

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PALO ALTO NETWORKS, INC.,
Petitioner,

v.

BT AMERICAS INC.,
Patent Owner.

IPR2023-00888
Patent 7,159,237 B2

Before KARL D. EASTHOM, GEORGIANNA W. BRADEN, and
SCOTT RAEVSKY, *Administrative Patent Judges*.

BRADEN, *Administrative Patent Judge*.

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

I. INTRODUCTION

Palo Alto Networks, Inc. (“Petitioner”) filed a Petition requesting an *inter partes* review of claims 1–42 (the “challenged claims”) of U.S. Patent No. 7,159,237 B2 (Ex. 1001, “the ’237 patent”). Paper 2 (“Pet.”). BT Americas Inc. (“Patent Owner”) filed a Preliminary Response. Paper 6 (“Prelim. Resp.”). With our permission (Ex. 3001), Petitioner filed a Reply, to address claim construction arguments. Paper 7 (“Reply”). Patent Owner filed a Sur-reply. Paper 8 (“Sur-reply”).

We have authority to determine whether to institute an *inter partes* review under 35 U.S.C. § 314 and 37 C.F.R. § 42.4. An *inter partes* review may not be instituted unless it is determined that “the information presented in the petition filed under section 311 and any response filed under section 313 shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314; *see also* 37 C.F.R. § 42.4(a) (2022) (“The Board institutes the trial on behalf of the Director.”). The reasonable likelihood standard is “a higher standard than mere notice pleading,” but “lower than the ‘preponderance’ standard to prevail in a final written decision.” *Hulu, LLC v. Sound View Innovations, LLC*, IPR2018-01039, Paper 29 at 13 (PTAB Dec. 20, 2019) (precedential).

For the reasons provided below and based on the record before us, we determine Petitioner has not demonstrated a reasonable likelihood that it would prevail in showing the unpatentability of at least one of the challenged claims. Accordingly, we decline to institute *inter partes* review on any of the alleged grounds of unpatentability.

II. BACKGROUND

A. Real Parties in Interest

Petitioner identifies only itself as real party in interest. Pet. 3. Patent Owner identifies itself and British Telecommunications plc as real parties in interest. Paper 4 (Patent Owner's Mandatory Notices), 1.

B. Related Proceedings

The parties identify the following district court cases involving the '237 patent: *British Telecommunications PLC v. Fortinet, Inc.*, 1:18-cv-01018-CFC-MPT (D. Del.) and *British Telecommunications PLC and BT Americas, Inc. v. Palo Alto Networks, Inc.*, 1:22-cv-01538 (D. Del.). Pet. 3; Paper 4, 1. The parties also identify *inter partes* review proceeding IPR2019-01325. *Id.*

Patent Owner further identifies *inter partes* review proceedings IPR2019-01324 and IPR2023-00889 before the Board as related matters. Paper 4, 1.

C. The '237 Patent (Ex. 1001)

The '237 patent is titled "Method and System for Dynamic Network Intrusion Monitoring, Detection and Response," and issued on January 2, 2007. Ex. 1001, codes (45), (54).

1. Written Description

The '237 patent relates to "network security and, more specifically, to methods and systems for dynamic network intrusion monitoring, detection and response." Ex. 1001, 1:7–9. More specifically, the '237 patent discloses "a managed security monitoring service (the 'MSM service') that monitors a customer's network activity using a probe or 'sentry' system, collects status data from monitored components, filters or otherwise analyzes the collected

data for activity possibly implicating security concerns, alerts and transmits information about such activity to trained security analysts working at secure operations centers (‘SOCs’), and then guides the security analysts and customer through an appropriate response (with appropriate follow-up, if necessary).” *Id.* at 1:50–59.

Figure 1 of the ’237 patent reproduced below:

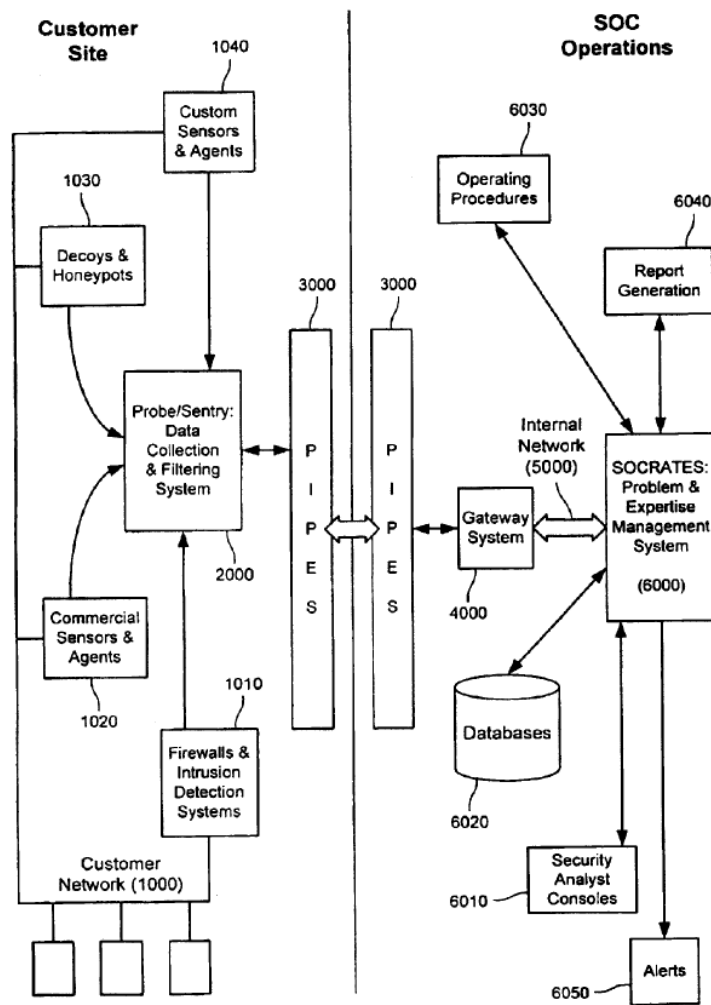


FIG. 1

Id. at Fig. 1. Figure 1 is a diagram depicting “an overview of the system architecture of an exemplary embodiment” disclosed in the ’237 patent. *Id.* at 3:60–61. Figure 1 is divided into two portions, components and systems that operate on the customer site (that is, within the customer’s firewall) and

components and systems that operate within the SOC (that is, within the SOC firewall). *Id.* at 4:38–42. Pipes 3000 provides an encrypted, secure communications path and message protocol for messages sent back and forth between probe/sentry system 2000 at the customer site and gateway system 4000 at the SOC. *Id.* at 5:44–48.

Probe/sentry system 2000 monitors sensors attached to customer network 1000 for evidence of potential security-related events happening on network 1000. *Id.* at 4:48–52. The sensors can include firewalls and intrusion detection systems 1010, commercially available sensors and agents 1020, decoys and honeypots 1030, and custom sensors and agents 1040. *Id.* at 4:52–57. Probe/sentry system 2000 can monitor and collect information from any network component that can be configured to provide a status data (including audit log data and other audit information) concerning the status of network 1000 and its components. *Id.* at 4:58–63.

Figure 2 of the '237 patent is reproduced below:

