

NOTE: This disposition is nonprecedential.

**United States Court of Appeals
for the Federal Circuit**

VIRNETX INC.,
Appellant

v.

**MANGROVE PARTNERS MASTER FUND, LTD.,
APPLE INC.,**
Appellees

**KATHERINE K. VIDAL, UNDER SECRETARY OF
COMMERCE FOR INTELLECTUAL PROPERTY
AND DIRECTOR OF THE UNITED STATES
PATENT AND TRADEMARK OFFICE,**
Intervenor

2020-2271

Appeal from the United States Patent and Trademark
Office, Patent Trial and Appeal Board in Nos. IPR2015-
01046, IPR2016-00062.

VIRNETX INC.,
Appellant

v.

**MANGROVE PARTNERS MASTER FUND, LTD.,
APPLE INC., BLACK SWAMP IP, LLC,**
Appellees

**KATHERINE K. VIDAL, UNDER SECRETARY OF
COMMERCE FOR INTELLECTUAL PROPERTY
AND DIRECTOR OF THE UNITED STATES
PATENT AND TRADEMARK OFFICE,**
Intervenor

2020-2272

Appeal from the United States Patent and Trademark Office, Patent Trial and Appeal Board in Nos IPR2015-01047, IPR2016-00063, IPR2016-00167.

Decided: March 30, 2023

STEPHEN BLAKE KINNAIRD, Paul Hastings LLP, Washington, DC, argued for appellant. Also represented by NAVEEN MODI, JOSEPH PALYS, IGOR VICTOR TIMOFEYEV, DANIEL ZEILBERGER; JEFFREY A. LAMKEN, MoloLamken LLP, Washington, DC.

JAMES T. BAILEY, Law Office of James T. Bailey, New York, NY, for appellee Mangrove Partners Master Fund, Ltd.

WILLIAM F. LEE, Wilmer Cutler Pickering Hale and Dorr LLP, Boston, MA, argued for Apple Inc. Also represented by MARK CHRISTOPHER FLEMING, LAUREN B. FLETCHER; BRITTANY BLUEITT AMADI, STEVEN JARED HORN, Washington, DC; THOMAS GREGORY SPRANKLING, Palo Alto, CA; SCOTT BORDER, JEFFREY PAUL KUSHAN, Sidley Austin

VIRNETX INC. v. MANGROVE PARTNERS MASTER FUND

3

LLP, Washington, DC.

THOMAS H. MARTIN, Martin & Ferraro, LLP, Hartville, OH, for appellee Black Swamp IP, LLC. Also represented by WESLEY MEINERDING.

MAUREEN DONOVAN QUELER, Office of the Solicitor, United States Patent and Trademark Office, Alexandria, VA for intervenor. Also represented by KAKOLI CAPRIHAN, DANIEL KAZHDAN, THOMAS W. KRAUSE, FARHEENA YASMEEN RASHEED; MICHAEL GRANSTON, SCOTT R. MCINTOSH, JOSHUA MARC SALZMAN Appellate Staff, Civil Division, United States Department of Justice, Washington, DC.

Before MOORE, *Chief Judge*, HUGHES and STARK, *Circuit Judges*.

STARK, *Circuit Judge*.

In this consolidated appeal, VirnetX Inc. (“VirnetX”) appeals from two final written decisions of the Patent Trial and Appeal Board (“Board”) holding the challenged claims of U.S. Patent Nos. 6,502,135 (“135 patent”) and 7,490,151 (“151 patent”) unpatentable. J.A. 1-28 (regarding ’135 patent); J.A. 29-60 (regarding ’151 patent). VirnetX also challenges Black Swamp IP, LLC’s (“Black Swamp”) joinder. We affirm.

I

VirnetX owns the ’135 and ’151 patents. Both are generally directed to a “secure mechanism for communicating over the internet.” ’135 patent cols. 2-3 ll. 66-67, 1-2; *see also* ’151 patent col. 3 ll. 8-11. These patents have been before us previously, *see, e.g., VirnetX Inc. v. Mangrove Partners Master Fund, Ltd.*, 778 F. App’x 897 (Fed. Cir. 2019) (“*Mangrove Appeal*”); *VirnetX, Inc. v. Cisco Sys., Inc.*,

767 F.3d 1308 (Fed. Cir. 2014) (“*Cisco Appeal*”), so we have had occasion to describe them, doing so as follows:

The ’135 and ’151 patents share a common specification disclosing a system in which, instead of a conventional DNS [“Domain Name Service”] receiving the request, a DNS proxy intercepts it and determines whether the request is for a secure site. If the proxy determines that a request is for a secure site, the system automatically initiates a virtual private network (“VPN”) between the proxy and the secure site. If the browser determines that the request was for a non-secure website, then the DNS proxy forwards the request to a conventional DNS for resolution.

Cisco Appeal, 767 F.3d at 1315 (internal citations omitted).

A

The ’135 patent is entitled “Agile Network Protocol for Secure Communications with Assured System Availability.” Independent claim 1 is representative, with emphasis added to the term principally in dispute:

1. A method of transparently creating a *virtual private network (VPN) between a client computer and a target computer*, comprising the steps of:

(1) generating from the client computer a Domain Name Service (DNS) request that requests an IP address corresponding to a domain name associated with the target computer;

(2) determining whether the DNS request transmitted in step (1) is requesting access to a secure web site; and

(3) in response to determining that the DNS request in step (2) is requesting access to a secure target web site, automatically initiating the VPN between the client computer and the target computer.

