

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PALO ALTO NETWORKS, INC.,
Petitioner

v.

BT AMERICAS INC.,
Patent Owner

Case IPR2023-00889
U.S. Patent No. 7,895,641

**PETITION FOR *INTER PARTES* REVIEW OF
U.S. PATENT NO. 7,895,641**

Mail Stop PATENT BOARD
Patent Trial and Appeal Board
U.S. Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

I.	Introduction	1
II.	Mandatory Notices (37 C.F.R. § 42.8)	2
III.	Grounds for Standing.....	4
IV.	Identification of Challenge.....	4
	A. Citation of prior art	4
	B. Statutory Grounds for the Challenge.....	6
V.	The '641 Patent.....	6
	A. Overview	6
	B. Prosecution History.....	9
	C. Previous <i>Inter Partes</i> Review	10
	D. Level of Ordinary Skill in the Art	11
	E. Claim Construction	11
VI.	Grounds of Unpatentability.....	13
	A. Ground 1: Claims 1-7 and 15-17 are obvious over Duvall and Chu.....	13
	1. A POSA would have been motivated to combine Duvall with Chu.	13
	2. Independent Claim 1	23
	(a) [1-pre] “A system...”	23
	(b) [1A] “a sensor...”	26
	(c) [1B] “a filtering subsystem...”.....	29
	(d) [1C] “a communications system...”	37
	(e) [1D] “a receiver...”.....	40
	(f) [1E] “a modification control system...”	41
	3. Claim 2	42
	4. Claim 3	43
	5. Claim 4	44
	6. Claim 5	44
	7. Claim 6	44

Petition for Inter Partes Review
U.S. Pat. No. 7,895,641

8.	Claim 7	47
9.	Claim 15	47
10.	Claim 16	48
11.	Claim 17	49
B.	Ground 2: Claims 7-13 and 16 are obvious over Duvall, Chu, and Trcka.....	50
1.	A POSA would have been motivated to combine the Duvall-Chu system with Trcka.....	50
2.	Claims 7, 8 and 12	52
1.	Claims 9 and 13	54
2.	Claim 10	54
3.	Claim 11	56
4.	Claim 16	57
C.	Ground 3: Claims 14-15 are obvious over Duvall, Chu, Trcka, and Ziese.....	58
1.	A POSA would have been motivated to combine the Duvall-Chu-Trcka system with Ziese.....	58
2.	Claim 14	62
3.	Claim 15	63
D.	Ground 4: Claims 18-25 are obvious over Duvall, Chu, and Cogger.....	64
1.	A POSA would have been motivated to combine the Duvall with Chu and Cogger.....	64
2.	Independent Claim 18	67
(a)	[18-pre] “A method...”	67
(b)	[18A] The “creating” step	68
(c)	[18B] The “correlating” step	69
(d)	[18C] The “using” step	72
(e)	[18D] The “consolidating” step.....	74
(f)	[18E] The “providing” step	74
3.	Claim 19	75
4.	Claim 20	78

Petition for Inter Partes Review
U.S. Pat. No. 7,895,641

5.	Claim 21	79
6.	Claim 22	80
7.	Claims 23 and 24	82
8.	Claim 25	84
VII.	The Board should not exercise its discretion to deny the Petition.....	84
A.	The Board should not deny the Petition under <i>Fintiv</i>	84
B.	<i>Advanced Bionics</i> strongly favors institution.	85
VIII.	No Evidence of Secondary Considerations.	86
IX.	Conclusion.....	86
X.	Appendix A: Challenged Claims.....	87

EXHIBIT LIST

<i>Exhibit #</i>	<i>Description</i>
1001	U.S. Patent No. 7,895,641 to Schneier <i>et al.</i> (“’641 patent”)
1002	Prosecution History of U.S. Patent No. 7,895,641 (“Prosecution History”)
1003	Declaration of Dr. Kevin Jeffay in Support of Petition for <i>Inter Partes</i> Review of U.S. Patent No. 7,895,641 (“Jeffay Declaration”)
1004	U.S. Patent No. 5,884,033 to Duvall <i>et al.</i> (“Duvall”)
1005	Yang-hua Chu, “Trust Management for the World Wide Web, M.I.T. (June 13, 1997) (“Chu”)
1006	U.S. Patent No. 5,970,149 to Johnson (“Johnson”)
1007	U.S. Patent No. 6,088,804 to Hill <i>et al.</i> (“Hill”)
1008	Lane B. Warshaw <i>et al.</i> , “VenusIDS: An Active Database Component for Intrusion Detection,” Applied Research Laboratories / Department of Computer Sciences, The University of Texas at Austin, Annual Computer Security Application Conference (1999) (“Warshaw”)
1009	U.S. Patent No. 6,704,874 to Porras <i>et al.</i> (“Porras”)
1010	U.S. Patent No. 7,159,237 to Schneier <i>et al.</i> (“237 patent”)
1011	<i>Fortinet Inc. v. BT Americas, Inc.</i> , IPR2019-01324, Paper 9 (Institution Decision) (P.T.A.B. Jan. 7, 2020)
1012	<i>British Telecommunications PLC v. Fortinet, Inc.</i> , Civil Action No. 18-1018, Memorandum Order re: Claim Construction (D. Del. Aug. 5, 2021)
1013	<i>British Telecommunications PLC v. Fortinet, Inc.</i> , Civil Action No. 18-1018, Claim Construction Order (Aug. 18, 2021 D. Del.)
1014	U.S. Patent Pub. No. 2001/0039579 to Trcka <i>et al.</i> (“Trcka”)
1015	U.S. Patent No. 6,484,315 to Ziese (“Ziese”)

Petition for Inter Partes Review
U.S. Pat. No. 7,895,641

<i>Exhibit #</i>	<i>Description</i>
1016	<i>British Telecommunications PLC v. Fortinet, Inc.</i> , Civil Action No. 18-1018, Dkt. No. 161 (D. Del. Dec. 31, 2021)
1017	Prosecution History of U.S. Patent No. 7,159,237 (“237 Prosecution History”)
1018	Declaration of Dr. James L. Mullins regarding the authenticity and public accessibility of Chu
1019	Curriculum Vitae of Dr. James L. Mullins
1020	DSpace@MIT Listing for Chu, available at https://dspace.mit.edu/handle/1721.1/43534
1021	OPAC Listing for Chu showing availability at Barker Library
1022	MARC Record for Chu
1023	OPAC MIT Libraries search for “trust management”
1024	WorldCat Listing for Chu, available at https://www.worldcat.org/title/trust-management-for-the-world-wide-web/oclc/38271519&referer=brief_results
1025	WorldCat search for “trust management world wide web,” available at https://www.worldcat.org/search?q=k%3Atrust+management+world+wide+web&qt=results_page#%2528x0%253Abook%2Bx4%253Athesis%2529for%E2%80%A6
1026	Sinrod et al., “ <i>Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws</i> ,” Santa Clara High Technology Law Journal (January 2000)
1027	Guttman et al., “ <i>Implementing Internet Firewall Security Policy</i> ,” National Institute of Standards and Technology (April 13, 1998)
1028	Rothfuss et al., “ <i>Go Ahead, Visit Those Websites, You Can’t Get Hurt ... Can You?</i> ,” Lawrence Livermore National Laboratory (June 3, 1997)
1029	Capture of Merriam Webster definition of “empirical,” www.merriam-webster.com/dictionary/empirical

Petition for Inter Partes Review
U.S. Pat. No. 7,895,641

<i>Exhibit #</i>	<i>Description</i>
1030	Coates, et al., “ <i>Melissa Virus Exposes High-Tech Vulnerability</i> ,” Chicago Tribune (March 30, 1999)
1031	Abie, “ <i>An Overview of Firewall Technologies</i> ,” Norwegian Computing Center (January 2000)
1032	Curriculum Vitae of Kevin Jeffay, Ph.D.
1033	U.S. Patent No. 6,859,783 to Cogger <i>et al.</i> (“Cogger”)
1034	<i>British Telecommunications PLC v. Fortinet, Inc.</i> , Civil Action No. 18-1018, Claim Construction Report and Recommendation (Apr. 15, 2021 D. Del.)
1035	<i>British Telecommunications PLC & BT Americas, Inc. v. Palo Alto Networks, Inc.</i> , 1:22-cv-01538, Complaint (Nov. 28, 2022 D. Del.)
1036	U.S Patent No. 6,775,657 to Baker (“Baker”)
1037	Escamilla, T., “ <i>Intrusion Detection: Network Security Beyond the Firewall</i> ,” Wiley Press, 263-281 (1998) (excerpt)
1038	U.S. Patent No. 5,261,044 to Dev <i>et al.</i> (“Dev”)
1039	U.S. Patent No. 5,768,501 to Lewis (“Lewis”)

I. Introduction

Palo Alto Networks, Inc. (“PAN”) petitions for *inter partes* review of claims 1-25 (“challenged claims”) of U.S. Patent No. 7,895,641 (“’641 patent,” “EX1001”). The Board should institute this proceeding because the ’641 patent claims nothing more than well-known techniques developed long before the ’641 patent’s earliest possible priority date.

The claims are simple in operation: data is collected and filtered at a probe; if the data does not correspond to a positive or negative filter, the data is analyzed; and information about the data is sent to a human for feedback. Although the ’641 patent describes “monitoring, detecting and responding to computer network intrusions,” the patent and claims are broadly directed to “monitoring of any system,” “filtering the data from the monitoring for noteworthy events happening in or affecting any system,” and “alerting human beings to any such noteworthy events.” *Id.*, 15:59-67.

During prosecution, applicant argued that one claim element was allegedly not found in the prior art: “an analysis of post-filtering residue, wherein the post-filtering residue is neither discarded nor selected by the filtering.” EX1001, 34:25-30; EX1002, ’641 File History, 0218, 0220; EX1017, 0300-301, 0255, 0219. This claim element, the applicant argued, requires “three kinds of data: 1) data selected by filtering, 2) data discarded by filtering and 3) post-filtering residue that is neither

of the first two.” EX1017, 0300-301. But this type of analysis was disclosed in prior art that was not of record. For example, Duvall (EX1004)¹ and Chu (EX1005)² disclose multi-stage filters that (i) *allow* or select certain data, (ii) *block* or discard other data, and (iii) analyze residue data that is neither allowed nor blocked.

Duvall discloses that such residual data, after analysis, may still be unknown data, thus requiring default actions—pass or block. Chu, in contrast, discloses that information about such unknown data may be sent to a human for resolution. A skilled artisan would have been motivated to combine Duvall and Chu because Chu offers an improvement to Duvall, which is to incorporate human review of such residual data. EX1003, Jeffay Decl., ¶¶99-115. Such human review provides feedback to the system, which can be used to update the probe using the Duvall’s disclosed updating mechanism. *Id.*

None of the other prior art relied on here was before the Office. The Board should institute this proceeding and find the challenged claims unpatentable.

II. Mandatory Notices (37 C.F.R. § 42.8)

Real Party In Interest: The real party-in-interest is Palo Alto Networks, Inc. (“PAN”).

¹ U.S. Patent No. 5,884,003 (EX1004).

² “Trust Management for the World Wide Web” by Yang-hua Chu (EX1005).

Petition for Inter Partes Review
U.S. Pat. No. 7,895,641

Related Matters: The '641 patent is asserted against PAN in *British Telecommunications PLC & BT Americas, Inc. v. Palo Alto Networks, Inc.*, 1:22-cv-01538 (D. Del.), filed November 28, 2022.

The '641 patent was previously asserted against Fortinet in *British Telecommunications PLC v. Fortinet Inc.*, No. 1:18-cv-01018-CFC-MPT (D. Del.) (the "Fortinet Litigation"). The Fortinet Litigation was subsequently dismissed.

The '641 patent was the subject of a petition for *inter partes* review filed by Fortinet in IPR2019-01324 (the "Fortinet IPR Proceeding"), which the Board denied. EX1011, IPR2019-01324 Paper 9, 22.

PAN was not involved in the Fortinet Litigation or the Fortinet IPR Proceeding.

Lead and Backup Counsel: Pursuant to 37 C.F.R. § 42.8(b)(3) and 42.10(a), Petitioner appoints **Jonathan Tuminaro** (Reg. No. 61,327) as its lead counsel, and **Daniel S. Block** (Reg. No. 68,395), **Michael D. Specht** (Reg. No. 54,463), and **Steven M. Pappas** (Reg. No. 73,904) as its back-up counsel, all at the address: STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C., 1100 New York Avenue, N.W., Washington, D.C. 20005; phone number: (202) 371-2600; and facsimile: (202) 371-2540.

Service Information: Petitioner consents to electronic service by email at the email addresses: **jtuminar-PTAB@sterneessler.com**, **mspecht-**

PTAB@sternekessler.com, dblock-PTAB@sternekessler.com, spappas-PTAB@sternekessler.com, and PTAB@sternekessler.com.

III. Grounds for Standing

Petitioner certifies that the '641 patent is available for *inter partes* review and that Petitioner is not barred or estopped from requesting an *inter partes* review challenging the '641 patent claims.

IV. Identification of Challenge

A. Citation of prior art

The '641 patent was filed October 20, 2006, and is a continuation of an application filed January 19, 2001. EX1001, Cover (63). The '641 patent further claims priority to a provisional application filed March 16, 2000. *Id.*, Cover (60). Petitioner does not concede that the challenged claims of the '641 patent are entitled to the provisional application filing date. Nonetheless, all references relied on here qualify as prior art even if it is.

Reference	Prior Art Basis
Duvall (EX1004)	§§102(a), 102(b), and/or 102(e)
Chu (EX1005)	§102(b)
Trcka (EX1014)	§102(e)
Ziese (EX1015)	§102(e)
Cogger (EX1033)	§102(e)

Chu is a thesis published by the Massachusetts Institute of Technology (“M.I.T.”). EX1018, ¶36; EX1005, Chu, 1. Chu is prior art because it was publicly available and accessible by February 4, 1998 or earlier. EX1018, ¶¶57-59. Chu itself includes an authored date of “Jun 13, 1997,” a copyright date of “1997,” and a stamp showing “OCT 29, 1997,” which Dr. Mullins explains is the date Chu was received by M.I.T. and ready for cataloging/indexing. EX1005, 1; EX1018, ¶¶41-42; *see also* EX1020, 1 (“Date issued 1997”). The online public access catalog (OPAC) MARC record for Chu further establishes that Chu was cataloged, indexed, and searchable within a few months, showing the catalog entry created on January 27, 1998. EX1021, MARC Record, 1 (field 008); EX1018, ¶¶47-49. The MARC record also shows that Chu was meaningfully indexed, by title and author, as well as searchable by keyword, allowing a person of ordinary skill exercising reasonable diligence to find Chu. EX1018, ¶¶47, 50-56; *In re Hall*, 781 F.2d 897, 899-900 (Fed. Cir. 1986). Chu indicates that no access restrictions were placed upon the public, stating, “[t]he author hereby grants to M.I.T. permission to reproduce [and] distribute publicly paper and electronic copies of this thesis and to grant others the rights to do so.” EX1005, 1. Therefore, Chu was publicly accessible at least two years before the earliest possible priority date of the ’641 patent. EX1018, ¶¶57-59.

B. Statutory Grounds for the Challenge

Ground	References	Basis	Challenged Claims
1	Duvall and Chu	§ 103	1-7, 15-17
2	Duvall, Chu, and Trcka	§ 103	7-13, 16
3	Duvall, Chu, Trcka, and Ziese	§ 103	14-15
4	Duvall, Chu, and Cogger	§ 103	18-25

V. The '641 Patent

A. Overview

The '641 patent is directed to “network security” and explains that “[f]irewalls prevent unauthorized traffic from entering a company’s internal network,” but “such products cannot be relied upon to work perfectly.” EX1001, 1:18-33; EX1003, ¶¶43-53. The patent contends that “[s]ystem administrators normally do not have the time or ability to read through large amounts of constantly updated audit information, looking for attacks on their systems [and] also do not have the time to continuously monitor hacker activities [or] become experts on every kind of intrusion and to maintain that expertise.” EX1001, 1:36-43. The '641 patent attempts to address these issues through review of potential threats by using a human analyst. *Id.*, 1:34-36; 1:44-50.

Specifically, the '641 patent “provide[s] a managed security monitoring service (the ‘MSM service’) that monitors a customer’s network activity” to determine “activity possibly implicating security concerns.” EX1001, 1:57-65. The patent involves human analysts by “transmit[ting] information about such activity” to them to determine an “appropriate response.” *Id.*, 1:65-2:2. The patent explains, “[t]he MSM service is not intended to replace but to supplement . . . a customer’s existing preventative security products,” including traditional “firewalls, servers, [and] routers.” *Id.*, 2:3-8.

Figure 2 provides “a system overview of an exemplary embodiment of a probe/sentry system.” EX1001, 8:41-42.

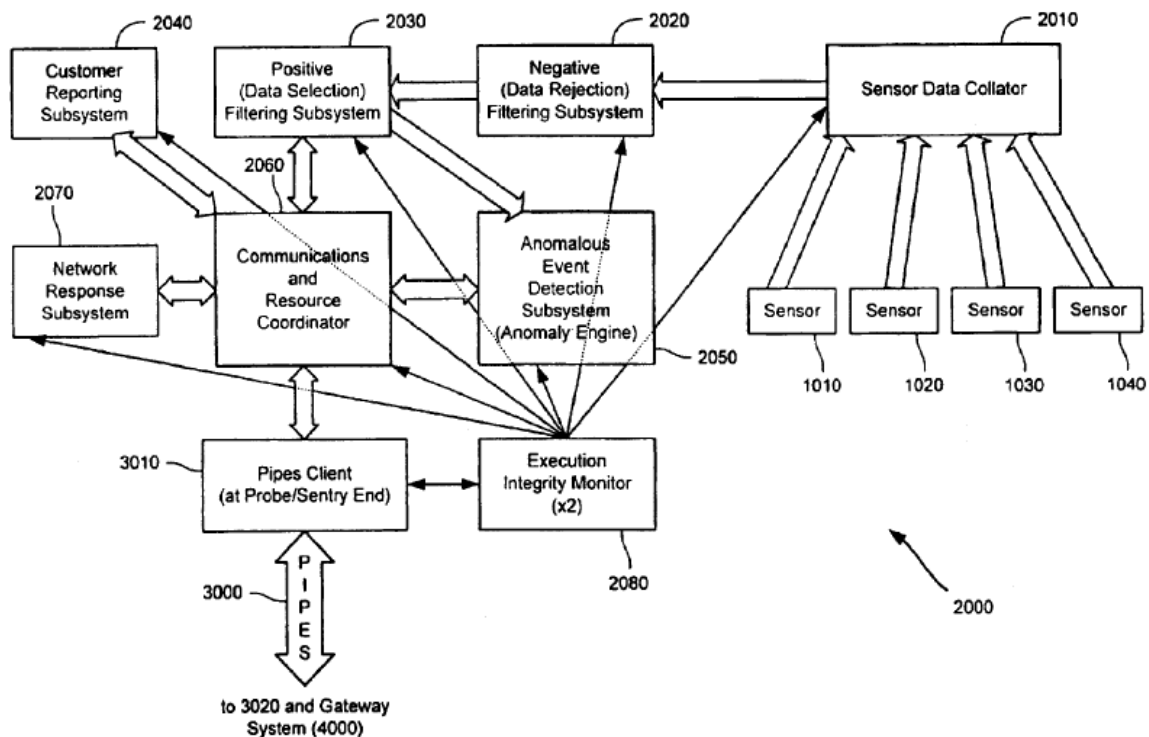


FIG. 2

EX1001, FIG. 2.