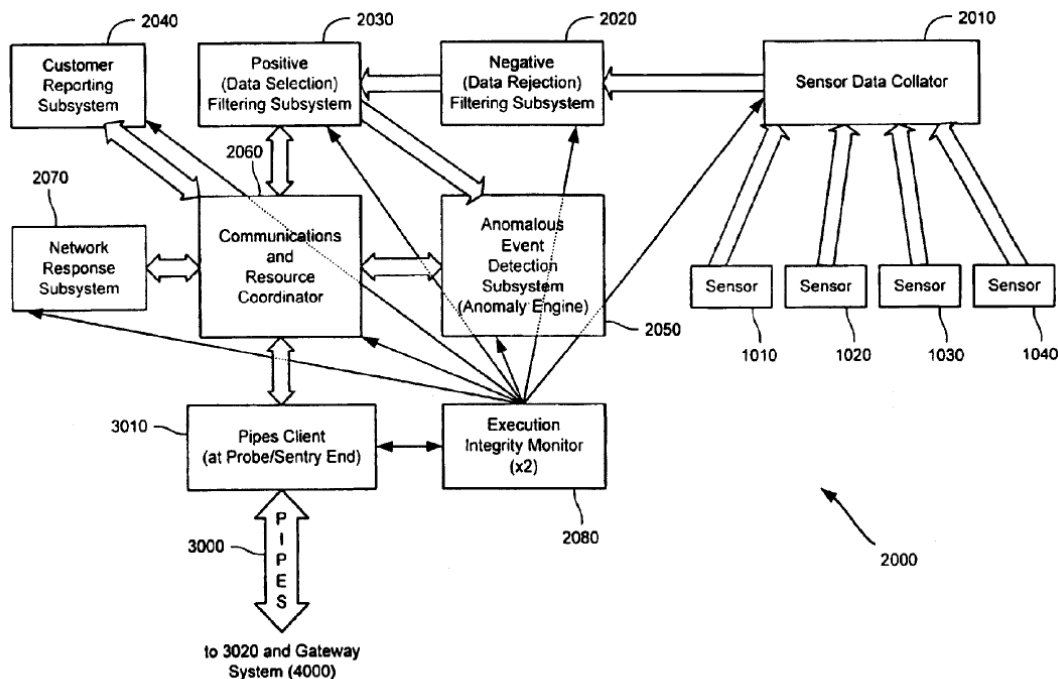


FIG. 2

Figure 2 is a diagram depicting “a system overview of an exemplary embodiment of a probe/sentry system in an exemplary embodiment” disclosed in the ’237 patent. *Id.* at 3:62–64. According to the ’237 patent, “[d]ata collected by sensors 1010, 1020, 1030 and 1040 are collated by sensor data collator 2010.” *Id.* at 8:41–45. “Once collated, the data is first filtered by negative filtering subsystem 2020, which discards uninteresting information, and then by positive filtering subsystem 2030, which selects possibly interesting information and forwards it to communications and resource coordinator 2060.” *Id.* at 8:45–50. “Data neither discarded by negative filtering subsystem 2020 nor selected out as interesting by positive filtering subsystem 2030 form the ‘residue,’ which is sent to anomaly engine 2050 for further analysis.” *Id.* at 8:50–53. “Anomaly engine 2050 determines what residue information may be worthy of additional analysis and sends such information to communications and resource coordinator 2060 for forwarding to the SOC.” *Id.* at 8:53–57. “Communications and resource coordinator 2060 creates sentry messages out of the interesting status data and forwards those messages on to gateway system 4000.” *Id.* at 8:60–62.

The ’237 patent further discloses a Secure Operations Center Responsive Analyst Technical Expertise System (“SOCRATES”). *Id.* at 3:55. According to the ’237 patent, “[t]he SOCRATES system is a consolidated system used to manage customers’ problems and the supporting data helpful in resolving such problems.” *Id.* at 9:50–52. The SOCRATES system “provides security analysts at a SOC a single, integrated system with which to track information concerning, for example, problems, companies, people, contacts, tools, and installed network components and known vulnerabilities.” *Id.* at 9:52–56.

In another embodiment, the managed security monitoring service allows for customization and complex data analysis. *Id.* at 2:21–22. For example, the service may be customized, either dynamically or offline, to accommodate network-specific needs and to reflect feedback received about the demonstrated efficacy of a real-world response to an actual event. *Id.* at 2:23–26. The '237 patent discloses that status data collected, filtered, or otherwise analyzed by probe/sentry system 2000 can either remain in the customer's hands or be provided to service personnel for further analysis (e.g., cross-customer analysis). *Id.* at 5:19–26. According to the '237 patent, in a preferred embodiment, the software and filters of probe/sentry system 2000, may be adaptive or, alternatively, may be manually updated offline or dynamically (that is, during actual operation). *Id.* at 5:26–29. The '237 explains that, updates can be sent from the SOC to the probe/sentry system and signed, verified and then securely installed. *Id.* at 5:30–32.

2. *Illustrative Claims*

As noted previously, Petitioner challenges claims 1–42 of the '237 patent, of which claims 1, 18, and 26 are independent. Pet. 1; Ex. 1001, 35:38–38:47. Claim 1 is illustrative of the challenged subject matter and is reproduced below.

1. A method of operating a probe as part of a security monitoring system for a computer network, comprising:
 - a) collecting status data from at least one monitored component of said network;
 - b) analyzing status data to identify potentially security-related events represented in the status data, wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering;
 - c) transmitting information about said identified events to an analyst associated with said security monitoring system;

- d) receiving feedback at the probe based on empirically-derived information reflecting operation of said security monitoring system; and
- e) dynamically modifying an analysis capability of said probe during operation thereof based on said received feedback.

Ex. 1001, 35:39–57.

D. Asserted Challenges to Patentability and Evidence of Record

Petitioner challenges the patentability of claims 1–42 of the '237 patent based on the following reference or combination of references:

Claims Challenged	35 U.S.C. §	Reference(s)/Basis
1–7, 15–23, 26–32, 40–42	103 ¹	Duvall ² , Chu ³
7–13, 16, 24, 32–38, 41	103	Duvall, Chu, Trcka ⁴
14–15, 25, 39–40	103	Duvall, Chu, Trcka, Ziese ⁵

In support of its patentability challenge, Petitioner relies on, *inter alia*, the Declaration of Kevin Jeffay, Ph.D. (“Dr. Jeffay”). Ex. 1003. In support of its Preliminary Response, Patent Owner relies on, *inter alia*, the Declaration of Wenke Lee, Ph.D. (“Dr. Lee”). Ex. 2001.

¹ The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) (“AIA”), included revisions to 35 U.S.C. § 103 that became effective as of March 16, 2013. The application for the '237 patent was filed before March 16, 2013. Ex. 1001, code (22). Accordingly, for purposes of institution, we apply the pre-AIA version of 35 U.S.C. § 103.

² US Patent 5,884,033, issued Mar. 16, 1999; filed May 15, 1996 (“Duvall,” Ex. 1004).

³ Yang-hua Chu, *Trust Management for the World Wide Web*, M.I.T. (June 13, 1997) (“Chu,” Ex. 1005)

⁴ US Patent Application Publication No. 2001/0039579 A1, published Nov. 8, 2001 (“Trcka,” Ex. 1014).

⁵ US Patent 6,484,315 B1, issued Nov. 19, 2002; filed Feb. 1, 1999 (“Ziese,” Ex. 1015).

III. PRELIMINARY MATTERS

A. Claim Construction

A claim “shall be construed using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. [§] 282(b).” 37 C.F.R. § 42.100(b). Under that standard, the “words of a claim ‘are generally given their ordinary and customary meaning.’” *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc).

Petitioner asserts that “no claim terms require an explicit construction” and that “the challenged claims are unpatentable under either the ordinary and customary meaning as understood by one of ordinary skill in the art at the time of the invention in light of the specification and the prosecution history, or the district court’s previous claim constructions. Pet. 14.

Petitioner acknowledges that the limitation “post-filtering residue is data neither discarded nor selected by filtering” in independent claims 1, 18, and 26 was construed in a district court case to which it was not a party. Pet. 33. According to Petitioner, the parties in the that district court case agreed that limitation should be construed as “status data that undergoes negative and positive filtering, but is neither discarded by such negative filtering nor selected by such positive filtering.” *Id.* (citing Ex. 1013, 4). Petitioner contends that “under either this agreed-upon construction or the claim’s plain language, Duvall teaches” the limitation. *Id.* (citing Ex. 1003 ¶ 125); *see also* Pet. 35 (citing Ex. 1003 ¶ 130; Ex. 1004, 4:27–30, 4:65–5:7).

Patent Owner asserts that “post-filtering residue” has been misconstrued and misapplied by Petitioner. Prelim. Resp. 28–32. According to Patent Owner, Petitioner’s implicit construction of the

limitation suggests “that the ‘plain language of this element does not require any data to actually be ‘discarded’ or ‘selected by filtering’—only that the ‘post-filtering residue is data neither discarded nor selected by filtering.’” *Id.* at 30. Patent Owner contends Petitioner omits the requirement that the “residue” be “post-filtering” and impermissibly broadens the residue to include (1) any data, not just status data, and (2) in-flight or mid-filtering data—that is, data that is still in the process of being filtered. *Id.* at 30–31. Patent Owner admits that the IP addresses used in the Duvall references are status data, but then argues that “Petitioner bears the burden to show how Duvall actually analyzes any leftover status data to identify potentially security related events.” *Id.* at 31.

We agree with Patent Owner that limitation b) requires a filtering process that produces the claimed residue from the filtering, followed by an analysis of the post-filtering residue. We also agree that the filtering and analysis is performed on status data. Nonetheless, as discussed in detail below, we find Duvall teaches the disputed limitation even under Patent Owner’s construction.