'135 patent col. 47 ll. 20-32.

Mangrove Partners Master Fund, Ltd. (“Mangrove”) petitioned for *inter partes* review (“IPR”) of claims 1, 3-4, 7-8, 10, and 12 of the '135 patent, alleging that these claims were anticipated by a 1996 article authored by Kiuchi and Kaihara, entitled “C-HTTP – The Development of a Secure, Closed HTTP-based Network on the Internet” (“Kiuchi”), and that claim 8 was obvious based on Kiuchi in view of Mockapetris, Request for Comment 1034, “Domain Names – Concepts and Facilities,” Nov. 1997 (“RFC 1034”). J.A. 5. Once the Board instituted review, Apple Inc. (“Apple”) filed additional IPR petitions and was joined to Mangrove’s IPR proceeding. *See Mangrove Appeal*, 778 F. App’x at 900-01.

B

The '151 patent is entitled “Establishment of a Secure Communication Link Based on a Domain Name Service (DNS) Request.” Independent claim 13 is representative, again with emphasis added to the terms in dispute:

13. A computer readable medium storing a *domain name server (DNS) module* comprised of computer readable instructions that, when executed, cause a data processing device to perform the steps of:

(i) *determining* whether a DNS request sent by a client corresponds to a secure server;

(ii) when the DNS request does not correspond to a secure server, *forwarding* the DNS request to a DNS function that returns an IP address of a nonsecure computer; and

(iii) when the intercepted DNS request corresponds to a secure server, automatically *creating* a secure channel between the client and the secure server.

'151 patent col. 48 ll. 18-29.

Mangrove petitioned for IPR of claims 1-2, 6-8, and 12-14 of the '151 patent, alleging they were anticipated by Kiuchi and obvious based on (a) Kiuchi in view of RFC 1034, (b) Kiuchi in view of a 1996 reference by Rescorla and Schiffman, entitled "The Secure Hypertext Transfer Protocol" ("Rescorla"), and (c) Kiuchi in view of RFC 1034 and in further view of Rescorla. J.A. 33. Apple was also joined to the proceeding. *See Mangrove Appeal*, 778 F. App'x at 900-01. Black Swamp then petitioned for IPR of claims 1-2, 6-8, and 12-14 and moved for joinder, which the Board granted. *See id.* at 901 n.1.

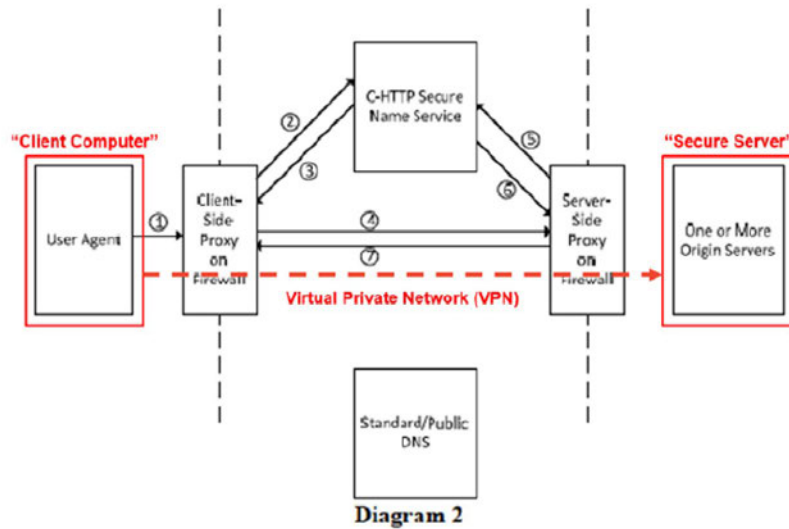
In the remainder of this opinion, we will refer to Mangrove, Apple, and Black Swamp collectively as "Petitioners."

C

Kiuchi is the only reference at issue in this appeal. This is because Kiuchi provided some or all of the bases on which the Board predicated its unpatentability decisions

with respect to the challenged claims in the '135 and '151 patents. *See* J.A. 26; J.A. 58.¹

Kiuchi's secure network was developed to ensure the "[s]ecure transfer of patient information for clinical use" in a hospital setting. J.A. 5266. A depiction of an embodiment of Kiuchi – prepared by Petitioners' expert, annotated by Petitioners' counsel, and then relied on by the Board –



¹ The Board determined that the challenged claims of the '135 patent were all anticipated by Kiuchi and did not reach Mangrove's additional unpatentability ground. J.A. 26. With respect to the '151 patent, the Board found that Kiuchi anticipated claims 13 and 14 and the combination of Kiuchi and Rescorla rendered claims 1-2, 6-8, and 12-14 obvious. J.A. 58. This appeal presents no issues relating to Rescorla or RFC 1034. Given that the only issues on appeal relate to Kiuchi, our affirmance of the Board's judgment of anticipation by Kiuchi of claims 13 and 14 of the '151 patent leads us also to affirm the Board's determination that claims 1-2, 6-8, and 12-14 of the same patent are unpatentable due to obviousness.

is reproduced and explained below. J.A. 12-13; *see also* J.A. 7066.