Here, “[d]ata collected by sensors 1010, 1020, 1030 and 1040 . . . are collated by sensor data collator 2010.” EX1001, 8:47-51. “[T]he 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” *Id.*, 8:51-55.

Subsequently, “[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.*, 8:55-59. “Interesting” data is then forwarded to a gateway system 4000 via pipes 3000 for review by a human analyst. *Id.*, 8:66-9:2, 9:13-21, 9:54-62.

The patent explains, “[t]hose skilled in the art will realize [] that the present invention is usable generally for (i) **monitoring of any system**; (ii) filtering the data from the monitoring **for noteworthy events happening in or affecting any system**; (iii) alerting human beings to any such noteworthy events; and (iv) providing for a response by human beings to any such alert.” *Id.*, 15:62-16:6.³ The independent claims of the ’641 patent reflect this broad applicability, reciting “a security monitoring system for a computer network” and “identify[ing] potentially security-related events.” EX1003, ¶52.

³ All emphasis added unless otherwise indicated.

B. Prosecution History

The '641 patent was rejected twice before being allowed. The Office rejected claims 45-61 (issued claims 1-17) for obviousness-type double patenting over its parent, U.S. Patent No. 7,159,237 (EX1011, “'237 patent”). EX1002, 0136, 0197.

During prosecution, Applicant made one substantive amendment to the independent claims:

b) <u>analyzing status data to identifying potentially security-related events represented in the ~~pertaining to said network by analyzing said 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;~~</u>
--

EX1017, 0219 (excerpt).

Applicant's arguments for allowance focused solely on this claim amendment. EX1017, 0226-27. The Examiner, however, issued a new obviousness rejection, asserting that U.S. Patent No. 6,704,874 (“Porras”) disclosed the amended “post-filtering residue” limitations. *Id.*, 0237-38.

In response, Applicant argued Porras disclosed “data that is selected by filtering” and “data [that] is discarded in the filtering process,” but not “data that could be considered post-filtering residue.” *Id.*, 0300-301. The Examiner agreed and issued a notice of allowance. *Id.*, 0326.

During prosecution of the '641 patent, the Applicant also overcame rejections to 62-68 and 70 (issued claims 18-25) by making a similar amendment to the claims:

creating an event record for information received about an identified potentially security-related event occurring on the network, <u>wherein the potentially security-related event is identified by filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is neither discarded nor selected by the filtering;</u>

EX1002, 0218.

But techniques for analyzing “post-filtering residue” were well known at the time of the '641 patent, as illustrated by Duvall and Chu.

C. Previous *Inter Partes* Review

The '641 patent was the subject of a petition for *inter partes* review in IPR2019-01324, which the Board denied. EX1011, 22. The petitioner there—Fortinet Inc.—alleged that claims 1-25 of the '641 patent were obvious over Hill (EX1007) in view of Warshaw (EX1008). EX1011, 6-7.

Fortinet presented two theories for the “post-filtering residue” limitations of the independent claims—one based on Hill, and one based on Hill in view of Warshaw. *Id.*, 13. The Board disposed of Fortinet’s first theory because Hill allegedly did not teach “data . . . discarded . . . by filtering.” *Id.*, 17-18.

The Board, however, did not dispute Warshaw’s alleged teaching of analyzing “post-filtering residue.” *Id.*, 18-19. The Board instead was not persuaded

“that [Fortinet’s] rationale for combining Hill and Warshaw is supported by sufficient rational underpinning.” *Id.*, 18-21. The Board thus denied institution. *Id.*, 22. Petitioner here—PAN—had no involvement with Fortinet’s previous IPR petition.

D. Level of Ordinary Skill in the Art

A person of ordinary skill in the art (“POSA”) at the time of the ’641 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. EX1003, ¶¶63-64.

Petitioner’s expert, Dr. Kevin Jeffay, has more than ordinary skill in the art. *Id.*, ¶64. His opinions are supported by not only his decades of experience, but also the references cited in this Petition as well as the additional reasoning and documents cited in his declaration. *See, e.g., id.*, ¶¶112-113; EX1036, EX1037, EX1038, EX1039.

E. Claim Construction

The following terms were construed in a district-court litigation between the Patent Owner (“British Telecommunications”) and Fortinet:

- “*status data*”;

- “*dynamically*”;
- “*probe*”;
- “*information received about an identified potentially security-related event occurring on the network wherein the potentially security related event is identified by filtering followed by an analysis of post-filtering residue*”;
- “*customer information*”; and
- “*problem ticket*.”

EX1013, 1-2; EX1012; *see also* EX1034.⁴ British Telecommunications and Fortinet agreed that the phrase “*post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering*” 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.” EX1013, 4.

Here, no claim terms require an explicit construction. Nonetheless, Petitioner shows below that the challenged claims are unpatentable under both the ordinary and customary meaning as understood by one of ordinary skill in the art at the time

⁴ The district-court case between British Telecommunications and Fortinet was terminated on January 4, 2022. D.I. 161. Infringement and invalidity issues were not decided.

of the invention in light of the specification and the prosecution history or the district court's constructions.⁵

VI. Grounds of Unpatentability

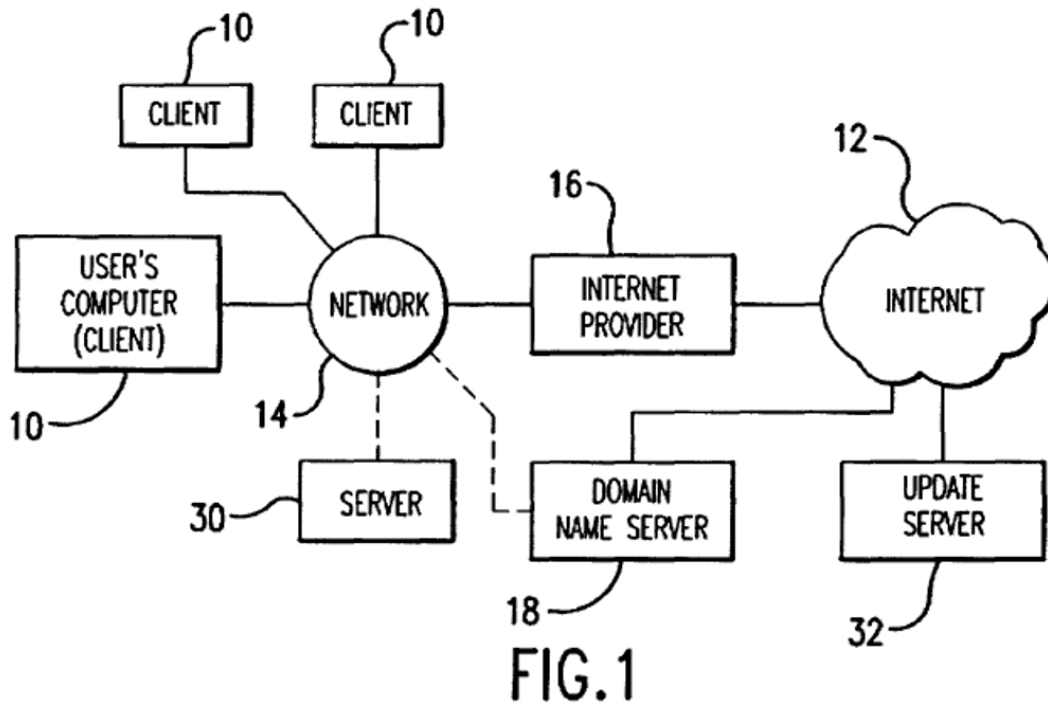
A. Ground 1: Claims 1-7 and 15-17 are obvious over Duvall and Chu.

1. A POSA would have been motivated to combine Duvall with Chu.

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. EX1004, Duvall, 1:7-24; EX1003, ¶¶68-79, 99. “Congress recently passed the Communications Decency Act (CDA) to outlaw transmission of indecent material over the Internet.” EX1004, 1:18-20. Duvall’s techniques prevent transmission of such content by “allow[ing] Internet users to filter material transmitted over the Internet.” EX1004, 1:27-29.

Duvall’s Figure 1 illustrates an example “network with a client computer for accessing the Internet.” EX1004, 2:24-25; EX1003, ¶100.

⁵ The district court’s previous claim constructions are not binding here because neither the PTAB nor Petitioner were “a party to the earlier district court litigation and cannot be bound by its outcome.” *In re Trans Texas Holdings Corp.*, 498 F.3d 1290, 1297 (Fed. Cir. 2007). Petitioner reserves the right to challenge the claims under 35 U.S.C. § 112 in other proceedings.



EX1004, FIG. 1.

“A user uses a computer which serves as a client 10 to communicate with other computers over Internet 12.” EX1004, 2:34-35. In one embodiment, “a filtering system resides in client computer 10” and includes a “filter database 24,” as shown in Figure 2. *Id.*, 3:41-45.

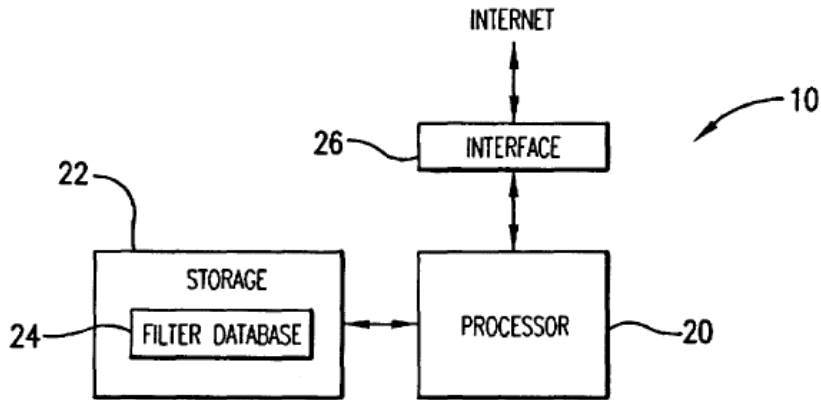


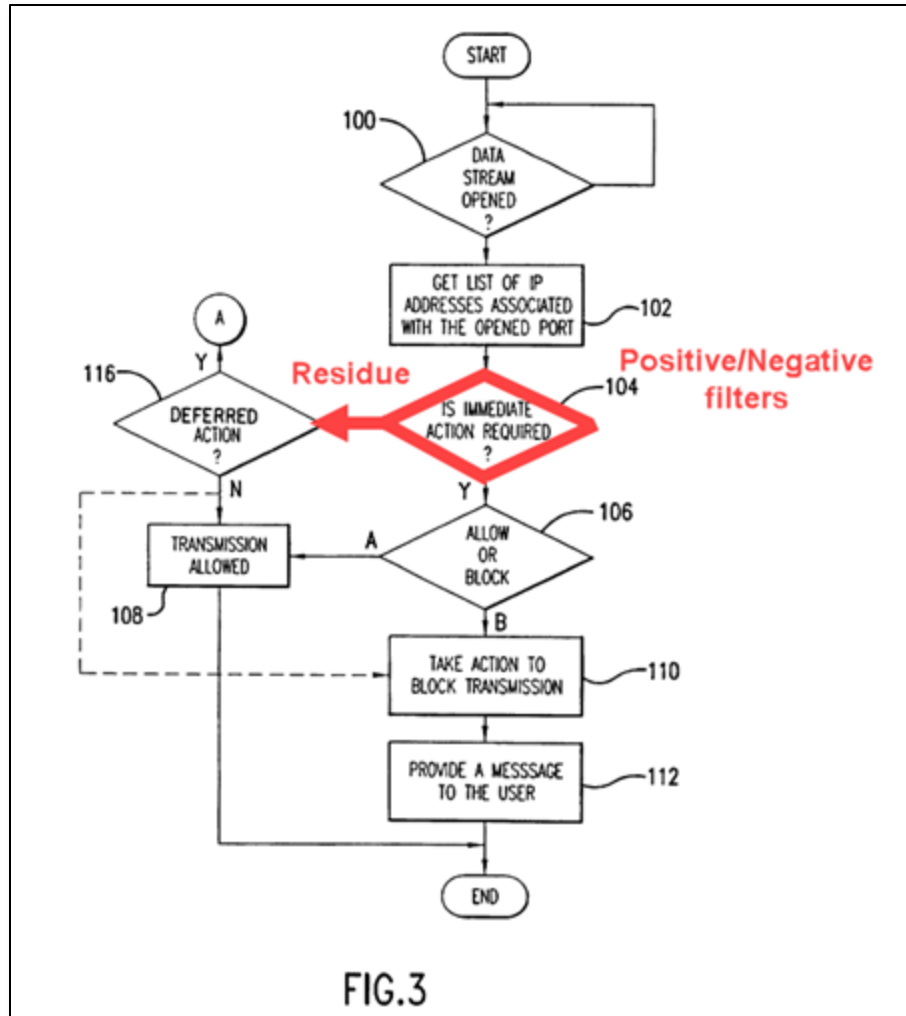
FIG.2

EX1004, FIG. 2.

In another embodiment, “the filtering system can be provided from a server 30 that is on the client’s own network 40.” EX1004, 8:18-21. Duvall explains, “[s]uch a topology may be more desirable, for example, in a corporate network that has a limited size and a uniform set of filters for many users.” *Id.*, 8:21-23. “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.*, 8:23-26.

Duvall discloses filtering techniques that include ALLOW filters, BLOCK filters, and deferred-action filters. EX1004, 1:59-64, 3:64-66. An ALLOW filter *allows* data transmissions to pass through. *Id.*, 3:64-66. A BLOCK filter *blocks* data transmissions from passing through. *Id.* And a deferred-action filter specifies additional analysis of data transmissions that are neither ALLOWED nor BLOCKED. *Id.*, 4:65-5:19; EX1003, ¶103.

In a preferred embodiment, the filters are sequentially implemented so that “the system searches ALLOW filters first, BLOCK filters next, and deferred action filters last.” EX1004, 4:22-5:1; EX1003, ¶104. Certain data transmissions may not match any ALLOW or BLOCK filters, leaving post-filtering residue. EX1003, ¶104. Referring to Figure 3 (below), Duvall’s system (1) at block 104 “check[s] to determine if any [filters] require immediate action, i.e., if unconditional allowing or blocking is required (steps 104 and 106)” and (2) if allowing and blocking filters are not applied (i.e., there is residue data), “it is determined [at block 116] whether a deferred action must be taken.” *Id.* at 4:38-5:1; EX1003, ¶104.



EX1004, FIG. 3 (annotated).

The data transmissions that do not match the immediate action ALLOW or BLOCK filters in step 104 (i.e., the residue data) are further analyzed by the system in “deferred filters,” as shown by the example in FIG. 4 of Duvall. EX1004, 5:8-29; EX1003, ¶105.

Figure 4 discloses techniques for analyzing residue data, such as keyword matching and pattern matching, to determine what to do with that data. EX1004,

5:20-29. Depending on the results of the matching, the residue data can be blocked, discarded, replaced, or edited. *Id.*, 5:30-51.

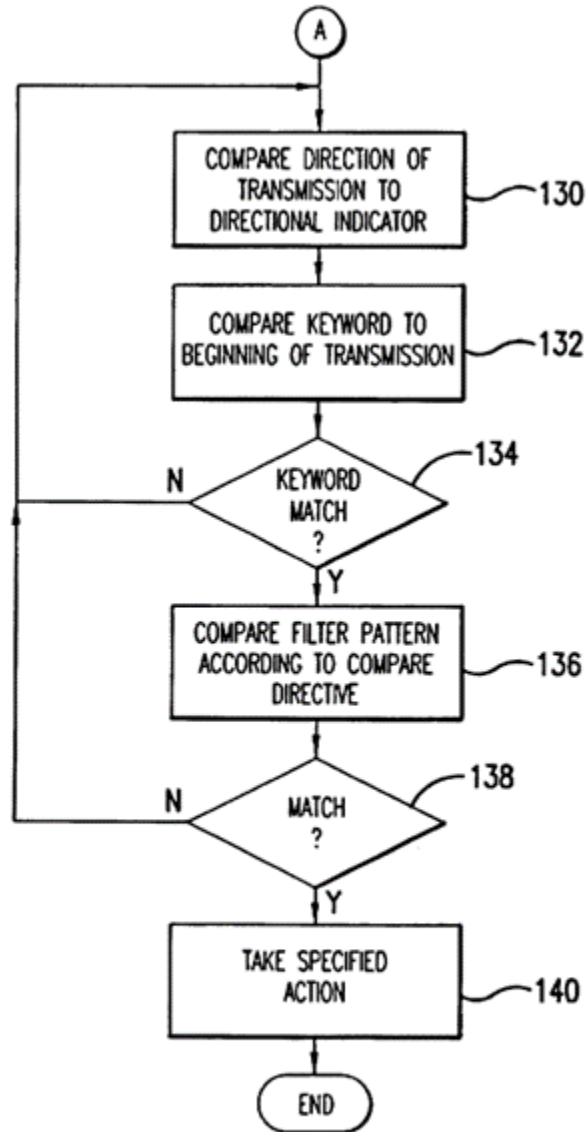


FIG.4

EX1004, FIG. 4.

Duvall contemplates that residue data may not trigger a deferred action and therefore the system may default to allowing or blocking the residue data. Duvall discloses, “[i]f there is no deferred action, the system can default to allow the transmission (step 108 [of FIG. 3]), or it can default to block the transmission (steps 110 and 112).” EX1004, 5:1-3; EX1003, ¶106.

A POSA would have recognized, however, that applying a default action of allow or block for residue data could lead to, as Duvall discloses, **“the filtering system . . . filtering too much or too little.”** EX1004, 8:6-8. A POSA would have recognized that a default action for residue data (i.e., data that matches neither an ALLOW or BLOCK filter at step 104 of Figure 3) can lead to allowable data being blocked, or more importantly, harmful data being allowed through the system. EX1003, ¶107. Duvall 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.**” EX1004, 8:2-8. Thus, a POSA implementing Duvall’s system would have been motivated to seek techniques for more accurately resolving residue data to ensure transmissions are correctly blocked or allowed. EX1003, ¶107.