We do not construe any other limitations or terms of the challenged claims because construction is needed only for those terms “that are in controversy, and only to the extent necessary to resolve the controversy.” *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

B. Principles of Law Regarding Obviousness

A claim is unpatentable under 35 U.S.C. § 103 if “the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) where in evidence, objective evidence of non-obviousness.⁶ *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). When evaluating a combination of teachings, we must also “determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)). Whether a combination of prior art elements would have produced a predictable result is considered in the ultimate determination of obviousness. *Id.* at 416–417.

In an *inter partes* review, the petitioner must show with particularity why each challenged claim is unpatentable. *Harmonic Inc. v. Avid Tech.*,

⁶ Patent Owner states that it raised arguments regarding indicia of non-obviousness in response to a prior petition challenging the ’237 patent but that Petitioner failed to address those considerations in its Petition. Prelim. Resp. 12–13 (citing *Robert Bosch Tool Corp. v. SD3, LLC*, IPR2016-01753, Paper 15 at 28 (PTAB Mar. 22, 2017)). We note that the decision cited by Patent Owner, *Robert Bosch Tool*, denied institution where, amongst other things, a Petitioner failed to discuss indicia of non-obviousness in its Petition despite having such evidence in a related ITC proceeding where Petitioner was a party. That is not the case here. In the present case, the only previously filed Board proceeding (1) does not involve Petitioner and (2) does not have readily identifiable indicia of non-obviousness. Specifically, in the present Preliminary Response, Patent Owner does not cite where in its prior Preliminary Response the indicia of non-obviousness may be found, nor does Patent Owner introduce sufficient evidence regarding objective indicia of non-obvious at this stage in the proceeding. Thus, Patent Owner’s arguments are accorded no weight in our analysis.

Inc., 815 F.3d 1356, 1363 (Fed. Cir. 2016); 37 C.F.R. § 42.104(b). The burden of persuasion never shifts to the patent owner. *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015).

We analyze the challenges presented in the Petition in accordance with the above-stated principles.

C. Level of Ordinary Skill in the Art

In determining the level of ordinary skill in the art, various factors may be considered, including the “type of problems encountered in the art; prior art solutions to those problems; rapidity with which innovations are made; sophistication of the technology; and educational level of active workers in the field.” *In re GPAC, Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995) (quotation marks omitted). Furthermore, the prior art itself can reflect the appropriate level of ordinary skill in the art. *Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001).

Here, Petitioner asserts a person of ordinary skill in the art at the time of the ’237 patent, “would have had a B.S. degree in Computer Science, Computer Engineering, or an equivalent field, as well as at least 2–3 years of academic or industry experience in the design, analysis, and monitoring of computer networks, including issues of network security and network administration, or comparable industry experience.” Pet. 12 (citing Ex. 1003 ¶¶ 61–62).

Patent Owner does not assert a different level of skill in the art at the time of the alleged invention at this time. Prelim. Resp. 28.

For the purposes of this Decision, we adopt Petitioner’s level of ordinary skill in the art because it appears consistent with the problems addressed in the ’237 Patent and the prior art of record, except that we

delete the qualifier “at least” in the phrase “at least 2–3 years” to eliminate vagueness as to the stated amount of academic or industry experience.

D. Overview of Asserted Prior Art of Record

1. Duvall (Ex. 1004)

Duvall is a U.S. Patent, issued March 16, 1999, titled “Internet Filtering System for Filtering Data Transferred over the Internet Utilizing Immediate and Deferred Filtering Actions.” Ex. 1004, codes (19), (45), (54). Duvall relates to “filtering messages transmitted between the Internet and a client computer.” *Id.* at 1:7–8. Duvall discloses a client-based filtering system compares portions of incoming and/or outgoing messages with filtering information stored in a filter database. and determines whether to block or allow the incoming and/or outgoing transmissions of messages in response to the comparison. *Id.* at 1:31–35. Duvall explains that in response to a match between certain information in portions of the message and the filtering information, the system can employ one of a number of different specified blocking options, including discarding incoming data, preventing execution of an open command. or replacing parts of received data. *Id.* at 1:35–40.

One embodiment of Duvall is shown in Figure 1, reproduced below:

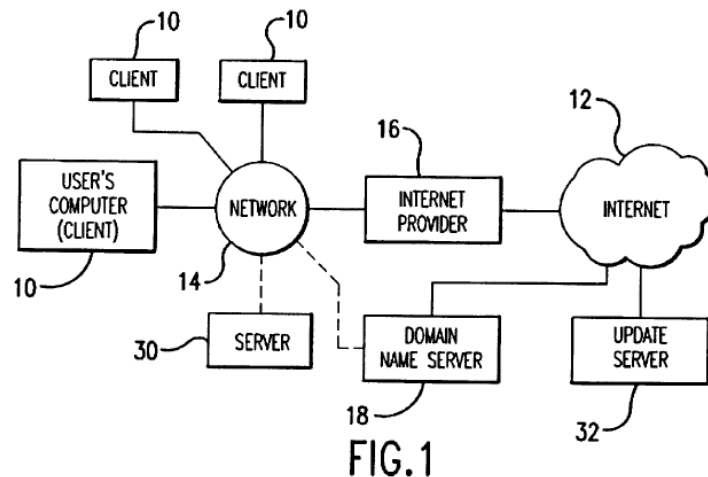


Figure 1 depicts “a block diagram of a network with a client computer for accessing the Internet.” *Id.* at 2:24–25. The network includes a user with a computer that serves as client computer 10 that communicates with other computers over Internet 12.” *Id.* at 2:34–35. According to Internet Protocol version 4, each computer on or connected to the Internet has an IP address that identifies the location of the computer. *Id.* at 2:51–53. Duvall’s filter system can filter messages on the basis of IP address. *Id.* at 4:5–11, 4:37–39.

Another embodiment of Duvall is shown in Figure 2, reproduced below:

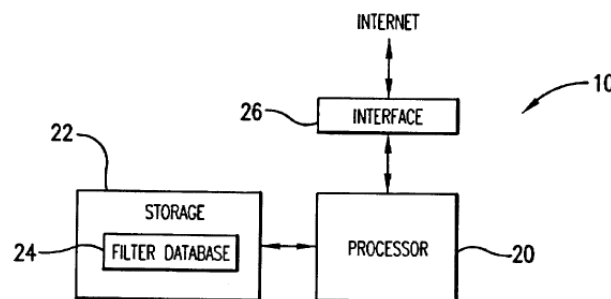


Figure 2 depicts a block diagram of client computer 10 with a filtering system. *Id.* at 2:26–27. In this embodiment, as shown in Figure 2, “a filtering system resides in client computer 10.” *Id.* at 3:43–44. “Processing by the filtering system is carried out by the computer’s processor 20. and the system uses the computer’s storage 22 to store a filter database 24.” *Id.* at 3:44–46. Duvall also discloses an embodiment in which “the filtering system can be provided from a server 30 that is on the client’s own network 40.” *Id.* at 8:18–21. “This version of the filtering system uses the same type of filter database as a client-based filtering system, but the filter database is located on server 30.” *Id.* at 8:23–26.

Duvall discloses a “filter database [that] has lists of filters, some of which are identified as either ALLOW filters or BLOCK filters for respectively allowing or blocking transmission.” *Id.* at 3:64–66. “Each filter entry in the filter database also has a field for specifying an action to be taken by the client if that filter were retrieved.” *Id.* at 4:12–14. “These actions are essentially divided into two groups, direct action or deferred action.” *Id.* at 4:14–15. “Direct actions indicate that the system should unconditionally allow or unconditionally block the transmission.” *Id.* at 4:15–17. “If . . . it is determined that no immediate action must be taken, it is determined whether a deferred action must be taken.” *Id.* at 4:65–67. Additionally, a filter can indicate that a deferred action should be taken. *Id.* at 4:65–5:1; 6:19–20.

Duvall discloses filters “stored so that the system searches ALLOW filters first, BLOCK filters next, and deferred action filters last.” *Id.* at 4:27–29. Duvall further discloses, “[i]f there is no deferred action, the system can default to allow the transmission . . . , or it can default to block the transmission.” *Id.* at 5:1–3. Deferred filter entries preferably have

additional fields, including fields for (1) a keyword, typically a command such as GET; (2) a filter pattern to be compared to data in the message, typically a string of characters; (3) a directional indicator (IN/OUT) for indicating incoming or outgoing transmissions; (4) a compare directive for the type of match; and (5) an action to be taken. typically to allow or block the transmission. *Id.* at 5:8–15.

