010/0005297
1014	Fortinet's Infringement Contentions	Dkt. 36-10 in <i>Netskope v. Fortinet</i> , Case 4:26-cv-08886-HSG (N.D. Cal. 2026)
1015	NIST SP 800-46	Souppaya, M. & Scarfone, K., (2016), <i>Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security</i> (NIST Special Publication 800-46 Rev. 2) National Institute of Standards and Technology.
1016	NIST SP 800-77	Barker, E., Dang, Q., Frankel, S., Scarfone, K., & Wouters, P. (2020). <i>Guide to IPsec VPNs</i> (NIST Special Publication 800-77 Rev. 1). National Institute of Standards and Technology.
1017	NIST SP	Joint Task Force. (2020). <i>Security and Privacy Controls</i>

IPR2027-00011
Petition for *Inter Partes* Review
Of U.S. Pat. No. 11,916,902

Exhibit	Shorthand	Description
	800-53	<i>for Information Systems and Organizations</i> (NIST Special Publication 800-53, Rev. 5). National Institute of Standards and Technology.
1018	Bareket	U.S. Pat. App. Pub. No. 2018/0213574
1019	Starr	U.S. Pat. App. Pub. No. 2022/0103523

CLAIM LISTING

Claim	Limitation	Claim Language
1	1[pre]	A method for reducing network threats, the method comprising:
	1[a]	receiving, by a processing device, a request to access a known network from a known access device connected through a remote network,
	1[b]	wherein the known network is a private network that authorizes credentials associated with the known access device, and the remote network is external to the known network;
	1[c]	scanning, by the processing device of the known access device, the remote network through which access to the known network is to be established, wherein the scanning is configured to identify an unsecure network element on the remote network;
	1[d]	based at least in part on identifying at least one unsecure network element on the remote network, denying, by the processing device, access to the known network; and
	1[e]	based at least in part upon on failure to identify any unsecure network element on the remote network, requesting a grant of access from the known network to the processing device,
	1[f]	wherein mitigating a security issue of the unsecure network element includes starting, by the processing device, a virtual private network application, and wherein requesting the grant of access from the known network to the processing device is done over a virtual private network.
2	The method of claim 1, wherein access by the processing device to the known network is granted upon a combination of the requesting a grant of access from the known network to the processing device and a correct authorization credential presented by the processing device to	

Claim	Limitation	Claim Language
		the known network.
3		The method of claim 1, wherein the unsecure network element is an Internet of Things (IoT) device.
4		The method of claim 1, wherein administration of the processing device and the known network is controlled by a common administration entity.
5		The method of claim 1, the method further comprising: upon denying access to the known network by the processing device, providing a message to a user of the processing device requesting the user to access the known network via another remote network.
6	6[a]	The method of claim 1, the method further comprising: mitigating a security issue of the unsecure network element; and
	6[b]	based at least in part upon mitigating the security issue of the unsecure network element, requesting a grant of access from the known network to the processing device.
7		The method of claim 6, wherein mitigating the security issue of the unsecure network element includes connecting, by the processing device, the processing device to another remote network.
8	8[a]	The method of claim 1, the method further comprising: using, by the processing device, a network connection between the processing device and the known network; and
	8[b]	while using the network connection between the processing device and the known network, scanning, by the processing device, the remote network through which access to the known network is established, wherein the scanning is configured to identify an unsecure network element on the remote network.
9		The method of claim 8, the method further comprising: upon identifying an unsecure network element on the remote network while using the network connection between the processing device and the known

Claim	Limitation	Claim Language
		network, disconnecting, by the processing device, the processing device from the known network.
10		The method of claim 9, the method further comprising: upon disconnecting the processing device from the known network by the processing device, providing a message to a user of the processing device requesting the user to access the known network via another remote network.
11	11[pre]	A system comprising: one or more processing resources; a non-transitory computer-readable medium coupled to one or more processing resources, wherein the non-transitory computer-readable medium has stored thereon instructions that when executed by one or more processing resources cause the one or more processing resources to:
	11[a]	receive a request to access a known network from a known access device connected through a remote network,
	11[b]	wherein the known network is a private network that authorizes credentials associated with the known access device, and the remote network is external to the known network;
	11[c]	scan the remote network through which access to the known network is to be established, wherein the scanning is configured to identify an unsecure network element on the remote network;
	11[d]	based at least in part on identifying at least one unsecure network element on the remote network, deny access to the known network; and
	11[e]	based at least in part upon on failure to identify any unsecure network element on the remote network, request a grant of access from the known network to the processing device.

Claim	Limitation	Claim Language
	11[f]	wherein mitigating a security issue of the unsecure network element includes starting, by the processing device, a virtual private network application, and wherein requesting the grant of access from the known network to the processing device is done over a virtual private network-
12		The system of claim 11, wherein access to the known network is granted upon a combination of the requesting a grant of access from the known network to the processing device and a correct authorization credential presented by the processing device to the known network.
13		The system of claim 11, wherein the unsecure network element is an Internet of Things (IoT) device.
14	14[pre]	A non-transitory computer-readable storage medium embodying a set of instructions, which when executed by one or more processing resources of a computer system, causes the one or more processing resources to perform a method comprising:
	14[a]	receiving, by a processing device, a request to access a known network from a known access device connected through a remote network,
	14[b]	wherein the known network is a private network that authorizes credentials associated with the known access device, and the remote network is external to the known network;
	14[c]	scanning, by the processing device of the known access device, the remote network through which access to the known network is to be established, wherein the scanning is configured to identify an unsecure network element on the remote network;
	14[d]	based at least in part on identifying at least one unsecure network element on the remote network, denying access to the known network; and

Claim	Limitation	Claim Language
	14[e]	based at least in part upon on failure to identify any unsecure network element on the remote network, requesting a grant of access from the known network to the processing device.
	14[f]	wherein mitigating a security issue of the unsecure network element includes starting, by the processing device, a virtual private network application, and wherein requesting the grant of access from the known network to the processing device is done over a virtual private network-
15	The non-transitory computer-readable storage medium embodying the set of instructions of claim 14, which when executed by one or more processing resources of the computer system, causes the one or more processing resources to perform the method further comprising: upon denying access to the known network by the processing device, providing a message to a user of the processing device requesting the user to access the known network via another remote network.	
16	16[a]	The non-transitory computer-readable storage medium embodying the set of instructions of claim 15, which when executed by one or more processing resources of the computer system, causes the one or more processing resources to perform the method further comprising: mitigating a security issue of the unsecure network element; and
	16[b]	based at least in part upon mitigating the security issue of the unsecure network element, requesting a grant of access from the known network to the processing device.
17	17[a]	The non-transitory computer-readable storage medium embodying the set of instructions of claim 15, which when executed by one or more processing resources of the computer system, causes the one or more processing resources to perform the method further comprising: using a network connection between the processing device and the known network; and

Claim	Limitation	Claim Language
	17[b]	while using the network connection between the processing device and the known network, scanning the remote network through which access to the known network is established, wherein the scanning is configured to identify an unsecure network element on the remote network.
18	The non-transitory computer-readable storage medium embodying the set of instructions of claim 14, which when executed by one or more processing resources of the computer system, causes the one or more processing resources to perform the method further comprising: upon identifying an unsecure network element on the remote network while using the network connection between the processing device and the known network, disconnecting the processing device from the known network.	

I. INTRODUCTION

The Board should cancel the '902 patent's claims because they issued solely due to Examiner error. Twice during prosecution, the Examiner rejected the independent claims over Loza, Bansal, and Dupont, and rejected the original dependent claims 8/18—which related to using virtual private networks (“VPN”)—over those references plus Bareket. Yet later during prosecution, the Examiner said that incorporating those rejected claims 8/18 into the independent claims would make them allowable. The applicant did so, and the Examiner allowed the amended independent claims because “the prior art of record fails to teach” that same VPN limitation—forgetting the Examiner's own prior findings that Bareket taught it. Because that limitation and all others were in the prior art, as the Examiner originally found, the claims should not have issued.

Separately, the combination of Mishaev and Schwartz—prior art that was never considered by the Office—renders all claims unpatentable. Accordingly, Petitioner respectfully requests cancellation of all claims of the '902 patent.

II. MANDATORY NOTICES

A. Real Party-in-Interest

Netskope, Inc. is the sole real party-in-interest.

B. Related Matters

Patent Owner originally asserted the '902 patent against Petitioner in the United States District Court for the Northern District of California, Case No. 4:25-cv-02360-HSG. That claim has now been severed into Case No. 4:26-cv-08886-HSG (the “parallel litigation”).

C. Counsel and Service Information

Lead Counsel: Thomas N. Millikan (Reg. No. 72,316).

Back-up counsel: Joseph P. Reid (Reg. No. 72,317), Andrew Klein (*pro hac vice* forthcoming), and Lu Ling (Reg. No. 78,121).

These attorneys can be reached by mail at Sheppard, Mullin, Richter & Hampton LLP, 12275 El Camino Real, Suite 100, San Diego, California, 92130, by phone at (858) 720-8900, and by fax at (858) 509-3691.

Petitioner consents to electronic service. All services and communications to the attorneys listed above may be sent to: LegalTm-NetskopeFortinetII-IPRs@sheppard.com.

A Power of Attorney for Petitioner has been filed.

D. Fees

Petitioner paid the required fees. The Office is authorized to charge any fee deficiency, or credit any overpayment, to Deposit Account No. 50-4561.

III. IPR REQUIREMENTS

A. Standing

The '902 patent is available for IPR. Petitioner is not barred from challenging the claims.

B. Challenged Claims: 1-18

C. Grounds

Ground	Basis	References	Claims
1	§103	Loza, Bansal, Dupont, Bareket	1-4, 6, 8-9, 11-14, 16-18
2	§103	Loza, Bansal, Dupont, Bareket, Sahay	5, 7, 10, 15
3	§103	Mishaev, Schwartz	1-18
4	§103	Mishaev, Schwartz, Durbin	1-18

All references are prior art. The '902 patent's earliest claimed priority date is February 25, 2021. Loza published December 15, 2005; Bansal was filed October 30, 2019; Dupont published December 10, 2009; Bareket published July 26, 2018; Sahay issued April 22, 2014; Mishaev published July 30, 2020; Schwartz issued December 3, 2019; and Durbin published December 17, 2015.

Petitioner also relies on the declaration of Dr. Michael Franz (Ex-1003), a distinguished professor and expert of the relevant field (*see* Ex-1004).

D. Discretionary Denial Is Unwarranted

Discretionary denial is unwarranted because:

- 1) There are no settled expectations. The '902 patent issued only two years ago (February 27, 2024). Additionally, the scope of claims changed less than two months ago (September 8, 2026) when the Office granted patentee's Certificate of Correction ("CoC"). (Ex-1002, 1.)
- 2) No schedule is set in the parallel litigation.
- 3) Petitioner has not taken inconsistent positions on claim construction—indeed, claim construction has not begun in the parallel litigation.
- 4) Netskope is a U.S.-based cloud security company.
- 5) The Examiner made a material error under *Advanced Bionics, LLC v. Med-El Electromedizinische Geräte GmbH*, IPR2019-01469, Paper 6 (PTAB Feb. 13, 2020) (precedential). As detailed in Section V.B, the Examiner twice found that Bareket disclosed element 1[f], yet never addressed that finding when later allowing the claims. (Ex-1002, 46; *see Eden Park Illumination, Inc. v. Neister*, IPR2023-00695, Paper 16 at 17-19 (PTAB Sept. 19, 2023) (finding material error where Examiner evaluated a reference's teachings against dependent claims but failed to carry those teachings forward when assessing the limitation that became the basis for allowing the independent claim);

CSPC Pharm. Grp. Ltd. v. Ipsen Biopharm Ltd., IPR2025-00505, Paper 11 at 3 (Director Jul. 16, 2025) (referring petition based on evidence of material error where Examiner overlooked teachings of prior art that previously served as basis of rejection).) Here, rather than overlook a teaching, the Examiner found Baraket taught a limitation, proposed moving that *exact* limitation into the independent claims, then allowed the claims on the premise that no prior art teaches it. That is clear error.

IV. BACKGROUND

A. Remote Network Access

For decades, organizations controlled access to their computing resources by physically securing their networks and requiring users to be on-premises and use passwords to connect. (Ex-1009, ¶0002.) That model was displaced as cloud computing and remote connectivity matured: employees and other users started accessing organizational networks and services from off-site locations. (*Id.*, ¶¶0003-04.) Systems implementing remote access used established methods, including VPN and dialup connections, integrated with wired and wireless local access. (Ex-1007, ¶0005.)

By 2016, telework and remote access were ubiquitous, and it was well-understood that telework technologies should be secured against the assumption that external, uncontrolled networks and devices “contain hostile threats that will attempt to gain access to the organization’s data and resources,” and that communications over such networks are “susceptible to eavesdropping, interception, and modification.” (Ex-1015, 8.; Ex-1003, ¶45; Ex-1009, ¶¶0005-07.)

B. Network Access Control

Given such security gaps, it thus became standard practice to evaluate a device’s security posture, or the security of the network through which it was connecting, before granting that device access to a protected network rather than relying on authentication alone. (Ex-1015, 23.) This scan-before-access approach was implemented in numerous network-access-control products and systems well before the challenged patent, in which a connecting device or its network would be assessed for vulnerabilities, and access would be granted, denied, or conditioned accordingly. (Ex-1005, ¶¶0040-41; Ex-1007, ¶¶0005-08, ¶0060; Ex-1009, ¶0009; Ex-1010, Figs. 2, 5; Ex-1003, ¶46.)

C. Insecure IoT Devices

The proliferation of Internet of Things (“IoT”) devices—e.g., internet-connected cameras, printers, and thermostats—also created network

vulnerabilities: being “notorious for poor security” and often running on default usernames and passwords, IoT devices became common vectors for malware, DDOS attacks, and data theft undetectable by traditional point security solutions. (Ex-1006, ¶0003.) Thus, any network containing such IoT devices faced materially elevated risk, making their detection on a network a known, sensible precondition before trusting that network for sensitive communications (e.g., network scanning, fingerprinting, etc.). (*Id.*, Abstract, ¶0034; Ex-1003, ¶47.)