This would have led a POSA to search for and locate Chu. EX1003, ¶108. In the same field of endeavor, Chu provides techniques for determining whether to block or allow residue data. EX1005, 9, 44; EX1003, ¶108. Chu protects users from untrustworthy information available on the World Wide Web and provides

examples of trust-management issues, such as a user attempting to download software (e.g., a game) from a Web page. EX1005, 9, 23. Chu explains that the user may have “concerns that prevent her from downloading the game on her machine,” such as “[d]oes this game contain a virus that would erase her hard drive? (security issue).” *Id.* Chu therefore discloses various trust policies that allow computer systems to make trust decisions about user data (e.g., Web requests) transmitted over the Internet. *Id.*, 28, 35-43.

For example, Chu discloses policies addressing the question of “should I download the active content at this URL.” EX1005, 43-48. Similar to Duvall, Chu’s exemplary policies make use of a “blacklist” (i.e., “sites or directories [the system] should not download codes from”) and a “whitelist” (i.e., “sites know[n] to be trustworthy”). *Id.*, 44; EX1003, ¶109. Like Duvall’s BLOCK filter, an exemplary Chu policy (shown below) *blocks* URLs in the blacklist; and like Duvall’s ALLOW filter, Chu’s policy *allows* URLs in the whitelist. EX1005, 44; EX1003, ¶109. If a URL is unknown (i.e., it’s not in the blacklist or whitelist), the user is prompted for attention. EX1005, 44; EX1003, ¶109.

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.

Profiles-0.92

```
(threshold-and
  2
  (not (url-match URL ("http://www.harvard.edu"
    "http://www.caltech.edu"))) ← Block filter
  (url-match URL ("http://web.mit.edu")) ← Allow filter
  unknown) ← Unmatched residue for human review
```

EX1005, 44 (annotated).

While Chu discloses that “[t]he blacklist and whitelist ensure good automation of the trust decision process if the lists are reasonably complete,” Chu recognizes that data transmissions not matching the blacklist or whitelist need human intervention. EX1005, 44; EX1003, ¶110. Chu thus explains that “[u]ser intervention is needed only when the given URL is in neither the blacklist nor the whitelist.” EX1005, 44; EX1003, ¶110.

A POSA 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 nor resolved by Duvall’s post-filtering residue analysis, as depicted in FIG. 4. EX1003, ¶111. Again, Duvall discloses “allow[ing] the user to make custom changes [to filters] if the user believes that the filtering system is filtering too much or too little.” EX1004, 8:5-7. In Duvall’s corporate

environment, where a “uniform set of filters for many users” is provided, a POSA would have understood that the person making the changes to these filters would be a person trained in network administration and security, not each individual employee at their own computer. EX1004, 8:18-26; EX1003, ¶112. Indeed, Duvall discloses that the “editing manager” is “preferably separately password protected” to prevent unauthorized modification of the filters. EX1004, 8:7-9; EX1003, ¶112. A POSA would have understood that the person may also be part of a specialized third-party network-security service, rather than a corporate employee. EX1003, ¶113. *See also* EX1037, 277 (“A network operations center is staffed 7 X 24, and a specific expert is assigned to your account. When an event is detected, IBM’s security experts notify you and help you respond to the event.”).

A POSA would have had a reasonable expectation of success incorporating such techniques because this amounts to nothing more than incorporating well-known techniques (providing information to a human user for analysis) into Duvall’s known system. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 419-421 (2007); EX1003, ¶114. Duvall already suggests reviewing system activity to determine whether “the filtering system is filtering too much or too little,” EX1004, 8:5-7, and further “provides a screen on the user’s display” for viewing information about data transmissions, *id.*, 4:61-64; EX1003, ¶114. Moreover, Duvall and Chu filter transmissions based on similar information, such as a URL or IP address.

Compare EX1004, 4:38-40, *with* EX1005, 44. Thus, a POSA would have recognized that information about data transmissions not matching any of Duvall's filters could be provided to a user with only minor changes to Duvall's overall process. EX1003, ¶114.

A POSA would have been further motivated to combine Duvall and Chu because both are in the same field of preventing unsecure data transmissions over the Internet. EX1004, 1:7-24; EX1005, 9, 44; EX1003, ¶115. Both implement techniques for determining whether to allow or block data transmissions, and Chu further discloses the utility of involving a human to properly address residue transmissions. EX1003, ¶115. Therefore, a POSA would have been motivated to combine, with a reasonable expectation of success, Duvall and Chu, and the results of the combination would have been predictable. *Id.*, ¶115.

2. Independent Claim 1⁶

(a) [1-pre] "A system..."

To the extent the preamble is limiting, Duvall discloses it.

Duvall discloses "*a security monitoring system for a computer network.*"

Duvall is directed to "filtering messages transmitted between the Internet and a client computer" to ensure content that implicates security concerns does not reach

⁶ The claims are provided in Appendix A.

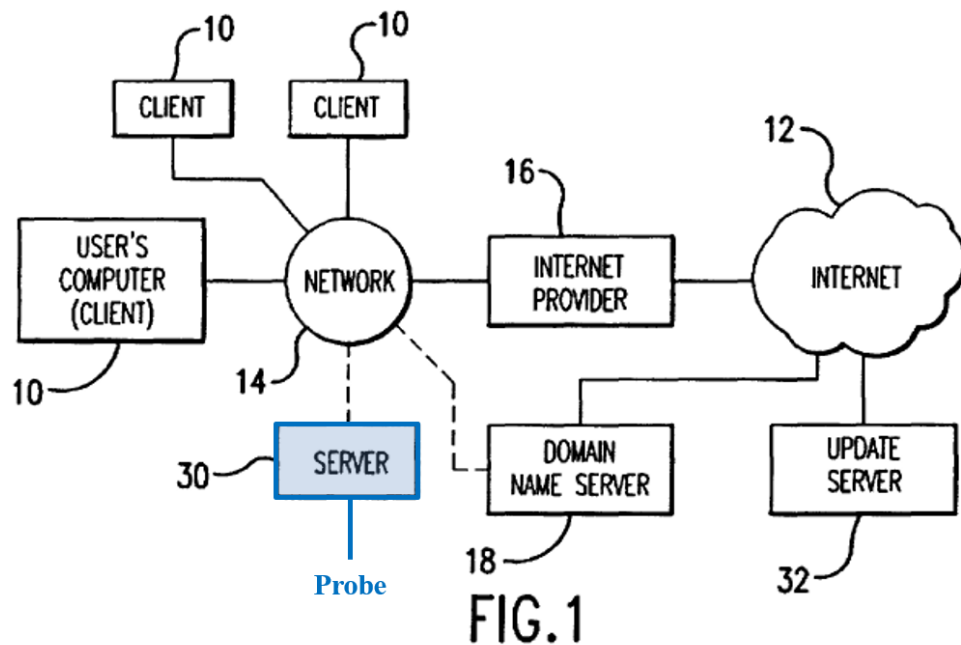
recipients. EX1004, 1:7-24; EX1003, ¶117. For example, Duvall’s techniques prevent illegal transmission (*e.g.*, under the “Communications Decency Act” (CDA)) of “objectionable materials, especially sexually explicit materials,” by “allow[ing] Internet users to filter material transmitted over the Internet.” EX1004, 1:12-20, 1:27-29; EX1003, ¶117. A POSA would have understood that such objectionable material often presented security risks to recipients and recipients’ organizations. EX1003, ¶117.

The ’641 patent broadly recites that “exemplary implementations of the present invention [are] directed at monitoring, detecting, and responding to computer network intrusions” but that, more broadly, “the present invention is usable generally for (i) monitoring of any system; (ii) filtering data from the monitoring for noteworthy events . . . (iii) alerting human beings to any such noteworthy events, and (iv) providing for a response by human beings to any such alert.” EX1001, 15:62-67. Nonetheless, to the extent Patent Owner argues that monitoring for objectionable, illegal material is not expressly “security monitoring,” a POSA would have been motivated to also block other security-implicating content, such as network attacks, from reaching a user. EX1003, ¶118. For example, a POSA would have recognized that data transmissions from unknown or questionable sources can carry viruses or malware, as noted, for example, by Chu. *See, e.g.*, EX1005, 23 (noting that content from the Internet may “contain a virus

that would erase [the user's] hard drive" or "secretly collect information from [the user's] computer"); EX1003, ¶118.

Duvall's filtering system monitors for questionable content that should be blocked. *See* EX1004, 3:33-37, 5:8-15, 6:10-42; EX1003, ¶119. In addition, a POSA would have been motivated to block content that may have carried viruses or malware. EX1003, ¶119. Indeed, 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. *See, e.g.*, EX1004, 6:10-27; EX1003, ¶119.

Duvall's "filtering system can be provided from a server 30 [(i.e., "a probe")].” EX1004, 8:18-21; *see also id.*, 1:60-64, FIG. 1 (reproduced below).

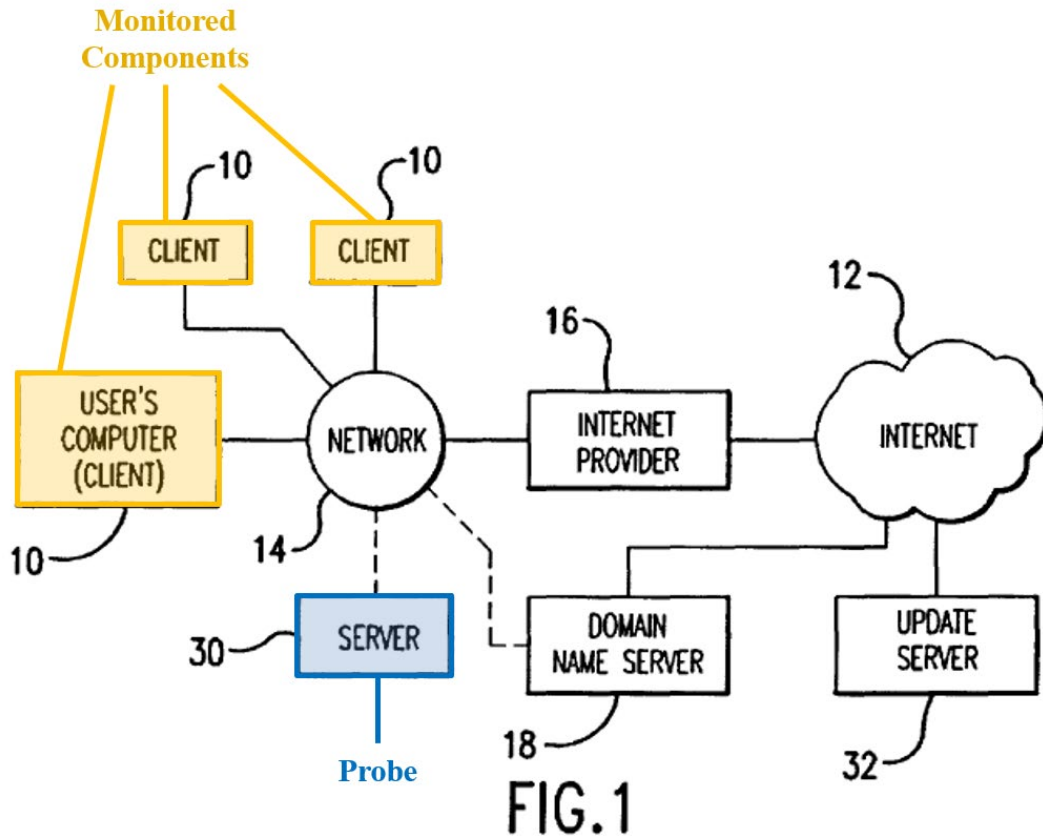


EX1004, FIG. 1 (annotated).

Duvall's server 30 is "*a probe*." As noted in Section V.E, the district court construed a "*probe*" as "a component that collects data from one or more network components to which it is attached, filters or otherwise analyzes the data that has been collected, transmits noteworthy information, and receives feedback in order to update its capabilities of analysis." EX1013, 2. Duvall's server 30 collects and analyzes data from other network components to which it is attached, such as clients 10, as illustrated in Figure 1 and as discussed further for [1A]. Duvall explains, "[s]uch a topology may be [] desirable, for example, in a corporate network that has a limited size and a uniform set of filters for many users." EX1004, 8:21-23. Duvall also discloses that its filtering system may be part of a firewall—*i.e.*, it collects data from the firewall. EX1004, 1:59-64. Accordingly, Duvall discloses the preamble. EX1003, ¶¶119-20.

(b) [1A] "a sensor..."

Duvall's server 30 analyzes data received from clients 10, which reside on the same network (*i.e.*, "*at least one monitored component of said network*").



EX1004, FIG. 1 (annotated).

Specifically, Duvall discloses, “[a] user uses a computer which serves as a client 10 to communicate with other computers over Internet 12.” EX1004, 2:35-37. “Messages are transmitted over the Internet among computers with a transport protocol known as Transmission Control Protocol/Internet Protocol (TCP/IP).” *Id.*, 2:42-44. Duvall discloses, “[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.**” *Id.*, 4:22-27. And Duvall’s “filtering system can be provided

from a server 30 that is on the client's own network." *Id.*, 8:18-21. Thus, Duvall discloses "*collect[ing] ... data from at least one monitored component of said network,*" e.g., information from data streams communicated to and from client computers 10. *Id.*, 4:22-27; EX1003, ¶¶121-22. A POSA would have understood that Duvall's server 30 is "*a sensor coupled to collect ... data from at least one monitored component of [said] network*" because it collects data that is being transmitted or received, e.g., "[w]hen a message is transmitted." EX1004, 4:22-27; EX1003, ¶122.

The information received by Duvall's filtering system is "*status data.*" As noted in Section V.E, the district court construed "*status data*" as "data extracted from or generated about the traffic or system processing it that is informative as to the status of the network and its components." EX1013, 1. Duvall explains that information about the data stream can include "a particular port and IP address" with which a client is attempting to communicate, as well as protocol information, URLs, and associated commands (e.g., an HTTP "GET command"). EX1004, 4:39-42, 5:66-6:27. This information is "data extracted from . . . the traffic or system processing it." EX1013, 1; EX1003, ¶123. And it "is informative as to the status of the network and its components" because it is informative as to the activity of clients 10, the type, protocol, destination, domains, and content of requests and responses flowing through the network, and the entities with which clients 10 are

communicating. EX1003, ¶123. Indeed, the district court found the same data as disclosed in Duvall to be “*status data*,” explaining that the “items listed in Table 6 [of the ’237 patent], including **an IP address**, are examples of ‘status data.’”

EX1034, 13 n.47; *see also* EX1035, 13; EX1003, ¶124.

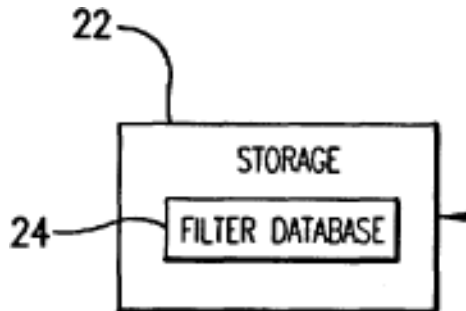
(c) [1B] “a filtering subsystem...”

(i) Duvall discloses “a filtering subsystem coupled to analyze status data..., wherein the analysis includes filtering.”

Duvall discloses “*a filtering subsystem*” residing on its server 30: “Referring again to FIG. 1, ... the filtering system can be provided from a server 30 that is on the client’s own network 40.” EX1004, 8:18-21. Duvall discloses that its filtering system “*analyz[es] status data*,” and that this “*analysis includes filtering*.” EX1003, ¶125. Specifically, Duvall uses “direct action” filters, which “indicate that the system should unconditionally allow or unconditionally block [a] transmission.” EX1004, 4:12-21, 5:8-29; EX1003, ¶125.

For example, Duvall discloses filtering based on IP address (i.e., “*status data*”) and other information: “When 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.” EX1004, 4:22-27. Duvall’s “filter database” is illustrated in Figure 2 and “is located on server 30” in Duvall’s server-based embodiment. *Id.*, 8:18-26, FIG. 2.



EX1004, FIG. 2 (excerpt).

Duvall explains, “[t]he filter database has lists of filters, some of which are identified as either ALLOW filters or BLOCK filters for respectively allowing or blocking transmission.” EX1004, 3:64-66. “Each 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.*, 4:12-15. Duvall explains, “[t]he filters 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.*, 4:27-30; EX1003, ¶¶126-27.

As described for Figure 3, Duvall’s “filtering” determines whether to allow or block data transmissions: “The filtering system detects when the client opens the data stream for a particular port and IP address (step 100), and searches the filter database for matching filters.” EX1004, 4:37-42; EX1003, ¶128. Matching filters

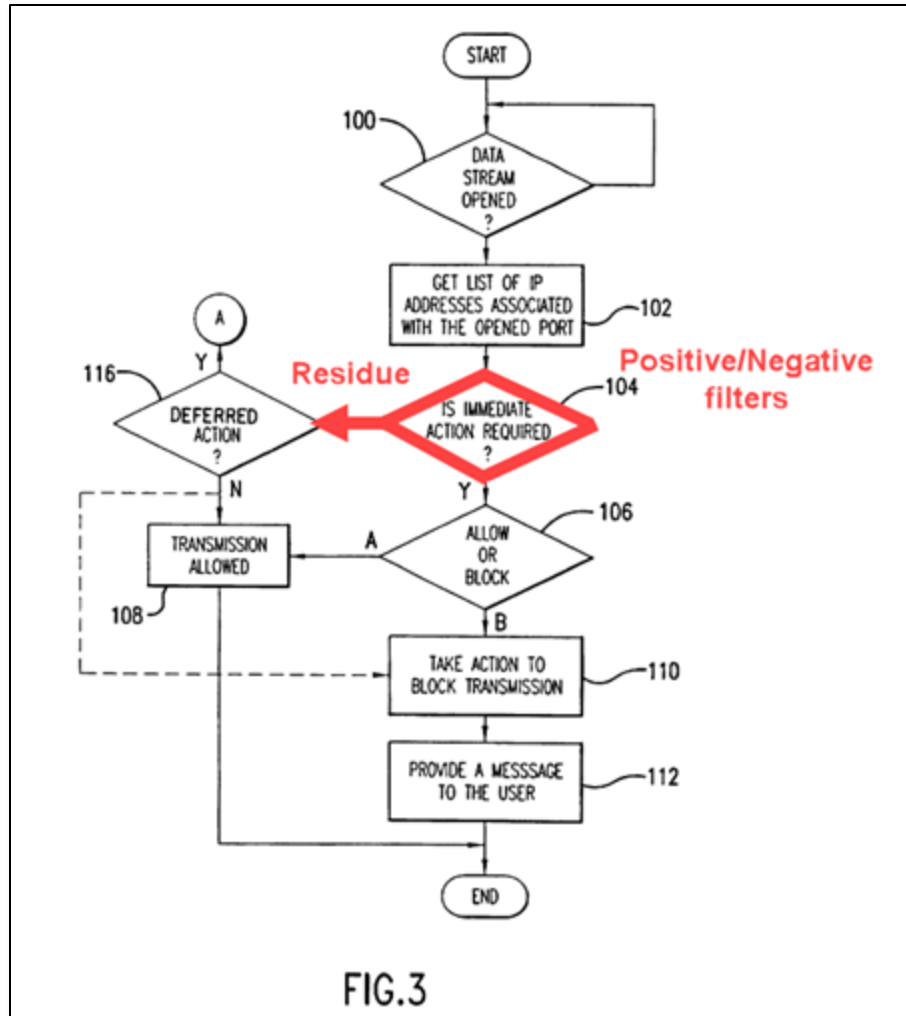
are retrieved, for example, by comparing the port and IP address of the data transmission, and “[t]he retrieved filters are checked to determine if any require immediate action, i.e., if unconditional allowing or blocking is required (steps 104, 106).” EX1004, 4:42-49. If so, and the action specified by the matching filter “is to allow the transmission, the system allows the transmission to proceed normally (step 108).” *Id.*, 4:49-51. If the action “is to block the transmission, the system takes action to block the transmission (step 110).” *Id.*, 4:51-54. Duvall’s operation is consistent with Patent Owner’s application of the claims in district court, accusing “filtering based on an IP address” to decide whether to “allow or block traffic.” EX1035, ¶¶50-53.