2. *Chu (Ex. 1005)*

Chu is a Master's thesis titled "Trust Management for the World Wide Web" submitted to the Massachusetts Institute of Technology Department of Electrical Engineering and Computer Science. Ex. 1005, 3.

Chu relates to "trust management . . . in the context of the World Wide Web. *Id.* For example, Chu discloses sample policies addressing the question of "should I download the active content at this URL." *Id.* 43–48. Chu discloses policies that employ a "blacklist" and a "whitelist." *Id.* at 44. The blacklist is a list of sites or directories the computer should not download codes from. *Id.* According to Chu, the use of such lists "can be very effective in practice . . . [because] Firewall vendors can compile a blacklist of Web sites that serve potentially dangerous active codes, and place the list in clients' firewalls." *Id.* Chu states that "[t]he blacklist and whitelist ensure good automation of the trust decision process if the lists are reasonably complete." *Id.* If the request URL is neither in the blacklist nor the white list, then Chu discloses that the system can return the term "unknown."

One embodiment of Chu is reproduced below:

Policy in English

Do not download the code if the URL is served from Harvard or CalTech Web servers. Download it automatically if served from MIT. Prompt me for my attention otherwise.
--

As shown above, Chu directs the system to send the user an attention prompt in that case and states “[u]ser intervention is needed only when the given URL is in neither the blacklist nor the whitelist.” *Id.*

3. *Trcka (Ex. 1014)*

Trcka is a U.S. Patent Application Publication, published on November 8, 2001, titled “Network Security and Surveillance System.” Ex. 1014, codes (12), (43), (54).

Trcka relates to “[a] network security and surveillance system [that] passively monitors and records the traffic present on a local area network, wide area network, or other type of computer network, without interrupting or otherwise interfering with the flow of the traffic.” Ex. 1014, code 57. According to Trcka, “[a] set of analysis applications and other software routines allows authorized users to interactively analyze the low-level traffic recordings to evaluate network attacks, internal and external security breaches, network problems, and other types of network events.” *Id.*

Trcka discloses “analysis applications [that] can . . . be used to view, analyze and process . . . traffic data,” including “functionality for performing such actions as displaying user-specified types of network events, conducting pattern searches of selected packet data, reconstructing transaction sequences, and identifying pre-defined network problems.” *Id.* ¶ 16. Trcka also discloses “analysis tools . . . for allowing authorized users to perform interactive, off-line analyses of recorded traffic data.” *Id.* ¶ 53. Trcka discloses a “graphical user interface (GUI)” through which “the user can launch and control the various analysis applications . . . through a common set of menus and controls.” *Id.* ¶ 79.

4. *Ziese (Ex. 1015)*

Ziese is a U.S. Patent, issued November 19, 2002, titled “Method and System for Dynamically Distributing Updates in a Network.” Ex. 1015, codes (12), (45), (54). Ziese discloses “dynamically distributing intrusion detection and other types of updates in a network that substantially eliminate or reduce disadvantages and problems associated with prior methods and systems.” *Id.* at 2:2–6. According to Ziese, “programs are automatically updated by downloading and distributing an update in response to an automated event,” and “[a]s a result, systems with a common program separately running at several sites may update each site with no or minimal operator interaction.” *Id.* at 2:39–44.

IV. ANALYSIS

A. *Alleged Obviousness of Claims 1–7, 15–23, 26–32, and 40–42 in view of Duvall and Chu*

Petitioner contends claims 1–7, 15–23, 26–32, and 40–42 would have been obvious to a person of ordinary skill in the art in view of the combined teachings of Duvall and Chu. Pet. 14–59. Patent Owner disputes Petitioner’s contentions. Prelim. Resp. 32–64. For the reasons discussed below, at this stage of the proceeding, we are not persuaded that Petitioner has established a reasonable likelihood of success on this challenge.

1. *Analysis of Independent Claim 1*

a) *“A method of operating a probe as part of a security monitoring system for a computer network”*

Petitioner contends that Duvall discloses a “a security monitoring system for a computer network,” because Duvall is directed to “filtering messages transmitted between the Internet and a client computer” to ensure content that implicates security concerns does not reach recipients. Pet. 25

(citing Ex. 1004, 1:7–24, 1:12–20, 1:27–29; Ex. 1003 ¶ 113). According to Petitioner, “Duvall’s filtering system monitors transmissions for questionable content that should be blocked.” *Id.* (citing Ex. 1004, 3:33–37, 5:8–15, 6:10–42; Ex. 1003 ¶ 115). Petitioner argues that a person of ordinary skill in the art “would have been motivated to block content that may have carried viruses or malware” and that “no modifications would be needed in Duvall’s system—domains (e.g., URLs or IP addresses) believed to carry security-implicating content (e.g., viruses) would simply be included in Duvall’s blocking filters.” *Id.* at 26 (citing Ex. 1004, 6:10–27; Ex. 1003 ¶ 115).

Petitioner further contends that Duvall’s server 30 is a probe that provides a filtering system. Pet. 26–27 (citing Ex. 1004, 8:18–21, 1:60–64, Fig. 1; Ex. 1013 ¶ 2). According to Petitioner, “Duvall’s server 30 collects and analyzes data from other network components to which it is attached, such as clients 10” and that its “filtering system may be part of a firewall.” *Id.* at 27–28 (citing Ex. 1004, 1:59–64, 8:21–223).

Patent Owner has not provided any arguments regarding this specific claim limitation and the application of Duvall and Chu. *See generally* Prelim. Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

“Whether to treat a preamble term as a claim limitation is determined on the facts of each case in light of the claim as a whole and the invention described in the patent.” *Am. Med. Sys., Inc. v. Biolitec, Inc.*, 618 F.3d 1354, 1358 (Fed. Cir. 2010) (internal quotation marks omitted). “Absent clear reliance on the preamble in the prosecution history, or in situations where it is necessary to provide antecedent basis for the body of the claim, the preamble generally is not limiting.” *Symantec Corp. v. Computer Assocs.*

Int'l, Inc., 522 F.3d 1279, 1288 (Fed. Cir. 2008) (internal quotation marks and citation omitted). Additionally, preamble language that merely states the purpose or intended use of an invention generally is not treated as limiting the scope of a claim. See *Boehringer Ingelheim Vetmedica, Inc. v. Schering-Plough Corp.*, 320 F.3d 1339, 1345 (Fed. Cir. 2003); *Rowe v. Dror*, 112 F.3d 473, 478 (Fed. Cir. 1997). Yet, when the limitations in the body of the claim rely upon or derive essential structure from the preamble, then the preamble acts as a necessary component of the claimed invention and is limiting. See *Eaton Corp. v. Rockwell Int'l Corp.*, 323 F.3d 1332, 1339 (Fed. Cir. 2003).

Our reviewing court has explained, however, that a “conclusion that some preamble language is limiting does not imply that other preamble language, or the entire preamble, is limiting.” *Cochlear Bone Anchored Sols. AB v. Oticon Med. AB*, 958 F.3d 1348, 1355 (Fed. Cir. 2020); see *TomTom, Inc. v. Adolph*, 790 F.3d 1315, 1322-23 (Fed. Cir. 2015) (holding the court erred in determining that it had to construe the entire preamble if it construed a portion of it), citing *Loctite Corp. v. Ultraseal Ltd.*, 781 F.2d 861, 868 (Fed. Cir. 1985), *overruled in part on other grounds by Nobelpharma AB v. Implant Innovations, Inc.*, 141 F.3d 1059, 1068 (Fed. Cir. 1998) (en banc in part). The Court in *Cochlear Bone Anchored* specifically held that even when a phrase in a preamble provides a necessary structure for a claim, that preamble structure does not necessarily convert the entire preamble into a limitation, particularly one that only states the intended use of the invention. 958 F.3d at 1355.

Based on the current record, we find at least part of the preamble limiting because (1) the claim limitation relating to “probe,” relies on the preamble for antecedent basis. Accordingly, we find at least this portion of

the preamble recites an essential structure of the security monitoring system and is limiting. We need not reach a determination on whether the entirety of the preamble is limiting because at this stage of the proceeding, we are satisfied Petitioner has shown that Duvall in combination with the teachings of Chu would have render the preamble obvious to a person of ordinary skill in the art at the critical time.

b) *“collecting status data from at least one monitored component of said network”*

Petitioner contends that meets this limitation because Duvall’s server 30 analyzes (i.e., monitors) data received from clients 10, which reside on the same network. Pet. 28. Specifically, Petitioner argues Duvall’s filtering system, which is on a client’s own network server, compares the IP address from a transmitted message to determine if some action is needed. *Id.* at 29 (citing Ex. 1004, 4:22–27, 2:35–37, 2:42–44). According to Petitioner, the IP address of a message is “status data” because it is data extracted from network traffic and provides the status of the network and its component. *Id.* at 30 (citing Ex. 1004, 4:39–42, 5:66–6:27; Ex. 1013 ¶ 119).