As shown, in Kiuchi a client or “user agent” first sends a uniform resource locator (“URL”) to the client-side proxy (step 1 in Diagram 2). J.A. 5267; *see also* J.A. 5454. Next, the client-side proxy sends the URL to the C-HTTP secure name service, which checks if the client-side proxy is permitted to connect with the host (also known as an “origin server”) to which the URL corresponds (step 2). *See* J.A. 5267. If the client-side proxy is authorized to communicate with that host, “the C-HTTP name server sends the IP address and public key of the server-side proxy and both request and response Nonce values” or returns an error code (step 3). *Id.* Then, the client-side proxy sends a connection request to the server-side proxy (step 4). *Id.* The server-side proxy checks with the C-HTTP name server to verify that the client-side proxy is “an appropriate member of the closed network” (steps 5 and 6). J.A. 5267-68. If so, “the C-HTTP name server sends the IP address and public key of the client-side proxy [to the server-side proxy] and both request and response Nonce values, which are the same as those sent to the client-side proxy” (step 7). J.A. 5268. Both the client-side proxy and server-side proxy then authenticate each other, and a secure connection – the dashed line “Virtual Private Network (VPN)” in Diagram 2 – is established. *Id.*

As the Board stated, Kiuchi teaches that after the steps outlined above, “a VPN between the user agent and the origin server that passes through the client-side proxy and server-side proxy” is established. J.A. 12. At that point, the “client-side proxy forwards HTTP/1.0 requests from the user agent in encrypted form using C-HTTP format” to the server-side proxy, and the “server-side proxy forwards requests to the origin server.” J.A. 5268. Thereafter, the origin server’s response is “encrypted in C-HTTP format by the server-side proxy and is forwarded to the client-side

proxy” which decrypts it, and the response is ultimately sent to the user agent. *Id.*

D

In September 2016, the Board issued a final written decision finding all challenged claims of the ’135 patent unpatentable. J.A. 1723-58. VirnetX had argued that the preamble of claim 1, which recites a *virtual private network (VPN) between a client computer and a target computer*, was limiting and must be construed in light of a disclaimer VirnetX had made during reexamination of its ’135 patent. *See, e.g.*, J.A. 1737-38. VirnetX argued that it had “disclaimed any virtual private networks and virtual private network communication links that are not direct,” J.A. 1192, and had done so to distinguish Aventail, a prior-art reference teaching “a system and architecture for transmitting data between two computers using the SOCKS protocol,” J.A. 7763-64. The Board disagreed, finding no disclaimer. *See* J.A. 1738.

VirnetX then appealed to this Court. *See Mangrove Appeal*, 778 F. App’x at 909-10. Contrary to the Board, we determined that “[t]he statements VirnetX made during reexamination constitute disclaimer.” *Id.* at 910. The source of this disclaimer is VirnetX’s 2010 response to an Office Action rejection based on Aventail. *See* J.A. 7760, 7763-66. In that response, VirnetX stated:

Aventail discloses a system where a client on a public network transmits data to a SOCKS server *via a singular, point-to-point SOCKS connection at the socket layer of the network architecture*. The SOCKS server then *relays* that data to a target computer on a private network on which the SOCKS server also resides. All communications between the client and target stop and start at the intermediate SOCKS

server. The client cannot open a connection with the target itself.

J.A. 7766 (internal citations omitted and emphasis added). In the *Mangrove* Appeal, we held:

VirnetX described a system in which a client computer communicates with an intermediate server via a singular, *point-to-point connection*. That intermediate server then *relays* the data to a target computer on the same private network on which the server resides. VirnetX stated that because the computers “do not communicate directly with each other” and “[t]he client cannot open a connection with the target itself,” the computers are not on the same VPN. This clearly and unmistakably states that a “VPN between the client computer and the target computer” requires direct communication between the client and target computers.

Id. at 910 (quoting J.A. 7766) (internal citations omitted and emphasis added).

We vacated the Board’s judgment of unpatentability and remanded for the Board to consider whether, as a factual matter, Kiuchi taught a direct-communication VPN – in which case it would anticipate the challenged claims of the ’135 patent – or whether, instead, Kiuchi taught an indirect-communication VPN – which would bring Kiuchi within the scope of VirnetX’s disclaimer and, consequently, render it non-anticipating. *See id.*

On remand, the Board issued a second final written decision in July 2020. J.A. 1-28 (“2020 ’135 FWD”). There, the Board again found all the challenged claims in the ’135

patent unpatentable. J.A. 26. In particular, the Board found that Kiuchi disclosed a *virtual private network (VPN) between a client computer and a target computer* with direct communication and, thus, Kiuchi anticipated the challenged claims. J.A. 18. After considering VirnetX's description of its claimed VPN as one "where data can be addressed to one or more different computers across the network, regardless of the location of the computer," and VirnetX's expert's testimony that "direct communication refers to direct addressability," the Board concluded that "the ability to address data to a particular computer is a key aspect of the claimed VPN." J.A. 14. The Board reasoned that "Kiuchi's system, unlike the disclaimed scope, allows a client (the user agent) to connect to a remote [origin] server transparently and access resources with only the single URL identifying the remote resource." J.A. 15. Therefore, according to the Board, Kiuchi discloses a direct-communication VPN between the client and target and anticipates the challenged claims of the '135 patent. J.A. 18.