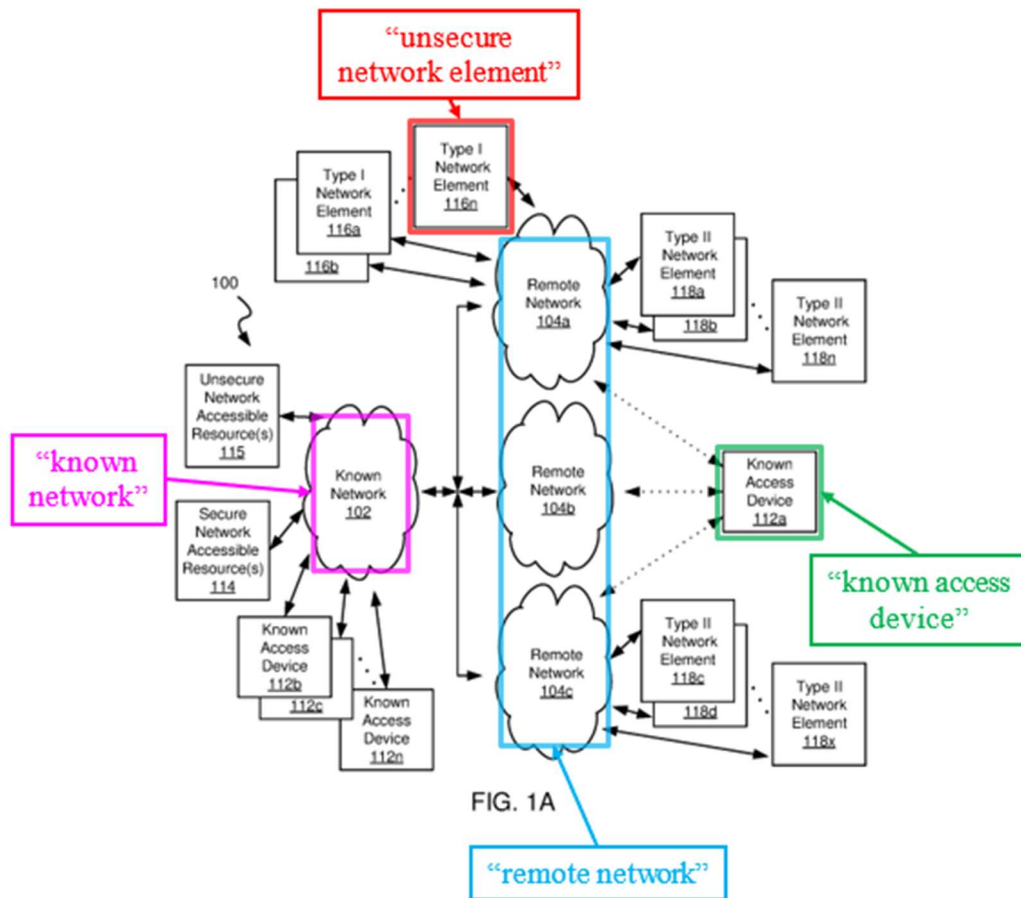
D. Virtual Private Networks

A VPN was a well-known, common mechanism for establishing a secure, encrypted channel between a client and remote network gateway, particularly where the device’s local network connection could not be trusted. (Ex-1007, ¶0005.) While VPNs were traditionally manually initiated, automating that process was common before the challenged patent. (Ex-1011, Fig. 4; Ex-1018, Abstract, ¶0066; Ex-1003, ¶48.)

V. ’902 PATENT

A. Alleged Invention

Years later, the ’902 patent recognized what was already known in the art. It describes “identifying potential threats included in a remote network by a network access device prior to requesting access to a known secure network via the remote network.” (Ex-1001, 1:43-47.) Fig. 1A is reproduced and annotated below.



The '902 patent describes familiar components in a typical telework setting. (*Id.*, 2:36-50.) Fig. 1A depicts a “known access device” (green)—e.g., a “corporate access device”—connected to at least one “remote network” (blue)—e.g., a “home network.” (*Id.*, 2:46-50, 3:8-10, 8:8-10.) Upon request, the known access device may be granted access to a “known network” (pink)—e.g., a “corporate network”—and its “resource(s)” (unannotated) through one of the remote networks so long as it contained no “unsecure network element” (red). (*Id.*, 8:11-20, 8:63-67, 9:39-45, 10:7-14, 13:36-47.)

The known access device determines whether a selected remote network contains such an unsecure network element by scanning that network. (*Id.*, 9:28-37.) If none are identified, the known access device requests a grant of access to the known network; otherwise, the device instead attempts mitigation (e.g., starting a VPN), and requests access only if that mitigation succeeds, otherwise denying itself access and potentially messaging the user if it fails. (*Id.*, 9:58-10:6, 11:4-27; 16:12-22; Ex-1003, ¶¶33-36.)

B. Prosecution History

The Examiner issued two successive Office Actions, each rejecting original claims 1-4, 6, 8-10, 12-15, and 17-20 over Loza, Bansal, and Dupont, original claims 5, 7, 11, and 16 in further view of Sahay, and, notably, original claims 8 and 18 in further view of Bareket, as illustrated below. (Ex-1002, 133-156, 180-199.)

However, Bareket teaches wherein mitigating the security issue of the unsecure network element includes starting, by the processing device, a virtual private network application, and wherein requesting the grant of access from the known network to the processing device is done over a virtual private network (Par. [0066], As shown at 106, the probe agent 222 automatically initializes (invokes, launches) the VPN client 224 according to the determined accessibility, i.e. the probe

(Ex-1002, 154-55, 197-98.)

Despite these two rejections, the Examiner said that “bring[ing] in claim 8 into the independent claims” would result in “compact prosecution of the case”:

IPR2027-00011
Petition for *Inter Partes* Review
Of U.S. Pat. No. 11,916,902

From: Champakesan, Badri <Badri.Champakesan@USPTO.GOV>
Sent: Tuesday, November 29, 2022 8:19 AM
To: Doug Hamilton <DHamilton@hdciplaw.com>
Subject: RE: App. 17185542 (FORT-041900(20065))

If you can bring in claim 8 into the independent claims, we can proceed for compact prosecution of the case.

(*Id.*, 165.) Applicant declined. (*Id.*)

Following a RCE with immaterial amendments, the Examiner again indicated the claims would be allowable if claim 8 was incorporated into the independent claims.

Date of Interview: 20 October 2023

Issues Discussed:

Other

The examiner proposed to include claim 8 into the independent claims after discussing the prior arts of record in detail and updated search in response to the filed rce. The attorney obtained the client's approval the filed the same. Agreement reached.

(*Id.*, 49.) Applicant agreed, authorizing an Examiner's amendment to cancel original claims 8/18 and to amend the independent claims to recite those claims' "wherein" clauses directed to starting a VPN application and requesting access over a VPN (i.e., 1[f]/11[f]/14[f]). (*Id.*) The Examiner then granted allowance, finding the "prior arts of record fail to teach" the amended language. (*Id.*, 46.)

The claims that first issued omitted this VPN limitation. (Ex-1001, 18:41-44, 19:47-50; 20:15-18.). A recent CoC added it. (Ex-1002, 1)

VI. LEVEL OF ORDINARY SKILL

A POSITA at the '902 patent's priority date would have had at least a bachelor's degree in computer science, computer engineering, electrical engineering, or a related field, and at least two years of work or research experience with computer networks and computer network security. Work experience can substitute for formal education and vice versa. (Ex-1003, ¶25.)

VII. CLAIM CONSTRUCTION

The claims should be given their plain and ordinary meaning except:

A. “processing device”/“processing resource”

“[P]rocessing device”/“processing resource” as recited in claims 1/11/14 are means-plus-function terms under §112(f). They recite the nonce words “device” and “resource,” which simply refer to generic computing hardware that performs certain functions. (*See Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1350 (Fed. Cir. 2015).)

“Processing device”/“processing resource” perform the following functions:

(1) “receiving...a request to access the known network from a known access device connected through a remote network;” (2) “scanning...the remote network through which access to the known network is to be established...to identify an unsecure network element on the remote network;” (3) “denying...access to the known network” based on identifying an unsecure network element; (4)

“requesting a grant of access from the known network” based on failing to identify an unsecure network element and (5) “starting...a virtual private network application” and “requesting the grant of access from the known network...over a virtual private network.”

For “scanning,” the specification states: “Network element identification module 154 may use any process and/or circuitry known in the art for identifying network elements 116, 118 on the selected remote network 104.” (Ex-1001, 9:34-37.) For “receiving,” the specification states: “determin[ing] whether a request to access a known network is received” can be the result of the known access device “detect[ing]” the “preparing [of] an authorization credential.” (*Id.*, 12:57-64.) The specification also discloses that (1) network security devices can be implemented as “general-purpose computers...with appropriate software operable to perform the one or more security functions” or custom ASICs (*id.*, 3:59-64) and (2) “computer system 144 includes...one or more processing resources (e.g., processing circuitry 182)” and that “[n]on-limiting examples of processing circuitry 182 include, but are not limited to: Intel Quad-Core, Intel i3, Intel i5, Intel i7, Apple M1, AMD Ryzen, or AMD® Opteron® or Athlon MP® processor(s), Motorola® lines of processors, FortiSOC™ system on chip processors or other future processors” (*id.*, 11:30-44).

While Petitioner contends these structures are insufficient to comply with §112(f), the references relied upon in this Petition squarely teach or suggest the disclosed structures—as the Examiner repeatedly found during prosecution—mooting the need to construe the outer boundaries of these terms. (*See U.S. Surgical Corp. v. Ethicon, Inc.*, 103 F.3d 1554, 1568 (Fed. Cir. 1997) (holding claim construction is not necessary when it is not “directed to, or has been shown reasonably to affect, the determination of obviousness”).) But if the Board agrees there is “possibly insufficient corresponding structure in the specification, the Board must either (1) determine whether the claim is indefinite and then whether such indefiniteness renders it impossible to adjudicate a prior-art challenge on the merits, or (2) resolve the prior-art challenge to the patentability of the claims despite the potential indefiniteness of the means-plus-function term.” (*Sisvel Int’l S.A. v. Sierra Wireless, Inc.*, 82 F.4th 1355, 1370 (Fed. Cir. 2023).)

B. “providing a message to a user of the processing device requesting the user to access the known network via another remote network”

Printed matter has no patentable weight unless it is functionally or structurally related to the substrate that carries it. (*Praxair Distrib., Inc. v. Mallinckrodt Hosp. Prods. IP Ltd.*, 890 F.3d 1024, 1031-33 (Fed. Cir. 2018).) Under the printed matter doctrine, claims 5/10/15’s “providing a message to a user

of the processing device requesting the user to access the known network via another remote network,” and claims 16-17’s inclusion of the same by dependency, should be construed such that the content of the claimed “message” is not given patentable weight.

Here, claims 5/10/15 recite “providing a message to a user of the processing device” and then what that “message” should say—i.e., “requesting the user to access the known network via another remote network” is printed matter. The claims, however, do not recite anything to establish a functional relationship. At most, the claims recite conditions that must occur *before* the message is provided (i.e., “denying” or “disconnecting access”). This only explains what causes the “providing a message” and not what the “message” itself causes. Claims 16-17 are similarly silent. Accordingly, “requesting the user to access the known network via another remote network” should be afforded no patentable weight.

VIII. SPECIFIC GROUNDS

A. Ground 1: Loza with Bansal, Dupont, and Bareket Renders Claims 1-4, 6, 8-9, 11-14, and 16-18 Obvious

As the Office already found, claims 1-4, 6, 8-9, 11-14, and 16-18 are obvious over Loza with Bansal, Dupont, and Bareket. (Ex-1003, ¶53.)

1. Loza

Loza discloses a system and method for enforcing secure network connections for remote and mobile users. (Ex-1005, Abstract.) Loza provided “a method of providing a warning of an insecure network connection between a client device and a server.” (*Id.*, ¶0013, Fig. A (below).)

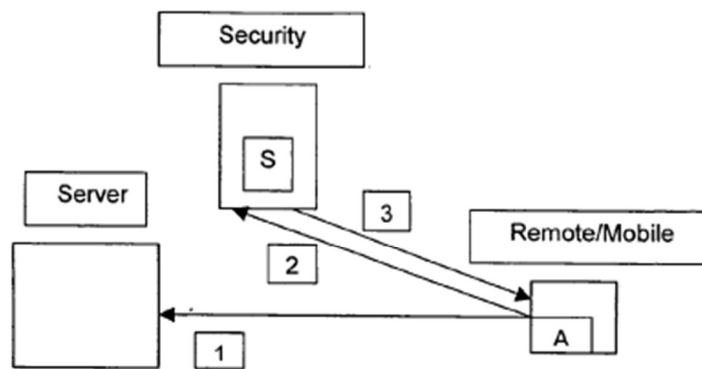


Figure A. Remote user establishing a network connection to a corporate server and requesting security scan on its network connectivity

When a remote user attempts to connect to a corporate server, an agent on the user’s machine connects to a security scanner, which assesses the security of the machine’s external network connectivity and identifies the number and severity of any discovered vulnerabilities. (*Id.*, ¶¶0040-41, ¶0048.) Based on a security policy, the agent can then notify the user that the connection is insecure or prevent the machine from establishing a network connection. (*Id.*, ¶0042.) An IT administrator can set the applicable security policy centrally, including triggering a

message instructing the user to install a required security measure before access is granted. (*Id.*, ¶¶0053; Ex-1003, ¶¶54-55.)

2. Bansal

Bansal discloses systems and methods for security and control of IoT and ZeroConf devices using cloud services. (Ex-1006, Abstract; Fig. 4 (below).)

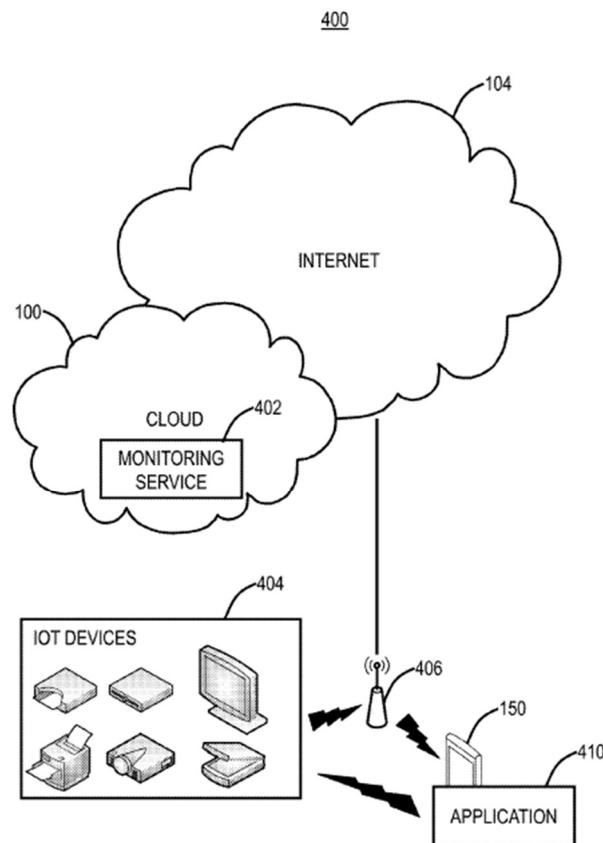


FIG. 4

An application running on a user's device operates in a promiscuous mode to look for vulnerable and compromised machines on the local network,

fingerprinting IoT and ZeroConf devices based on their static and dynamic behavior. (*Id.*, Abstract, Fig. 5 (below).) The application discovers hosts on the network and uses a cloud-based service to detect malicious IoT devices with known vulnerabilities. (*Id.*, ¶0014, Fig. 5; Ex-1003, ¶¶56-57.)

