Ryan Iwahashi (CA SBN 284766)
ryan@gishpllc.com
**GISH PLLC**
50 California Street, Suite 1500
San Francisco, CA 94111
Phone: (415) 630-2000

Andrew D. Gish (NY SBN 4918454) *(pro hac vice)*
andrew@gishpllc.com
Christopher Gerson (NY SBN 4595708) *(pro hac vice)*
Chris.Gerson@gishpllc.com
**GISH PLLC**
41 Madison Avenue, Floor 31
New York, NY 10010
Phone: (212) 518-7380

*Attorneys for Fortinet, Inc.*

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

| | |
|---|---|
| NETSKOPE, INC.,<br><br>Plaintiff,<br><br>vs.<br><br>FORTINET, INC,<br><br>Defendant. | CASE NO. 4:25-cv-02360-HSG<br><br>**FORTINET'S PRELIMINARY INVALIDITY CONTENTIONS** |



Netskope, Ex. 2002
Fortinet v. Netskope, IPR2026-00042

## I. INTRODUCTION

Pursuant to P.R. 3-3 & 3-4 of this Court, Defendant Fortinet, Inc. ("Fortinet" or "Defendant") hereby serves these Preliminary Invalidity Contentions on Plaintiff Netskope, Inc. ("Netskope" or "Plaintiff") for U.S. Patent Nos. 8,356,336 (the "'336 Patent"), 8,543,710 (the "'710 Patent"), 8,117,639 (the "'639 Patent"), 8,224,983 (the "'983 Patent"), 8,327,426 (the "'426 Patent"), 7,593,936 (the "'936 Patent"), 8,397,282 (the "'282 Patent"), 8,661,153 (the "'153 Patent"), and 8,635,697 (the "'697 Patent") (collectively, the "Asserted Patents"). These Invalidity Contentions are based on Fortinet's current knowledge of the Asserted Patents and prior art, along with its understanding of Plaintiff's infringement allegations set forth in Plaintiff's July 1, 2025 Disclosure of Asserted Claims and Infringement Contentions ("Infringement Contentions"). Based on Plaintiff's Infringement Contentions, Plaintiff is currently asserting the following claims against Fortinet (collectively, the "Asserted Claims"):

| Patent | Asserted Claim(s) |
|---|---|
| '336 Patent | 1-3, 5-6, and 9-20 |
| '710 Patent | 1, 2, 6, 7, 13-20 |
| '639 Patent | 1-27 |
| '983 Patent | 1-9 |
| '426 Patent | 1-7 |
| '936 Patent | 1-22 |
| '282 Patent | 1-35 |
| '153 Patent | 1-20, 22, 24 |
| '697 Patent | 1-25 |

Fortinet submits these Invalidity Contentions without waiving any arguments about the sufficiency or substance of Plaintiff's Infringement Contentions, and without waiving any challenges to Plaintiff's apparent claim constructions. Based in whole or in part on the claim interpretations that Plaintiff appears to be asserting, and its alleged application of those interpretations to the accused products, Fortinet contends that each cited prior art reference listed below anticipates or renders obvious the Asserted Claims, as described below and in the associated claim charts, attached hereto and incorporated by reference as if fully set forth herein.

Identifying these items of prior art and other defenses in connection with these Invalidity Contentions does not serve as an admission or waiver of any argument or position refuting that any alleged "Accused Product," including any current or past version of any alleged "Accused Product," is covered by, or infringes any of the Asserted Claims (or any other claim of the Asserted Patents), particularly when the Asserted Claims are properly construed. Further, Fortinet's Invalidity Contentions should not be construed as an admission regarding the proper construction of any asserted claim, should not be deemed to represent or limit the claim constructions that Fortinet will advance in this action, and should not be deemed to relate to the non-infringement positions Fortinet may advance in this action.

Fortinet's Invalidity Contentions reflect Fortinet's current knowledge and contentions as of this early stage of this action regarding Plaintiff's patents. Fortinet's Invalidity Contentions are based in whole or in part on its present understanding of the Asserted Claims and Plaintiff's apparent position as to the scope of the Asserted Claims as applied in its Local Patent Rule 3-1 disclosure. Accordingly, Fortinet's Invalidity Contentions (including the attached invalidity claim charts) reflect, to the extent possible, Plaintiff's expected alternative and potentially inconsistent positions as to the claim construction and claim scope.

Fortinet reserves the right, to the extent permitted by the Court and the applicable statutes and rules, to modify and supplement, without prejudice, these Invalidity Contentions. In addition, Fortinet reserves the right, to the extent permitted by the Court and the applicable statutes and rules, to raise additional prior art and invalidity defenses not included in these Preliminary Invalidity Contentions, including those based on additional discovery or other issues raised by Plaintiff in this action or any related action. Fortinet further reserves the right, to the extent permitted by the Court and the applicable statutes and rules, to amend these Invalidity Contentions should, for example, Plaintiff provide any information that it failed to provide in its Initial Disclosures and/or its Infringement Contentions.