E

Meanwhile, also in September 2016, the Board issued its first final written decision concerning the challenged claims of the '151 patent. *See* J.A. 4233-70. In it, the Board found that all challenged claims (1-2, 6-8, and 12-14) were unpatentable as anticipated by Kiuchi or obvious in view of Kiuchi and other references. *Id.* We addressed VirnetX's subsequent appeal as part of our opinion in the *Mangrove Appeal*, 778 F. App'x at 906. As with the '135 patent, we disagreed with the Board, holding that "[s]ubstantial evidence does not support the Board's finding that the C-HTTP name server [of Kiuchi] performs the functions of the claimed DNS proxy module" in the '151 patent. *Id.*

Accordingly, we vacated the Board's judgment and remanded for further proceedings. *See id.* at 911.

On remand, in July 2020, the Board issued a second final written decision regarding the '151 patent. J.A. 29-60 ("2020 '151 FWD"). The Board explained that Petitioners were asserting that Kiuchi's "client-side proxy – working in concert with the C-HTTP name server – is a domain name server (DNS) proxy module that intercepts DNS requests sent by a user agent acting as a client." J.A. 38-39. The Board agreed with Petitioners' analysis, finding that Kiuchi's client-side proxy and C-HTTP name server together perform all the DNS module's pertinent claim limitations and, therefore, that Kiuchi anticipates claims 13 and 14, *see* J.A. 39-47, and Kiuchi in combination with Rescorla renders all of the challenged claims obvious, J.A. 58.²

F

VirnetX timely appealed the Board's determinations that Kiuchi anticipates the challenged claims of the '135 patent, as the Board explained in the 2020 '135 FWD, and anticipates claims 13 and 14 of the '151 patent, as explained in the 2020 '151 FWD. On appeal, VirnetX's main contention with respect to the '135 patent is that Kiuchi does not teach direct communication but, instead, only indirect communication, which brings Kiuchi within the scope of VirnetX's disclaimer and outside the scope of its

² On appeal, VirnetX challenges only the Board's assessment of Kiuchi; it presents no non-Kiuchi-based criticism of the Board's obviousness analysis. VirnetX does not dispute that if we affirm the Board's determination that claims 13 and 14 of the '151 patent are anticipated by Kiuchi then we must also affirm the Board's conclusion that all of the challenged claims of the '151 patent are unpatentable as obvious. We will do so.

claims. Its principal argument with respect to the '151 patent is that Kiuchi does not teach a DNS proxy module capable of performing the determining, forwarding, and creating steps of the challenged claims. Finally, VirnetX argues that the Board improperly joined Black Swamp to the IPR concerning the '151 patent (i.e., IPR2015-01047).³

We have jurisdiction to review final written decisions of the Board under 28 U.S.C. § 1295(a)(4)(A).

II

We review the Board's legal determinations de novo and its factual findings for substantial evidence. *See Almirall, LLC v. Amneal Pharms. LLC*, 28 F.4th 265, 271 (Fed. Cir. 2022). Substantial evidence is "such relevant evidence as a reasonable mind might accept as adequate to support a conclusion." *Consol. Edison Co. v. NLRB*, 305 U.S. 197, 229 (1938). "[T]he possibility of drawing two inconsistent conclusions from the evidence does not prevent an administrative agency's finding from being supported by substantial evidence." *Consolo v. Fed. Maritime Comm'n*, 383 U.S. 607, 620 (1966).

Anticipation presents a question of fact we review for substantial evidence. *See Husky Injection Molding Sys. Ltd. v. Athena Automation Ltd.*, 838 F.3d 1236, 1248 (Fed. Cir. 2016). The Board's conclusions about what a prior-art reference discloses are also reviewed for substantial

³ VirnetX initially challenged the authority of Acting Director Commissioner Hirshfeld to issue final decisions in light of *United States v. Arthrex, Inc.*, 141 S. Ct. 1970 (2021). The government intervened to address this challenge. VirnetX later acknowledged that this argument is foreclosed by our decision in *Arthrex, Inc. v. Smith & Nephew, Inc.*, 35 F.4th 1328 (Fed. Cir. 2022). *See* No. 20-2271 ECF No. 107. Therefore, we do not address it.

evidence. See *Elbit Sys. of Am. v. Thales Visionix, Inc.*, 881 F.3d 1354, 1357 (Fed. Cir. 2018).

To anticipate under 35 U.S.C. § 102, a single prior-art reference “must not only disclose all elements of the claim within the four corners of the document, but must also disclose those elements ‘arranged as in the claim.’” *NetMoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1369 (Fed. Cir. 2008) (quoting *Connell v. Sears, Roebuck & Co.*, 722 F.2d 1542, 1548 (Fed. Cir. 1983)). “The requirement that the prior art elements themselves be arranged as in the claim means that claims cannot be treated . . . as mere catalogs of separate parts, in disregard of the part-to-part relationships set forth in the claims and that give the claims their meaning.” *Therasense, Inc. v. Becton, Dickinson & Co.*, 593 F.3d 1325, 1332 (Fed. Cir. 2010) (internal quotation marks omitted).

III

Substantial evidence supports the Board’s conclusion that Kiuchi teaches a direct-communication VPN and is therefore within the scope of the claims of VirnetX’s ’135 patent, and not an indirect-communication VPN, which would have brought Kiuchi within the scope of VirnetX’s disclaimer. It follows that Kiuchi, which is undisputedly prior art to the ’135 patent, anticipates the challenged claims of the ’135 patent.