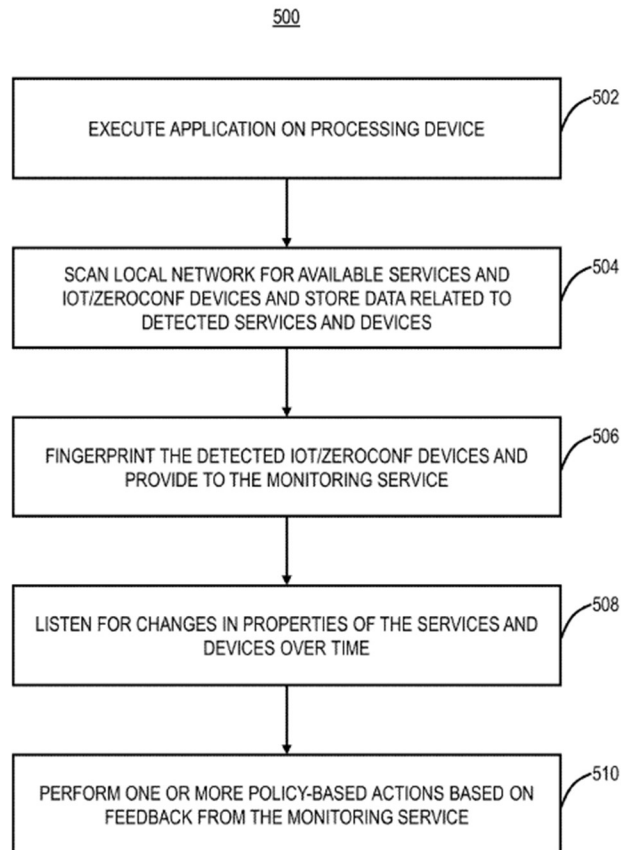
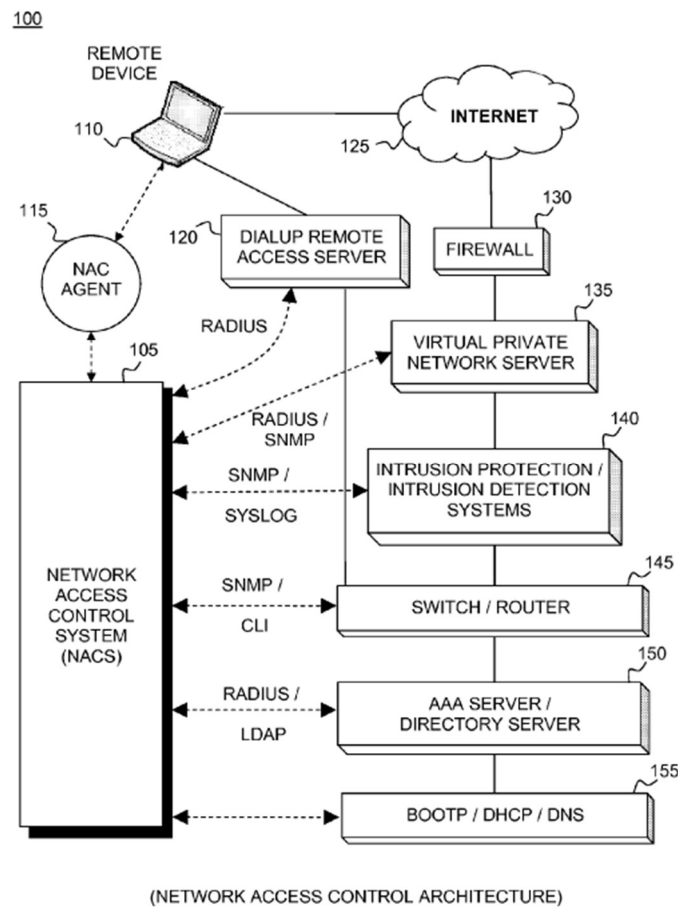


FIG. 5

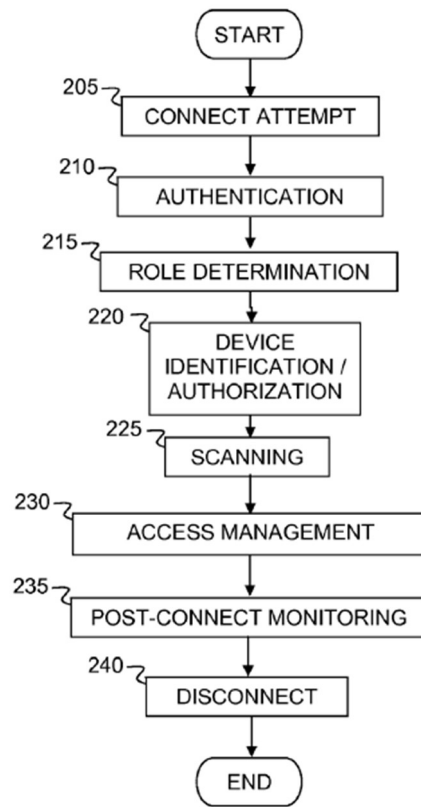
3. Dupont

Dupont discloses a network access control (“NAC”) system and method for devices connecting to a network using remote access control methods. (Ex-1007, Abstract; Fig. 1 (below).)



Dupont’s system automatically performs authentication, assessment, authorization, provisioning, and remediation of a connecting host by collecting information about the user and the host from sources, the remote access device, and an on-host agent,

builds a model of the host, and uses that model to govern the host's actual network access once it connects. (*Id.*, Abstract, Fig. 2 (below).)



(OPERATIONAL STAGES / PHASES)

FIG. 2

A successful vulnerability scan results in a host identity being created for the connecting device, after which the system removes the access-restricting filters for that session, effectively granting it network access. (*Id.*, ¶0060.) Once connected, ongoing passive monitoring happens, including periodic vulnerability scanning,

and if a vulnerability is discovered, the host is marked at-risk and either disconnected or has filters reapplied. (*Id.*, ¶0061; Ex-1003, ¶¶58-60.)

4. Bareket

Bareket discloses a method of automatically establishing a VPN over an unsecure wireless network. (Ex-1018, Abstract, Fig. 1 (below).)

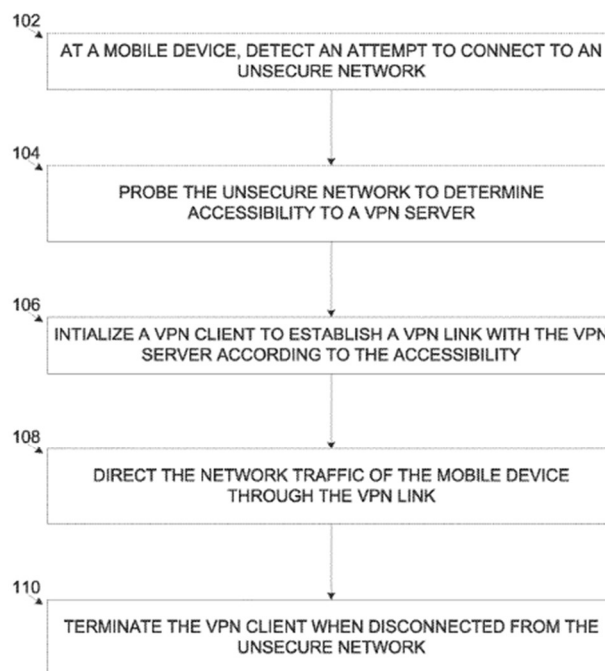


FIG. 1

A mobile device detects an attempt to connect to the internet via an unsecure wireless network and probes that network to determine whether a VPN server is accessible. (*Id.*, Abstract, ¶¶0060-61.) Based on that, the mobile device initializes a

VPN client, which establishes a VPN link to the VPN server over the network. (*Id.*, ¶0066.) The device then directs its traffic through that VPN and terminates the VPN client when disconnecting from the network. (*Id.*, Abstract, ¶0066; Ex-1003, ¶¶61-62.)

5. Combining Loza with Bansal, Dupont, and Bareket

As the Examiner found, a POSITA would have found it obvious to modify Loza using the teachings of Bansal, Dupont, and Bareket. (Ex-1002, 137-55.)

a. A POSITA Would Have Used Bansal’s Unsecure Element Identification in Loza

As the Examiner correctly found, Loza discloses scanning a remote network and denying access to a known network if vulnerabilities are found, but does not specify those vulnerabilities relate to an unsecured network element—e.g., IoT device. (Ex-1002, 138.) Bansal, however, discloses an “application that discovers all hosts on the network and uses a cloud service such as via a cloud-based system to detect potentially malicious IoT devices with known vulnerabilities.” (*Id.*, citing Ex-1006, ¶0014.)

The Examiner found Loza and Bansal were analogous references “as they both pertain to...scanning a network and identifying vulnerabilities,” and it “would have been obvious...to modify Loza using the method of identifying an unsecured network element as taught by of Bansal.” (Ex-1002, 138.) The stated rationale was

that “[s]uch modification enables protecting the known network since attackers can gain access to secured networks through an unsecured network element on a remote network that a user is using to connect to the secured network.” (*Id.*) The Examiner stated that “[t]he combination of Loza and Bansal teaches a method of scanning a network and identifying an unsecure element.” (*Id.*, 139; Ex-1003, ¶¶64-66.)

b. A POSITA Would Have Modified Loza-Bansal to Grant Access When No Unsecure Network Element Is Found and to Make Mitigation Decisions

As the Examiner correctly found, Loza-Bansal meets scanning a remote network to identify an unsecure network element as a basis for denying access but does not address what should happen if no vulnerabilities are discovered—i.e., when no unsecure network element is found. (Ex-1002, 139.) Dupont, however, discloses that a “successful scan” results in a “host identity” being created and any access-restricting filters being removed for that session, effectively granting the host network access. (*Id.*, citing Ex-1007, ¶0060.)

The Examiner found that Loza-Bansal-Dupont were analogous references “as they pertain to a method of scanning a network and identifying vulnerabilities,” and that it “would have been obvious...to modify the combination of Loza and Bansal using the method of requesting access to a network after the scanning

confirms that there are no unsecured elements in the network.” (Ex-1002, 139.) The stated rationale was that “[s]uch modification will reduce network threats since the network where remote access is requested from is confirmed to be secure.” (*Id.*)

The Examiner found the Loza-Bansal-Dupont combination “teaches [a] method of mitigating security vulnerabilities of unsecured network.” (*Id.*, 154.) As the Examiner found, it would have been obvious “to further modify the combined teaching of Loza, Bansal, Dupont in claim 1 by using the method of mitigating vulnerabilities and requesting access as taught by Dupont” to “enable to selectively allow users to connect to a known network if vulnerabilities are mitigated and not permanently block them.” (*Id.*, 142; Ex-1003, ¶¶67-70.)

c. A POSITA Would Have Modified Dupont to Perform Mitigation Using a VPN

The Examiner also correctly found that Loza-Bansal-Dupont described mitigating a detected security issue and, following that mitigation, requesting renewed access to the known network but did not specify starting a VPN application as the mitigation mechanism or routing the renewed access request over a VPN. (Ex-1002, 154.) Bareket closes that gap by, upon detecting an unsecure wireless network, a probe agent automatically initializes a VPN client, which establishes a VPN link to a VPN server over the unsecure wireless network

and directs the device's network traffic through that encrypted link. (*Id.*, 154-55 citing Ex-1018, ¶0066.)

The Examiner confirmed it “would have been obvious...to modify the combined teaching of Loza, Bansal and Dupont...by starting a VPN application and requesting access through the VPN application as taught by Bareket.” (Ex-1002, 155.) The stated rationale was that “[s]uch modification will make the known network more secure since a VPN provides a secure encrypted connection.” (*Id.*; Ex-1003, ¶¶71-73.)

6. Element-by-Element Analysis

a. 1[pre]/11[pre]/14[pre]

If the preamble is limiting, the Examiner correctly found Loza disclosed or rendered it obvious.¹ Loza disclosed “a method of providing a warning of an insecure network connection between a client device and a server.” (Ex-1002, 147 citing Ex-1005, ¶0013.) Loza also disclosed “a system for enforcing secure network connection for remote/mobile users comprises.” (Ex-1002, 144 citing Ex-

¹ The CoC changed “a processing resource” to “one or more processing resources.” (Ex-1002, 1.) This does not impact the analysis. *See Convolv, Inc. v. Compaq Computer Corp.*, 812 F.3d 1313, 1321 (Fed. Cir. 2016).

1005, ¶10.) Loza further disclosed “one or more processing resources” by disclosing “an agent installed on a machine connected to the network and accepting connections from remote users.” (Ex-1002, 144 citing Ex-1005, ¶10.)

The Examiner also correctly found Bansal taught the other recited components (e.g., “non-transitory computer-readable medium coupled to the processing resource”) by disclosing “[m]oreover, some exemplary embodiments may include a non-transitory computer-readable storage medium having computer readable code stored thereon for programming a computer, server, appliance, device, processor, circuit, etc. each of which may include a processor to perform functions as described and claimed herein.” (Ex-1002, 145, 148 citing Ex-1006, ¶54; Ex-1003, ¶¶74-76.)

b. 1[a]/11[a]/14[a]

As the Examiner correctly found, Loza disclosed “receiving, by a processing device, a request to access a known network” by disclosing “a program or agent on the remote user’s machine (i.e., processing device) may automatically connect to a security scanner upon the user’s attempt (i.e., request) to connect to the corporate server.” (Ex-1002, 137 citing Ex-1005, ¶0048.)

The Examiner correctly found Loza disclosed “from a known access device connected through a remote network.” In the Advisory Action, the Examiner found Loza’s scanned network is “remote”:

The examiner strongly refutes the arguments. The argument’s main allegation is that the other scanned external network is not a remote network. The network connected machine starts scanning the external (i.e., remote) network once it gets the external (i.e., remote) IP address as envisaged in paras. [0038-42]. The network connected machine is not responsible for the security of, or not known or not governed by the external network (i.e., remote) as indicated by the application’s spec....The arguments do not indicate why an external network is not considered to be a ‘remote’ network.

(Ex-1002, 118.) The Examiner further found “a local/external network whose channel is sought by a connecting device to connect to the external resource(s), shall consider the local network as remote,” because “the security of such a network connection is not known, not governed nor controlled by the connecting entity, as the entity seeks the external IP” and “[t]he entity (network connected machine), shall scan the security of the its external network, is typically ‘remote’ to such a network as envisaged in the prior art.” (*Id.*)

Additionally, the Examiner identified Loza’s “network connected machine” as the device scanning the remote network. That machine is a “known access device,” which the ’902 patent describes as “a device that includes a module governing access to a known network via a remote network.” (Ex-1001, 3:10-12.)

The “network connected machine” has an “agent (A) installed on [the] machine that is connected to the Internet/network” that causes the network server to respond to a network connection request from the network connected machine, after which the “[n]etwork connected machine start[s] assessing security of its own external network connectivity by using its built-in scanner.” (Ex-1005, ¶¶0038-40.) Depending on a policy, the agent may then “notify a user that this particular location that is used to connect to the Internet/network is insecure, or prevent user’s machine to establish any network connection.” (Ex-1005, ¶0042; Ex-1003, ¶¶77-82.)

c. 1[b]/11[b]/14[b]

As shown in the last element, the Examiner correctly found Loza disclosed or rendered obvious that “the remote network is external to the known network.” Briefly, in the Advisory Action, the Examiner equated “external” with “remote,” explaining “[t]he network connected machine starts scanning the external (i.e., remote) network once it gets the external (i.e., remote) IP address” and that the network connected machine’s external network is “typically remote.” (Ex-1002, 118.) Loza’s own description of its invention confirms this as “equally applicable to other types of networks in which security breaches on connections from outside of a particular known network could be a concern,” treating the connecting

machine's network and the "particular known network" it seeks to reach as separate, external environments. (Ex-1005, ¶0049.)

While the Examiner did not expressly address the remaining limitation ("wherein the known network is a private network that authorizes credentials associated with the known access device"), Loza disclosed it or rendered it obvious. In Loza, a remote machine first connected to a security scanner before obtaining "permission to connect to the corporate network server" given "by way of a unique key to the remote machine, or a message to the corporate server to accept a connection or another method that would fulfill the function of signalling permission of the remote machine to connect to the corporate system." (Ex-1005, ¶0048). These are well-known forms of authorizing credentials the corporate network employs to authorize access, associated with the specific remote machine. Corporations and similar entities typically run their own private networks ("known networks")—for at least security reasons, as Loza recognizes (Ex-1005, ¶¶0002-04)—and control access to them by requiring credentials to connect. Often, a teleworker uses a "known device" to connect "back" to the known corporate network—also called the "corporate environment" or "corporate network" in Loza (*id.*, ¶0004, ¶0015)—where both the known device and the known network are under the control of the corporation's IT administration staff, so that arranging for

such a roaming device to be associated with credentials enabling it to connect “back” is straightforward and obvious. (Ex-1003, ¶¶83-88.)

d. 1[c]/11[c]/14[c]

As the Examiner correctly found, Loza disclosed “scanning, by the processing device of the known access device, the remote network through which access to the known network is to be established” by disclosing that “[n]etwork connected machine starts assessing security of its own external network connectivity by using its built-in scanner (S).” (Ex-1002, 137 citing Ex-1005, ¶0040.) Loza also disclosed “wherein the scanning is configured to identify an unsecure network element on the remote network” by disclosing that “[t]he built-in security scanner identifies a number and a severity level of discovered, if any, security vulnerabilities for this particular machine’s external network connection.” (Ex-1002, 137-38 citing Ex-1005, ¶0041.)