(ii) Duvall discloses “an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering.”

The plain language of this element does not require any data to be “discarded” or “selected by filtering”—only that the “*post-filtering residue is data neither discarded nor selected by filtering.*” EX1001, Claim 1; EX1003, ¶129. The parties in the BT-Fortinet litigation (which did not include Petitioner) agreed that “*post-filtering residue, wherein the [post-filtering] residue is data neither discarded nor selected by filtering*” 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.” EX1013, 4. Under either this construction

or the claim's plain language, Duvall teaches "*an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering.*" EX1003, ¶129.

Duvall's filtering system results in data that is (i) allowed, (ii) blocked, and (iii) neither allowed nor blocked. Specifically, Duvall discloses ALLOW filters and BLOCK filters, which Duvall explains may be sequentially implemented "so that the system searches ALLOW filters first [and] BLOCK filters next" EX1004, 4:27-30. These filters are illustrated in Duvall's Figure 3 (reproduced and annotated below) and explained more below. EX1003, ¶130.



EX1004, FIG. 3 (annotated).

Referring to Figure 3 above, Duvall's system, at step 104, "checks for and retrieves any filters that match the particular IP address. The retrieved filters are checked to determine if any require immediate action, i.e., if unconditional allowing or blocking is required (steps 104, 106)." EX1004, 4:46-50. If immediate action is required, one of two things happens:

- If the data is allowed, "the system allows the transmission to proceed normally (step 108)." *Id.*, 4:50-52.

- If the data is blocked, then “the system takes action to block the transmission (step 110).” *Id.*, 4:52-54.

This data allowing and blocking comprises “positive filtering” and “negative filtering” consistent with the BT-Fortinet litigants’ agreed-upon construction. EX1003, ¶¶130-33.

If immediate action is not required (i.e., data is neither blocked nor allowed at block 104 (i.e., the data is residue data)), the data is passed for further analysis. This residue data is 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.” EX1003, ¶134.

This “post-filtering residue” is subject to analysis by Duvall’s deferred action filters. EX1004, 4:27-30 (“The filters are preferably stored so that the system searches ALLOW filters first, BLOCK filters next, and deferred action filters last, and takes action based on the first matched filter.”); 4:65-5:7. This post-filtering residue analysis includes keyword and pattern matching, as depicted in FIG. 4. *Id.* at 5:8-29; EX1003, ¶135.

Analysis loop for post-filter residue data

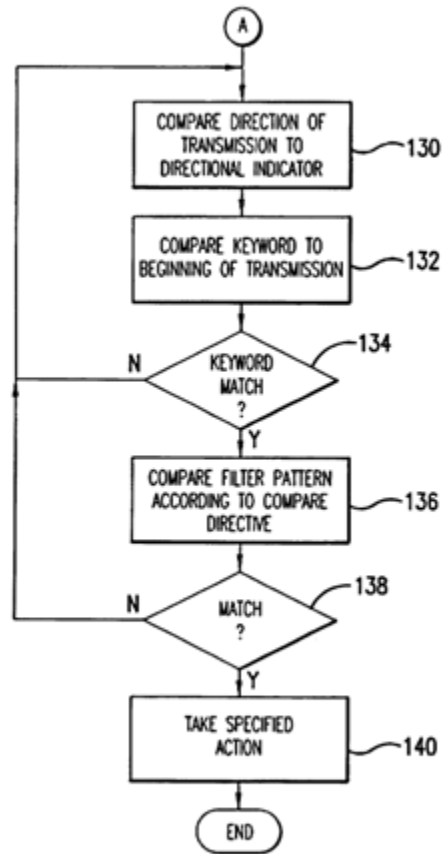


FIG.4

EX1004, FIG. 4 (annotated).

Therefore, Duvall discloses the “*post-filtering residue*” elements of claim 1.

EX1003, ¶¶129-136.

- (iii) Duvall’s analysis is to “identify potentially security-related events represented in the status data.”

Duvall’s filtering ensures that content implicating security concerns does not reach recipients. EX1004, 1:7-24; EX1003, ¶137. As discussed for [1-pre], data

blocked by Duvall's filtering system, as well as those not matching any filters, are "*potentially security-related events represented in the status data*" because they may relate to requests for, or transmissions of, "indecent material," which may be illegal (e.g., "outlaw[ed]") and/or threaten the security of the requesting user or client device. EX1004, 1:7-24; *see also id.*, 4:61-64 ("[A]dvis[ing] the user on how to get back to the state before the user tried to open the stream and send the message."); EX1005, 23; Section VI.A.2(a); EX1003, ¶137. Thus, Duvall performs analysis to identify these "*potentially security-related events*" through the additional analysis of residue data, as discussed in Section VI.A.2(c)(ii).

To the extent Patent Owner argues that identification of illegal or indecent material in a data transmission is not a "*potentially security-related event[]*" (which it is), it still would have been obvious to apply Duvall's and Chu's techniques to filter and identify data representing "*potentially security-related events*." EX1003, ¶138. This is suggested, for example, by Chu's blacklists, which contain lists of "Web sites that serve potentially dangerous active codes." EX1005, 44; *see also id.*, 23 (discussing virus-ridden downloadable content). And, as Dr. Jeffay explains, Duvall's and Chu's filtering techniques apply equally well in other security contexts, such as malware or intrusion detection, without needing any modifications. EX1003, ¶138. Filters would include, for example, IP addresses or other criteria (e.g., URLs) associated with malware or potentially security-related

content. *Id.* Applying Duvall’s techniques in this manner amounts to nothing more than use of known techniques to improve similar devices, methods, or products in the same way (e.g., to detect malware or a potential intrusion instead of objectionable material). *Id.*; *KSR*, 550 U.S. at 417.

(d) [1C] “a communications system...”

Duvall at Figure 4 acknowledges that, in some cases, its *post-filtering residue* analysis may not keyword match the data at step 134 or pattern match the data at step 138. EX1004, FIG. 4. In such case, Duvall discloses taking a default block or allow action but recognizes that default blocking or allowing could result in “filtering too much or too little.” EX1004, 8:6-8; Section VI.A.1; EX1003, ¶140.

To avoid this pitfall, a POSA would have been led to search for and locate Chu to optimize the handling of such residue data. Section VI.A.1; EX1003, ¶141. In the case of residue data, Chu prompts for human intervention, as illustrated in the following highlighted excerpt from Chu. EX1003, ¶141.

Profiles-0.92 is capable of taking the policy a step further by returning *unknown* if the requested URL is neither in the blacklist nor in the whitelist (sites know to be trustworthy):

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.

Profiles-0.92

```
(threshold-and
  2
  (not (url-match URL ("http://www.harvard.edu"
                      "http://www.caltech.edu"))))
  (url-match URL ("http://web.mit.edu"))
  unknown)
```

The blacklist and whitelist ensure good automation of the trust decision process if the lists are reasonably complete. User intervention is needed only when the given URL is in neither the blacklist nor the whitelist.

EX1005, 44 (annotated).

In the Duvall-Chu combination, the human intervention would take the form of an analyst system having people trained to manage Duvall's corporate network. Specifically, Duvall discloses that its system is appropriate for a server-based system in, for example, "a corporate network that has limited sized and a *uniform set of filters for many users*." EX1004, 8:18-23. Because a corporate environment requires a "uniform set of filters," the decision of how to handle unresolved data would not be left to each user individually, but rather, to a group of people trained in making such decisions, such as analysts at a network-security service. EX1003, ¶142. Indeed, Duvall discloses that its "editing manager" is "password protected," indicating that the persons editing filters in a corporate network are trained professionals. EX1004, 8:8-10; EX1003, ¶142. Thus, in the Duvall-Chu

combination, information about the residue data would be sent to an analyst system having trained professionals for handling the unresolved residue data.

A POSA would have been motivated, with a reasonable expectation of success, to incorporate into Duvall's system Chu's sending data to an analyst system for feedback because, as Duvall itself recognizes, Duvall's residue analysis may result in a default allow/block, causing the system to filter too much or too little. EX1004, 8:3-10 (Duvall's "editing Manager" "allows the user to make custom changes [to the filters] if the user believes that the filtering system is filtering too much or too little."); Section VI.A.1; EX1003, ¶143. A POSA would have understood that, in the corporate context of Duvall, the "user" of Duvall's "editing manager" would be a trained professional associated with the corporate network and filtering system, not the user trying to access the illicit content—particularly because Duvall teaches that in the corporate context the filters are uniform across the users. EX1003, ¶143; EX1004, 8:18-23. This group of trained professionals responsible for maintaining uniformity of the filters is "*an analyst system ... associated with said security monitoring system,*" as required by the claim. EX1003, ¶143; EX1004, 8:18-23. Moreover, a POSA would have been motivated to assign the role of managing and editing filters to a group of people having the expertise to properly evaluate whether "the filtering system is filtering

too much or too little,” rather than the individual receiving the illicit content.

EX1004, 8:6-8; EX1003, ¶144.

(e) [1D] “a receiver...”

As discussed for [1C], in the Duvall-Chu combination, information about residue data is sent to an analyst for handling. Duvall-Chu discloses feedback in the form of an “editing Manager” that allows “edit[ing] the database to add, delete, or modify filters in the database.” EX1004, 8:2-5. A POSA would recognize that Duvall’s editing manager thus provides “*a receiver for receiving feedback . . . based on empirically-derived information reflecting operation of said security monitoring system*” because the information is only provided to the trained professional if the data is residue data—meaning that the data did not match any allow/block filters and passed through subsequent analysis (*e.g.*, keywords and pattern matching) without any resolution. *Id.*, 5:8-18, EX1003, ¶¶146-147. Thus, decisions made by the trained professional (*e.g.*, whether the filters should be modified) would be based on observable information about the data (*e.g.*, transmission path, URL, etc.). EX1003, ¶147. Feedback is received “*at the probe*” because Duvall’s editing manager is part of the filtering system implemented on server 30. *See* EX1004, 8:2-5, 8:18-21; EX1003, ¶148.

(f) [1E] “a modification control system...”

As discussed for [1D], the Duvall-Chu combination discloses “*receiving feedback*” from an analyst via Duvall’s “editing Manager,” which “allows the user to edit the database to add, delete, or modify filters in the database.” Section VI.A.2(e); EX1004, 8:2-5; EX1003, ¶149. 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.” EX1004, 4:22-27; *see also id.*, 4:27-30, 4:40-43. That is, Duvall’s system searches filters in the database when determining whether to allow or block a data transmission. EX1003, ¶150. As filters are added, deleted, or modified, Duvall’s analysis would reflect these updates. EX1004, 8:3-16; EX1003, ¶150.

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.” EX1004, 7:18-21; 2:16-18. Given the rapidity of updates, a POSA 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. EX1003, ¶151. To avoid this disadvantage, Duvall “provid[es] updates online” so

that “the system can adapt as new sites and servers are added to the Internet.”

EX1004, 2:16-18.

Duvall’s filtering system accommodates dynamic updates because it searches “filter entries stored in the database” when performing its analysis, EX1004, 4:22-30, which would reflect changes to filters as they are edited. *Id.*, 4:22-43, 8:3-16; EX1003, ¶152. A main benefit of databases is that entries can be edited or added without taking the system offline, which prevents the filtering system from being down during updates. EX1003, ¶153. Since Duvall’s system “searches the filter database for matching filters” when opening a new data stream, the “*analysis capability of said probe*” always reflects the latest and current set of filters. EX1004, 4:40-43; EX1003, ¶153.

3. Claim 2

As discussed for [1B], Duvall performs “*a multi-stage analysis of the status data.*” Section VI.A.2(c); EX1003, ¶156. For example, Duvall searches filters in multiple stages: “The filters are preferably stored so that the system searches ALLOW filters first, BLOCK filters next, and deferred action filters last...”

EX1004, 4:27-30. Duvall evaluates status data in multiple stages, first “determin[ing] if any require immediate action,” and then “determin[ing] whether a deferred action must be taken with respect to any of the retrieved filter[s].” *Id.*, 4:38-50, 4:65-5:1, 5:8-29 (discussing additional analysis performed for deferred

actions); EX1003, ¶156. Duvall's Figure 4 shows an iterative analysis of residue transmission data, providing "*a multi-stage analysis of the status data.*" EX1003, ¶157. Moreover, Duvall in view of Chu teaches an additional analysis stage involving a user (e.g., trained professional) to further evaluate residue data transmissions. *Id.*; Section VI.A.2(c); EX1005, 44.

4. Claim 3

The '641 patent explains, "[n]egative filtering, positive filtering, and residue analysis are examples of data discrimination analyses, other types of which are well-known to those skilled in the art." EX1001, 8:62-65. Thus, "*discrimination analysis*" is merely analysis that differentiates certain data from other data. EX1003, ¶160. The Duvall-Chu combination teaches such analysis.

As discussed for [1B], the filtering system of the Duvall-Chu combination differentiates between data that should be allowed through the network and data that should be blocked. *See* Section VI.A.2(c). This is consistent with the '641 patent's description of "*discrimination analysis*," which explains that "[n]egative filtering, positive filtering, and residue analysis are examples of data discrimination analyses, other types of which are well-known to those skilled in the art." EX1001, 8:57-59; EX1003, ¶161. And the purpose of the '641 patent's "negative filtering" and "positive filtering" is to determine whether to select or discard certain data. *See* EX1001, 8:45-50; EX1003, ¶161.

The Duvall-Chu combination performs negative filtering, positive filtering, and residue analysis, as described for [1B]. Section VI.A.2(c); EX1003, ¶162. For example, Duvall's "ALLOW" and "BLOCK" filters are used, respectively, to select data to allow through the network and discard data that the system determines to block, preventing the data from passing through the network. EX1004, 3:64-66, 4:12-15, 4:27-30, 4:50-55; EX1003, ¶162. And Chu similarly discloses negative filtering, positive filtering, and residue analysis in the form of a "blacklist," "whitelist," and user intervention for "unknown" data not meeting either list. EX1005, 44; EX1003, ¶162.

5. Claim 4

The Duvall-Chu combination renders obvious claim 4 for the reasons discussed for claim 3. EX1003, ¶165.

6. Claim 5

The Duvall-Chu combination renders obvious claim 5 for the reasons discussed for claim 3. EX1003, ¶167.

7. Claim 6

As discussed for claim 2, Duvall's "*multi-stage analysis includes analysis at the probe and at a secure operations center,*" including evaluating status data in multiple stages. Section VI.A.5; EX1004, 4:27-30, 4:39-49, 4:65-5:1, 5:8-29; EX1003, ¶169. The Duvall-Chu combination teaches analysis at a probe followed by analysis at an analyst system. *See* Sections VI.A.2(c) (at the probe), VI.A.2(d)

(by a group of people at an analyst system); EX1005, 44; EX1003, ¶169. As discussed further below, a POSA would have understood the analyst system could be on-site or at a secure remote site, i.e., “*a secure operations center configured to receive data from the probe.*” EX1003, ¶¶169-170; *see also* EX1037, 277 (“Instead of staffing your own team of security experts, you can use IBM’s strength in this area. A network operations center is staffed 7 X 24, and a specific expert is assigned to your account. When an event is detected, IBM’s security experts notify you and help you respond to the event. Up-front planning and response policy design also are available.”).

Specifically, Duvall discloses that its filtering system can “be incorporated into a firewall [or] gateway.” EX1004, 1:60-64. A POSA would have recognized that accessing a firewall or gateway can be, and most typically is, accessed remotely, e.g., from a separate “network operations center.” EX1003, ¶171 (citing EX1037, 277). Further Duvall discloses that the filtering system is accessed through an “editing manager” that is “preferably password protected.” EX1004, 8:2-9, 8:21-23. Thus, Duvall recognizes the need for security and a POSA would have recognized that the security analyst system would likewise be secure, including communications between the analyst system and the firewall (e.g., through HTTPS, SSL, TLS, etc.). EX1003, ¶171.

Moreover, it was common in the industry at the time to provide off-site security (*e.g.* hosted by a third party). EX1003, ¶172, *see also, e.g.*, EX1037, 277. Indeed, Duvall discloses off-site operations where the “updating mechanism in the filtering system can locate a particular HTTP or FTP update server 32 over the Internet [T]he updating mechanism causes the filtering system to download from the update server . . . filters.” EX1004, 7:21-29. Customers of Duvall’s system are “given an opportunity to obtain a subscription . . . to obtain further [filter] updates.” *Id.*, 7:35-40. Thus, a POSA would have recognized that the trained professionals need not be located at the corporate firewall, but can be located remotely (possibly as a third party subscription service), in their “*secure operations center*” such as a network operations center (“NOC”). EX1003, ¶172. Accordingly, an analyst system would receive residue data, evaluate that data, update the respective filters, and provide those updates to the corporation per the terms of the subscription. EX1003, ¶172.