A

As we explained in the *Mangrove* Appeal, when VirnetX distinguished Aventail during reexamination of the ’135 patent, VirnetX disclaimed “a system in which a client computer communicates with an intermediate server via a singular, point-to-point connection.” 778 F. App’x at 910. To be within the scope of VirnetX’s claims, therefore, “requires direct communication between the client and target computers.” *Id.* We remanded for the Board to make a factual determination as to whether Kiuchi involves

“singular, point-to-point connection[s]” with intermediate components sitting between a client and a target computer, or whether, instead, Kiuchi involves “direct communication” between a client and target computer, even if intermediate components sit between the client and target. *Id.*

On remand, the Board found “by a preponderance of evidence that Kiuchi discloses direct communication that satisfies the claimed VPN.” J.A. 18. In doing so, the Board expressly found “that Kiuchi’s system does not use a singular, point-to-point connection as was disclaimed,” and as had been used in Aventail. *Id.* The Board rejected VirnetX’s contrary arguments as “conflat[ing] link with connection,” J.A. 13, and focused instead on the “nature of the overall connection,” J.A. 14. In particular, the Board found that “Kiuchi’s user agent does not communicate with the client-side proxy using a singular, point-to-point connection because the user agent addresses the desired endpoint and the VPN provides the required message routing for the user agent to receive a response from the desired endpoint.” J.A. 15.

The Board’s conclusions are grounded in its reading of Kiuchi and the ’135 patent. Its conclusions are supported by substantial evidence.⁴

We agree with the Board the VirnetX “provides no explanation of why Kiuchi’s connection is a point-to-point connection.” J.A. 16. To the contrary, as the Board explained:

Kiuchi’s system . . . allows a client (the user agent) to connect to a remote server transparently and access

⁴ The Board stated that a declaration filed by Petitioners’ expert, Dr. Guerin, “d[id] not drive [its] conclusion on any disputed issue.” J.A. 24; J.A. 56.

resources with only the single URL identifying the remote resource. Kiuchi's system operates like the '135 patent's TARP,^[5] which allows the system to route a packet as required to reach the destination address provided by the client computer. Kiuchi's user agent does not communicate with the client-side proxy using a singular, point-to-point connection because the user agent addresses the desired endpoint and the VPN provides the required message routing for the user agent to receive a response from the desired endpoint.

J.A. 15 (internal citations omitted).

As the Board further found, Kiuchi's proxy servers *forward* data packets and do not, instead, *relay* data packets from point to point. *See, e.g.,* J.A. 12; *see also* J.A. 5268 (Kiuchi using language such as "client-side proxy forwards," "[f]orwarding requests to an origin server," "server-side proxy forwards," "[a]n HTTP/1.0 response sent from the origin server to the server-side proxy is encrypted in C-HTTP format by the server-side proxy, and is forwarded to the client-side proxy"). Forwarding is within the scope of the claims, while relaying – which involves point-to-point communication, as data packets are accumulated at an intermediate point before being relayed to their next destination – is within the scope of VirnetX's disclaimer. We know this from Aventail, which is the basis for VirnetX's disclaimer, and in which the SOCKS server "*relays . . . data to*

⁵ TARP is the '135 patent's "Tunneled Agile Routing Protocol." *See, e.g.,* J.A. 4. TARP routing, which is expressly within the scope of the claims, uses "multiple links between two TARP terminals." J.A. 14.

a target computer on a private network on which the SOCKS server also resides.” J.A. 7766 (emphasis added); *see also Mangrove Appeal*, 778 F. App’x at 910 (describing VirnetX’s disclaimer as encompassing systems where “intermediate server then relays the data to a target computer”). In this way, communications between the client and target “stop and start at the intermediate SOCKS server,” preventing “[t]he client [from] open[ing] a connection with the target itself.” *Id.* at 909. Kiuchi, by using forwarding, instead involves direct communication within the scope of VirnetX’s claims.⁶

Additionally, the Board found that Kiuchi discloses “direct addressability,” which is “the ability to address data to a particular computer,” a “key aspect of the claimed VPN.” J.A. 14. The Board found that Kiuchi teaches direct addressability because “Kiuchi’s user agent generates a request that includes a resource address (in the form of a

⁶ VirnetX argues that Kiuchi’s proxies “modif[y] HTML documents” and that this prevents direct communication. *See, e.g.*, Opening Br. 42 (citing J.A. 5267-68). As Petitioners point out, however, there is substantial evidence that Kiuchi transmits at least some data, like image or sound data, without modification. *See, e.g.*, Answering Br. 31 (citing J.A. 5893 (VirnetX’s expert agreeing that Kiuchi “can transfer files of various kinds”); J.A. 5910 (VirnetX’s expert unable to “recall” anything in Kiuchi “that said that sound or image data files are modified when they are transferred from an origin server to a user agent”)). This is sufficient to satisfy the requirement for direct communication. *See* J.A. 17 (“Kiuchi’s disclosures of at least those types of resources [e.g., image and sound objects] maintain the requirement for direct communication.”).

URL).” *Id.* (citing portions of Kiuchi).⁷ As support, the Board observed that a VirnetX expert, Dr. Monroe, “testified that Kiuchi’s URL provided by the user agent is an address of the resource on an origin server.” J.A. 14-15. To the extent “direct communication refers to direct addressability,” as another VirnetX expert, Dr. Jones, testified (J.A. 6206), substantial evidence supports the Board’s finding that Kiuchi discloses direct addressability and, therefore, direct communication.