Additionally, Loza taught a “processing device of the known access device” in the form of a network-connected machine with an agent where the Agent is software and it would have been obvious to a POSITA that there is a processing device on which the software runs. *See* 1[a-b]/11[a-b]/14[a-b]; *supra* VIII.A.6.b; (Ex-1005, ¶0038, ¶0040; Ex-1003, ¶¶89-93.)

e. 1[d]/11[d]/14[d]

As the Examiner correctly found, Loza discloses that, “[b]ased on a security policy, an agent (A) installed on this particular machine that is connected to the Internet/network may notify a user that this particular location that is used to connect to the Internet/network is insecure, or prevent user’s machine to establish any network connection.” (Ex-1002, 138 citing Ex-1005, ¶0042.) The Examiner found that Loza discloses “scanning a remote network for vulnerabilities and denying access to a known network if vulnerabilities are found” but not that the vulnerabilities “relate to at least one unsecured network element.” (*Id.*)

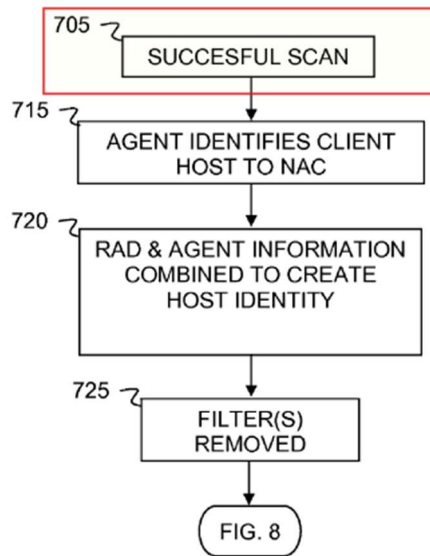
Thus, the Examiner relied on Bansal’s disclosure that “the application discovers all hosts on the network and uses a cloud service...to detect potentially malicious IOTs with known vulnerabilities.” (Ex-1002, 138 citing Ex-1006, ¶0014.)

As noted *supra* Section VIII.A.5.a, the Examiner confirmed that a POSITA would have been motivated to combine Loza and Bansal. (Ex-1002, 139; Ex-1003, ¶¶94-98.)

f. 1[e]/11[e]/14[e]

As the Examiner correctly found, Dupont taught “based at least in part upon on failure to identify any unsecure network element on the remote network” by

disclosing a “successful scan” in block 705 in Fig. 7, reproduced and annotated below. (Ex-1002, 139 citing Ex-1007, Fig. 7.)



(Ex-1003, ¶100 (annotating Ex-1007, Fig. 7).)

As the Examiner correctly found, Dupont also taught “requesting a grant of access from the known network to the processing device” by disclosing that “[a] successful scan 705 is accompanied by host characteristics that identify the client host to NACS 715”—which the Examiner said is “requesting access.” (Ex-1002, 139 citing Ex-1007, ¶0060.)

As noted in Section VIII.5.b, the Examiner confirmed that a POSITA would have been motivated to combine Loza, Bansal, and Dupont. (Ex-1002, 139; Ex-1003, ¶¶99-103.)

g. 1[f]/11[f]/14[f]

As the Examiner correctly found, Bareket disclosed these limitations. Baraket disclosed that “the probe agent 222 automatically initializes (invokes, launches) the VPN client 224 according to the determined accessibility, i.e. the probe agent 222 invokes the VPN client 224 in case the accessibility is determined valid (feasible)” and that “[t]he VPN client 224 then establishes the VPN link with the VPN server 214 over the unsecure wireless network 210.” (Ex-1002, 154-55 citing Ex-1018, ¶0066.)

As noted in Section VIII.5.c, the Examiner confirmed that a POSITA would have been motivated to combine Loza, Bansal, Dupont, and Bareket. (Ex-1002, 155; Ex-1003, ¶¶104-09.)

h. 2/12

As the Examiner correctly found, Dupont taught “wherein access by the processing device to the known network is granted” by disclosing that “NACS commands the RAD to remove the filters for the affected session 725.” (Ex-1002, 140 citing Ex-1007, ¶0060.) Dupont also taught “upon a combination of the requesting a grant of access from the known network to the processing device” by disclosing that “[a] successful scan 705 is accompanied by host characteristics that identify the client host to NACS.” (Ex-1002, 140 citing Ex-1007, ¶0060.) Dupont

further taught “and a correct authorization credential presented by the processing device to the known network” by disclosing that “[i]f authentication 310 is successful 325, the process flows to capture user identity 335, capture RAD location 340, and determine authorization 345” and “RADIUS is used to provide authentication for connecting users and to integrate RAD with NACS.” (Ex-1002, 140 citing Ex-1007, ¶0047.)

It would have been obvious to a POSITA “to further modify the combined teaching of Loza, Bansal, and Dupont in claim 1 by using the method of presenting authorization credential as taught by Dupont” to “reduce the threat to the known network since both the user/device and the network from which connection is requested from are authenticated.” (Ex-1002, 140; Ex-1003, ¶¶110-15.)

i. 3, 13

As the Examiner correctly found, Bansal taught that “[t]he application discovers all hosts on the network and uses a cloud service such as via a cloud-based system to detect potentially malicious IOTs with known vulnerabilities.” (Ex-1002, 140-41 citing Ex-1006, ¶0014.) The Examiner confirmed that it would have been obvious to a POSITA “to further modify the combined teaching of Loza, Bansal, and Dupont in claim 1 by using the method of detecting an unsecured IoT device in a network as taught by Bansal” to prevent threats from IoT devices that

are abundant in may remote works which in turn will increase the security of a known network. (Ex-1002, 140; Ex-1003, ¶¶116-19.)

j. 4

As the Examiner correctly found, Loza disclosed “wherein administration of the processing device and the known network” by disclosing that “the IT administrator...by setting the policy could require it prior to granting access”—which the Examiner equated to “administering the processing device”—where the set policy would “automatically prevent access further into a network”—which the Examiner equated to “administration of network.” (Ex-1002, 141 citing Ex-1005, ¶0053.) Loza further disclosed “is controlled by a common administration entity” by its reference to the IT administrator. (Ex-1002, 141; Ex-1005, ¶0019, ¶¶0052-53; Ex-1003, ¶¶120-23.)

k. 6[a]/6[b]/16[a]/16[b]

As the Examiner correctly found, Dupont disclosed “mitigating a security issue of the unsecure network element” by disclosing that “[u]sers may be required 620 to disconnect to remediate 630 or remediate from the restricted network while still connected 625.” (Ex-1002, 142 citing Ex-1007, ¶0058.) Dupont also disclosed “based at least in part upon mitigating the security issue of the unsecure network element” by disclosing “[o]nce remediation is complete.” (Ex-1002, 142 citing Ex-

1007, ¶0058.) Dupont further disclosed “requesting a grant of access from the known network to the processing device” by disclosing that “[i]f the user does disconnect to remediate, he then returns to the steps of FIG. 2 with another connect attempt”—which the Examiner equated to “requesting grant of access.” (Ex-1002, 142 citing Ex-1007, ¶0058.)

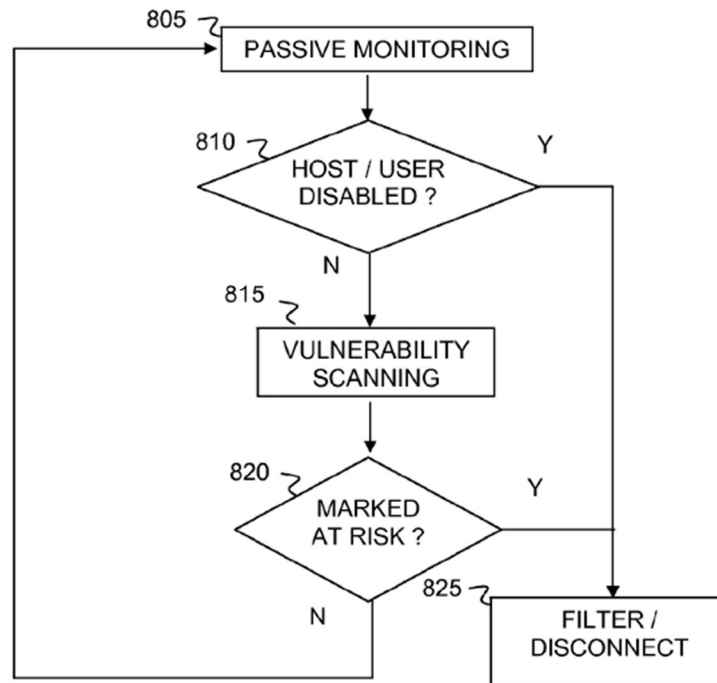
As noted in Section VIII.5.b, it would have been obvious to a POSITA “to further modify the combined teaching of Loza, Bansal and Dupont in claim 1 by using the method of mitigating vulnerabilities and requesting access as taught by Dupont” to “enable to selectively allow users to connect to a known network if vulnerabilities are mitigated and not permanently block them.” (Ex-1002, 142; Ex-1003, ¶¶124-29.)

I. 8[a]/8[b]/17[a]/17[b]

As the Examiner correctly found, Dupont taught “using, by the processing device, a network connection between the processing device and the known network” by disclosing that “NACS commands the RAD to remove the filters for the affected session 725”—which the Examiner equated to “using network connection.” (Ex-1002, 142-43 citing Ex-1007, ¶0058.) Dupont also taught “while using the network connection between the processing device and the known network” by disclosing Fig. 8 (below) which “is a simplified flow chart of an

embodiment of post-connect monitoring 800.” (Ex-1002, 143 citing Ex-1007, ¶0061.)

800



(Ex-1007, Fig. 8). Dupont further taught (i) “scanning, by the processing device, the remote network through which access to the known network is established” by disclosing that “[p]assive monitoring 805 determines the client state 810 within NACS and involves optional periodic vulnerability scanning 815 where a client may be marked at-risk 820” and (ii) “wherein the scanning is configured to identify an unsecure network element on the remote network” by disclosing that “if a client

fails a security compliance scan or is found to be disabled 810, it proceeds to be filtered or disconnected 825.” (Ex-1002, 143 citing Ex-1007, ¶0061.)

The Examiner confirmed that it would have been obvious to a POSITA “to further modify the combined teaching of Loza, Bansal and Dupont in claim 1 by using the method of scanning a network after access has been granted as taught by Dupont” to “further reduce threat to a known network by continuously monitoring a remote network and identifying potential vulnerabilities that might arise after access has been granted.” (Ex-1002, 143; Ex-1003, ¶¶130-36.)

m. 9/18

As the Examiner correctly found, Dupont taught “upon identifying an unsecure network element on the remote network while using the network connection between the processing device and the known network” by disclosing that “[p]assive monitoring 805 determines the client state 810 within NACS and involves optional periodic vulnerability scanning 815 where a client may be marked at-risk 820.” (Ex-1002, 144 citing Ex-1007, ¶0061.) Dupont also taught “disconnecting, by the processing device, the processing device from the known network” by disclosing that “[i]f a client is marked at risk, it may be disconnected” or “if a client fails a security compliance scan or is found to be disabled 810, it proceeds to be...disconnected 825.” (Ex-1002, 144 citing Ex-1007, ¶0061.)

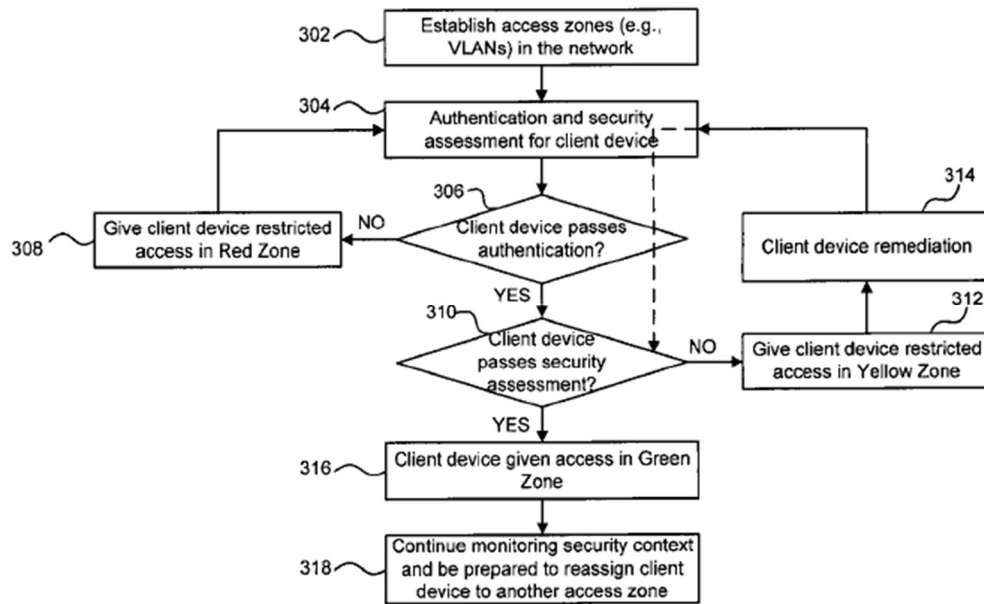
The Examiner confirmed that it would have been obvious to a POSITA “to further modify the combined teaching of Loza, Bansal and Dupont of claim [8] by using the method of disconnecting a device from a known network when vulnerabilities are discovered as taught by Dupont” to “reduc[e] threats to known network by isolating vulnerable devices.” (Ex-1002, 144; Ex-1003, ¶¶137-41.)

B. Ground 2: Loza with Bansal, Dupont, Bareket, and Sahay Renders Claims 5, 7, 10, and 15 Obvious

As already confirmed by the Office, claims 5, 7, 10, and 15 are obvious over Loza-Bansal-Dupont-Bareket with Sahay. (Ex-1002, 133-156, 180-199; Ex-1003, ¶142.)

1. Sahay

Sahay disclosed a technique for providing secure network access by establishing a plurality of access zones in a network, in which client devices assigned to different access zones have different access privileges and are isolated from one another. (Ex-1008, Abstract, Fig. 3 (below).)



(*Id.*, Fig. 3.)

A client device is assigned to one of the access zones based on an assessment of a security context associated with the device and its connection to the network. (*Id.*, Abstract.) A client device may continue to be monitored for its security context after connecting, and that an access controller may reassign the client device to another access zone or VLAN based on triggering events, including a change in the security context, a security violation by the client device, a security violation detected in the network, or an operator-initiated request to reassign the client device. (*Id.*, 3:37-44; Ex-1003, ¶¶143-44.)

2. Combining Loza, Bansal, Dupont, and Bareket with Sahay

A POSITA would have found it obvious to modify the teachings of Loza, Bansal, Dupont, and Bareket with Sahay, as detailed below.

a. A POSITA Would Have Modified the Denial/Disconnection Response to Redirect Access to Another Remote Network

As the Examiner correctly found, the combined teaching of Loza, Bansal, and Dupont described denying access to the known network upon detecting an unsecure element and disconnecting the processing device from the known network upon later detecting an unsecure element during an established connection, together with providing the user a message following denial or disconnection. (Ex-1002, 151-53.) However, that combination did not specify that the message to the user requests the user to access the known network via another remote network, nor that mitigating the security issue includes connecting the processing device to another remote network. (*Id.*) Sahay closes that gap by disclosing that, upon a triggering event such as a security violation or a change in security context, the access controller reassigns the client device to another access zone or VLAN. (Ex-1002, 151-53 citing Ex-1008, 3:37-44.)