Other than agreeing that IP addresses are status data, Patent Owner has not provided any arguments regarding this specific claim limitation and the application of Duvall and Chu. Prelim. Resp. 31. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

At this stage of the proceeding, we are satisfied Petitioner has shown that Duvall in combination with the teachings of Chu would have render this limitation obvious to a person of ordinary skill in the art at the critical time. Specifically, we are satisfied because IP addresses are status data and

Duvall's monitors transmitted messages on client 10 and then compares the IP address from a transmitted message to determine if some action is needed. *See* Ex. 1004, 4:22–27, 2:35–37, 2:42–44.

c) *“analyzing status data to identify potentially security-related events represented in the status data”*

Petitioner contends that Duvall meets the claim limitation because Duvall discloses filtering based on IP address (i.e., “status data”) and other information: “[w]hen a message is transmitted, whether that message is incoming or outgoing with respect to the client computer, the filtering system compares the IP address and/or other information in the data stream to the filter entries stored in the database to determine whether some action needs to be taken.” Pet. 31 (citing Ex. 1004, 4:22–27).

Petitioner further contends that Duvall teaches “identify[ing] potentially security-related events” because the purpose of Duvall’s deferred filtering analysis is to identify threats that do not match Duvall’s initial “ALLOW or BLOCK filters”—i.e., unknown threats. Reply 3 (citing Pet. 17–19; Ex. 1003 ¶¶ 99–101). According to Petitioner “[k]nown threats would have been blocked at this initial step while permitted data would have been allowed.” *Id.* Petition argues that Duvall’s deferred action step analyzes any residual data to identify any potential threats that were not originally blocked by the BLOCK filters—i.e., unknown threats. *Id.* (citing Ex. 1004, 5:8–19, 6:19–41 (identifying transmissions to/from sources that include “a potentially objectionable phrase” such as “sex” or “xxx”); Pet. 18–19; Ex. 1003 ¶¶ 100–101). Petitioner further argues that the ’237 patent does not limit the scope of what may be considered “security-related,” because the ’237 patent states that “the present invention is usable generally

for [] monitoring of any system.” *Id.* at 4 (citing Ex. 1001, 15:63–16:5; Pet. 9).

Patent Owner disputes Petitioner’s interpretation of the claim and disputes that Duvall and Chu analysis post-filtered status data to identify a potentially security-related event. Prelim. Resp. 34–37. According to Patent Owner, Duvall and Chu only teach filtering for things that are already known, but “[n]either of them analyzes any data to identify *potential* threats after filtering (*i.e.*, previously unknown threats from the post-filtering residue).” *Id.* at 34. Patent Owner argues that subjectively objectionable material is different than an objectively identified security-related event. *Id.*; *see also* Sur-Reply 4 (“‘[O]bjectionable material’ is different from ‘security related’ material.”).

At this stage of the proceeding, we are satisfied Petitioner has shown that Duvall in combination with the teachings of Chu would have render this limitation obvious to a person of ordinary skill in the art at the critical time. Specifically, we are satisfied because the term “potentially security-related events” is broad enough to encompass the objectionable material disclosed in Duvall and/or the black list sites of Chu. Specifically, we credit the testimony of Dr. Jeffay, who explains that Duvall’s and Chu’s techniques apply to other security-related contexts, and that objectionable material also presents virus- and malware-related risks. *See* Ex. 1003 ¶¶ 113–14, 134. Patent Owner attempts to unreasonably limits claims with arguments that are not commiserate with the scope of the claims as issued.

d) wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering”

Petitioner contends that Duvall meets the claim limitation because Duvall uses “direct action” filters on all transmissions to indicate whether the system should allow or block a transmission. Pet. 30–31 (citing Ex. 1004, 4:12–21, 5:8–29; Ex. 1013 ¶ 119). Petitioner argues that Duvall’s “filter database has lists of filters, some of which are identified as either ALLOW filters or BLOCK filters for respectively allowing or blocking transmission.” *Id.* at 31 (citing Ex. 1004, 3:64–66). According to Petitioner, “[e]ach filter entry in the filter database [] has a field for specifying an action to be taken by the client if that filter were retrieved,” and “[t]hese actions are essentially divided into two groups, direct action or deferred action.” *Id.* at 31–32 (citing Ex. 1004, 4:12–15). Petitioner notes that Duvall’s filters are implemented in sequence as they “‘are preferably stored so that the system searches ALLOW filters first, BLOCK filters next, and deferred action filters last,’ where the ‘ALLOW’ and ‘BLOCK’ filters are direct action filters.” *Id.* at 32–33 (citing Ex. 1004, 4:27–30; Ex. 1003 ¶¶ 122–123). Petitioner argues that if immediate action is not required by the filters, then what is left is “residue data” that is passed for further analysis by Duvall’s deferred action filters. *Id.* at 35 (citing Ex. 1004, 4:27–30, 4:65–5:7).

Petitioner further contends that such “data allowing and blocking comprises ‘positive filtering’ and ‘negative filtering’ in accordance with the” claim construction that Patent Owner agreed to in a district court litigation where the ’237 patent was asserted previously. *Id.* at 35 (citing Ex. 1003 ¶¶ 126–129). Petitioner argues that the district court’s claim construction does mean that “the ‘residue’ cannot be subject to further filtering as part of

the analysis, as long as that analysis occurs *after* (i.e., ‘post’) the negative and positive filtering. Reply 1. And, according to Petitioner, the ’237 patent describes performing stages of “negative filtering” and “positive filtering,” followed by further analysis by an “anomaly engine,” but the type of analysis performs in limited or restricted—only that the “anomaly engine” “determines what residue information may be worthy of additional analysis,” which may include additional filtering. *Id.* at 2 (citing Ex. 1001, 8:45–57). Thus, Petitioner concludes that Duvall’s IP addresses are residue status data “that underwent negative and positive filtering, but is neither discarded by such negative filtering nor selected by such positive filtering—i.e., ‘post-filtering residue,’” and therefore, meet the claim limitation. Pet. 35–36 (citing Ex. 1003 ¶ 130).

Patent Owner disputes Petitioner’s interpretation of the claim and disputes that Duvall meets the claim limitation. Prelim. Resp. 29–31. Patent Owner first acknowledges the claim construction used in the district court litigation where “post-filtering residue, wherein the postfiltering residue is data neither discarded nor selected by filtering” was construed to mean “status data that undergoes negative and positive filtering, but is neither discarded by such negative filtering nor selected by such positive filtering.” *Id.* at 29 (citing Ex. 1013, 4). Then, Patent Owner contends that Duvall does not create “post-filtering residue” because Duvall does not analyze status data after all filtering is completed. *Id.* at 30–31. Rather, according to Patent Owner, “the filtering process must be distinct from the analysis that follows the filtering” and that Petitioner’s use of “in-fight” or mid-filtered data is still in the process of being filtered and therefore would not qualify as “post-filter[ed] residue.” *Id.*

Patent Owner further contends that the '237 patent supports its interpretation of the claim because “the anomaly engine, which performs the further analysis, is distinct from the positive and negative filtering subsystems that produce the “post-filtering residue.” Sur-Reply 1–2 (citing Ex. 1001, 8:50–57).

At this stage of the proceeding, we are satisfied Petitioner has shown that Duvall in combination with the teachings of Chu would have render this limitation obvious to a person of ordinary skill in the art at the critical time for the reasons discussed below.

Claim 1 specifies that the analysis of status data must include “filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering.” The specification explains that, in one embodiment, “data is first filtered by negative filtering subsystem 2020, which discards uninteresting information, and then by positive filtering subsystem 2030, which selects possibly interesting information and forwards it to communications and resource coordinator 2060.” Ex. 1001, 8:45–50. According to the '237 patent, “[d]ata neither discarded by negative filtering subsystem 2020 nor selected out as interesting by positive filtering subsystem 2030 form the ‘residue,’ which is sent to anomaly engine 2050 for further analysis.” *Id.* at 8:5–53. Figure 2 of the '237 shows anomaly engine 2050 as a separate box or entity from negative filtering subsystem 2020, which in turn is shown as a separate box or entity from positive filtering subsystem 2030. *Id.* at Fig. 2.