The Board’s factual finding that Kiuchi discloses direct communication within the scope of VirnetX’s claims, and not indirect communication within the scope of VirnetX’s disclaimer, is also consistent with the infringement claims VirnetX has litigated. In the *Cisco* Appeal, we affirmed a judgment that Apple’s VPN On Demand service infringed the ’135 patent, finding substantial evidence existed to support the conclusion that VPN On Demand involved direct communication even though it used “security measures including VPN servers, VPN authentication servers, proxy servers, and firewalls,” all placed between a client and target computer. 767 F.3d at 1321.

In the same opinion, we affirmed a finding that certain embodiments of Apple’s FaceTime service infringed claims of related patents. *See id.* at 1319-20. Part of the *Cisco* Appeal involved VirnetX’s assertion of U.S. Patent Nos. 7,418,504 and 7,921,211 against Apple’s FaceTime servers. *Id.* at 1313. The asserted claims included a “secure communication link” limitation that required direct

⁷ VirnetX argues that Kiuchi’s use of a URL cannot alone distinguish direct communication from indirect communication. *See, e.g.*, Reply Br. 7. We agree, but we do not read the Board’s decision as stating otherwise. *See, e.g.*, J.A. 14-15 (explaining that once connection is established, IP addresses of proxies are used, and proxies forward packets to user agent or origin server as needed).

communication, just like the claims of the '135 patent. *Id.* at 1314. We rejected Apple's contention that it was entitled to judgment of non-infringement as a matter of law, a request Apple based on its argument that the accused FaceTime servers addressed communication to intermediate network address translators ("NATs") rather than directly to the receiving device, preventing – according to Apple – direct communication. *See id.* at 1319-20.

To the contrary, we determined that the district court did not err in concluding that there was "substantial evidence to support the jury's finding that NAT routers used by FaceTime do not impede direct communication" "because they merely translate addresses from the public address space to the private address space, but do not terminate the connection" between the FaceTime server and the receiving device. *Id.*; *see also id.* at 1314 ("Apple's FaceTime server . . . forwards the invitation to a network address translator ('NAT') which, in turn, readdresses the invitation and sends it on to the receiving device."). We found support for this conclusion in the district court's claim construction, which provided that "routers, firewalls, and similar servers . . . do not impede 'direct' communication." *Id.* at 1320 (quoting *VirnetX Inc. v. Apple Inc.*, 925 F. Supp. 2d 816, 831 (E.D. Tex. 2013)).

Further confirmation for our holding today is found in the fact that, in the litigation leading to the *Cisco* Appeal, VirnetX agreed that another FaceTime embodiment – the relay embodiment – did *not* have an infringing direct-communication VPN. Specifically, VirnetX "concede[d] that the [FaceTime] feature does not infringe if calls are routed through a relay server, because there is *no direct communication through a relay server.*" *VirnetX Inc.*, 925 F. Supp. 2d at 830 (emphasis added). In this respect, the relay server embodiment of FaceTime was like the Aventail embodiment VirnetX has clearly and unmistakably disclaimed.

Thus, again, substantial evidence supports the Board's finding that Kiuchi anticipates the challenged claims of the '135 patent.⁸

B

In its reply brief, VirnetX refined its argument as to what constitutes "direct communication," now asserting that its claims specifically require "a *transport-layer* [or TCP] connection directly between the user agent and the origin server." Reply Br. 3 (emphasis added).⁹ At oral argument, VirnetX placed significant emphasis on this new argument, suggesting that the '135 patent's claims only encompass direct connections between a user and target computer at the transport layer, so direct connections at any of the other six layers would be outside the scope of its claims

⁸ We recognize that in the *Cisco* Appeal, 767 F.3d at 1324, we affirmed the district court's entry of judgment of no invalidity, based on the jury having "heard expert testimony that Kiuchi's client-side and server-side proxies terminate the connection, process information, and create a new connection – actions that are not 'direct' within the meaning of the asserted claims." That we upheld this verdict, which was based on a finding that Apple failed to prove anticipation by clear and convincing evidence, did not preclude the Board from finding, on a different record, anticipation by its own standard of a preponderance of the evidence.

⁹ VirnetX was referring to the seven-layer Open Systems Interconnection ("OSI") model, which consists of the following layers: physical, data link, network, transport, session, presentation, and application. See Reply Br. 2; see also '135 patent col. 4 ll. 3-6 (referencing network layer, data link layer, and application layer); '151 patent col. 4 ll. 11-14 (same).