Further, a POSA would have been motivated to ensure that the trained professionals managing Duvall’s filtering system were doing so as part of a “*secure operations center*.” *Id.*, ¶173. This would ensure unauthorized users could not edit, add, or remove filters that could allow malicious traffic into the corporate network. *Id.*

8. Claim 7

As discussed for [1A], Duvall's IP addresses comprise "*status data*." Duvall also explains that, in the server environment, there may not be "ready access to the Internet's domain name services." EX1004, 8:28-33. So Duvall discloses a "domain name table" for "rapidly converting a domain name into . . . an IP address." *Id.* The "domain name table" includes a list of 32-bit values (IP addresses) that each correspond to a domain name. *Id.*, 8:34-38. "This list is searched associatively for an entry which matches the domain name being looked up." *Id.*, 8:36-37.

Duvall's "domain name table" at the server ("*probe*") aggregates the IP addresses ("*status data*") by collecting these IP addresses in a list. EX1003, ¶175. And Duvall's "domain name table" at the server ("*probe*") synthesizes the IP addresses ("*status data*") by making this list associatively searchable. *Id.*, ¶175.

9. Claim 15

As explained for [1E], Duvall's filtering system always searches the latest and current set of filters when performing its filtering analysis. Section VI.A.2(f); EX1004, 4:22-43, 8:3-16; EX1003, ¶177. Thus, when filters are updated in Duvall's system, the analysis is "*instantaneously self-tun[ed]*" because Duvall is

programmed to use the updated filters in subsequent analysis.⁷ EX1003, ¶177.

Additionally, as discussed for [1B]-[1D], the “*self-tuning*” in the Duvall-Chu combined system is “*based on previously collected status data*” because filter edits are based on the user’s analysis of previously collected information associated with potentially security-related events. *See* Sections VI.A.2(c)-(e); EX1003, ¶177.

10. Claim 16

As discussed for [1D], the Duvall-Chu combination teaches “*receiving feedback*” in the form of “an editing Manager that allows the user to edit the database to add, delete, or modify filters in the database.” Section VI.A.2(e); EX1004, 8:3-6; EX1003, ¶180. Duvall further discloses the “editing Manager” “allows the user to make custom changes if the user believes that the filtering system is filtering too much or too little.” EX1004, 8:3-8. Thus, a POSA would have understood that the Duvall-Chu combination prompts a user—such as trained professionals—to consider past network activity (i.e., “*non-real-time information*”)

⁷ As Dr. Jeffay explains, although software can perform operations quickly, these operations cannot literally be “*instantaneous*” because the software must execute some instruction or a series of instructions to perform an operation. EX1003, ¶177. The claims therefore must encompass a timeframe reasonable for software to perform the recited “*self-tuning*” operation. *Id.*

to determine how to edit the filters, and that activity is part of “*ongoing security research efforts*” because the activity analyzed by the user includes “*potentially security-related events*.” See Sections VI.A.2(c), (e); EX1003, ¶180.

11. Claim 17

As discussed for [1C] and [1D], the Duvall-Chu combination discloses prompting a user when a data transmission does not match any of Duvall’s filter criteria, and receiving feedback through Duvall’s editing manager. Sections VI.A.2(d), (e); EX1003, ¶182. Chu teaches these prompts are received in real time to ensure untrusted content is not downloaded. EX1005, 44; EX1003, ¶182. And a POSA would have recognized that Chu’s user would respond to the prompt “*in substantially real time*” to ensure the system knew whether to block or allow the requested download. EX1003, ¶182. Similarly, a POSA would have been motivated to respond to a prompt regarding unknown data in Duvall’s system “*in substantially real time*” to ensure the filtering system does not continue to improperly block or allow data. *Id.* Duvall itself suggests providing feedback “*in substantially real time*,” teaching the benefit of ensuring the filters are accurate to avoid “the filtering system [] filtering too much or too little.” EX1004, 8:5-7. And Duvall further provides mechanisms for alerting users of events of interest in real time, such as “provid[ing] a screen on the user’s display indicating that [a] transmission was blocked.” *Id.*, 4:61-64.

B. Ground 2: Claims 7-13 and 16 are obvious over Duvall, Chu, and Trcka.

1. A POSA would have been motivated to combine the Duvall-Chu system with Trcka.

Duvall discloses 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.” EX1004, 8:2-7. Thus, Duvall suggests that a user (e.g., trained professional) reviews network activity to ensure the filters accurately allow and block data transmissions. *Id.*; EX1003, ¶184. But neither Duvall nor Chu expressly discloses how the user performs this review. Although a POSA familiar with network security and filtering mechanisms would have understood numerous ways for performing this review, to the extent they would have needed additional guidance, Trcka provides such details. EX1003, ¶184.

Trcka is directed to “[a] network ... 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.” EX1014, Abstract; EX1003, ¶¶84-88. Trcka’s system includes “[a] set of analysis applications and other software routines allow[ing] 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.” EX1014, Abstract; *see also id.*, ¶15, ¶16 (“The

analysis applications can [] be used to view, analyze and process traffic data.”), ¶53.

Trcka further provides a “graphical user interface (GUI)” through which “the user can launch and control the various analysis applications.” *Id.*, ¶79; EX1003, ¶185.

A POSA would have been motivated to incorporate Trcka’s techniques for recording and viewing past network activity in Duvall-Chu’s system to enable the user to analyze whether “the filtering system is filtering too much or too little.” EX1004, 8:5-7; EX1003, ¶186. Duvall already suggests that the user, such as trained professionals, should have access to past network activity to accurately update filters, EX1004, 8:2-7, and Trcka’s analysis applications would enable the user to interact with such information as part of the user’s analysis. EX1003, ¶186. Indeed, Duvall performs filtering based on data contained in network packets, such as “port number and IP address,” EX1004, 3:64-4:55, and Trcka captures and presents packet-level data, including “headers of all packets transferred over the network,” EX1014, ¶¶38-39. Duvall and Trcka thus operate upon similar traffic data, ensuring that Trcka’s analysis techniques would apply equally well to the data in Duvall-Chu’s system. EX1003, ¶186.

A POSA would have had a reasonable expectation of success implementing Trcka’s analysis techniques, which would amount to nothing more than combining prior-art elements (i.e., Duvall-Chu’s filtering system and editing manager with Trcka’s data-analysis applications) according to known methods to yield predictable

results. EX1003, ¶187; *KSR*, 550 U.S. at 417. Duvall discloses processing and storage mechanisms, such as those implemented on server 30, as well as a “display” from which the user can view information. EX1004, 3:42-46, 4:61-64, 8:18-26; EX1003, ¶187. Thus, a POSA would encounter no technical hurdles implementing applications for interacting with past network activity, as in Trcka, in the system of Duvall-Chu. EX1003, ¶¶187-188.

2. Claims 7, 8 and 12

Trcka discloses both “*aggregating and synthesizing the status data at the probe*” and “*cross-correlating data*” across different monitored devices. For example, Trcka’s “Audit” and “Problem Determination” applications correlate “*the status data*” and other data from different devices to “particular types of network problems” occurring within a specific timeframe. EX1014, ¶¶112, 116; EX1003, ¶190. A user then views this information on screen, as illustrated in Figure 19, which correlates network activity from different devices to rejected logon attempts. EX1014, ¶¶142-43, FIG. 19; EX1003, ¶190. As shown in the figure below, the collected “*status data*” is displayed in aggregate, and in a meaningful, synthesized format.

ACTIVITY **REJECTED LOGONS**

PERIOD DATE, FROM: 10/23/96 START TIME: 1:00 AM

TO: 10/23/96 END TIME: 8:30 PM

TIME	DATE	CHNL	ADDR	DST ADDR	USER ID
08:31 AM	10/23	E03	023456	345892	BOB
08:35 AM	10/23	E03	458962	536536	KTF
08:40 AM	10/23	D12	023456	345892	BOB
08:42 AM	10/23	D10	345892	023456	JENNY
08:45 AM	10/23	E03	023456	345892	BOB
08:48 AM	10/23	E03	023456	345892	BOB
09:01 AM	10/23	E02	456901	873456	MARY
09:05 AM	10/23	D06	876456	456901	FRANK
09:10 AM	10/23	D03	637899	369304	JACK
09:15 AM	10/23	E03	023456	345892	BOB
09:18 AM	10/23	D03	637899	369304	JACK

OPTIONAL ZOOM IN DATA **FILTER** **SEARCH** ...more

FIG. 19

EX1014, FIG. 19.

As another example, Trcka's "Network Operating Characteristics Application" "cross-correlat[es]" activity from different devices for indications of "congestion," "traffic throughput," and "network outages." EX1014, ¶¶124-25; EX1003, ¶191. Similarly, Trcka's "Network Problem Solving Application" cross-correlates activity from different devices to detect "network-level problems" such as "transmissions to nonexistent entities." EX1014, ¶¶126-27; EX1003, ¶191. Such metrics are derived by "aggregating and synthesizing" the collected "status data," generating metrics representative of the collected "status data" as a whole. EX1003, ¶191. Additionally, a POSA would have understood that Trcka's aggregation and

synthesis occurs “*at the probe*” where the data would be stored. *See* Section VI.B.1; EX1003, ¶191.

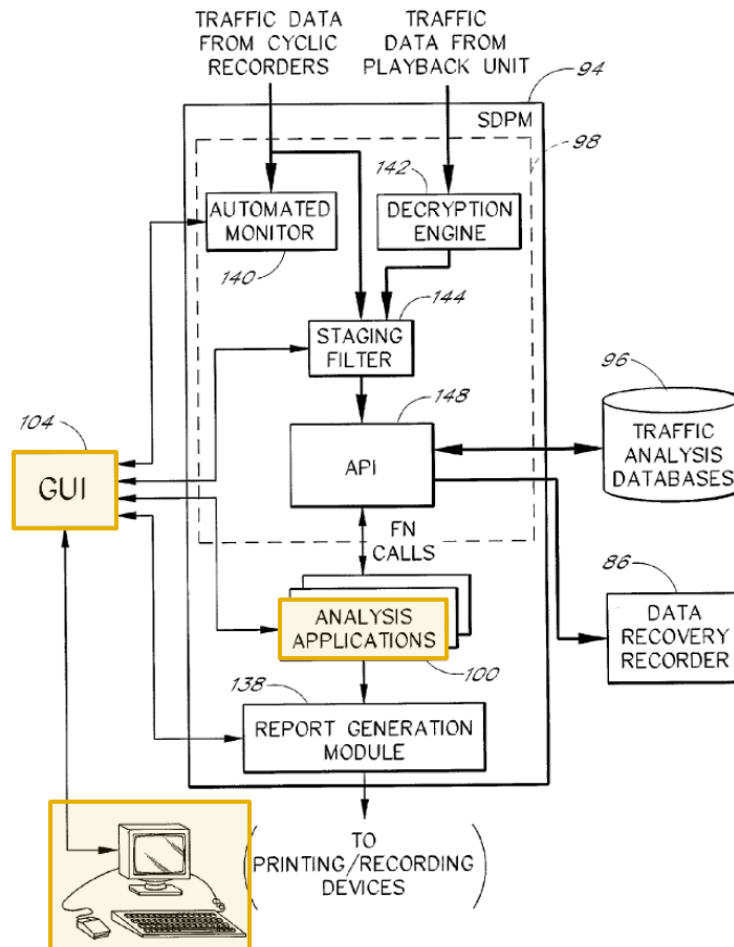
1. Claims 9 and 13

Trcka discloses “*analyzing the frequency of occurrence of*” potentially security-related events, such as “repeated unsuccessful logon attempts from an outside client” and “frequent transfers of files to outside entities.” EX1014, ¶¶122-23; EX1003, ¶194. Trcka enables the user to view the frequency of potentially security-related events in its “Audit” and “Problem Determination” applications, for example, events related to “NETWORK ERRORS,” “FILE ACTIVITY/ACCESS,” and user “TRANSACTIONS.” EX1014, ¶142; EX1003, ¶194. Using these techniques disclosed in Trcka, a POSA would have been motivated to analyze the frequency of events in Duvall’s system, such as data requests transmitted to blocked or unknown URLs, to make the user aware of such events and ensure filters can be properly updated, thus preventing the system from “filtering too much or too little.” EX1004, 8:5-7; EX1003, ¶194. And a POSA would have had a reasonable expectation of success in doing so, as discussed in Section VI.B.1; EX1003, ¶194.

2. Claim 10

As discussed for claim 6, a POSA would have understood that Duvall’s “corporate network” provides a “*secure operations center*” within which users can operate. Section VI.A.7; EX1003, ¶197. And as discussed in Section VI.B.1, Trcka

discloses “*computer-based analysis*” in the form of “analysis applications,” as shown in Figure 7. EX1014, ¶¶15, 16, 53, 79; EX1003, ¶197.



EX1014, FIG. 7 (annotated).

For reasons discussed in Section VI.B.1, a POSA would have been motivated to incorporate Trcka’s “*computer-based analysis*” techniques—recording and viewing past network activity using analysis applications, which execute on a computer—into the Duvall-Chu system to enable the user to analyze whether “the

filtering system is filtering too much or too little.” EX1004, 8:5-7; EX1014, ¶¶15, 16, 53, 79; EX1003, ¶198.

3. Claim 11

Claim 11 recites, “*wherein the computer-based analysis includes aggregating, synthesizing, and presenting alerts on an ensemble basis.*”

Trcka discloses as part of viewing past network activity, the analysis applications include a “Report Generator Module.” EX1014, ¶113. Trcka explains, “[t]he Report Generation Module [] manipulates the data to match a format pre-selected by the user” and “can then be delivered to a printer or display, or can be saved to a file.” *Id.*, ¶104. Reports in Trcka’s system can include information such as “transaction activity,” “unauthorized accesses to restricted files and databases,” “statistics on congestion, peak loads, traffic throughput, network outages, and utilization,” and “frequent transfers of files to outside entities.” *Id.*, ¶¶112, 123, 125. This report data is “*aggregate[ed]*” and “*synthesiz[ed]*” because it is data generated from raw network activity and synthesized into a meaningful format. EX1003, ¶200.

By viewing past network activity in Duvall-Chu-Trcka’s system, as discussed in Section VI.B.1, the combination discloses “*aggregating, synthesizing, and presenting alerts on an ensemble basis.*” EX1003, ¶201. For example, such techniques would allow trained network professionals to view aggregated

information regarding blocked or unknown data transmissions in a synthesized data format, alerting the trained professionals to all such activity at the same time (i.e., “*on an ensemble basis*”). EX1014, ¶104; EX1003, ¶201. And this operation is consistent with the description in the ’641 patent, which discusses a “report generation module” that generates reports of past network activity. EX1001, 8:7-31; EX1003, ¶201.

4. Claim 16

In addition to the reasons discussed in Ground 1, Trcka further discloses “*consideration of non-real-time information*” in its analysis applications—for example a user “selectively viewing and generating audit trails from the **archived** traffic data,” allowing the user to “specify such parameters as **start time/date, end time/date**, the type of event/s of interest.” EX1014, ¶112. As discussed in Section VI.B.1, a POSA would have been motivated to incorporate Trcka’s techniques for recording and viewing past network activity (i.e., “*non-real-time information*”) in Duvall-Chu’s system to enable the user to analyze whether “the filtering system is filtering too much or too little.” EX1004, 8:5-7; EX1003, ¶204.

Additionally, a POSA would have understood that the analysis of such data in Duvall-Chu-Trcka’s system is part of “*ongoing security research efforts*” because the user is researching past data to identify potential security issues that have not previously been identified. EX1003, ¶205. Again, these ongoing research

efforts enable trained professionals to determine when Duvall's "filtering system is filtering too much or too little," and to update filters accordingly. EX1004, 8:5-7; EX1003, ¶205.

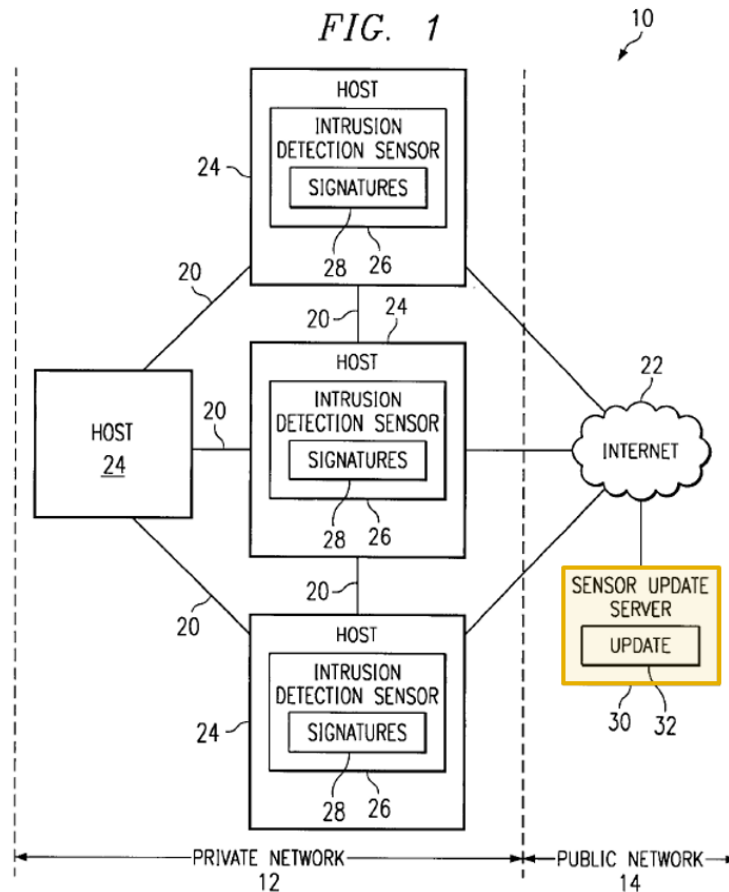
C. Ground 3: Claims 14-15 are obvious over Duvall, Chu, Trcka, and Ziese.

1. A POSA would have been motivated to combine the Duvall-Chu-Trcka system with Ziese.

Ziese is directed to "dynamically distributing updates in a network." EX1015, 1:7-9; EX1003, ¶¶89-93. Ziese explains, "[l]ike the Internet, private networks also have become common means for communicating important information," and such private networks may be distributed over "wide area networks (WANs)" that include "disparate network sites." *Id.*, 1:26-27, 2:29-36. Ziese further explains that many network security systems make use of "intrusion detection ... signatures to detect malicious activity." *Id.*, 1:46-48. However, "[b]ecause new types of attacks appear more frequently than network administrators typically check with an intrusion detection provider for new signatures, networks often remain vulnerable to new types of attacks even though new signatures are available to identify and prevent such attacks." *Id.*, 1:62-67; EX1003, ¶207.

Ziese thus discloses techniques "for 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."