The Examiner correctly found it “would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to

modify the combined teaching of Loza, Bansal, and Dupont using a method of prov[id]ing a message to a user requesting to access a known network via another network as taught by Sahay.” (Ex-1002, 151-52.) The stated rationale was that “[s]uch modification helps reduce threat[s] to a known network by preventing access from a vulnerable remote network.” (Ex-1002, 152.)

While the Examiner did not refer to Bareket in his analysis of Sahay because the Examiner’s rejection based on Bareket was for a set of dependent claims that were moved into the independent claims via amendment *after* the Examiner’s rejections. Still, a POSITA would have found it obvious to combine Sahay with Loza-Bansal-Dupont-Bareket because combining Sahay’s access-zone/VLAN reassignment teaching with the VPN-based mitigation-and-reconnection mechanism disclosed by Bareket would have been a straightforward application of known techniques, each addressing the same underlying security gap—preventing continued or renewed access to the known network through a remote network shown to pose a security risk—using predictable means and yielding no more than the predictable result of a more secure, appropriately rerouted connection. (Ex-1003, ¶¶146-49; *see KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398 (2007).)

3. Element-by-Element Analysis

a. 5/15

As the Examiner correctly found, Loza disclosed “upon denying access...requesting the user to” by disclosing that “the present invention can be used as a trigger to provide a message to a user to download and properly install a particular security measure on the remote machine, as directed by a corporate IT policy etc.” which “would enable an IT administrator to set a policy, so as to automatically prevent access further into a network until the security measure is installed and working on the remote machine.” (Ex-1002, 151 citing Ex-1005, ¶0053.)

As the Examiner correctly found, Sahay disclosed “access the known network via another remote network” by disclosing that “the access controller may reassign the client device to another access zone or VLAN based on one or more triggering events” that may include “a change in security context, security violation by the client device, a security violation detected in the network, and an operator-initiated request to reassign the client device.” (Ex-1002, 151 citing Ex-1008, 7:37-44.)

The Examiner confirmed that it would have been obvious to a POSITA “to modify the combined teaching of Loza, Bansal and Dupont using a method of

proving a message to a user requesting to access a known network via another network as taught by Sahay” to “help[] reduce threat[s] to a known network by preventing access from a vulnerable remote network.” (Ex-1002, 151-52; Ex-1003, ¶¶150-54.)

b. 7

As the Examiner correctly found, Sahay disclosed that “the access controller may reassign the client device to another access zone or VLAN based on one or more triggering events” such as “a change in security context, security violation by the client device, a security violation detected in the network, and an operator-initiated request to reassign the client device.” (Ex-1002, 152 citing Ex-1008, 7:37-44.) It would have been obvious to a POSITA “to modify the combined teaching of Loza, Bansal and Dupont using a method of proving a message to a user requesting to access a known network via another network as taught by Sahay” to “help[] reduce threat[s] to a known network by preventing access from a vulnerable remote network.” (Ex-1002, 152; Ex-1003, ¶¶155-58.)

c. 10

As the Examiner correctly found, Loza disclosed “upon disconnecting...to a user of the processing device” by disclosing that “the present invention can be used as a trigger to provide a message to a user to download and properly install a

particular security measure on the remote machine, as directed by a corporate IT policy etc.” which “would enable an IT administrator to set a policy, so as to automatically prevent access further into a network until the security measure is installed and working on the remote machine.” (Ex-1002, 153 citing Ex-1005, ¶0053.)

As the Examiner correctly found, Sahay disclosed “access the known network via another remote network” by disclosing that “the access controller may reassign the client device to another access zone or VLAN based on one or more triggering events” that may include “a change in security context, security violation by the client device, a security violation detected in the network, and an operator-initiated request to reassign the client device.” (Ex-1002, 153 citing Ex-1008, 7:37-44.)

The Examiner confirmed it would have been obvious to a POSITA “to modify the combined teaching of Loza, Bansal and Dupont using a method of proving a message to a user requesting to access a known network via another network as taught by Sahay” to “help[] reduce threat[s] to a known network by preventing access from a vulnerable remote network.” (Ex-1002, 153; Ex-1003, ¶¶159-63.)

C. Ground 3: Mishaev with Schwartz Renders Claims 1-18 Obvious

Combining Mishaev and Schwartz also renders all claims obvious.

1. Mishaev

Like the '902 patent, Mishaev relates to “remote access computer security,” targeting the “many enterprises t[hat] allow a mobile workforce to remotely access protected enterprise computing services” and simultaneous “growing number of sophisticated cyber attacks that [have] targeted organizational computing resources and cloud services.” (Ex-1003, ¶¶165-66 (annotating Ex-1009, Fig. 1B (below); *Compare* Ex-1009, ¶¶0001-05, *with* Ex-1001, 2:21-56.)

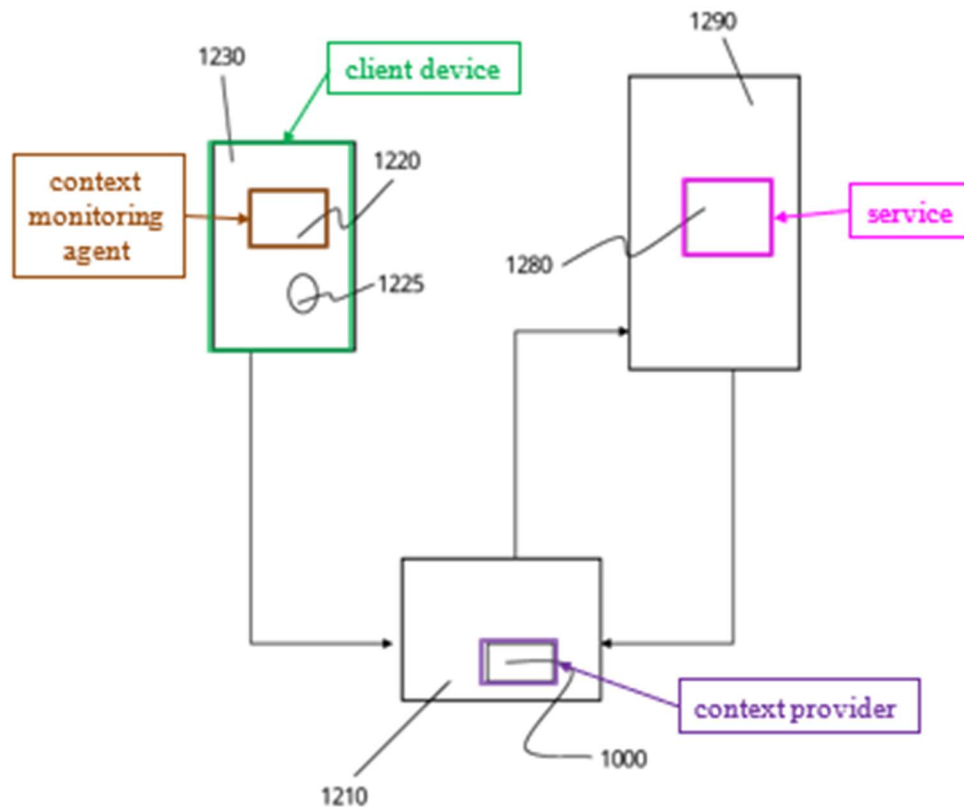


Fig. 1B

Fig. 1B depicts a typical telework setting: a “client device” (green)—e.g., “an employee’s smart phone or laptop”—remotely accessing a “service” (pink)—e.g., “an organization’s computing resource”—via an undepicted “network.” (Ex-1009, ¶¶0119-20, ¶0081.) The client device connects to the network at its access point (“AP”)—e.g., “a public [AP] of a restaurant or bar” not “operated by [the] organization.” (*Id.*, ¶¶0103-04, ¶0140, ¶0166, ¶¶0150-53 (describing connecting to a “:Dragon Bar—Free” public AP); Ex-1003, ¶166.)

Whenever the device's user attempts to login and establish a "session" with the organization's service, the attempt is "redirect[ed]" to a "context provider"² (purple), and a connection is established via, e.g., "SSL (Secure Sockets Layer)." (Ex-1009, ¶0126, ¶¶0119-20, ¶¶0186-87.) The context provider may be part of the organization's service. (*See id.*, ¶¶0043-44, ¶0109, ¶0132.) The context provider decides to allow or block the login, limit access, and/or take other user-access-related actions "as known in the art" by weighing data received from the client, including: "data on the user," "data on the device used by the user," and "data on the network used by the user." (*Id.*, ¶¶0156-57, ¶0081, ¶¶0187-91; Ex-1003, ¶167.)

"Data on the user" includes a "username, password, or biometric data provided by the user on the client device." (Ex-1009, ¶0098.) The context provider uses this to "authenticate[]" the user and client device using authentication techniques "known in the art." (*Id.*, ¶¶0098-99, ¶¶0123-25; Ex-1003, ¶168.)

² This context provider is also called "apparatus 1000." (Ex-1009, ¶0106.) Mishaev's disclosures for other figures apply to Fig. 1B's context provider/apparatus. (*E.g., id.*, ¶0100, ¶¶0185-93.)

“Data on the device” includes data indicating installation of a “context monitoring agent” (“CMA”)³ (brown), which is also used when authenticating the user and client device to “increase[] confidence in the security of the established session.” (Ex-1009, ¶¶0087-90, ¶0110, ¶¶0123-26, ¶¶0137-39, ¶0259 (numbering omitted).) For instance, using the context provider, the organization “download[s] and install[s]” the CMA onto the client device as a “prerequisite for the remote access” such that, if the client device does not produce a “digital certificate that indicates installation of the [CMA]” upon request, then “the user is not allowed access to the [organization’s] service.” (*Id.*, ¶0172, ¶¶0187-91; Ex-1003, ¶169.)

“Data on the network” includes data “identifying the [AP] that the user’s client device is connected to” and other APs. (Ex-1009, ¶0059, ¶0140.) It also includes data indicating whether each AP’s network is “malicious” or otherwise “risky,” which the client device determines using the discussed CMA. (Ex-1009, ¶0059, ¶¶0166-67.) Mishaev provided examples of how this security determination is done; however, as Mishaev clarifies, the CMA can use any technique “as known

³ The CMA is also called a “client application,” and its related teachings apply across figures. (Ex-1009, ¶0110, ¶0164, ¶0187, ¶0215.)

in the art” to determine the security of the network used for access. (Ex-1009, ¶0167; Ex-1003, ¶170.)

After security determination is sent to the context provider, the context provider weighs it with the other received data to decide, e.g., whether to “block or allow the user’s attempt to login into the service,” and/or whether less restrictive user-related-actions should be taken. (Ex-1009, ¶¶0075-78, ¶0081, ¶0127, ¶¶0156-57; Ex-1003, ¶171; *see, e.g.*, Ex-1009, ¶¶0073-74 (explaining how data on an exemplary whitelisted “:CORO-001” AP would be signaled by the CMA as “:Allowable” and access would be granted to the client device accordingly, though limited based on the data on the device indicating a “:Jail Broken” status).)

Lastly, even after access is granted and a connection established, the context provider “continues to monitor the connection...throughout the time period of the connection,” such as by having the CMA “repeat[] periodically” the security determination on the network. (Ex-1009, ¶0192, ¶¶0180-82, ¶0257.) “An organization may thus be able to dynamically monitor, condition, and control remote access to [its] services...in a continuous or nearly continuous manner.” (*Id.*, ¶0102, ¶0038.) For instance, weighing “new data on the user, client device, [and] network” received from the client device during a session, the context provider continuously decides whether to “disconnect the user from the service” using, e.g.,

“SLO (Single Logout),” which thereafter would require a new login by the user.
(*Id.*, ¶¶0038, ¶¶0075-78, ¶¶0100-02, ¶0157; Ex-1003, ¶172.)

2. Schwartz

Schwartz, like Mishaev, “relates to cybersecurity systems” but is directed “more particularly to detection of vulnerable wireless networks coexisting in a secured environment.” (*Compare* Ex-1010, 1:7-9, with Ex-1009, ¶¶0001-05.) Schwartz explained that its teachings, like Mishaev’s, apply to the typical telework setting, as depicted in Fig. 1. (Ex-1010, 3:50-4:4; Ex-1003, ¶¶173-74 (annotating Ex-1010, Fig. 1).

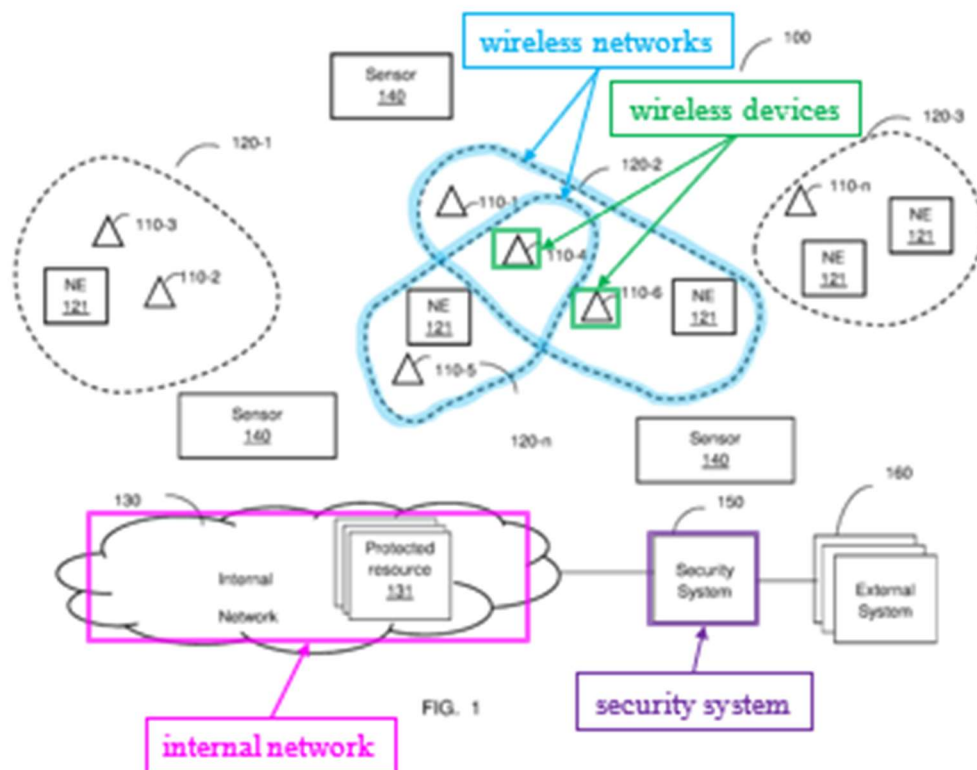


Figure 1's teleworking arrangement includes "wireless devices" (green)—e.g., a laptop, PC, smartphone, or IoT device. (Ex-1010, 4:5-11) Each device is connected to one or more "wireless networks" (blue) that may contain other wireless devices and network elements (unannotated). (*Id.*, 3:50-64, 5:39-44, 6:21-26, Figs. 1-2.) Using a wireless network, a wireless device remotely accesses a "internal network [(pink)] of an organization." (*Id.*, 3:65-4:3, 5:47-55, 9:27-36; Ex-1003, ¶¶174-75; Ex-1010, 5:66-6:11 (describing wireless network "not part of," and thus external to, "the IT infrastructure of the organization").)