(and therefore do not anticipate). *See* Oral Arg. at 6:20-6:36 (VirnetX counsel distinguishing TARP embodiments, which are within scope of '135 patent's claims, from Kiuchi, based on TARP routers' operation at network layer).¹⁰

VirnetX's argument that direct connections at layers other than the transport layer are irrelevant was not made in its opening brief and is forfeited. *See Quanergy Sys., Inc. v. Velodyne Lidar USA, Inc.*, 24 F.4th 1406, 1415 n.6 (Fed. Cir. 2022) (party's failure to challenge Board's findings in opening brief constituted forfeiture). "[F]orfeiture is the failure to make the timely assertion of a right." *United States v. Olano*, 507 U.S. 725, 733 (1993). At oral argument, VirnetX's counsel conceded that VirnetX had not, as the Court put it, made "this much more fine-tuned distinction between saying . . . connection means one thing in the network layer and a different thing in the transport layer" in its opening brief. Oral Arg. at 30:25-41. Even considering the parties' uninvited post-argument letters (No. 20-2271 ECF Nos. 111, 112), we have been pointed to nowhere in our record where VirnetX made this distinction prior to its reply brief in this appeal.¹¹ Accordingly, this issue is

¹⁰ Oral Argument ("Oral Arg."), available at https://oralarguments.ca9.uscourts.gov/default.aspx?fl=20-2271_09082022.mp3.

¹¹ Perplexingly, VirnetX attached to its letter excerpts from a brief and oral presentation *Petitioners* made to the Board. *See* No. 20-2271 ECF No. 111 Exs. A & B. VirnetX also now insists it raised the issue in its opening brief. *See* No. 20-2271 ECF No. 111 at 1. But all it said there was the following:

forfeited and we need not, and will not, address it. *See generally* *Quanergy Sys., Inc.*, 24 F.4th at 1415 n.6 (“Quanergy failed to challenge these findings in its opening brief, and its attempt to do so in its reply brief is untimely.”); *see also* *SmithKline Beecham Corp. v. Apotex Corp.*, 439 F.3d 1312, 1319 (Fed. Cir. 2006) (“Our law is well established that arguments not raised in the opening brief are waived.”).

Accordingly, we affirm the Board’s finding that Kiuchi anticipates the challenged claims of the ’135 patent.

IV

Substantial evidence also supports the Board’s conclusion that Kiuchi teaches a domain name server (“DNS”) module and, therefore, anticipates claims 13 and 14 of the ’151 patent.

Claim 13 of the ’151 patent requires a DNS module to “perform the steps” of “*determining* whether a DNS request

TARP is a packet-routing protocol that, like the IP protocol, operates at or below the network layer of Internet communications. End-to-end “connections” between computers are formed at a higher layer, the transport layer, typically using the TCP protocol. . . . TARP routing does not affect how computers form connections or engage in direct or indirect communication.

Opening Br. 36 (internal citations omitted). As is evident, VirnetX did *not* argue in its opening brief that only connections at the transport layer matter for assessing infringement, anticipation, or the scope of VirnetX’s claims or disclaimer.

sent by a client corresponds to a secure server;” “when the DNS request does not correspond to a secure server, *forwarding* the DNS request to a DNS function that returns an IP address of a nonsecure computer;” and “when the intercepted DNS request corresponds to a secure server, automatically *creating* a secure channel between the client and the secure server.” ’151 patent col. 48 ll. 18-29 (emphasis added). In the *Mangrove* Appeal, we held that substantial evidence did not support the Board’s finding that Kiuchi’s C-HTTP name server alone taught the *determining, forwarding, and creating* limitations of claim 13. *See* 778 F. App’x at 906-07. In particular, we determined that Kiuchi’s C-HTTP name server “does not forward a DNS request to a DNS function.” *Id.* at 906.

On remand, Petitioners argued that Kiuchi’s “client-side proxy, working with the C-HTTP name server, acts as the claimed DNS proxy module.” J.A. 38.¹² The Board adopted this mapping of Kiuchi onto claim 13 and found anticipation. *See, e.g.*, J.A. 43-44. We find substantial evidence, primarily Kiuchi itself, supports the Board’s finding.

As an initial matter, we agree with the Board that the ’151 patent explicitly teaches that its “claims are not limited to a particular arrangement of hardware,” as even VirnetX acknowledges. J.A. 42-43; *see also* Opening Br. 49 (“[T]he claims [of the ’151 patent] are not limited to a particular arrangement of hardware.”) (emphasis omitted).

¹² Notwithstanding VirnetX’s argument to the contrary, *see, e.g.*, Opening Br. 13, Petitioners have, from the outset of the IPR, mapped two of Kiuchi’s parts – the client-side proxy and the C-HTTP server – to the DNS proxy module. *See, e.g.*, J.A. 2652 (Mangrove, in its petition for institution of IPR, arguing, “[f]or example, Kiuchi’s client-side proxy – working in concert with the C-HTTP name server – is a domain name server (DNS) proxy module . . .”).

The '151 patent's specification contemplates combining the functions of DNS proxy 2610 and DNS server 2609 for convenience. See '151 patent col. 38 ll. 30-32; see also, e.g., *id.* col. 38 ll. 22-24 ("Gatekeeper 2603 can be implemented on a separate computer (as shown in FIG. 26) or as a function within modified DNS server 2602.").

Nonetheless, VirnetX asserts that Kiuchi's client-side proxy and C-HTTP name server are "two distinct modules/sets of instructions" that do not "disclose the single DNS module of the claims." See, e.g., Opening Br. 49. We disagree. Nothing in the record warrants limiting the module of claim 13 in the way VirnetX insists we must. Nor does VirnetX persuasively explain why a "module" cannot be composed of components in a client-server relationship. See, e.g., Opening Br. 47-51; Reply Br. 13-18. As we have already noted, the specification contemplates different arrangements of hardware, and VirnetX cites no meritorious reason why two components of Kiuchi could not comprise one module.