EX1015, 2:2-6. For example, “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.*, 2:39-44. Such updates may be distributed from a centralized update server, as shown in Figure 1. EX1003, ¶208.



EX1015, FIG. 1 (annotated).

While Duvall discloses an “editing manager” to edit filters when “the filtering system is filtering too much or too little,” EX1004, 8:2-7, Duvall expressly

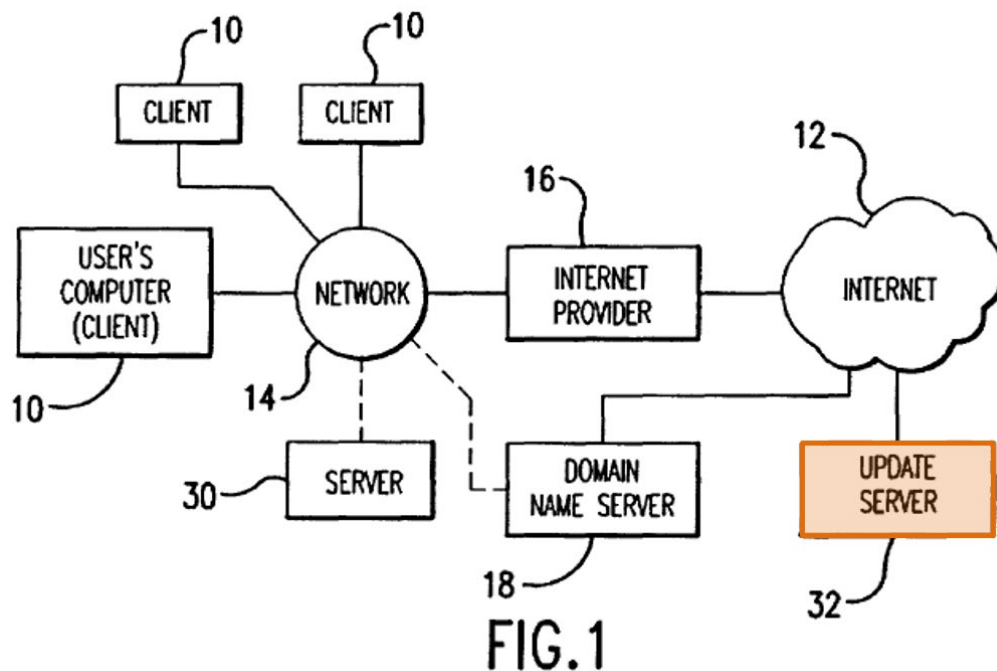
discloses only a single “server 30” on which the filtering system is running in a “corporate network,” *id.*, 8:18-26. EX1003, ¶209. But both Duvall and Ziese explain that clients may be distributed widely outside of a traditional local area network (LAN). *See* EX1004, 2:35-38 (“A number of **clients are typically linked** to a network 14, such as a local area network (LAN) **or a broad-based commercial service.**”); EX1015, 1:26-28 (“Private networks” include “wide area networks (WANs)”; 2:29-32 (“[T]he downloaded update may be **distributed to disparate network sites**”); 2:41-44; EX1003, ¶209.

In such a distributed corporate network, a POSA would have understood that Duvall’s “filtering system” would employ multiple “server[s] 30” to serve local clients within each network site, i.e., “on the client’s own network.” EX1004, 8:18-21; EX1003, ¶210. This arrangement would ensure that the filtering system applies filters to data transmissions before the transmission is allowed to enter a public network, such as the Internet. EX1003, ¶210.

Implementing Duvall’s “editing manager” on each local server, however, would require common filter updates (i.e., updates that would apply to all clients within a corporation) to be made on each individual server. EX1003, ¶211. Ziese’s techniques resolve this problem, allowing updates to be made centrally and automatically distributed to “disparate network sites.” EX1015, 2:25-46. A POSA would have thus been motivated in Duvall-Chu-Trcka’s system to allow trained

professionals for a distributed corporate network to centrally analyze and update filters, and to have the filters automatically distributed to individual network sites. EX1003, ¶211.

A POSA would have had a reasonable expectation of success incorporating Ziese's automatic update distribution techniques into Duvall-Chu-Trcka's system. EX1003, ¶212. Duvall already suggests the use of centralized updates, further disclosing (similar to Ziese) an "updating mechanism" for distributing filter updates to its filtering system "over the Internet." EX1004, 7:15-67; FIG. 1.



EX1004, FIG. 1 (annotated).

Duvall explains, "the updating mechanism causes the filtering system to download from the update server one of a number of new sets of filters, and

preferably causes some or all of the existing filters in the filter database to be replaced with the newly downloaded filters.” *Id.*, 7:25-29; *see also id.*, 7:19-22.

Therefore, incorporation of Ziese’s techniques would amount to nothing more than use of known technique (i.e., Ziese’s automatic distribution of updates) to improve similar methods or products (i.e., Duvall-Chu-Trcka’s filtering system) in the same way. EX1003, ¶212; *KSR*, 550 U.S. at 417.

2. Claim 14

As discussed above, for a distributed corporate network, a POSA would have understood that Duvall’s “filtering system” would employ multiple “server[s] 30” to serve local clients within each network site. Section VI.C.1; EX1004, 8:18-21; EX1003, ¶214. And as discussed for claims 8 and 12, the Duvall-Chu-Trcka combination discloses analyzing and correlating network activity across different devices within the network. Section VI.B.2; EX1003, ¶214. In Duvall-Chu-Trcka-Ziese’s system in which analysis of network activity is performed from a central location, a POSA would have understood that the analyzed network activity would span the multiple “server[s] 30” (i.e., “*different probes*”), and thus data would be correlated not only across monitored devices, but also across the multiple different probes. EX1003, ¶214.

3. Claim 15

Duvall in view of Chu, Trcka, and Ziese further renders claim 15 obvious. EX1003, ¶¶217-18. As discussed above, Ziese discloses techniques in which “programs are automatically updated by downloading and distributing an update in response to an automated event.” EX1015, 2:39-41; Section VI.C.1. This automated process ensures that updates are distributed when they are available, rather than waiting for a user to initiate the update. EX1015, 1:54-67; EX1003, ¶217.

By automatically distributing updates in Duvall-Chu-Trcka-Ziese’s system, for example in response to trained professionals completing a filter edit/addition, Duvall’s filtering system would “*instantaneously*” have access to the most up-to-date filters. EX1003, ¶218. And as discussed for [1E], when filters are updated in Duvall’s filtering system, the analysis is “*instantaneously self-tun[ed]*” because Duvall is programmed to use the updated filters in subsequent analysis. Section VI.A.2(f); EX1004, 4:22-43, 8:3-16; EX1003, ¶218. Additionally, as discussed for [1B]-[1D], this “*self-tuning*” is “*based on previously collected status data*” because filter edits are based on the user’s analysis of previously collected information associated with potentially security-related events. *See* Sections VI.A.2(c)-(e); EX1003, ¶218.

D. Ground 4: Claims 18-25 are obvious over Duvall, Chu, and Cogger.

1. A POSA would have been motivated to combine the Duvall with Chu and Cogger.

As discussed in section VI.A.1, a POSA would have been motivated to incorporate Chu's user intervention into Duvall's system to more accurately resolve the status of residue data transmissions to ensure transmissions are correctly blocked or allowed. EX1003, ¶220. Duvall in view of Chu, however, acknowledges that "Internet sites are being added to the Internet at a fast rate" and a corporation may not have the resources to keep its filtering up to date. EX1004, 7:16-29. A POSA, therefore, would have been motivated to use a third party that may have more expertise in identifying what data transmissions to allow and what data transmissions to block. And, a POSA would have been motivated to adapt Duvall in view of Chu to process residue data by a third party having that expertise. EX1003, ¶220.

Cogger discloses a "system and method for opening and tracking trouble tickets over the public Internet." EX1033, Cogger, Abstract. In Cogger, "customer profile information is used to prepopulate data fields in dialogs used to open a trouble ticket. Once a trouble ticket is opened, the customer workstation tracks the existing trouble tickets through a browser based graphical user interface." *Id.*

Cogger illustrates an example "trouble ticket" in Figure 8(g):

Service Inquiry

File Edit View Tools Help

Create Query Find Refresh Help Cust Service

Details for Ticket Number 9803270000014

Ticket Customer Circuit Call

287a 287b 287c 287d 283

Ticket No.: 9803270000014

Product: DATA Service:

Trouble Desc.: NEXTGEN TKT UPFRONT 992 Open Date:

MCI Priority: 1

Occurred Date (GMT): 1998-03-27 Occurred Time (GMT): 20:04

Occurred Date (Local): Occurred Time (Local):

Originating Org: WEM Service ID: MDC895410468

Code

547

547

547

547

547

547

547

OK Clone Modify Remarks Activities

FIG. 8(g)

EX1033, FIG. 8(g).

As shown above, Cogger's "trouble ticket" can include various information about a network event, for example a description, customer information, time and date of occurrence, and priority. EX1033, 20:1-15; EX1003, ¶¶221-23. And Cogger discloses that this information is customizable and "will be different for different types of tickets." EX1033, 20:13-15.

A POSA would have been motivated to incorporate Cogger's techniques for generating and transmitting trouble tickets in Duvall-Chu's system for use in prompting Cogger's network administrators to resolve residue data. EX1003, ¶224. Transmitting "trouble tickets" with sufficient information about residue data to

Cogger's network administrators would ensure that the service can appropriately evaluate and resolve such data transmissions. This would allow Cogger's network administrators to efficiently update the corporation's filter database as appropriate, adding new filters to address newly-discovered Internet sites. EX1003, ¶224.

Cogger's trouble tickets would also provide a tracking mechanism to Duvall's network administrators of each corporate network to assure residue data is resolved in a timely manner. EX1033, 2:50-3:3; EX1003, ¶224.

Moreover, Cogger discloses that its "trouble tickets" can include "[r]emarks" that "enable the customer to describe the trouble in his/her own words." EX1033, 20:50-64. Allowing the client user or network administrator in Duvall-Chu's system to include remarks regarding a residue data transmission would allow Cogger's network administrators to better diagnose whether the residue data should be allowed or blocked. EX1003, ¶225. As Dr. Jeffay explains, Cogger's networks administrators would have more expertise as Cogger describes a system intended to support many disparate customers, leading to a better database of troubleshooting solutions. *Id.*

A POSA also would have had a reasonable expectation of success incorporating Cogger's techniques into Duvall-Chu's system because this would amount to nothing more than incorporating well-known techniques (generating and transmitting tickets about network events) into Duvall-Chu's known filtering

system. *KSR*, 550 U.S. at 419-421; EX1003, ¶226. Chu, for example, already discloses alerting a user with expertise to resolve residue data. EX1004, 7:21-23, FIG. 1; EX1005, 44. Thus, a POSA would have encountered no issues generating a problem ticket for residue data for resolution by a network administrator in Cogger's system. EX1003, ¶226.

2. Independent Claim 18

(a) [18-pre] "A method..."

As discussed for [1-pre], Duvall-Chu discloses "*a security monitoring system for a . . . computer network.*" Section VI.A.2(a); EX1003, ¶228. A POSA would have been motivated to incorporate Cogger's "trouble ticket" techniques into Duvall-Chu's system to prompt a network administrator, as disclosed in Cogger, to resolve residue data transmissions. Section VI.D.1; EX1003, ¶228.

Cogger discloses "*operating a secure operations center*" in the form of a "Customer Service Management System" (CSM) that receives trouble tickets transmitted from customers. EX1033, 3:65-66; EX1003, ¶229. For example, Cogger discloses that communication between customers and the CSM is "*secure,*" providing "**secure web servers and back end services** to provide applications that establish user sessions . . . and communicate with adaptor programs to simplify the **interchange of data across the network.**" EX1033, 5:46-50; *see also id.*, 7:55-60 (Data is communicated "by establishing a **secure** TCP messaging session with one

of the DMZ network MCI Interact Web servers 24 via an Internet **secure communications path** 22 established, preferably, with a **secure sockets SSL version of HTTPS.**”); EX1003, ¶229. Therefore, the CSM receiving and resolving trouble tickets provides “*a secure operations center*” for communicating with customers. EX1003, ¶229.

In the Duvall-Chu-Cogger system, Cogger’s CSM would be implemented as part of Duvall-Chu’s network-administrator resolution pathway for receiving and analyzing tickets transmitted from subscriber networks. EX1003, ¶230; Section VI.D.1. Thus, Duvall-Chu-Cogger’s residue data-review system, like Cogger’s CSM, provides “*a secure operations center as part of a security monitoring system for a customer computer network.*” EX1003, ¶230.

Moreover, a POSA would have been motivated to ensure personnel operating Duvall-Chu-Cogger’s service were doing so securely because the service would receive network activity from private customer networks (e.g., “a corporate network”). EX1004, 8:21-23; EX1003, ¶231. Therefore, a POSA would have understood that Duvall-Chu-Cogger’s service would be operated as part of a “*secure operations center.*” EX1003, ¶231.

(b) [18A] The “creating” step

As discussed for [1B], Duvall discloses identifying a “*potentially security-related event occurring on the network, wherein the potentially security-related*

event is identified by filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is neither discarded nor selected by the filtering.”

Section VI.A.2.c; EX1003, ¶232. As discussed for [1B] and [1C], Duvall-Chu further discloses that information about the potentially security-related event is identified at the server (“*a probe*”) and transmitted to a trained professional, in accordance with the district court’s claim construction. EX1013, 1-2; EX1012; *see also* EX1034. A POSA would have understood that the transmitted information is “*an event record*” because it is information about the network event. EX1003, ¶232.

Moreover, as discussed in Section VI.D.1, a POSA would have been motivated to incorporate such information into a “trouble ticket,” as in Cogger, to efficiently and coherently provide the information to a trained professional (e.g., Cogger’s network administrators). EX1003, ¶233. The information as recorded in the trouble ticket thus also provides “*an event record*.” EX1003, ¶233.

(c) [18B] The “correlating” step

Cogger discloses that when a customer opens a new trouble ticket, customer information may be “prepopulat[ed]” to minimize the amount of required user input. EX1033, 3:36-53. Figure 8(g) of Cogger shows the “*customer information*” as part of the trouble ticket, illustrated as “customer tab 287(b).” EX1033, 20:6-13; EX1003, ¶234.

FIG. 8(g)

EX1033, FIG. 8(g) (annotated).

A POSA would have been motivated to include customer information, as in Cogger, in the ticket transmitted to Duvall-Chu-Cogger's service to inform the service of the corporate network on which the event occurred. EX1003, ¶234.

Cogger's trouble tickets include "*a symptom record.*" *Id.*, ¶235. For example, Cogger discloses, "[t]he first step in the creation of a trouble ticket is to identify the Event-Type/Call-Type," and "[t]o do that the client front end asks the customer the problem/identifier type and then [to] narrow down the problem." EX1033, 21:23-31. An example is illustrated in Cogger's Figure 8(k), which populates problem

information (e.g., “Description of Problem”) based on customizable questions and answers. *Id.*, 21:55-22:6; EX1003, ¶235.

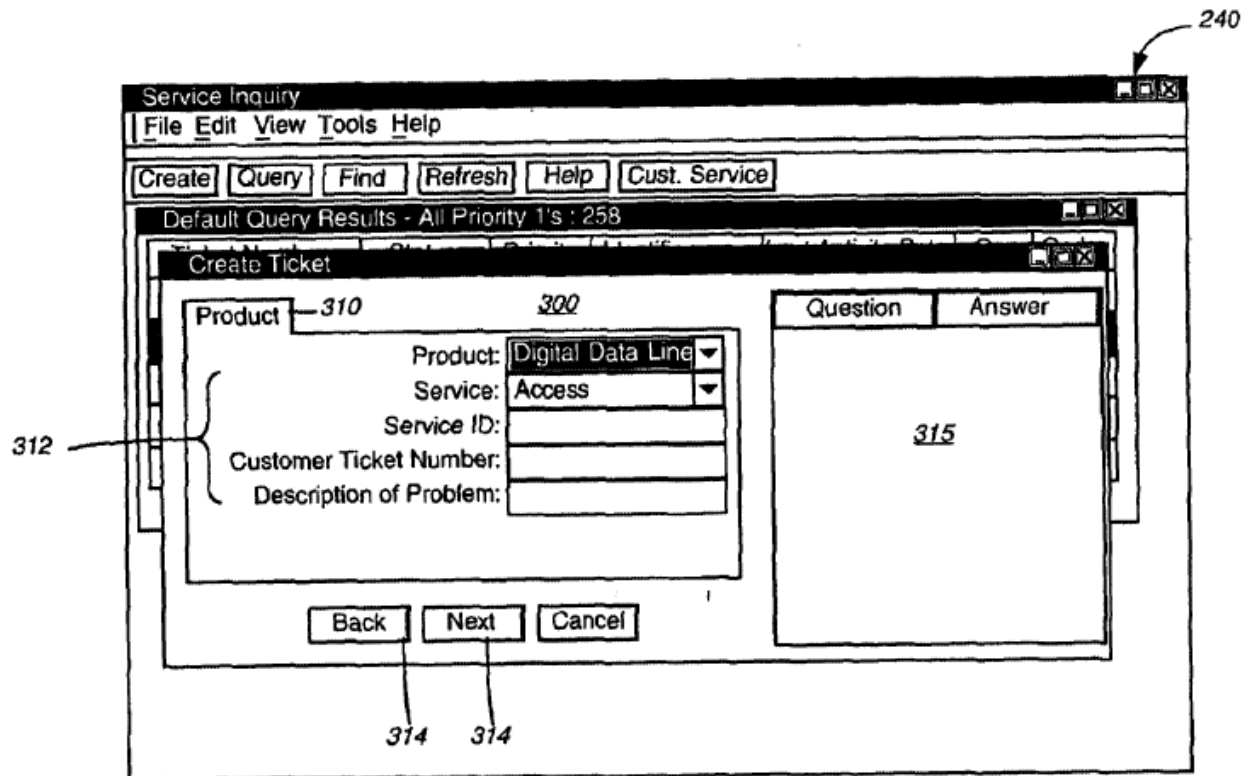


FIG. 8(k)

EX1033, FIG. 8(k).

Cogger states, “[t]he questions that need to be asked to open a ticket vary by product and problem type,” and thus a POSA would have understood that such information relates to “*symptom[s]*” of a particular problem. EX1033, 22:58-59; EX1003, ¶236. A POSA would have been motivated in Duvall-Chu-Cogger’s system to create a similar “*symptom record*” as part of the trouble ticket to relay information about the type of problem encountered. In the Duvall-Chu-Cogger system, such information related to the residue data might be communication

protocol, URL, file type, etc. EX1003, ¶236. This provides useful symptom information for use by Duvall-Chu-Cogger's service when analyzing the data. *Id.*

(d) [18C] The “using” step

Cogger discloses “*problem resolution information*”⁸ in the form of “remarks” added to a trouble ticket. EX1033, 20:33-62; EX1003, ¶238. These remarks “enable the customer to describe the trouble in his/her own words or add any comments” and “can aid in the resolution of a problem” (i.e., “*problem resolution information*”). EX1033, 20:59-62; EX1003, ¶238.