Based on the current record, we agree with Petitioner that the IP addresses in undergo both positive (ALLOW filters) and negative (BLOCK filters) filtering and the remaining IP address information is not discarded but it targeted for deferred action filters, which appears to quality as

“analysis” per the ’237 patent. *See* Ex. 1001, 8:45–57; Ex. 1004, 4:27–30, 4:46–5:29.

Contrary to Patent Owner’s argument that “the filtering process must be distinct from the analysis that follows the filtering,” there is nothing in the claims or the specification that commands such distinction. Rather, the claims merely require that filtering is followed by an analysis of post-filtering residue. And, if we accept the district court’s claim construction of “post-filtering residue,” then any status data that has been neither discarded by negative filtering nor selected by positive filtering would qualify. *See* Ex. 1013, 4.

Patent Owner’s arguments do not appear to be commensurate with the scope of the claims, but appear to be an attempt to import limitations from specific embodiments into the claims. *See* Prelim. Resp. 37–38; *see* Ex. 1001, 8:5–53, Fig. 2. In keeping with the guidance from our reviewing court, we decline to read limitations from embodiments into the claims. *See Ericsson, Inc. v. D-Link Systems, Inc.*, 773 F.3d 1201, 1218 (Fed. Cir. 2014) (stating that although patent claims must be read in light of the specification, it is important that a court avoids importing limitations from the specification into the claims); *3M Innovative Properties Co. v. Tredegar Corp.*, 725 F.3d 1315, 1321 (Fed. Cir. 2014) (“While we construe the patent’s claims in light of the specification, limitations discussed in the specification may not be read into the claims.”); *In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993) (holding that limitations are not to be read from the specification into the claims).

- e) *“transmitting information about said identified events to an analyst associated with said security monitoring system”*

Petitioner contends that the combined teachings of Duvall and Chu combination teach this element because a person of ordinary skill in the art would have looked to Chu to optimize the handling of unresolved residue data in order to avoid “filtering too much or too little” in Duvall.” Pet 38 (citing Ex. 1004, 8:6–8; Ex. 1003 ¶ 136–137). Petition argues that “[i]n the case of unresolved data, Chu prompts for human intervention, which “would take the form of someone trained to manage Duvall’s corporate network.” *Id.* (citing Ex. 1003 ¶ 137). Petition further argues that Duvall’s use of “uniform set of filters” for a corporate network means that “the decision of how to handle unresolved data would not be left to each user individually, but rather, to a person trained in making such decisions, such as analysts at a network-security service.” *Id.* at 39 (citing Ex. 1004, 8:18–23; Ex. 1003 ¶¶ 138–139). Indeed, according to Petitioner, Duvall discloses a “password protected” “editing manager” indicating that the person editing filters in a corporate network is someone trained to manage the system. *Id.* at 39–40 (citing Ex. 1004, 8:8–10; Ex. 1003 ¶ 139). Thus, Petitioner concludes that “in the Duvall-Chu combination, information about the unresolved residue data would be sent to a trained network analyst for handling of the unresolved residue data.” *Id.* at 40–41.

Patent Owner disputes Petitioner’s position arguing that Duvall only teaches a first level of analysis by the filter system and the combination of Duvall and Chu fails to teach second level of analysis by an analyst. Prelim. Resp. 38–43 (citing Ex. 2001 ¶ 150). Patent Owner argues that neither Duval nor Chu provides a suggestion to transmit information about previously identified events from a first-level of analysis to an analyst who

can determine whether the potential events are actual events and/or resolve them. *Id.* at 39 (citing Ex. 2001 ¶ 153), 42. According to Patent Owner, Chu does not fill the gaps in Duvall regarding transmitting to an analyst because (1) Chu does not have a first level of analysis that would trigger transmission to an analyst and (2) Chu does not “transmit” information to an analyst. *Id.* at 39–40, 42.

Patent Owner contends that Chu only filters URLs with whitelists and blacklists to automate a trust decision process but “[i]f the trust decision cannot be automated because the URL is neither in the whitelist nor the blacklist, then Chu simply returns control back to the end-user—alerting them that no decision could be made.” Prelim. Resp. 40 (citing Ex. 1005, 44). Patent Owner argues that this is Chu’s “user intervention,” which does not qualify as “transmitting information about said identified events to an analyst.” *Id.* (citing Ex. 2001 ¶ 156; EX1001, 2:36–43). Patent Owner further argues that it would not be logical “to redirect the alert away from the end-user to a (non-existent) analyst for any reason” and that there is not explanation of how to introduce an analyst into either Duvall or Chu. *Id.* (citing Ex. 2001 ¶ 157), 43.

At this stage of the proceeding, we are satisfied Petitioner has shown that Duvall in combination with the teachings of Chu would have render this limitation obvious to a person of ordinary skill in the art at the critical time for the reasons discussed below. Given the specific information disclosed in the both Duvall and Chu, we agree with Petitioner that the prior art contemplates transmitting information to a skilled user or analyst for further action. *See* Ex. 1004, 8:6–10, 8:18–23; Ex. 1005, 44). Additionally, we are not persuaded at this time by Patent Owner’s argument, which appears to be

premised on attacking the references individually when the challenge is predicated on the combination of the prior art teachings.

f) “*receiving feedback at the probe based on empirically-derived information reflecting operation of said security monitoring system*”

Petitioner contends that the combined teachings of Duvall and Chu combination teach this element because each reference “discloses feedback in the form of an ‘editing Manager’ that allows ‘edit[ing] the database to add, delete, or modify filters in the database.” Pet. 41 (citing Ex. 1004, 8:2–5). According to Petitioner, a person of ordinary skill in the art at the critical time would have recognized that this feedback would be “*based on empirically-derived information reflecting operation of said security monitoring system*” because the information is only provided to the network analyst if the data is unresolved residue data—meaning that the data did not match any allow/block filters and passed through subsequent residue analysis (e.g., keywords and pattern matching) without any resolution. *Id.* (citing Ex. 1004, 5:8–19; Ex. 1003 ¶ 146). Therefore, Petitioner argues that decisions made by the trained network analyst (e.g., whether the filters should be modified) would be based on observable information about the data (e.g., transmission path, URL, etc.), and that feedback is received “*at the probe*” because Duvall’s editing manager is part of the filtering system implemented on server 30. *Id.* at 41–42 (citing Ex. 1004, 8:2–5 (“the filtering system has an editing Manager”), 8:18–21; Ex. 1003 ¶¶ 147–148).

Patent Owner has not provided any arguments regarding this specific claim limitation and the application of Duvall and Chu. Prelim. Resp. 31. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

At this stage of the proceeding, we are satisfied Petitioner has shown that Duvall in combination with the teachings of Chu would have render this limitation obvious to a person of ordinary skill in the art at the critical time. Specifically, we are satisfied because Duvall discloses the use of a password protected “editing Manager” that allows a user to edit “the database to add, delete, or modify filters in the database.” And, based on the current record, we agree with Petitioner’s position that a person of ordinary skill in the art at the critical time would have recognized that this feedback would meet the claims limitation because the information would be provided to the network analyst only upon detecting unresolved residue data. *See* Ex. 1004, 5:8–19.

g) “dynamically modifying an analysis capability of said probe during operation thereof based on said received feedback”

Petitioner contends the Duvall-Chu combination meets this limitation because Duvall “provid[es] updates online” so that “the system can adapt as new sites and servers are added to the Internet,” and Duvall’s filtering system accommodates dynamic updates because it searches “filter entries stored in the database” when performing its analysis so as to reflect changes to filters as they are edited. Pet. 43 (citing Ex. 1004, 2:16–18, 4:22–43, 8:3–16; Ex. 1003 ¶¶ 150–151); Reply 4 (“‘dynamically’ merely means ‘during actual operation, rather than offline’.”). Petitioner argues that editing the filters in Duvall’s filter database “modif[ies] an analysis capability of said probe . . . based on said feedback” because Duvall operates by comparing “information in the data stream to the filter entries stored in the database to determine whether some action needs to be taken.” Pet. 42 (citing Ex. 1004, 4:22–27, 4:27–30, 4:40–43).