Further, like Mishaev, Schwartz taught that wireless networks can be "malicious" or "vulnerable." (*Compare* Ex-1010, 5:66-6:5, 11:17-27, *with* Ex-1009, ¶0059, ¶0167.) Like Mishaev's CMA, Schwartz's wireless device determines whether a connected wireless network is vulnerable using a "software application" (or "agent sensor"). (Ex-1003, ¶177. *Compare* Ex-1010, 10:5-7, 4:56-5:15, 9:54-65, 11:4-27, 12:27-53, *with* Ex-1009, ¶0059, ¶¶0166-67.)

Schwartz described security determination techniques not discussed in Mishaev, including determining whether any "malicious devices" or "unknown device[s]" have connected to the network. (Ex-1010, 11:4-53, 6:33-7:31, 5:39-6:9, 11:57-59.) Malicious devices include "unintentionally unsecured devices such as the Amazon Echo®" and other IoT devices. (*Id.*, 11:49-53.) Unknown devices are

devices not “authorized to access the internal network” as determined by, “e.g., an active directory of the organization” and may include IoT devices. (*Id.*, 6:33-7:3, 7:31-36.) If the agent sensor determines that a wireless network has connected to such devices, the wireless network may be deemed “vulnerable”; otherwise, a wireless network with only authorized, “legitimate” devices is “safe.” (*Id.*, 5:66-6:11, 7:4-42.) Other criteria may be considered, and a specific “risk factor”/“risk score” for the network may be assigned or adjusted accordingly. (Ex-1003, ¶178; *see, e.g., id.*, 6:12-32, 8:66-9:10.)

Based on the agent sensor’s security determination, an organization’s “security system” (purple) decides—like Mishaev’s context provider—whether and which user-access-related “mitigation actions” should be performed. (*Compare* Ex-1010, 4:56-5:55, 15:64-16:4, 6:19-32, *with* Ex-1009, ¶¶0075-78, ¶0081, ¶0127, ¶¶0156-57.) “[A] decision to perform a mitigation action is based on the determined risk score” made by the security system and/or the agent sensor “under the control of the security system.” (Ex-1010, 9:8-10, 4:56-5:22, 9:54-10:4, 13:17-22.) For instance, like Mishaev’s context provider and Schwartz’s security system, Schwartz’s agent sensor can decide—based on a wireless network being determined “vulnerable” and its associated “risk factor”/“risk score”—that any “traffic” from the wireless device should be “mitigate[d]” and “block[ed],” that

such traffic should be forced to “be transmitted through a secure connection,” that any “active connections” should be “disconnect[ed],” and/or even that the wireless device should be completely “block[ed]...from connecting to [the wireless] network.” (*Compare id.*, 4:56-5:22, 6:12-32, 8:66-9:10, 15:64-16:4, 13:17-37, 9:54-10:4, *with* Ex-1009, ¶¶0127, ¶¶0075-78, ¶¶0137-39. Ex-1003, ¶179.)

In fact, Schwartz discloses that there may even be other devices in a particular teleworking arrangement that can make such mitigation decisions. (Ex-1010, 14:49-61, 4:56-67, 13:17-37.) Schwartz described two device categories: “out-of-band device[s]” that exist outside of the wireless network containing the wireless device; and in-network (i.e., in-band) devices located within the wireless network, such as those in Fig. 3. (*Id.*, 4:23-29, 5:6-22, 9:27-46, 14:49-61; Ex-1003, ¶180 (annotating Ex-1010, Fig. 3 (below)); Ex-1017, 350 (explaining “out-of-band” versus “in-band” channels).)

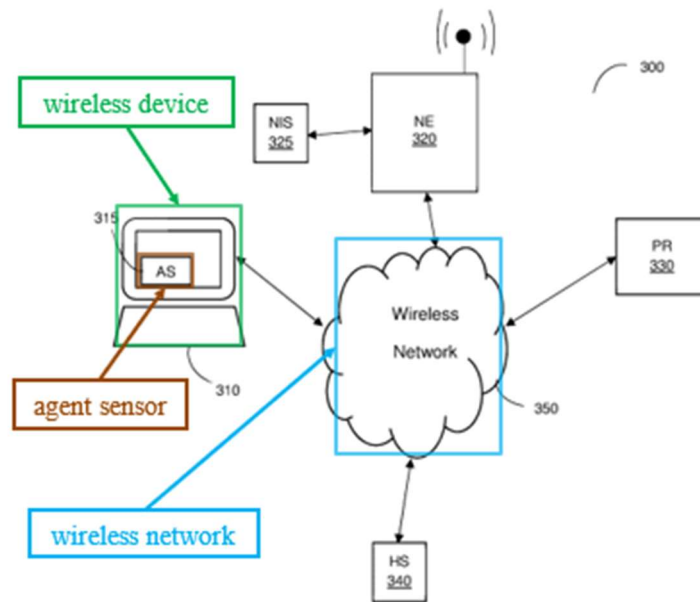


FIG. 3

In addition to the agent sensor (brown) on the wireless device (green), the wireless network (blue) connects to two separate in-band sensors (unannotated): a standalone “hardware sensor 340,” and a network-element-integrated “network infrastructure sensor 325,” each of which can “independently or collectively” make mitigation decisions. (Ex-1010, 14:49-61.) These sensors are not required for Schwartz’s teachings to apply. (*Id.*, 13:61-14:19; Ex-1003, ¶181.)

3. Combining Mishaev with Schwartz

A POSITA would have found it obvious to modify Mishaev using the Schwartz’s teachings.

a. A POSITA Would Have Used Schwartz's Security Determinations in Mishaev

Mishaev taught that an organization-provided CMA on a “client device” determines—both before and after for each access session with an organization’s “service”—whether the network used for access is “malicious” or “risky.” (Ex-1009, ¶¶0110, ¶¶0166-67, ¶¶0081, ¶¶0180-82, ¶¶0126.) The CMA may use any technique “as known in the art” to perform such security determinations. (*Id.*, ¶¶0167). Thus, Mishaev explicitly directs a POSITA to use known techniques for determining network security. (Ex-1003, ¶¶183.)

Such techniques are described in Schwartz. Schwartz taught that, in a teleworking arrangement like Mishaev’s, an “agent sensor” on a “wireless device” determines whether a “wireless network” is “malicious” or “vulnerable,” but using criteria including whether a “malicious”/“unknown device” is connected. (Ex-1010, 9:54-65, 10:5-7, 11:4-59, 5:39-6:9, 6:63-7:53.) “Malicious devices” include “unintentionally unsecured devices,” and “unknown devices” include devices not “authorized” to access an internal network. (*Id.*, 11:49-53, 6:33-7:3.) Both include IoT devices. (*Id.*, 7:31-53, 11:49-53.) Other criteria include “connection type” to the wireless network and “sensitivity” of data transmitted or accessed, which, combined, determine the wireless network’s “risk factor”/“risk score.” (*Id.*, 6:12-32, 4:12-22, 14:62-67, 11:14-40, 8:66-9:10; Ex-1003, ¶¶184.)

A POSITA would have been motivated to modify Mishaev's client device so that it performs Schwartz's known techniques for determining a network's security, as Mishaev explicitly directs. (Ex-1009, ¶0167.) Separately, a POSITA would have made this modification because Schwartz's techniques achieve the exact function of determining the network security that Mishaev requires. (See Ex-1009, ¶0167; Ex-1010, 11:4-53, 6:33-7:53; *Intel Corp. v. PACT XPP Schweiz AG*, 61 F.4th 1373, 1380 (Fed. Cir. 2023) (“[I]f there's a known technique to address a known problem using ‘prior art elements according to their established functions,’ then there is a motivation to combine.” (citation omitted)).) And since Schwartz performs these techniques in a device identical to Mishaev's client device and within the same telework setting, a POSITA would have had no difficulty modifying Mishaev's client device accordingly. (Ex-1003, ¶185. *Compare, e.g.*, Ex-1009, ¶0043, *with* Ex-1010, 4:5-11.)

Accordingly, in “Mishaev-Schwartz,” the CMA in Mishaev's client device determines network security both before and after accessing an organization's service based on, e.g., whether malicious/unknown devices are connected to the network (taught in Schwartz). If so, the network may be deemed risky; otherwise, the network may be deemed usable. In making such security determinations, the CMA considers other factors, including network connection type and data

sensitivity, and assigns/adjusts the network's risk factor/score accordingly. (Ex-1003, ¶186.)

b. A POSITA Would Have Modified Mishaev's Client Device to Make Mitigation Decisions

A POSITA would have further modified Mishaev so the CMA—and not just the context provider—decides whether to take user-access-related mitigation actions based on the discussed security determinations, including whether to allow its attempt to access the organization's service, whether any subsequent traffic should be transmitted through a secure connection, whether to disconnect any existing access, whether its connection should be completely blocked, and whether to perform other known mitigation actions.

First, it is well-established that a combination is “obvious to try” “[w]hen there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions....” (*KSR*, 550 U.S. at 421.) A POSITA would have recognized that, in Mishaev's teleworking arrangement, the context provider need not be the sole device deciding whether to allow/continue the client device's access to the service. (Ex-1003, ¶187.) Rather, a finite number of devices could make these mitigation decisions: the context provider and client device. Ex-1003, ¶187. Accordingly, modifying Mishaev's client device to also make

mitigation decisions would have been “the product not of innovation but of ordinary skill and common sense.” (*See KSR*, 550 U.S. at 421; Ex-1003, ¶191.)

Uber Technologies, Inc. v. X One, Inc. is instructive. (*See* 957 F.3d 1334 (Fed. Cir. 2020)). There, a reference disclosed a “mobile device” receiving a map and then performing a “plotting” operation, referred to as “terminal-side plotting.” *Id.*, 1338. Another reference disclosed a “server” performing the same “plotting” operation and then sending the plotted map to the mobile device, called “server-side plotting.” *Id.* The challenged claims required the latter, so petitioner argued “it would have been obvious to substitute” terminal-side plotting with server-side plotting, since the references demonstrated that both techniques were “well-known design choices in the prior art.” *Id.*

The Federal Circuit reversed a Board’s finding a lack of motivation to combine, because terminal-side and server-side plotting formed “two of a finite number of known, predictable solutions.” *Id.*, 1341. Both techniques “solv[ed] the same problem,” and indeed, the references themselves “undisputedly” addressed the same technological setting of “cellular networks.” *Id.*, 1341-42. Accordingly, the Court found that “a [POSITA] would have faced a simple design choice between” terminal-side and server-side plotting, and thus performing would have been obvious to try. *Id.*

Here, a POSITA would have similarly recognized Mishaev's teleworking arrangement presents "a finite number of known, predictable" devices that could decide whether to block the client device's login attempt, logout of any established session between the client device and service, and/or take any other user-access-related actions "known in the art." (Ex-1003, ¶188; *see* Ex-1009, ¶¶0156-57, ¶¶0075-78.) Mishaev taught that, after receiving the client device's login attempt and weighing the corresponding data on the user, device, and network, the context provider decides whether and which action should be taken regarding the client device's access to the service. (Ex-1009, ¶¶0119-20, ¶0127, ¶¶0186-87.) Schwartz is similar. In the same teleworking situation, and based on similar data gathered by the agent sensor, the "security system" decides whether to block a wireless device's traffic to an organization's internal network, disconnect any connection to that network, and/or perform other user-access-related "mitigation actions" and "the like." (Ex-1010, 15:40-16:4, 6:19-32; Ex-1003, ¶188.)

Schwartz additionally taught that the wireless device can make these same mitigation decisions "under the control of the security system" using the agent sensor and its gathered data. (Ex-1010, 4:56-5:20.) Thus, a POSITA would have known—or otherwise garnered from Schwartz—that Mishaev's client device was modifiable to make the same/similar type of user-access-related mitigation

decisions as the context provider while under its control. (Ex-1003, ¶189; *accord* Ex-1005, Fig. F, ¶¶0040-42 (describing an “agent” installed in a “Remote/Mobile” device operating similarly).)

Put differently, presented with Mishaev’s teleworking arrangement, a POSITA would have recognized that—similar to server-side plotting and terminal-side plotting in *Uber*—it could implement either context-provider-side mitigating or client-device-side mitigating. The depicted context provider could (1) directly decide the client device’s login attempt and any continuing access (done in Mishaev) or (2) indirectly decide, through the client device, e.g., whether any “traffic” from the client device (such as the login attempt and corresponding data) is to be “mitigate[d]”/“block[ed],” whether that traffic should “be transmitted through a secure connection,” whether any “active connection[]” with the service should be “disconnect[ed],” and/or whether to completely “block[]” the client device “from connecting to [the] network,” based on whether the network was determined as vulnerable and its assigned risk factor/score as done in Schwartz. (Ex-1010, 4:56-5:22, 15:64-16:4, 13:17-37, 9:54-10:4, 6:12-18, 8:66-9:10; Ex-1009, ¶¶0075-78, ¶0127, ¶¶0137-39, ¶¶0192-93; Ex-1003, ¶190.)

A third option also exists: combining options (1) and (2) such that both the context provider and client device make mitigation decisions. Schwartz taught that

multiple devices—including the security system and the wireless device via its agent sensor—can make mitigation decisions. (See Ex-1010, 14:49-61, 13:61-14:19, Fig. 1 (depicting both a security system and multiple security-system-controlled “sensors 140”)). The known availability of these three options shows there are “a finite number of known, predictable solutions” for “solving the same problem” of deciding, e.g., whether to allow the client device’s access attempt. (Ex-1003, ¶191; *Recor Med., Inc. v. Medtronic Ireland Mfg. Unlimited Co.*, 2025 WL 944511, at *4 (Fed. Cir. Mar. 27, 2025) (holding that the combined teaching of “ten thermal energy sources” across several references presented “a sufficiently finite universe of [source] options to support an obvious-to-try theory”).)

Second, a POSITA would have been motivated to have both the context provider and client device make mitigation decisions, as such would have delivered recognizable, known benefits, including improving security coverage. As Schwartz taught, by having multiple devices and sensors at different network locations making their own mitigation decisions under the control of the security system, a wireless device thus “can be probed and interrogated differently by different sensors...based on [each sensor’s] capabilities,” thereby expanding the security coverage beyond what just one device or sensor could achieve. (See Ex-1010, 12:10-17, 4:56-5:30; Ex-1017, 226 (recommending organizations adopt a

“defense-in-depth approach”—i.e., “strategically allocat[ing] security and privacy controls in the security and privacy architectures so that adversaries must overcome multiple controls to achieve their objective”).) Moreover, as a POSITA would have recognized, giving mitigation-decision-making capability to both Mishaev’s context provider and client device would have increased reliability by allowing one device to continue making mitigation decisions to protect the organization’s service if the other fails or is overtaken by an adversary. Ex-1003, ¶192; *see also* Ex-1017, 294 (explaining that defense-in-depth also “allow[s] the system to continue in a secure state even when one mechanism has failed”).

Finally, a POSITA would have had a reasonable expectation of success in making these modifications. As Schwartz taught, the mitigation-decision-making “agent sensor” can be “implemented as a software application installed on [a] wireless device” such as “a laptop.” (Ex-1010, 10:5-17.) Mishaev’s client device—being also “a laptop computer, etc.”—would have been easily programmed with such mitigation-decision-making software-functionality, especially given it already has a similar CMA application. (*See* Ex-1009, ¶0043, ¶0110, ¶¶0171-73; Ex-1003, ¶193.)

Accordingly, in Mishaev-Schwartz, the CMA of Mishaev’s client device—like Schwartz’s agent sensor—decides whether and which user-access-related

mitigation actions should be taken by the CMA based on whether the network is determined as vulnerable and the network's assigned risk factor/score. Such is decided in addition to the context provider making its own mitigation decisions independently. (Ex-1003, ¶194.)