⁸ Although claim 18 recites, “*problem resolution information*,” the claims and prosecution history indicate that this phrase refers to “*problem resolution assistance information*.” EX1002, 89. In any case, the prior art teaches this element with or without the word “assistance.” *See* EX1033, 20:33-34; EX1003, ¶¶238-41.

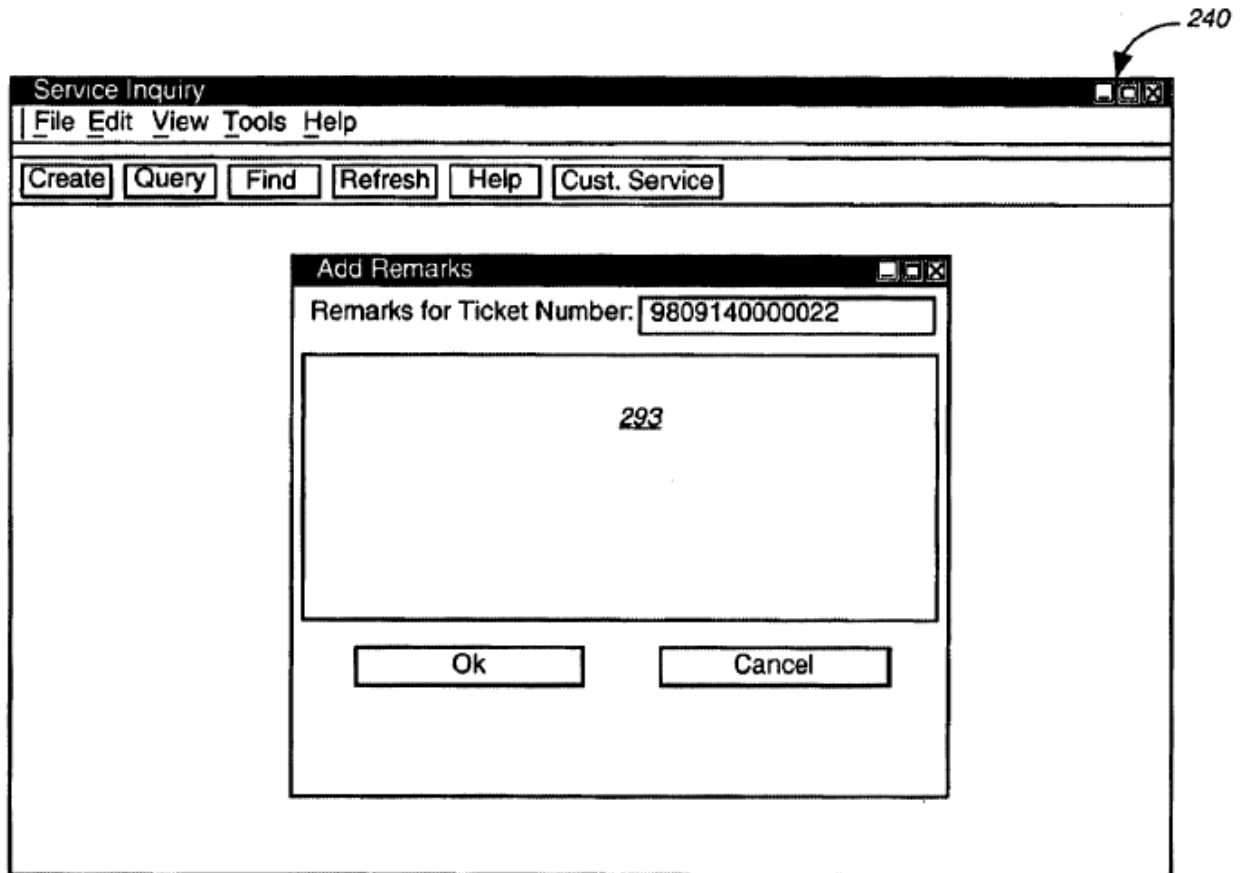


FIG. 8(i)

EX1033, FIG. 8(i).

In Duvall-Chu-Cogger's system, the remarks included in the trouble ticket would allow a client user or network administrator to add further commentary for use by the Duvall-Chu-Cogger's service in determining how to resolve the received event (i.e., whether and how filters need to be updated). EX1003, ¶239. In the Duvall-Chu-Cogger system this could include, for example, that a residue URL appears to be for a legitimate company, indicating to the network administrators that this is likely an allowable URL—*i.e.*, it “can aid in the resolution of a problem.” EX1003, ¶239.

Cogger discloses “*using the correlated symptom record to link the event record to problem resolution information*” in at least two ways. First, as discussed for [18B], creation of the “*symptom record*” is “[t]he first step in the creation of a trouble ticket” and is used to open the ticket. EX1033, 21:23-31, 21:39-47; EX1003, ¶240. Thus, because the “*symptom record*” is used to open the ticket, it allows the event information and remarks to be linked within the ticket. EX1003, ¶240. Second, Cogger discloses that the “questions and corresponding answers” associated with the “*symptom record*” “may be entered into [the] remarks section of the trouble ticket.” EX1033, 3:58-64. In this manner, the “*symptom record*” is used to create remarks (i.e., “*problem resolution information*”) that are linked to the event information within the trouble ticket. EX1003, ¶240.

(e) [18D] The “consolidating” step

As discussed for [18A]-[18C], Duvall-Chu-Cogger discloses the “*consolidating*” step through creation of a “trouble ticket.” Sections VI.D.1, VI.D.2(a)-(c); EX1003, ¶242.

(f) [18E] The “providing” step

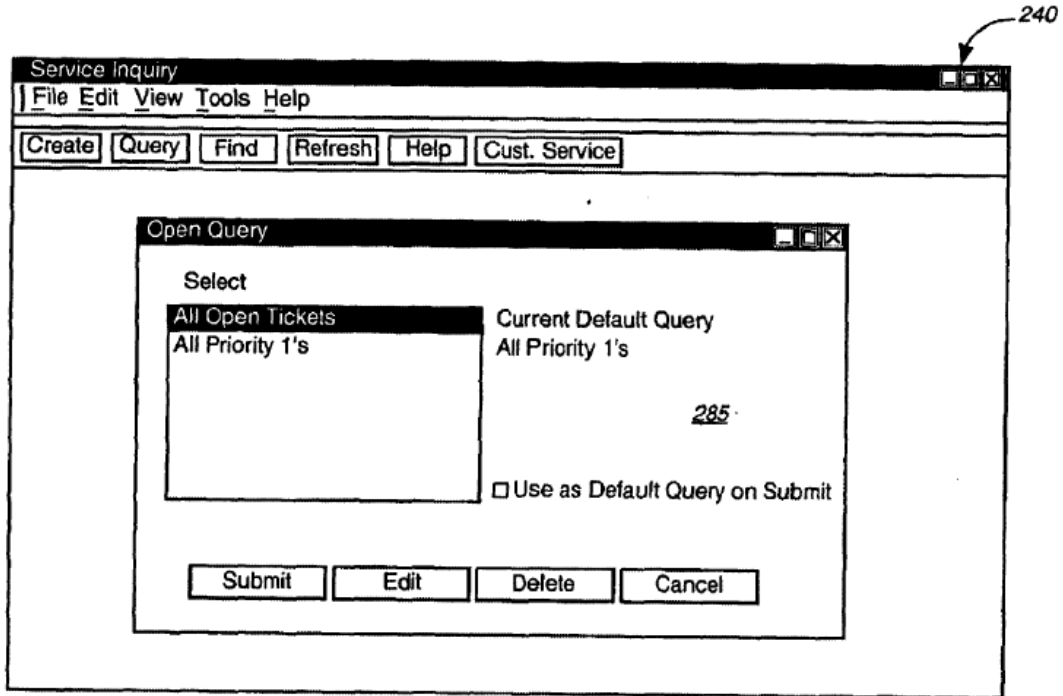
Cogger discloses that “the trouble ticket is submitted to [a] Customer Service Management System.” EX1033, 3:65-66. “When the CSM accepts the trouble ticket, a trouble ticket number is assigned.” *Id.*, 3:66-67. As discussed for [18-pre], in the system of Duvall-Chu-Cogger, Cogger’s CSM would be implemented as part

of Duvall-Chu's system to provide an outside service for assessing residue data—*i.e.*, by resolving tickets. EX1003, ¶243; EX1033, 2:24-30; Section VI.D.1.

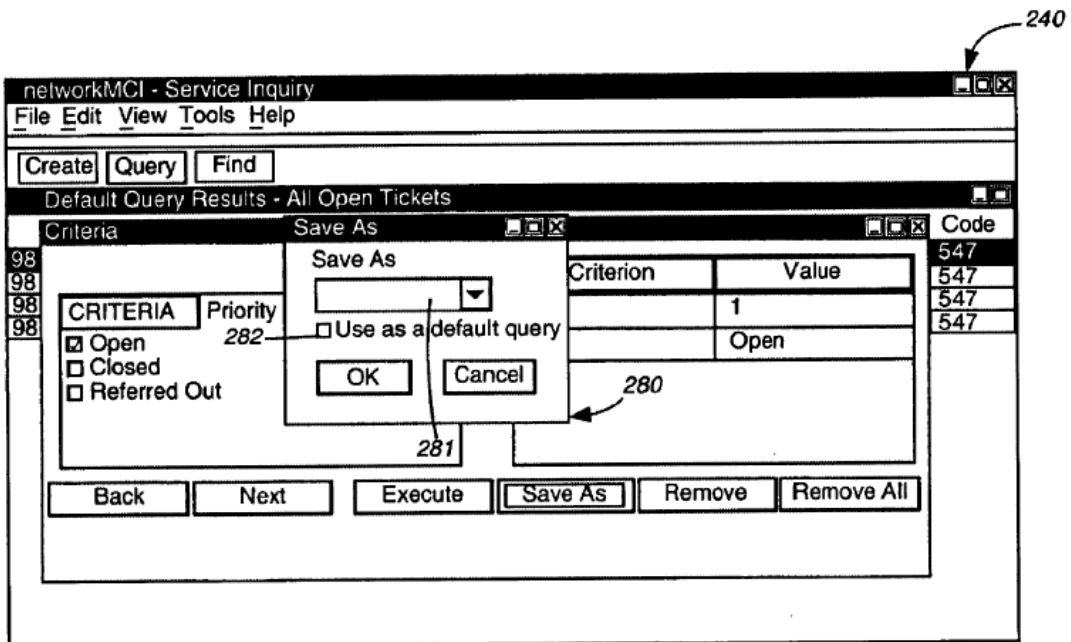
A POSA would have recognized that to resolve the ticket, a security analyst is required to view event information and update filters as appropriate. Section VI.D.1; EX1003, ¶244. As discussed for [1C], Duvall already teaches providing an “*analyst system*” to network administrators to view information about network events. Section VI.A.2(d); EX1003, ¶244. A POSA would have been motivated to provide a similar “*analyst console*” to analysts operating Duval-Chu-Cogger's service to analyze event information received in a trouble ticket and update filters as appropriate. EX1003, ¶244. Indeed, Cogger discloses receiving trouble tickets electronically (*see* [18-pre]), so a POSA would have understood analysts operating Duval-Chu-Cogger's third-party service would view ticket information from an “*analyst console*.” *Id.*

3. Claim 19

Cogger discloses that a “trouble ticket . . . may exist as a **data record in a database**,” and thus the event record contained in the trouble ticket is “*a pre-existing event record stored on an event database within the secure operations center*.” EX1003, ¶246. Cogger further discloses that a customer can search for and edit open tickets, as shown in the following interface screens:



EX1033, FIG. 8(f).



EX1033, FIG. 8(e).

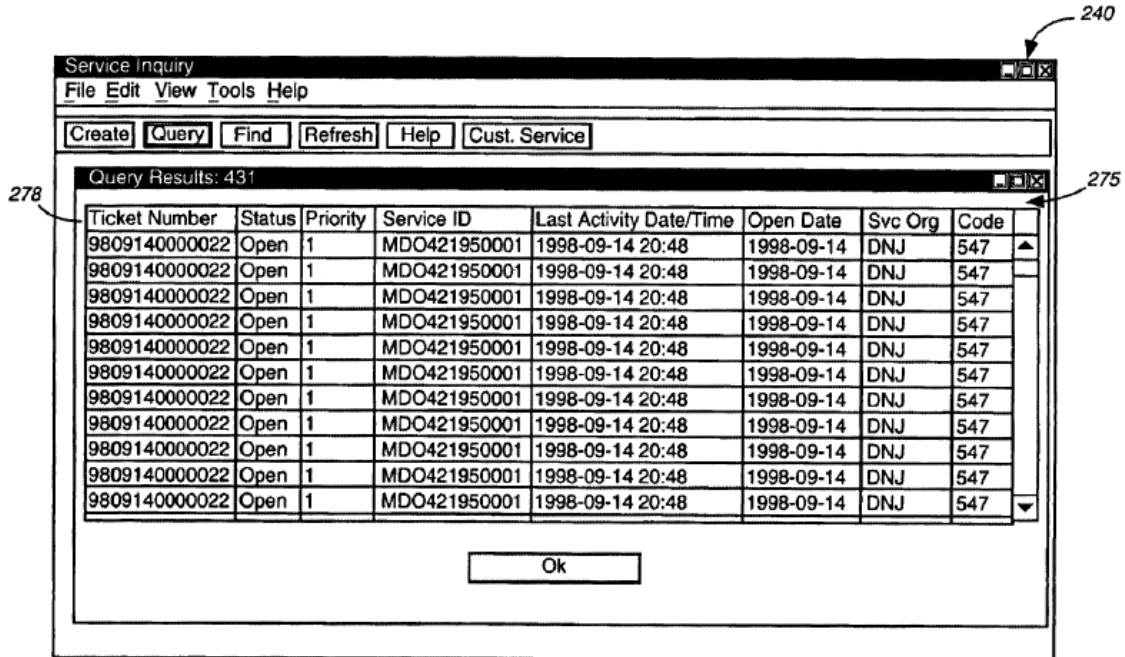


FIG. 8(c)

EX1033, FIG. 8(c).

When an open ticket is selected, a customer can edit details, including adding additional remarks to the ticket. EX1033, 20:50-59; EX1003, ¶247. A POSA would have understood that in Duvall-Chu-Cogger's system, certain events are related, for example multiple residue data transmissions to or from a URL with the same top-level domain. EX1003, ¶247. In such a case, a POSA would have been motivated to incorporate the related events in the same ticket for analysis by Duvall-Chu-Cogger's third-party service. *Id.* This would ensure that related events are analyzed and resolved together. *Id.* And Cogger provides a mechanism for doing so by adding the related event information as a new remark within an existing ticket, i.e.,

“linking the event record to an open problem ticket associated with the pre-existing event record.” EX1033, 20:50-59; EX1003, ¶247.

4. Claim 20

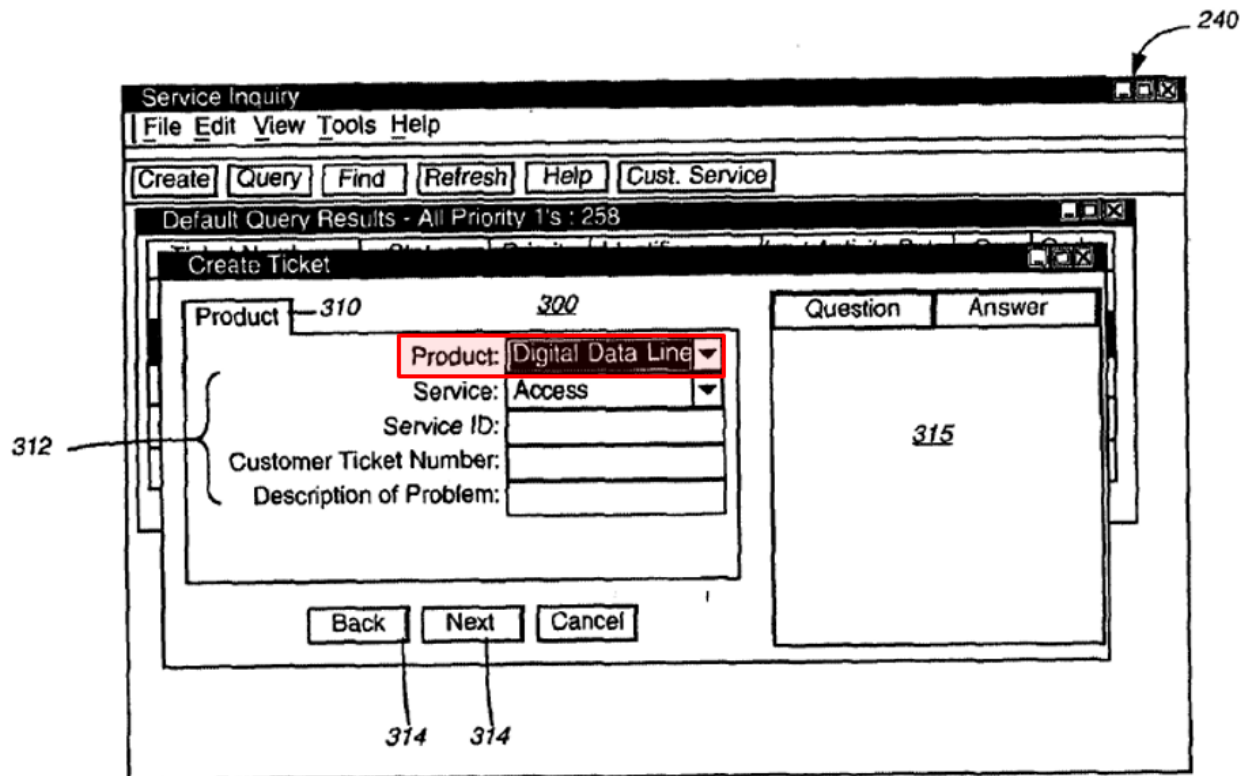
As discussed for [18B], Cogger discloses questions that are used to derive *“symptom[s]”* of the problem. EX1033, 21:55-22:6, 22:58-59; Section VI.D.2(c); EX1003, ¶249. Cogger further discloses that these questions are dynamic and used to diagnose the problem: **“QuestionTrees [] are essentially a set of questions for a particular product and problem type,”** and **“[w]ithin each group of Questions, there is one question that is designated as the decision point which is used to determine the next group of Questions** that need to be presented to the user.” EX1033, 23:15-16, 24:20-23; EX1003, ¶249. A POSA would thus understand that the particular questions and corresponding answers link symptoms of the problem to a diagnosis. EX1003, ¶249.