According to Petitioner, Duvall recognizes that “[b]ecause Internet sites are being added to the Internet at a fast rate . . . the filtering system

preferably also has an updating mechanism to keep filters current” and that “the system can adapt as new sites and servers are added to the Internet.” *Id.* (citing Ex. 1004, 7:18–21, 2:16–18). Petitioner further contends that “[g]iven the rapidity of updates, a POSA would have recognized that Duvall” needs to have dynamic modification of its probe’s “analysis capability. . . . during operation” because “taking the system offline each time an update was required would be disadvantageous.” *Id.* at 42–43 (citing Ex. 1003 ¶ 150). Petitioner concludes that “[t]o avoid this disadvantage, Duvall ‘provid[es] updates online’ so that ‘the system can adapt as new sites and servers are added to the Internet.’” *Id.* at 43 (citing Ex. 1004, 2:16–18); Pet. 42–43; Ex. 1003 ¶¶ 149–51.”).

We agree with Petitioner that the term “dynamically” means “during actual operation, rather than offline.” *See* Ex. 1001, 5:26–29 (the software and filters of the probe/sentry system 2000 . . . may be manually updated offline or dynamically (that is, during actual operation).” We do not agree, however, that simply because “dynamic modification” may offer advantages that it was, therefore, obvious. *See* Pet. 42–43; Reply 5.

The ’237 patent specifically teaches that updates that occur “dynamically” are updates made during actual operation. Ex. 1001, 5:26–29. As Patent Owner shows, “[t]he probe monitors and collects information from any component providing status data” “derived from traffic.” Prelim. Resp. 7 (citing Ex. 1001, 4:52–64). Although claim 1 indicates that “operation” “comprises” listed steps involving collecting, analyzing, and transmitting status data, claim 1 also indicates that “operation” includes receiving feedback, and dynamically modifying an analysis capability during operation thereof after receiving said feedback (i.e., “based on said feedback”). Because claim 1 is open-ended (i.e., recites “comprising” listing

the noted steps), this implies that the recited operation not only may involve one or more of the listed steps (after “receiving feedback at the probe”), but operation also may involve the probe monitoring devices for traffic, as indicated in Patent Owner’s description of the probe outlined above. *See id.* This understanding is further supported by the definition of “operation” found in the Microsoft Computer Dictionary 5th Ed. (*see* Ex. 3002 (“A specific action carried out by a computer in the process of executing a program.”)) and IEEE 100, The Authoritative Dictionary of IEEE Standard Terms, 7th Ed. (*see* Ex. 3003, “The process of running a computer system in its intended environment to perform its intended functions)), both of which reflect the common understanding of a person of ordinary skill in the art at the critical time.

Nevertheless, Petitioner fails to show sufficiently on this record how Duvall discloses dynamically modifying said probe during operation thereof after receiving feedback (“based on said feedback”). Petitioner points to Duvall’s editing manager and its disclosure of receiving automatic updates, but Petitioner does not explain sufficiently if editing or receiving updates occurs during some operation of the probe after receiving feedback, as called for in claim 1, as opposed to only manipulating the database. *See* Pet. 42–43. Petitioner also relies on Duvall’s teaching that it “operates by comparing ‘information in the data stream to the filter entries stored in the database to determine whether some action needs to be taken,” but this fails to explain sufficiently how this comparison modifies an analysis capability of the probe during operation based on feedback. *See id.* at 42 (citing Ex. 1004, 4:22–

27).⁷ A comparison of the input data to the filter entries does not modify the analysis capability. Additionally, we do not find dynamic modification of an analysis capability of a probe to be one of “a finite number of identified, predictable solutions [that] a person of ordinary skill has good reason to pursue.” *See KSR International Co. v. Teleflex Inc.*, 550 U.S. 398, 421 (2007). To be clear, this is not a matter of providing a person of ordinary skill with a simple design choice between two options. *See ACCO Brands Corp. v. Fellowes, Inc.*, 813 F.3d 1361, 1367 (Fed. Cir. 2016) (explaining that where an “ordinary artisan would . . . be left with two design choices . . . [e]ach of these two design choices is an obvious combination”). Rather, the

⁷ In other words, claim 1 is a method claim, not an apparatus claim that recites the mere capability of performing dynamic modification. *Cf. ParkerVision, Inc. v. Qualcomm Inc.*, 903 F.3d 1354, 1361 (Fed. Cir. 2018) (“[A] prior art reference may anticipate or render obvious an apparatus claim—depending on the claim language—if the reference discloses an apparatus that is reasonably capable of operating so as to meet the claim limitations, even if it does not meet the claim limitations in all modes of operation.”); IPR2023-00888, Paper 9 (related institution decision involving an apparatus claim that recites the capability of the same dynamic modification). Petitioner fails to point to a disclosure in Duvall showing that its identified probe performs the step of “dynamically modifying an analysis capability of said probe during operation thereof based on said received feedback.” Similarly, although claim 18 is an apparatus claim, it recites “said probe is *configured to* . . . dynamically modify an analysis capability of said probe during operation thereof based on said received feedback.” *See ParkerVision*, 903 F.3d at 1362 (noting that previous Federal Circuit “cases distinguish between claims with language that *recites capability*, and those that *recite configuration*,” and “where claim language recites ‘capability, as opposed to actual operation,’ *an apparatus that is ‘reasonably capable’ of performing the claimed functions ‘without significant alterations’ can infringe those claims.*” (quoting *Ericsson, Inc. v. D-Link Sys., Inc.*, 773 F.3d 1201, 1217 (Fed. Cir. 2014) (emphasis added)). Similar remarks apply to claim 26, which recites “[a] computer-readable medium.”

recited claim limitation is a technical feature that is not taught or even suggested by the combined teachings of Duvall and Chu. Petitioner explains sufficiently that dynamic modification provides an advantage and why a skilled artisan would want to use it in solving a problem, but fails to sufficiently demonstrate that the prior art provided such a solution.

Petitioner's declarant, Dr. Jeffay, cites to the Zeise reference to support Petitioner's argument that a person of ordinary skill in the art would have "recognized that Duvall's 'analysis capability of said probe' is 'dynamically modified . . . during operation thereof' because taking the system offline each time an update was required would be disadvantageous." Ex. 1003 ¶ 150 (citing Ex. 1015, 1:54–2:6). Zeise discloses "dynamically distributing updates in a network." Ex. 1015, 1:7–9, 2:1–6. Zeise teaches (1) downloading and distributing updates in response to an automated or timed event (*id.* at 2:39–41) and (2) that sensors may automatically connect to a remote site and download new signatures (*id.* at 2:49–51). But neither Dr. Jeffay nor Petitioner sufficiently explain how Zeise's "dynamically distributing" compares to the '237 patent's "dynamic modification" or if Zeise's system makes modifications during operation.⁸ Nor does Dr. Jeffay sufficiently explain how Zeise dynamically modifies a sensor/probe or a system in response to feedback, such that it would have rendered such an act obvious to one of ordinary skill in the art. Rather, Zeise appears to be related to automated or timed update events. *See* Ex. 1015, 2:39–41.

⁸ Petitioner discusses Ziese in its third challenge in the Petition, specifically addressing dependent claims 14, 15, 25, 39, and 40. *See* Pet. 69–71. The Petition does not sufficiently answer the questions relating Ziese to "dynamic modification" at any point. In fact, Petitioner's explanation regarding Ziese's automation appears to cut against Dr. Jeffay's reliance on "dynamically distributing" for claim 1.

Accordingly, we find Petitioner fails to show that the combined teachings of Duvall and Chu would have rendered it obvious to “dynamically modif[y] an analysis capability of [a] probe during operation based on said received feedback” as required by independent claim 1.

h) Rationale to Combine the Teachings of Duvall and Chu

Petitioner contends a person of ordinary skill in the art would have had reason to combine the teaching of Duvall and Chu. Pet. 14–24 (citing Ex. 1003 ¶¶ 66–77, 94–111). Petitioner specifically argues that Duvall can implement default actions for filtering data that can lead to a “filtering system [] filtering too much or too little.” *Id.* at 20 (citing Ex. 1004, 8:6–8). Petitioner notes that “Duvall itself provides an ‘editing Manager’ that ‘allows the user to make custom changes if the user believes that the filtering system is filtering too much or too little.’” *Id.* (citing Ex. 1004, 8:2–8). Thus, according to Petitioner, a person of ordinary skill in the art “implementing Duvall’s system would have been motivated to seek techniques for more accurately resolving the status of residue data transmissions to ensure transmissions are correctly blocked or allowed.” *Id.* (citing Ex. 1003 ¶ 103). Petitioner argues that this would have led the skilled artisan to look for and locate Chu. *Id.* (citing Ex. 1003 ¶ 104).