4. Element-by-Element Analysis

a. 1[pre]/11[pre]/14[pre]

If the preamble is limiting, Mishaev-Schwartz includes Mishaev's "client device" that performs the steps described *infra* Sections VIII.C.4.b-VIII.C.4.g (collectively, 1[pre]'s "method"). The client device is, e.g., "an employee's smart phone or laptop," which a POSITA would have understood includes a general-purpose processor (11[pre]/14[pre]'s "processing resource") and memory storing instructions for the processor to perform the discussed steps (11[pre]/14[pre]'s "medium" and "instructions"). (Ex-1009, ¶0132, ¶0043, ¶¶0110-17; *see also* Ex-1001, 11:28-46 (explaining that a "processing resource" includes a general-purpose processor)). These steps allow an organization to control access by the client device to—thereby reducing "threats" and "cyber attacks" on—the organization's "service." (Ex-1009, ¶¶0023-25; Ex-1010, 1:7-2:27; Ex-1003, ¶195.)

b. 1[a]/11[a]/14[a]

Mishaev's client device ("known access device") connects to a "network" at its AP to "remote[ly] access" the organization's service, which includes the

“organization’s computing resource[s]” such as a “database” (“known network”). (Ex-1009, ¶¶0119-20, ¶0140, ¶0081, ¶0166; *see also* Ex-1001, 7:41-59 (explaining that a “known network” may include network-accessible “databases”).) The AP can be “a public [AP] of a restaurant or bar”—in contrast to “an [AP] operated by [the] organization”—thus meeting the claimed “remote network.” (Ex-1009, ¶¶0103-04; Ex-1003, ¶197; *see also* Ex-1001, 3:4-8.)

Before each session with the service, “the user attempts to login” and provides the client device with related data including a “username, password, or biometric data,” any of which meets the claimed “receiving, by a processing device, a request....” (Ex-1009, ¶¶0119-20, ¶0098, ¶0126; Ex-1003, ¶198; *see also* Ex-1001, 12:57-64 (explaining that “determin[ing] whether a request to access a known network is received” can be the result of the known access device “detect[ing]” the “preparing [of] an authorization credential”).)

Lastly, a POSITA would have understood that the client device—e.g., a “laptop”—would have included the discussed processor, memory, and any other components needed to perform the functions described hereinbelow (collectively, “processing device”). (*See* Ex-1009, ¶0132, ¶0043; Ex-1003, ¶199.)

c. 1[b]/11[b]/14[b]

Mishaev's organization implements a "context provider" as part of its service to "control[] the user's remote access." (Ex-1009, ¶¶0119-20, ¶¶0043-44, ¶0132). The context provider decides whether to allow the client device's login attempt and/or perform other known user-access-related actions by weighing data it receives from the client device, including "data on the user" and "data on the device used by the user." (*Id.*, ¶0081, ¶0119; Ex-1003, ¶201).

The "data on the user" includes the above-discussed, user-provided "username, password, or biometric data." (Ex-1009, ¶0098.) The "data on the client device" includes data indicating, e.g., whether an organization-provided CMA application is installed on the client device. (*Id.*, ¶¶0087-90, ¶0173, ¶¶0259.) As part of making user-access-related decisions, the context provider uses both data types to "authenticate[]" the user and client device, and thus either of such data from the client device is "credentials associated with access device." (*Id.*, ¶¶0098-99, ¶¶0123-27; Ex-1003, ¶202.)

Mishaev's context provider may be used by a specific organization and implemented as a part of its service. (Ex-1009, ¶¶0043-44, ¶0109, ¶0132.) In such a scenario, the context provider forms part of a "known network [that] is a private

network that authorizes” said credentials. (*See id.*, ¶¶0043-44, ¶0123, ¶0132; Ex-1003, ¶203.).

Lastly, the client-device-connected AP may be “public”—in contrast to being “operated by [the] organization”—and thus a “remote network [that] is external to the known network.” (Ex-1009, ¶¶0103-04; Ex-1001, 3:4-10; Ex-1003, ¶204.)

d. 1[c]/11[c]/14[c]

Mishaev’s user-access-related decisions weigh “data on the network used by the user,” including data indicating whether the public AP’s network is “malicious” or “risky.” (Ex-1009, ¶0081, ¶0059, ¶¶0166-67.) To determine the network security, Mishaev’s client device uses the CMA, which in Mishaev-Schwartz utilizes known—e.g., Schwartz’s—network-security-determination techniques. (*See* Ex-1009, ¶0167; *supra* Section VIII.C.3.a; Ex-1003, ¶206.)

The CMA determines whether a “malicious”/“unknown” device is connected to the network used to access the organization’s service. (*See* Ex-1010, 9:54-65, 10:5-7, 11:4-59, 5:39-6:9, 6:63-7:53.) Either device is an “unsecure network element on the remote network”: “malicious devices” include “unintentionally *unsecured* devices,” whereas “unknown devices” are not “authorized” by, “e.g., an active directory of the organization.” (*See* Ex-1010,

11:49-53 (emphasis added), 6:33-7:3; Ex-1001, 13:32-43 (explaining “unsecure network elements” may be “designated” as such the known network).) If the CMA identifies either, the network may be risky; otherwise, the network may be allowable. (See Ex-1010, 5:39-6:9, 7:31-53, 11:4-53; *supra* Section VIII.C.3.a). By determining whether such devices are on the network, the client device performs “scanning.” (See Ex-1010, 13:38-55 (describing these security determinations as “vulnerability *scans*” (emphasis added); Ex-1003, ¶207.)

e. 1[d]/11[d]/14[d]

Mishaev taught that the client device’s login attempt for accessing the service may be “block[ed]” by the context provider, and that other known user-access-related actions may be taken, if the network of an AP—including a public AP—is risky. (See Ex-1009, ¶¶0119-20, ¶0081, ¶¶0156-57, ¶¶0166-67, ¶¶0150-53 (describing accessing a service via a public “:Dragon Bar—Free” AP as “requir[ing] further clearance” due to being unknown to the organization), ¶0104 (describing limiting access to the organization’s service if “the user switches to a public [AP]”).) In Mishaev-Schwartz, such security determinations and resulting “mitigation actions” are performed by the CMA of Mishaev’s client device as well—ranging from “mitigat[ing]”/“blocking” any traffic, such as the client device’s login attempt and corresponding data on the user, device, and network, to

completely blocking any network connection—based on the network being deemed vulnerable and the associated risk factor/score as taught in Schwartz. (*See supra* Section VIII.C.3.) Accordingly, in Mishaev-Schwartz, the client device’s CMA “mitigate[s]”/“block[s]” the client device’s login attempt and corresponding data from being sent to the context provider—thus “denying...access,” as claimed, to the organization’s service—if, e.g., malicious/unknown devices are identified on the network. (*See* Ex-1010, 9:54-10:7, 5:39-6:9, 6:63-7:53, 11:4-59; Ex-1009, ¶¶0150-53; *supra* Section VIII.C.3; Ex-1003, ¶209.)

f. 1[e]/11[e]/14[e]

Mishaev also taught that, if the network—including the public AP—is allowable, then the context provider may instead “allow[...]the user’s login attempt.” (Ex-1009, ¶¶0119-20, ¶0104, ¶¶0073-74 (describing connecting to a “:CORO-001” AP deemed “:Allowable” and granting access accordingly, though limited based on the client device’s “:Jail Broken” status).) And again, in Mishaev-Schwartz, these security determinations and user-access-related mitigation decisions are made by both Mishaev’s context provider and client device. (Ex-1003, ¶211; *supra* Section VIII.C.3.)

For instance, like the context provider, the client device’s CMA may refrain from taking mitigating actions and thus “allow[.]” the traffic transmission—

including the client device's login attempt and corresponding data—if only authorized, “legitimate” devices are connected to the network and no other potential network vulnerability exists. (*See* Ex-1010, 5:66-6:11, 7:4-42, 4:56-67, 15:60-16:4; Ex-1009, ¶¶0119-20; Ex-1003, ¶211.) This login attempt is “redirect[ed]” to the context provider, which also makes user-access-related decisions on the login attempt by weighing the received data on the user, device, and network (the login attempt and corresponding data each thus meeting the claimed “request”). (*See* Ex-1009, ¶¶0186-87, ¶¶0119-20; *supra* Section VIII.C.3; Ex-1003, ¶212; *see also* Ex-1001, 8:67-9:3 (describing presenting an “authorization credential” to the known network “as part of requesting access”); *supra* Section VIII.C.4.c (explaining how data on the user and client device sent to the context provider are indeed such “credentials”).)

Separately, Mishaev taught that, by “redirect[ing]” the login attempt to the context provider, a connection from the client device to the context provider is established via, e.g., “an SSL...connection and handshake.” (Ex-1009, ¶¶0119-20, ¶¶0186-87.) A POSITA would have understood this as involving sending, specifically, “SSL handshake” connection-setup messages, which meets “requesting a grant of access.” (*See, e.g.*, Ex-1013, ¶0006-28; Ex-1003, ¶213.)

Lastly, Mishaev-Schwartz performs both the claimed “identifying at least one unsecure network element on the remote network[and] denying...” and 1[d]/11[d]/14[d]’s “fail[ing] to identify any unsecure network element on the remote network[and] requesting...” over two login/logout sessions, like the ’902 patent. For example, in the ’902 patent’s Fig. 2, block 214 queries “whether any unsecure network elements are included in the remote network.” (Ex-1001, 12:55-57, 13:52-55, Fig. 2.) From there, it branches into two paths: one for 1[e]/11[e]/14[e]’s “[w]here no unsecure network elements are included”; the other for 1[d]/11[d]/14[d]’s “where it is determined that unsecure network elements are included.” (*Compare id.*, 13:55-14:34, Fig. 2, *with id.*, claims 1[d]-[e]/11[d]-[e]/14[d]-[e].) Both branches then remain separate, reconverging only after the method returns to the beginning login step of “determin[ing] whether a request to access a known network is received” corresponding to 1[a]/11[a]/14[a] for a new login/logout loop to begin. (*See id.*, 12:57-64, Fig. 2, claims 1[a]/11[a]/14[a].) Indeed, before reconverging, both branches terminate with a session being either denied or disconnected. (*Id.*, 14:7-23, 14:26-34, Fig. 2.) The ’902 patent’s other figures are similar. (Ex-1003, ¶214; *see* Ex-1001, Figs. 3-6.)

Like the ’902 patent, Mishaev-Schwartz performs both claimed steps over two sessions. For instance, after a session is established from the client device’s

login attempt described herein under 1[e]/11[e]/14[e], the client device may subsequently “disconnect[] [the] active connection” due to, e.g., a newly connected malicious/unknown device. (*Supra* Section VIII.C.3.b; *see also* Ex-1009, ¶¶0157-58 (describing the context provider similarly forcing a “SLO (Single Logout)”); *infra* Section VIII.C.4.o.) Should a new login be attempted thereafter over the same network, such corresponding traffic from the client device would then be “mitigate[d]”/“block[ed]” by the CMA—at least until the malicious/unknown device is disconnected—and thus satisfy 1[d]/11[d]/14[d] for the reasons explained *supra* Section VIII.C.4.e. Moreover, it would have been obvious to reattempt login after either the discussed logout or blocking of access, given such login is required for each access to the service (e.g., Ex-1009, ¶0120), and establishing and securing such remote access is the purpose of Mishaev (e.g., *id.*, ¶0001). (Ex-1003, ¶215; *see also Perfect Web Techs., Inc. v. InfoUSA, Inc.*, 587 F.3d 1324, 1327-30 (Fed. Cir. 2009) (approving the “common sense application of the maxim ‘try, try again’”).)

g. 1[f]/11[f]/14[f]

In addition to “mitigat[ing]”/“block[ing]” traffic discussed above and *supra* Section VIII.C.4.e, the CMA in Mishaev-Schwartz may also perform additional mitigation actions based on the connected malicious/unknown device and other

relevant criteria, as described *supra* Section VIII.C.3.b. This includes forcing such traffic to “be transmitted through a secure connection” as taught in Schwartz. (Ex-1010, 13:27-37; Ex-1003, ¶217.)

Schwartz provided no further details or limits on this “secure connection.” A POSITA would have understood “secure connection” to include the well-known virtual private network (VPN) connection. (Ex-1003, ¶218; *see also Chiron Corp. v. Genentech, Inc.*, 363 F.3d 1247, 1254 (Fed. Cir. 2004) (“[A] patentee preferably omits from the disclosure any routine technology that is well known at the time of application.”).)

For instance, Durbin—filed three years before Schwartz—acknowledged that wireless networks pose particular security issues. (*Compare, e.g.*, Ex-1011, ¶0001, *with* Ex-1010, 1:22-27.) Like Schwartz, Durbin identifies the solution of “establish[ing] a *secure connection* on public wireless networks” while also highlighting this as a known “area of interest” in the field. (Ex-1011, ¶0001 (emphasis added).) Durbin then explained that, “[i]n particular,” this comprises “using advanced techniques such as secure *Virtual Private Network (VPN) connections*,” which “provide secure communication within public wireless networks” between, e.g., a “mobile device” and “information sensitive service center.” (*Id.*, ¶0001 (emphasis added), ¶0026.) Durbin thus explicitly identified

VPNs as a “secure connection” and described one as carrying out the exact function as Schwartz’s secure connection: providing the connection through which a device’s traffic is transmitted. (Ex-1003, ¶219. *Compare* Ex-1011, ¶¶0001, ¶0026, *with* Ex-1010, 13:27-37, 9:65-10:4 (explaining the agent sensor’s available mitigation actions include “initiating a secured communication protocol for transmitting information to and from the wireless device”).)

Other contemporaneous references confirm Schwartz’s usage and description of a “secure connection” would have been understood to include VPNs. (*E.g.*, Ex-1015, 15 (VPN provides “a secure remote access connection (tunnel) between a client device and the VPN gateway”); Ex-1016, 7 (defining a VPN as “provid[ing] a secure communications mechanism for data and control information transmitted between computers or networks”); Ex-1019, ¶¶0005, ¶¶0028-29 (describing an exemplary “secure connection” that routes network traffic to/from an endpoint device, over the Internet, and to/from a “VPN server”).) Given this recognition, a POSITA would have understood that, in Mishaev-Schwartz, the CMA’s forcing of traffic “through a secure connection” based on the network’s security would have included, specifically, forcing said traffic “through a [VPN] connection.” (Ex-1003, ¶220.)

Such VPN usage meets 1[f]/11[f]/14[f]. As the '902 patent clarifies, the claimed “starting” a VPN “application” is met when a “VPN application is installed and running on the known access device and network traffic is being routed via the VPN application.” (Ex-1001, 16:16-20, 17:39-43, Fig. 5.) Mishaev-Schwartz’s client device meets both conditions. As Mishaev taught, the client device’s CMA is indeed a “client *application*.” (Ex-1009, ¶0110 (emphasis added)). And again, in Mishaev-Schwartz, this CMA “application” forces the client device’s “traffic to be transmitted through a [VPN] connection.” (Ex-1003, ¶221.)

Moreover, by forcing particularly the previously “mitigate[d]”/“block[ed]” login attempt and corresponding data from above and *supra* Section VIII.C.4.e to be transmitted through the VPN, the claimed “requesting...over a virtual private network” is met. (Ex-1003, ¶222.)