Further, because discovery on Plaintiff's patents has only recently begun, Fortinet reserves the right, to the extent permitted by the Court and the applicable statutes and rules, to revise, amend, and/or supplement the information provided herein, including identifying and relying on additional prior art references should Fortinet's further search and analysis yield additional information or references,

consistent with the Local Patent Rules and the Federal Rules of Civil Procedure. Fortinet expressly reserves the right, to the extent permitted by the Court and the applicable statutes and rules, to rely on witness testimony about the prior art references identified below to supplement these Invalidity Contentions, where appropriate. Moreover, Fortinet reserves the right, to the extent permitted by the Court and the applicable statutes and rules, to revise its ultimate Invalidity Contentions concerning the invalidity of the Asserted Claims, which may change depending upon the Court's construction of terms of the Asserted Claims, any findings as to the priority date of the Asserted Claims, and/or positions that Plaintiff or its fact or expert witness(es) may take concerning claim construction, infringement, and/or invalidity issues.

The accompanying invalidity claim charts list specific examples of where prior art references disclose, either expressly or inherently, each limitation of the Asserted Claims and therefore anticipate the claim and/or examples of disclosures in view of which a person of ordinary skill in the art ("POSITA") at the time each of the alleged inventions was made, would have considered each limitation, and therefore the claim as a whole, obvious. The references, however, may contain additional support upon which Fortinet may rely that is not specifically identified in these contentions. The citations included in each chart are illustrative, not exhaustive. For any given quotation or excerpt, for example, Fortinet expressly reserves the right to introduce other text and images (including but not limited to surrounding, related, or explanatory text, images, or un-cited portions of the prior art references) from the same or other prior art references that may help to provide context to the quotation or excerpt. Furthermore, where Fortinet cites to a particular figure in a reference, the citation should be understood to encompass the caption and description of the figure and any text relating, in any manner, to the figure. Similarly, where Fortinet cites to particular text referring to a figure, the citation should be understood to include the corresponding figure as well. Fortinet may also rely on other documents and information, including cited references and prosecution histories for the Asserted Patents or related patents (including but not limited to patents and/or patent applications, within the same family or at any time assigned to Plaintiff), and witness testimony, including expert testimony, to explain, amplify, illustrate, demonstrate, provide context or aid in understanding the cited portions of the references.

## II. P.R. 3-3(a): IDENTIFICATION OF PRIOR ART

Pursuant to P.R. 3-3(a), and subject to Fortinet's reservation of rights, Fortinet contends that one or more Asserted Claims of the Asserted Patents are anticipated or rendered obvious by the prior art identified below and as reflected in the attached Exhibits A-1 through I-8. Fortinet also contends that the Accused Products do not infringe any Asserted Claim of any Asserted Patent.

Fortinet reserves the right, to the extent permitted by the Court and the applicable statutes and rules, to assert that the Asserted Claims are invalid under pre-AIA 35 U.S.C. § 102(f) in the event Fortinet obtains additional evidence that the named inventors of the Asserted Patents did not invent (either alone or in conjunction with others) the subject matter claimed in the Asserted Patents. Should Fortinet obtain such evidence, it will provide the name of the person(s) from whom, and the circumstances under which, the invention or any part of it was derived.

Fortinet further intends to rely on admissions of the named inventors and Plaintiff concerning the prior art, including statements found in the Asserted Patents, their prosecution histories, and/or other related patents or patent applications, any deposition testimony, and the papers filed, and any evidence submitted by Plaintiff in conjunction with this action. For example, Fortinet incorporates by reference the prior art from any petitions for *inter partes* review that are filed in the future.

Finally, Fortinet may rely on testimony from the authors or named inventors listed in the below references.

The following patents and patent publications are prior art to the Asserted Patents under at least pre-AIA 35 U.S.C. §§ 102(a), (b), (e), and/or (g).

| Chart(s) | Country/Patent Number | Publication/Filing Date |
|---|---|---|
| A-1 | UK Patent Application No. GB2389010 to Subbiah ("Subbiah") | November 26, 2003 |
| A-1 | WO 2002/0339237 to Hinton et al. ("Hinton 3") | May 16, 2002 |
| B-1 | U.S. Patent No. 9,398,037 to Roskind ("Roskind") | September 27, 2005 |
| B-2 | U.S. Patent Pub. No. 2003/0191966 to Gleichauf ("Gleichauf") | October 9, 2003 |