Kiuchi's client-side proxy and C-HTTP name server work cooperatively to "determin[e] whether a DNS request sent by a client corresponds to a secure server," as required by the *determining* limitation of claim 13. See J.A. 42-44. Kiuchi teaches that its "client-side proxy asks the C-HTTP name server whether it can communicate with the host specified in a given URL." J.A. 5267. The C-HTTP name server then "examines whether the requested server-side proxy is registered in the closed network and is permitted to accept the connection from the client-side proxy." *Id.* In this way, again, Kiuchi discloses the '151 patent's *determining* limitation.

Kiuchi's client-side proxy and C-HTTP name server also, together, teach the *forwarding* limitation. In Kiuchi, when the client-side proxy's request to communicate with a host is not permitted, the C-HTTP name server sends an error status code to the client-side proxy, which then

“performs DNS lookup, behaving like an ordinary HTTP/1.0 proxy.” J.A. 39; *see also* J.A. 5267. The Board found that “[b]ehaving like an ordinary proxy to perform the DNS lookup means that the client-side proxy will send the DNS request to a public DNS server,” citing numerous disclosures in Kiuchi as support. J.A. 41; *see also* J.A. 39-42 (citing J.A. 5266-67). Therefore, Kiuchi’s client-side proxy and C-HTTP name server work together, as a DNS module, to “forward[] the DNS request to a DNS function that returns an IP address of a nonsecure computer” “when the DNS request does not correspond to a secure server,” as required by claim 13.¹³

Kiuchi also teaches the *creating* limitation. Kiuchi’s client-side proxy “initiates an encrypted channel on public communication paths between the user agent and the origin server.” J.A. 44. The Board reasoned that claim 13 only requires a secure connection between the user and the secure server, *see id.*, and looked to the ’151 patent’s background-of-the-invention section to define “secure” as “immune to eavesdropping,” J.A. 46 (citing ’151 patent col. 1 ll.

¹³ Even if, as VirnetX argues (*see* Opening Br. 50-51), only the client-side proxy is involved in Kiuchi’s forwarding step, while the combination of the C-HTTP name server and client-side proxy disclose the *determining* limitation, our anticipation cases do not require that every component of the DNS module must be involved in performing every limitation of the challenged claims. VirnetX relies on *NetMoneyIN, Inc.*, 545 F.3d at 1371, and *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1343 (Fed. Cir. 2016), for its counter to Petitioners’ anticipation theory, but each of those cases involved different embodiments in a single prior-art reference. Here, by contrast, both the client-side server and C-HTTP name server of Kiuchi are part of the same embodiment and work together as the DNS module. Our cases do not preclude such a theory of anticipation.

34-35 (“It is desired for the communications to be secure, that is, immune to eavesdropping.”)). The Board was free to credit Petitioners’ evidence that Kiuchi taught the necessary secure channel “because data in Kiuchi’s C-HTTP network is encrypted when sent over public segments of the network path and protected using firewalls when sent over private segments.” J.A. 46 & n.9; *see also* J.A. 5266-67 (Kiuchi discussing communications between client-side and server-side proxies and user agents/origin servers, which are “within the firewalls”); J.A. 5268 (explaining that proxies encrypt information passing between them). Therefore, Kiuchi’s client-side proxy and C-HTTP name server work together to “automatically creat[e] a secure channel between the client and the secure server” “when the intercepted DNS request corresponds to a secure server,” as required by the *creating* limitation of claim 13 of the ’151 patent.

For all of these reasons, we affirm the Board’s conclusion that Kiuchi anticipates claims 13 and 14 of the ’151 patent.¹⁴ Therefore, we also affirm the Board’s conclusion that Kiuchi in view of Rescorla renders all challenged claims of the ’151 patent obvious.

V

Finally, VirnetX contends that Black Swamp was improperly joined in IPR2015-01047, regarding the ’151 patent, and asks us to vacate and remand the Board’s decision based on *Facebook, Inc. v. Windy City Innovations, LLC*, 973 F.3d 1321 (Fed. Cir. 2020). Opening Br. 63-65. The Board granted Black Swamp’s motion for joinder, over VirnetX’s opposition, in early 2016. J.A. 5249-55; *see also* J.A. 5213-22. VirnetX then appealed the Board’s finding

¹⁴ Claim 14 depends from claim 13. VirnetX raises no additional issues with respect to claim 14 that we have not already considered in connection with claim 13.

that certain claims of the '151 patent were unpatentable, but it did not in that appeal – which we have referred to as the *Mangrove* Appeal – raise any issue regarding the Board's joinder of Black Swamp. *See* 778 F. App'x at 901 n.1 (acknowledging Black Swamp's joinder); *id.* at 900 (VirnetX challenging Board's allowance of Apple's joinder but not challenging Black Swamp's joinder). Accordingly, the issue is forfeited. *See, e.g., Vivint v. Alarm.com Inc.*, 856 F. App'x 300, 304 (Fed. Cir. 2021) (explaining “it was [appellant's] obligation to raise its [issue] before the first court who could have provided it relief” and holding that failure to do so led to forfeiture). We need not, and will not, address this forfeited issue.

VI

The Board's findings that Kiuchi anticipates claims of the '135 and '151 patents are supported by substantial evidence. VirnetX's challenge to Black Swamp's joinder is forfeited. We have considered VirnetX's additional arguments and find them unpersuasive. Accordingly, we affirm.

AFFIRMED