Petitioner further contends that Chu is the same field of endeavor as Duvall and provides techniques for determining whether to block or allow residue data. *Id.* (citing Ex. 1005, 9, 44; Ex. 1003 ¶¶ 78–81, 92, 104). Petitioner argues that a person of ordinary skill in the art would have been motivated to incorporate Chu’s user intervention into Duvall’s system for data transmissions not matching any of Duvall’s positive/negative filters at step 104 of Figure 4, nor resolved by Duvall’s post-filtering residue analysis, and would have had a reasonable expectation of success for incorporating

such techniques. *Id.* at 22–23 (citing Ex. 1003 ¶¶ 107, 110; *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 419–421 (2007)).

Patent Owner disputes Petitioner’s position, arguing that Duvall and Chu have completely different focuses, and filter different things for different purposes in different ways. Prelim. Resp. 47–49. Patent Owner lists the following flaws it purports exists in the proposed combination of Duvall and Chu: (1) Duvall is unsuitable for use as a network security monitoring system; (2) Petitioner’s Motivation Relies on a Mischaracterization of Duvall’s concerns about subjectively “filtering too much or too little”; (3) Duvall and Chu use filters in different ways and for different purposes; (4) a person of ordinary skill in the art would not have combined Chu with Duvall given the differences in concerns, underlying assumptions, and goals; (5) Chu does not teach techniques for resolving the status of residue data; and (6) a person of ordinary skill in the art would not have arrived at the claims given the teachings of Duvall and Chu because (i) user intervention is not explained in Chu, and (ii) the combination would be inoperable. *Id.* at 49–64 (citing Ex. 2001 ¶¶ 179–219). Therefore, Patent Owner concludes that Petitioner has not shown that an ordinarily skilled artisan could have or would have made a combination with Duvall and Chu and arrived at the claimed invention. *Id.* at 47–48 (citing *Personal Web Tech. v. Apple Inc.*, 848 F.3d 987, 993–94 (Fed. Cir. 2017) (citing *Belden v. Berk-Tek LLC*, 805 F.3d 1064, 1073 (Fed. Cir. 2015))).

We agree with Patent Owner that Petitioner must articulate a reason why a person of ordinary skill in the art would have combined or modified the prior art references. *In re NuVasive, Inc.*, 842 F.3d 1376, 1382 (Fed. Cir. 2016); *see also Metalcraft of Mayville, Inc. v. The Toro Co.*, 848 F.3d 1358, 1366 (Fed. Cir. 2017) (“In determining whether there would have

been a motivation to combine prior art references to arrive at the claimed invention, it is insufficient to simply conclude the combination would have been obvious without identifying any reason why a person of skill in the art would have made the combination.”); *Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064, 1073 (Fed. Cir. 2015) (“[O]bviousness concerns whether a skilled artisan not only could have made but would have been motivated to make the combinations or modifications of prior art to arrive at the claimed invention.”) (citing *InTouch Techs., Inc. v. VGO Commc’ns, Inc.*, 751 F.3d 1327, 1352 (Fed. Cir. 2014)).

After considering the arguments and evidence presented by the parties, we are persuaded Petitioner has adequately demonstrated that the person of ordinary skill in the art would have had reason to combine Duvall and Chu. The references are in the same field of endeavor and both relate filtering and decisions related to filtered data from the internet in order to remove data from untrusted sites. *See* Ex. 1004, 1:11–24, 2:12–18; Ex. 1005, 3, 9–11, 44. We do not agree with Patent Owner that incorporating teachings from Chu into Duvall would render Duvall inoperable, not do we agree that Chu provides insufficient information regarding “user intervention” when Chu’s policy specifically states “[p]rompt me for my attention otherwise.” Accordingly, we are persuaded by Petitioner’s position that a person of ordinary skill in the art at the critical time would have understood the implications and results of “user intervention” as taught by Chu and how it would have been (and not just could have been) incorporated into Duvall given Duvall’s teachings for a password protected “editing Manager.” *See* Ex. 1004, 8:2–8.

2. *Analysis of Claims 2–7, 15–23, 26–32, and 40–42*

Independent claims 18 and 26 each recite “dynamically modifying an analysis capability of said probe during operation thereof based on said received feedback,” which is recited in independent claim 1. *See* Ex. 1001, 35:55–57, 36:61–63, 37:41–43. All dependent claims depend directly or indirectly from independent claims 1, 18, or 26, and therefore, require the same ability for “dynamically modifying.” *See id.* at 35:58–36:37, 36:64–37:23, 37:44–38:47.

Having reviewed Petitioner’s arguments and supporting evidence in this present record, including the arguments summarized above for claim 1, we determine Petitioner has not established adequately for purposes of this Decision that the combination of Duvall and Chu discloses the limitations of claims 2–7, 15–23, 26–32, and 40–42 for the same reasons Petitioner did not meet its burden regarding claim 1. Accordingly, we determine Petitioner has not demonstrated a reasonable likelihood that these claims would have been rendered obvious to a person of ordinary skill in the art at the critical time by the combined teachings of Duvall and Chu.

B. Alleged Obviousness of Claims 7–13, 16, 24, 32–38, and 41 in view of Duvall, Chu, and Trcka

Petitioner contends dependent claims 7–13, 16, 24, 32–38, and 41 would have been obvious to person of ordinary skill in the art in view of the combined teachings of Duvall, Chu, and Trcka. Pet. 50–69 (citing Ex. 1003 ¶¶ 198–219). Petitioner relies on Trcka’s “Audit” and “Problem Determination” applications to correlate “*status data*” and other data from different devices to “particular types of network problems” occurring within a specific timeframe. *Id.* at 62 (citing Ex. 1014 ¶¶ 112, 116; Ex. 1003 ¶ 204).

Patent Owner does not specifically dispute Petitioner's contentions regarding this challenge. *See generally* Prelim. Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Petitioner citations to and reliance on Trcka do not remedy the deficiencies of Duvall and Chu, and therefore, the combined teachings do not teach or suggest “dynamically modifying an analysis capability of said probe during operation thereof based on said received feedback” as required by all the independent claims. *See* Ex. 1001, 35:55–57, 36:61–63, 37:41–43.

Accordingly, for the reasons discussed previously, we are not persuaded that Petitioner has established a reasonable likelihood of success on this challenge.

C. Alleged Obviousness of Claims 14, 15, 25, 39, and 40 in view of Duvall, Chu, Trcka, and Ziese

Petitioner contends dependent claims 14, 15, 25, 39, and 40 would have been obvious to person of ordinary skill in the art in view of the combined teachings of Duvall, Chu, Trcka, and Ziese. Pet. 69–76 (citing Ex. 1003 ¶¶ 87–91, 221–232). Petitioner relies on Ziese to show correlation of data across multiple different probes (*id.* at 74–75) and for self-tuning probes (*id.* at 75–76) because Ziese discloses techniques in which “programs are automatically updated by downloading and distributing an update in response to an automated event.” *Id.* at 75 (citing Ex. 1015, 2:39–41). According to Petitioner, “the automated process ensures that updates are distributed when they are available, rather than waiting for a user to initiate the update process.” *Id.* at 75 (citing Ex. 1015, 1:54–67; Ex. 1003, ¶231).

Patent Owner does not specifically dispute Petitioner's contentions regarding this challenge. *See generally* Prelim. Resp. Nonetheless, the

burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Petitioner citations to and reliance on Ziese do not remedy the deficiencies of Duvall and Chu, and therefore, the combined teachings do not teach or suggest “dynamically modifying an analysis capability of said probe during operation thereof based on said received feedback” as required by all the independent claims. *See* Ex. 1001, 35:55–57, 36:61–63, 37:41–43.

Accordingly, for the reasons discussed previously, we are not persuaded that Petitioner has established a reasonable likelihood of success on this challenge.

V. CONCLUSION

After consideration of the Petition, the Preliminary Response, and the evidence of record, we are not persuaded that Petitioner has demonstrated a reasonable likelihood of prevailing in showing that any of claims 1–42 of the ’237 Patent is unpatentable on any asserted ground. On this record, we decline to institute *inter partes* review of 1–42 of the ’237 Patent.

VI. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that an *inter partes* is not instituted.

PETITIONER:

Jonathan Tuminaro
Dan Block
Michael Specht
Steven Pappas
STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
jtuminar-ptab@sternekessler.com
dblock-ptab@sternekessler.com
mspecht-ptab@sternekessler.com
spappas-ptab@sternekessler.com

PATENT OWNER:

Nolan M. Goldberg
Baldassare Vinti
PROSKAUER ROSE LLP
NGoldbergPTABMatters@proskauer.com
BVinti@proskauer.com

Jonathan A. Roberts
NIXON & VANDERHYE P.C.
jr@nixonvan.com