Furthermore, Cogger discloses that **“[b]oth the questions and the corresponding answers may be entered into a remarks section of the trouble ticket.”** EX1033, 3:62-64. **“[R]emarks are comments added to a ticket for historical purposes and can aid in the resolution of the problem.”** *Id.*, 20:33-34.

Therefore, Cogger discloses *“the problem resolution information,”* i.e., the remarks, *“links the symptom to a diagnosis.”* EX1003, ¶250.

5. Claim 21

Cogger discloses that tickets include a “[p]roduct type” to which the problem relates, as shown below. EX1033, 21:27-31, FIG. 8(k).



EX1033, FIG. 8(k) (annotated).

In Duvall-Chu-Cogger’s system, a POSA would have understood that the product types would relate to the customer devices sending or receiving data, e.g., the type of machine, and operating system, and/or browser associated with the network event. EX1003, ¶253. This understanding is consistent with the ’641 patent, which explains that “Technology” may refer to “[a]n operating system, software product or hardware product.” EX1001, 19:56-58; EX1003, ¶253.

Because the “*problem resolution assistance information*,” i.e., the remarks, include “*the symptom*,” as discussed for claim 20, the “*problem resolution assistance information links the symptom to a technology*” within the trouble ticket. EX1003, ¶254.

6. Claim 22

Cogger discloses that a “priority” is assigned to each trouble ticket. EX1033, 20:9-12, FIGs. 8(c), 8(g).

Service Inquiry

File Edit View Tools Help

Create Query Find Refresh Help Cust. Service

Query Results: 431

Ticket Number	Status	Priority	Service ID	Last Activity Date/Time	Open Date	Svc Org	Code
9809140000022	Open	1	MDO421950001	1998-09-14 20:48	1998-09-14	DNJ	547
9809140000022	Open	1	MDO421950001	1998-09-14 20:48	1998-09-14	DNJ	547
9809140000022	Open	1	MDO421950001	1998-09-14 20:48	1998-09-14	DNJ	547
9809140000022	Open	1	MDO421950001	1998-09-14 20:48	1998-09-14	DNJ	547
9809140000022	Open	1	MDO421950001	1998-09-14 20:48	1998-09-14	DNJ	547
9809140000022	Open	1	MDO421950001	1998-09-14 20:48	1998-09-14	DNJ	547
9809140000022	Open	1	MDO421950001	1998-09-14 20:48	1998-09-14	DNJ	547
9809140000022	Open	1	MDO421950001	1998-09-14 20:48	1998-09-14	DNJ	547
9809140000022	Open	1	MDO421950001	1998-09-14 20:48	1998-09-14	DNJ	547
9809140000022	Open	1	MDO421950001	1998-09-14 20:48	1998-09-14	DNJ	547

Ok

FIG. 8(c)

EX1033, FIG. 8(c) (annotated).

A POSA would have understood that such a priority indicates a “*vulnerability*,” defining the importance of resolving a particular network event. EX1003, ¶256.

Thus, Cogger discloses “*correlating the event record with a vulnerability*” within the trouble ticket. *Id.*

Cogger further discloses “*using the correlated vulnerability to link the event record to problem resolution assistance information*” because trouble tickets can be searched by priority. EX033, 58:14-15 (“wherein said trouble ticket search criteria includes an indication of priority of said trouble ticket”); EX1003, ¶257.

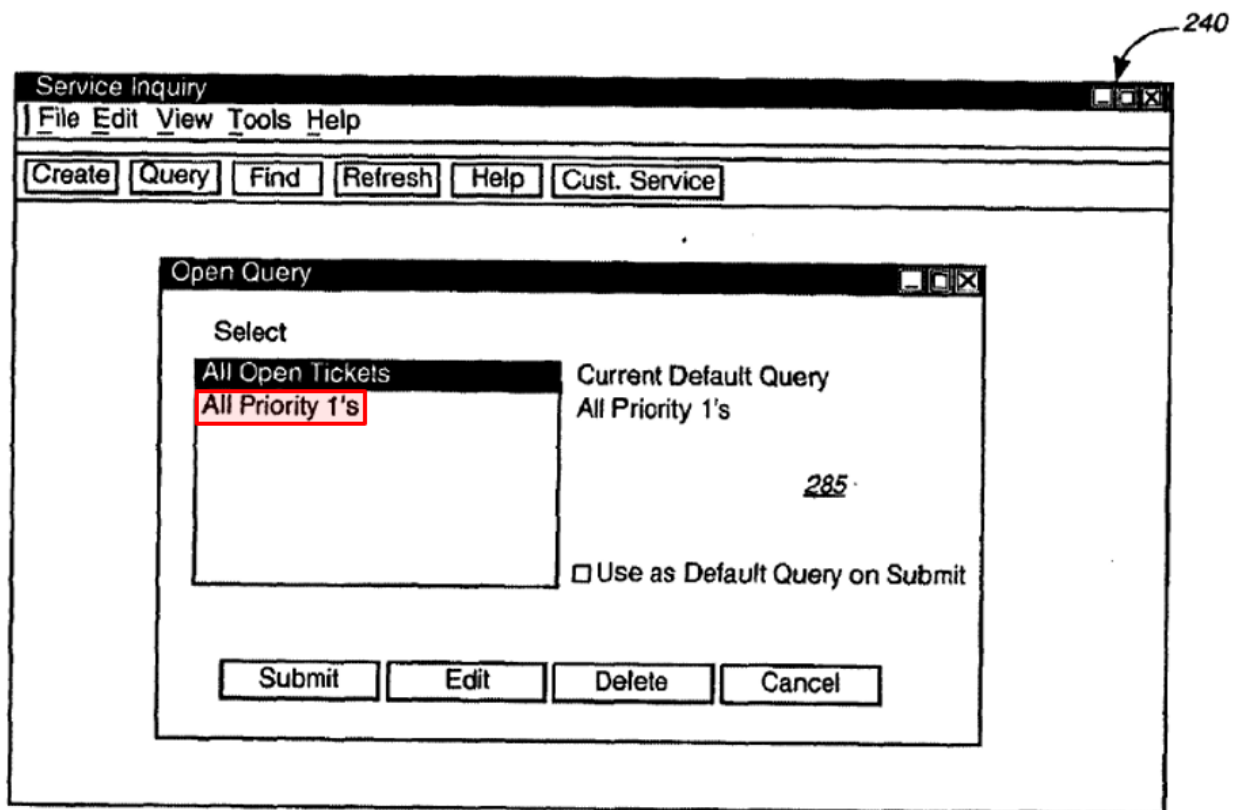


FIG. 8(f)

EX1033, FIG. 8(f) (annotated).

The results of the search query link the “*event record*,” as indicated by the ticket number, to the remarks contained within the ticket, i.e., “*problem resolution assistance information*.” See, e.g., EX1033, 19:55-57 (“The customer may then

view the results of a query, i.e., the details, remarks or activities of a Ticket chosen from a list of Tickets.”); EX1003, ¶258.

7. Claims 23 and 24

Cogger discloses that the remarks within a ticket (“*problem resolution assistance information*”) include diagnosis information, as discussed for claim 20. Section VI.D.4. Because the ticket priority (“*vulnerability*”) is linked to the remarks as part of the ticket, Cogger discloses that “*the problem resolution assistance information links the vulnerability to a diagnosis.*” EX1003, ¶260.

Cogger further discloses that ticket remarks can include information about “*a technology*,” such as the “CIRCUIT STATUS” or “DATA SPEED.” EX1033, FIG. 8(h).

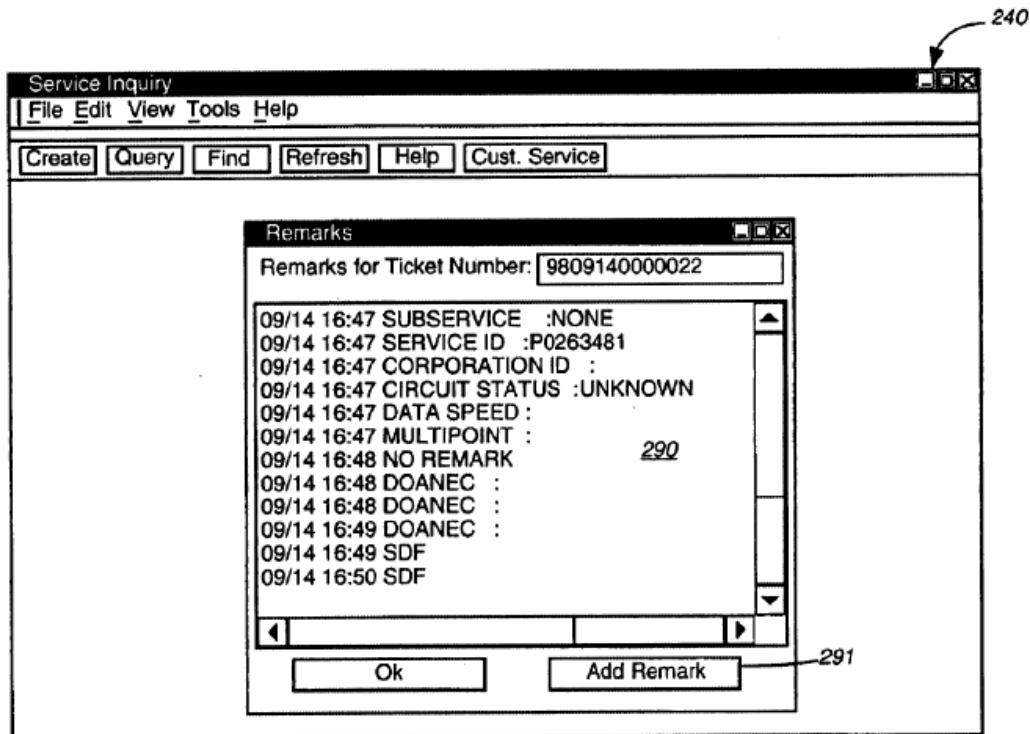


FIG. 8(h)

EX1033, FIG. 8(h).

In Duvall-Chu-Cogger's system, a POSA would have been motivated to include relevant technology information in the remarks to help "describe the trouble in his/her own words." EX1033, 20:59-62; EX1003, ¶¶261-62. As one example, Duvall discloses performing "pattern match[ing]" based on a "protocol" determined from the analyzed data transmission. EX1004, 6:5-9. If the data is residue, such protocol information would be useful to include in the trouble ticket to assist with analysis performed by Duvall-Chu-Cogger's third-party service. EX1003, ¶262. By including such information in the ticket remarks, Duvall-Chu-Cogger discloses "*the*

problem resolution assistance information links the vulnerability to a diagnosis.”

Id.

8. Claim 25

Cogger discloses that remarks may be “added on the ticket either by the customer or by the trouble ticket processing organization.” EX1033, 20:36-39.

Cogger further discloses that the customer is responsible for closing the ticket after a resolution:

[O]nce a ticket has been resolved the ticket is referred out to the customer’s organization. **If the customer is not satisfied with the problem resolution**, that customer may refer the ticket back to the ticket resolution enterprise organization.

Id., 22:44-49; EX1003, ¶264.

A POSA therefore would have been motivated to include the resolution information from the ticket-processing organization in the remarks so the customer could view the resolution. EX1003, ¶265. Indeed, Cogger teaches this operation, as the remarks include “comments added to a ticket for historical purposes,” e.g., memorializing the resolution. *Id.*

VII. The Board should not exercise its discretion to deny the Petition.

A. The Board should not deny the Petition under *Fintiv*.

The ’641 patent is currently involved in a parallel district-court case that was filed on November 28, 2022. *See British Telecommunications PLC et al. v. Palo*

Alto Networks, Inc., 1:22-cv-01538 (D. Del. Nov. 28, 2022). This case is in its earliest stages—no answer has been filed and no discovery has been served. Only initial motions to dismiss and to transfer venue have been filed, both of which remain pending. The '641 patent was previously asserted in district court, but the case did not involve Petitioner and, in any event, was dismissed with prejudice. *See* EX1016. No invalidity challenges were addressed or resolved in district court. Accordingly, *Fintiv* does not favor denial of institution.

B. *Advanced Bionics* strongly favors institution.

Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH, IPR2019-01469, DI, 7-8 (P.T.A.B. Feb. 13, 2020) (precedential) strongly favors institution because the IPR grounds here present new art and evidence not previously presented to or substantively considered by the Office.

None of Duvall, Chu, Trcka, Ziese, or Cogger was previously presented either during prosecution of the '641 patent or in the previous IPR filed against this patent. *See* EX1002; EX1011. Nor are these references cumulative of any reference previously presented. EX1003, ¶¶68-96. Indeed, as set forth herein, the Duvall-Chu combination teaches the very limitation—“*analysis of post-filtering residue*”—that the applicant claimed was not taught by the prior art during original prosecution of the '641 patent and its parent. Thus, §325(d) favors institution. *Advanced Bionics*, 7-9.

VIII. No Evidence of Secondary Considerations.

Petitioner is unaware of secondary considerations that would overcome the strong showing of obviousness. EX1003, ¶¶266-67.

IX. Conclusion

For the reasons provided above, *inter partes* review of claims 1-25 of U.S. Patent No. 7,895,641 is requested.

Respectfully submitted,
STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

/Jonathan Tuminaro/

Jonathan Tuminaro (Reg. No. 61,327)
Michael D. Specht (Reg. No. 54,463)
Daniel Block (Reg. No. 68,395)
Steven M. Pappas (Reg. No. 73,904)
Attorneys for Petitioner Palo Alto Networks, Inc.

Date: April 28, 2023

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600

X. Appendix A: Challenged Claims

1. [1-pre] A system for operating a probe as part of a security monitoring system for a computer network, the system comprising:

[1A] a) a sensor coupled to collect status data from at least one monitored component of the network;

[1B] b) a filtering subsystem coupled to analyze 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;

[1C] c) a communications system coupled to transmit information about the identified events to an analyst system associated with the security monitoring system;

[1D] d) a receiver for receiving feedback at the probe based on empirically-derived information reflecting operation of the security monitoring system; and

[1E] e) a modification control system for dynamically modifying an analysis capability of the probe during operation thereof based on the received feedback.

2. The system of claim 1, wherein the identifying step includes performing a multi-stage analysis of the status data.

3. The system of claim 2, wherein the multi-stage analysis includes performing a discrimination analysis on the status data.

4. The system of claim 3, wherein the discrimination analysis includes positive filtering.

5. The system of claim 3, wherein the discrimination analysis includes negative filtering.

6. The system of claim 2, wherein the multi-stage analysis includes analysis at the probe and analysis at a secure operations center configured to receive data from the probe.

7. The system of claim 1, wherein the identifying step includes aggregating and synthesizing the status data at the probe.

8. The system of claim 7, wherein the identifying step includes cross-correlating data across the monitored components.

9. The system of claim 7, wherein the identifying step includes analyzing the frequency of occurrence of the events.

10. The system of claim 1, further comprising after the step (c), a secure operations center coupled to perform further computer-based analysis and to receive data from the probe.

11. The system of claim 10, wherein the computer-based analysis includes aggregating, synthesizing, and presenting alerts on an ensemble basis.
12. The system of claim 10, wherein the identifying step includes cross-correlating data across the monitored components.
13. The system of claim 10, wherein the identifying step includes analyzing the frequency of occurrence of the events.
14. The system of claim 10, wherein the computer-based analysis includes cross-probe correlation.
15. The system of claim 1, further comprising instantaneously self-tuning the probe based on previously collected status data.
16. The system of claim 1, wherein the dynamic modifying step includes consideration of non-real-time information from ongoing security research efforts.
17. The system of claim 1, wherein the receiving feedback step occurs in substantially real time.
18. **[18-pre]** A method of operating a secure operations center as part of a security monitoring system for a customer computer network, comprising:

[18A] creating an event record for information received about an identified potentially security-related event occurring on the network, wherein the potentially security-related event is identified by filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is neither discarded nor selected by the filtering;

[18B] correlating the event record with customer information and a symptom record;

[18C] using the correlated symptom record to link the event record to problem resolution information;

[18D] consolidating the event record, correlated customer information and symptom record, and linked problem resolution assistance information into a problem ticket; and

[18E] providing the problem ticket to a security analyst console for analysis.

19. The method of claim 18, further comprising:

correlating the event record with a pre-existing event record stored on an event database within the secure operations center; and

linking the event record to an open problem ticket associated with the pre-existing event record.

20. The method of claim 18, wherein the problem resolution assistance information links the symptom to a diagnosis.
21. The method of claim 18, wherein the problem resolution assistance information links the symptom to a technology.
22. The method of claim 18, further comprising:

correlating the event record with a vulnerability; and

using the correlated vulnerability to link the event record to problem resolution assistance information.
23. The method of claim 22, wherein the problem resolution assistance information links the vulnerability to a diagnosis.
24. The method of claim 22, wherein the problem resolution assistance information links the vulnerability to a technology.
25. The method of claim 18, further comprising:

updating the problem resolution assistance information after the potentially security-related event is resolved.

**CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME
LIMITATION, TYPEFACE REQUIREMENTS, AND TYPE STYLE
REQUIREMENTS**

1. This Petition for *Inter Partes* Review complies with the type-volume limitation of 14,000 words, comprising 13,860 words, excluding the parts exempted by 37 C.F.R. § 42.24.

2. This Petition for *Inter Partes* Review complies with the general format requirements of 37 C.F.R. § 42.6 and has been prepared using Microsoft® Word 2010 in 14 point Times New Roman.

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

/Jonathan Tuminaro/

Jonathan Tuminaro
Registration No. 61,327
Attorney for Petitioner Palo Alto Networks, Inc.

Date: April 28, 2023

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600

CERTIFICATION OF SERVICE

The undersigned hereby certifies that on April 28, 2023, true and correct copies of the foregoing **PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 7,895,641**, Petitioner's Power of Attorney, and all associated exhibits were served in their entirety on the following via FedEx Express®:

NIXON & VANDERHYE, PC
901 North Glebe Road, 11th Floor
Arlington, VA 22203

PROSKAUER ROSE LLP
Eleven Times Square
New York, NY 10036-8299

*Correspondence Address of Record
for U.S. Patent No. 7,895,641*

*Additional Address Known to Petitioner
Likely to Affect Service*

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

/Jonathan Tuminaro/

Jonathan Tuminaro
Registration No. 61,327
Attorney for Petitioner Palo Alto Networks, Inc.

Date: April 28, 2023

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600