Lastly, as noted *supra* Section VIII.C.3, whether and which mitigation actions should be taken by the CMA—including forced-transmitting of traffic “through a secured,” or VPN, “connection”—is decided in Mishaev-Schwartz based not only on whether a “malicious”/“unknown” device is connected to the network but also other criteria, including network “connection type” and data “sensitivity,” which, combined, determine the network’s risk factor/score. (*See* Ex-1010, 6:12-32, 14:62-67, 11:14-40, 8:66-9:10.). Thus, even when no

“malicious”/“unknown” device is connected, any login attempt and corresponding data that would otherwise be “allow[ed]” to be transmitted from the client device—e.g., as described *supra* Section VIII.C.4.f—may nonetheless be forced “to be transmitted through a [VPN] connection” if such and other mitigation actions are so warranted, as based on these other risk-factor/score considerations. (Ex-1003, ¶223.)

h. 2/12

As explained *supra* Section VIII.C.4.f, Mishaev-Schwartz’s client device transmits various data to the context provider that, in doing so, meets “requesting a grant of access”: allowing the login attempt and transmitting corresponding data to the context provider; and as part of establishing the SSL connection with the context provider. Thereafter, the context provider performs its own mitigation decisions and, if none are taken, “authenticates” the user and client device using such received data (each meeting the claimed “authorization credential”). (Ex-1009, ¶¶0098-99, ¶¶0123-27; *supra* Section VIII.C.4.c.) Access to the service may be granted based on such data being satisfactory to the context provider, meeting claims 2/12’s remaining language. (*See, e.g.*, Ex-1009, ¶¶0259-60, ¶0098; Ex-1003, ¶225.)

i. 3/13

Schwartz’s malicious/unknown devices include IoT devices (e.g., a “smart-watch” or “Amazon Echo®.”). (Ex-1010, 7:31-53, 11:49-53, 4:5-11; Ex-1003, ¶227.)

j. 4

As explained, in Mishaev-Schwartz, the client device performs mitigation decisions under the control of the context provider. (*Supra* Section VIII.C.3.b; *see also* Ex-1009, ¶0173.) Further, the organization may implement the context provider as part of its service. (*Supra* Section VIII.C.4.c.) Thus, the administration of both the client device and service are controlled by the same organization. (Ex-1003, ¶229.)

k. 5/15

Schwartz’s mitigation actions include not only those discussed *supra* Section VIII.C.4.e but also “generating an alert.” (Ex-1010, claim 7, 6:19-32; Ex-1003, ¶230.) Other references confirm such alerting—including alerting, specifically, the client device’s user—was well-known. (*E.g.*, Ex-1005, ¶0006, ¶¶0040-42.) In Mishaev-Schwartz, the client device performs such known mitigation actions as explained *supra* Section VIII.C.3.b, thus meeting claims 5/15. (*See also supra* Section VII.A.) Indeed, a POSITA would have been motivated to implement such known alerting after mitigating/blocking the login attempt discussed *supra* Section

VIII.C.4.e, because doing so would allow the user to know that such blocking occurred and to then reattempt login as explained *supra* Section VIII.C.4.f. (Ex-1003, ¶231.)

l. 6[a]/6[b]/16[a]/16[b]

“[M]itigating a security issue of the unsecure network element” includes, as 1[f]/[11[f]/14[f] explains, starting a VPN application, which, as explained *supra* Section VIII.C.4.g, Mishaev-Schwartz performs. Indeed, the ’902 patent’s Fig. 5 shows establishing and routing traffic through a VPN may serve as the sole “mitigat[ion]” to “cure the identified unsecure network element(s).” (*See* Ex-1001, 17:22-49, Figs. 3, 5.) For similar reasons, Mishaev-Schwartz’s transmitting of the previously mitigated/blocked login attempt and corresponding data also explained *supra* Section VIII.C.4.g meets 6[b]/16[b]. (*See id.*, 17:22-49, Figs. 3, 5; Ex-1003, ¶233.)

m. 7

As explained *supra* Sections VIII.C.4.g-VIII.C.4.h, after transmitting the mitigated/blocked login attempt and corresponding data “through [the] secured”—i.e., VPN—“connection,” access to the service may be granted. But even so, as explained *supra* Section VIII.C.3.a, the CMA in Mishaev-Schwartz’s client device makes continuous security determinations, including by identifying newer

connections made by malicious/unknown devices to the network and continuously considering, e.g., “connection type[s]” with the network and “sensitivity” of data being transmitted or accessed by the client device, and adjusting the network’s risk factor/score accordingly. (See Ex-1010, 6:12-32, 14:62-67, 8:66-9:10, 16:12-19; Ex-1003, ¶235; *infra* Section VIII.C.4.n.)

Moreover, further mitigation actions may be taken based on these continuous security determinations. Such actions include, as explained *supra* Section VIII.C.3.b, completely “block[ing]” Mishaev-Schwartz’s client device “from connecting to [the] network.” (See Ex-1010, 9:54-10:4.) Further mitigation actions are available, including “establishing a containment network” and “forc[ing],” e.g., the client device to “connect to the established containment network.” (See Ex-1010, 13:17-35; Ex-1003, ¶236.)

Thus, even after establishing a VPN as explained *supra* Section VIII.C.4.g and then being granted access to the network, if for instance “the transmission of sensitive information is detected over the wireless network,” then the corresponding change to the network’s risk factor/score may cause the CMA to, e.g., force the client device into a containment network, meeting claim 7. (See Ex-1010, 7:65-8:4, 8:66-9:10, 13:17-35; *supra* Section VIII.C.3.b; Ex-1003, ¶237; *see*

also Ex-1014, 111 (asserting infringement based similarly on “segmenting or isolating/quarantining [of] devices”).)

Alternatively, should the client device be completely “block[ed]...from connecting to [the] network,” the obvious next step to a POSITA would have been to reattempt access using a different network. (*See Perfect Web*, 587 F.3d at 1327-30.) Mishaev acknowledged that organizations can pre-determine safe, “allowable” networks. (*E.g.*, Ex-1009, ¶¶0073-74.) Having been blocked from the previous network, a POSITA would have been motivated to connect to, *e.g.*, such other, allowable networks, since it was known that access would thereafter be established. (Ex-1003, ¶238.)

n. 8[a]/8[b]/17[a]/17[b]

Mishaev explained that, even after the attempted (or reattempted) access to the service has been granted (8[a]/17[a]’s “using, by the processing device, a network connection...”) (*see supra* Section VIII.C.4.h), the context provider may require the client device to “repeat[] periodically” the discussed security determination on the network. (Ex-1009, ¶¶0180-82, ¶0192, ¶0257.) And in Mishaev-Schwartz, this includes continuously determining, *e.g.*, whether malicious/unknown devices are connected to the network as taught in Schwartz—

i.e., 8[b]/17[b]’s “scanning.” (Ex-1003, ¶240; *see supra* Sections VIII.C.3.a, VIII.C.4.d; Ex-1010, 16:12-19.)

o. 9/18

Mishaev and Schwartz taught that continuous security determinations can be used to decide whether to perform mitigation actions during existing access, including “disconnecting [the] active connection[]” (the claimed “disconnecting”) if “new data” identifies, e.g., a “newly connected” malicious/unknown device (the claimed “upon identifying...”) or other “potential vulnerabilities.” (Ex-1010, 13:17-35, 15:37-16:19, 3:39-49, 6:19-26; Ex-1009, ¶¶0075-78, ¶¶0100-02.) As explained *supra* Section VIII.C.3.b, Mishaev-Schwartz’s client device itself makes such a mitigation decision as taught in Schwartz. (*See* Ex-1010, 13:17-35, 15:37-16; Ex-1003, ¶242.)

p. 10

Schwartz taught that “generating an alert” can be performed together with “disconnecting [the] active connection,” both of which are known mitigation actions. (*See* Ex-1010, claim 7, 13:27-35.) Other references acknowledge the same, confirming such disconnecting-and-alerting was conventional. (*E.g.*, Ex-1005, ¶0006, ¶¶0040-42.) In Mishaev-Schwartz, the client device performs these known mitigation action, thereby meeting claim 10. *See supra* Sections VIII.C.3.b, VII.A.)

Indeed, like with blocking access discussed *supra* Section VIII.C.4.k, a POSITA would have been motivated to have the client device alert its user after disconnecting access for similar reasons. (Ex-1003, ¶244.)

D. Ground 4: Mishaev-Schwartz-Durbin Renders Claims 1-18 Obvious

If Mishaev-Schwartz does not teach 1[f]/11[f]/14[f], Mishaev-Schwartz in view of Durbin does.

1. Durbin

Durbin explained that, “[g]enerally, public wireless networks are unsecured,” putting its users “at a risk of getting hacked and lo[]sing critical or important information.” (Ex-1011 ¶0001.) As Durbin acknowledged, “establish[ing] a secure connection on public wireless networks” has been an “area of interest,” “particular[ly],...using advanced techniques such as secure...VPN[] connections.” (*Id.*) Such VPNs “provide secure communication within public wireless networks,” allowing, e.g., a “mobile device” to transmit “sensitive information” to an “information sensitive service center” through “an unsecured public wireless network such as from a cyber café,” while preventing a “promiscuous” device (“e.g., device of a hacker in the café”) from “monitor[ing] and gather[ing] the sensitive information.” (*Id.*, ¶0026, ¶0024, ¶0049, ¶0037; Ex-1003, ¶247.)

Durbin explained that these VPNs may require “manual[]” setup, “which is technically complex and time consuming.” (Ex-1011, ¶0001.) Durbin thus proposed “[a]n approach for automatically securing a public wireless network.” (*Id.*, Abstract.) Specifically, an “application” installed on the mobile device “scan[s] for nearby” APs and determines whether they are to be “trusted.” (Ex-1011, ¶¶0040-42.) If none may be trusted, “then the application transmits a command to a VPN data center and/or VPN service provider to automatically establish the VPN for the mobile device.” (*Id.*, ¶0041.) Thus, when “trying to establish a connection to the information sensitive service center”—i.e., any entity that “may manipulate and/or store sensitive information”—through any such AP’s likewise “untrusted network,” a VPN is “automatically” established between the device and service center. (*Id.*, ¶0026, ¶0021, ¶0039; Ex-1003, ¶248.)

2. Combining Mishaev-Schwartz and Durbin

A POSITA would have been motivated to include forcing the device’s “traffic to be transmitted through a [VPN] connection” as an available mitigation action in Mishaev-Schwartz. And such is taught in Durbin.

Specifically, Schwartz taught that, through mitigation actions, agent sensors installed on wireless devices can “mitigate potential vulnerabilities,” including those arising from “vulnerable networks,” by, e.g., “initiating a secured

communication protocol for transmitting information to and from the wireless device.” (Ex-1010, 3:29-49, 4:56-5:15, 9:54-10:4.) Durbin’s VPN does just that: it provides mobile devices with “secure communication” through an otherwise “untrusted network”—as “automatically” established by a likewise device-installed “application”—thereby allowing even “sensitive information” to be transmitted by that device through the network. (*Id.*, ¶¶0026, ¶¶0021, ¶¶0039; Ex-1003, ¶250.)

Durbin’s teachings thus align with Schwartz’s in both function and implementation; a POSITA would have thus been motivated to utilize Durbin’s VPN as one of Schwartz’s mitigation actions as proposed and would have had no difficulty in doing so. (*See PACT*, 61 F.4th at 1380.) Indeed, notwithstanding such overlap, a POSITA would have been motivated to utilize Durbin’s VPN given its improvements to security and ease of functionality as discussed. (Ex-1003, ¶251.)

Accordingly, in “Mishaev-Schwartz-Durbin,” Mishaev-Schwartz is modified such that one of the mitigation actions utilized by the client device’s CMA includes establishing a VPN for transmitting traffic to/from the client device through a network, as taught in Durbin. (Ex-1003, ¶252.)

3. Analysis

As explained in Ground 3, Mishaev-Schwartz renders all challenged claims obvious, including, *inter alia*, because the CMA of Mishaev’s client device starts a

VPN application as one of its mitigation actions. (*See, e.g., supra* Section VIII.C.4.g.) As explained *supra* Section VIII.D.2, this does not change in Mishaev-Schwartz-Durbin. Mishaev-Schwartz-Durbin therefore operates identically to Mishaev-Schwartz and, thus, renders all challenged claims obvious for the same reasons explained *supra* Section VIII.C. (Ex-1003, ¶253.)

IX. CONCLUSION

Accordingly, the Board should institute IPR and cancel the challenged claims.

Dated: October 16, 2026

12275 El Camino Real, Ste 100
San Diego, California, 92130
Phone: (858) 720-8900
Fax: (858) 509-3691

Respectfully submitted,

SHEPPARD, MULLIN,
RICHTER & HAMPTON LLP

/s/ Thomas Millikan
Thomas Millikan (Reg. No. 72,316)

Back-up Counsel
Joseph P. Reid (Reg. No. 72,317)
Andrew Klein (*PHV* forthcoming)
Lu Ling (Reg. No. 78,121)

Attorneys for Netskope, Inc.

CERTIFICATE OF WORD COUNT UNDER 37 CFR §42.24(D)

Under 37 C.F.R. §42.24(d), the undersigned certifies that the word count for this Petition for *Inter Partes* Review totals 13959 words, excluding the parts exempted by 37 C.F.R. §42.24(a). The word count was made using the built-in word count function in the Microsoft® Word 365 software used to prepare this document.

Dated: October 16, 2026

12275 El Camino Real, Ste 100
San Diego, California, 92130
Phone: (858) 720-8900
Fax: (858) 509-3691

Respectfully submitted,

SHEPPARD, MULLIN,
RICHTER & HAMPTON LLP

/s/ Thomas Millikan
Thomas Millikan (Reg. No. 72,316)

Back-up Counsel
Joseph P. Reid, (Reg. No. 72,317)
Andrew Klein, (*PHV forthcoming*)
Lu Ling (Reg. No. 78,121)

Attorneys for Netskope, Inc.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that true copies of this petition for *Inter Partes* Review and supporting materials (Exhibits 1001-1011, 1013-1019 and Power of Attorney) have been served via USPS Express Mail, postage prepaid, at the following correspondence address of record:

176502 - FORTINET/Jaffery Watson Hamilton & DeSanctis LLP
7501 Village Square Drive, Suite 206
Castle Pines, CO 80108
UNITED STATES

In addition, the undersigned certifies that a true copy of the petition and supporting materials have been served on Patent Owner via email to its legal counsel:

Ryan Kiyoto Iwahashi - ryan@gishpllc.com
Andrew Gish - andrew@gishpllc.com
Josef Bryks Schenker - josef.schenker@gishpllc.com
Christopher M. Gerson - chris.gerson@gishpllc.com
David A. Nelson - davenelson@quinnemanuel.com
Athena Diane Dalton - athenadalton@quinnemanuel.com
Harrison Rose - harrisonrose@quinnemanuel.com
Alexander Rudis - alexanderrudis@quinnemanuel.com
Jeffrey S. Gerchick - jeffgerchick@quinnemanuel.com
Andrew Michael Holmes - drewholmes@quinnemanuel.com
Steven Carl Cherny - stevencherny@quinnemanuel.com
Ognjen Zivojnovic - ogizivojnovic@quinnemanuel.com
Justin Jeffery Sorensen - justinsorensen@quinnemanuel.com

Dated: October 16, 2026

12275 El Camino Real, Ste 100
San Diego, California, 92130
Phone: (858) 720-8900
Fax: (858) 509-3691

Respectfully submitted,

SHEPPARD, MULLIN,
RICHTER & HAMPTON LLP

/s/ Thomas Millikan
Thomas Millikan (Reg. No. 72,316)

Back-up Counsel
Joseph P. Reid, (Reg. No. 72, 317)
Andrew Klein, (*PHV forthcoming*)
Lu Ling (Reg. No. 78,121)

Attorneys for Netskope, Inc.