| Chart(s) | Country/Patent Number | Publication/Filing Date |
|---|---|---|
| B-3 | U.S. Patent Pub. No. 2004/0047356 to Bauer ("Bauer") | September 6, 2002 |
| Appendix B | U.S. Patent Pub. No. 2003/0023708 to Jung ("Jung") | January 30, 2003 |
| Appendix B | U.S. Patent No. 6,832,256 to Toga ("Toga") | December 27, 1996 |
| Appendix B | U.S. Patent No. 7,966,078 to Hoffberg et al. ("Hoffberg") | February 27, 2006 |
| Appendix B | U.S. Patent No. 6,400,996 to Hoffberg et al. ("Hoffberg '996") | June 4, 2002 |
| Appendix B | U.S. Patent No. 6,636,894 to Short et al ("Short '894") | October 21, 2003 |
| C-1 | U.S. Patent Pub. No. 2003/0152067 to Richmond ("Richmond") | September 20, 2002 |
| C-2 | U.S. Patent No. 6,463,474 to Fuh ("Fuh") | July 2, 1999 |
| C-3 | WO 2001/031843 to Short ("Short 2") | October 20, 2000 |
| Appendix C | WO 2001/011452 to Wood ("Wood") | July 31, 2000 |
| Appendix C | U.S. Patent No. 5,623,492 to Teraslinna ("Teraslinna") | March 24, 1995 |
| Appendix C | U.S. Patent Pub. No. 2002/0010776 to Lerner ("Lerner") | Dec. 28, 2000 |
| Appendix C | U.S. Patent No. 7,197,044 to Kadambi ("Kadambi") | March 17, 2000 |
| D-1 | U.S. Patent No. 7,194,554 to Short et al. ("Short") | October 20, 2000 |
| D-2 | U.S. Patent Pub. No. 2003/0163581 to Moran et al. ("Moran") | June 25, 2002 |
| D-3 | U.S. Patent Pub. No. 7,257,640 to Callocchia et al. ("Callocchia") | April 16, 2002 |
| D-4 | U.S. Patent No. 6,324,184 to Hou et al. ("Hou") | September 4, 1998 |
| D-5 | U.S. Patent No. 6,427,174 to Sitaraman et al. ("Sitaraman") | November 12, 1998 |
| D-6 | U.S. Patent No. 7,433,943 to Ford et al. ("Ford") | December 20, 2001 |
| D-7 | U.S. Patent Pub. No. 2003/0061263 to Riddle ("Riddle") | September 26, 2001 |
| D-8 | U.S. Patent No. 7,073,055 to Freed et al. ("Freed") | February 22, 2001 |
| D-9 | U.S. Patent Pub. No. 2003/0152067 to Richmond et al. ("Richmond") | September 20, 2002 |
| E-1 | U.S. Patent Pub. No. 2006/0021019 to Hinton et al. ("Hinton 1") | July 21, 2004 |
| E-2 | U.S. Patent Pub. No. 2006/0236382 to Hinton et al. ("Hinton 2") | April 1, 2005 |
| E-3 | U.S. Patent No. 7,793,342 to Ebrahimi et al. ("Ebrahimi 1") | October 15, 2002 |

| Chart(s) | Country/Patent Number | Publication/Filing Date |
|---|---|---|
| E-4 | U.S. Patent Pub. No. 2007/0136786 to Gong et al. ("Gong") | December 8, 2005 |
| E-5 | U.S. Patent Pub. No. 2007/0234408 to Burch et al. ("Burch") | March 31, 2006 |
| F-1 | U.S. Patent No. 7,225,343 to Honig et al. ("Honig") | January 27, 2003 |
| F-2 | U.S. Patent Pub. No. 2004/0230834to McCallam et al. ("McCallam") | May 14, 2003 |
| F-3 | U.S. Patent No. 6,327,550 to Vinberg et al. ("Vinberg") | March 5, 2001 |
| F-4 | U.S. Patent No. 6,457,015 to Eastham et al. ("Eastham") | May 7, 1999 |
| F-5 | U.S. Patent Pub. No. 2005/0022209 to Lieblich et al. ("Lieblich") | July 24, 2003 |
| Appendix F | U.S. Patent No. 6,591,377 to Evoy et al. ("Evoy") | November 24, 1999 |
| Appendix F | U.S. Patent Pub. No. 2005/0005171 to Oliphant et al. ("Oliphant") | July 1, 2003 |
| Appendix F | U.S. Patent App. No. 60/484,085 ("Oliphant Provisional") | July 1, 2003 |
| Appendix F | U.S. Patent No. 7,788,699 to Largman et al. ("Largman") | March 6, 2002 |
| Appendix F | U.S. Patent No. 9,503,470 to Gergner et al. ("Gertner") | December 24, 2002 |
| G-1 | U.S. Patent No. 6,519,703 to Joyce ("Joyce") | February 11, 2003 |
| G-2 | U.S. Patent No. 6,154,775 to Coss et al. ("Coss") | November 28, 2000 |
| G-3 | U.S. Patent No. 6,550,012 to Villa et al ("Villa") | April 15, 2003 |
| G-4 | U.S. Patent Pub. No.2005/0022011 to Swander et al. ("Swander") | June 6, 2003 |
| Appendix G | U.S. Patent Pub. No. 2003/0231632 to Haberlen ("Haberlen") | December 18, 2003 |
| Appendix G | U.S. Patent Pub. No. 2003/0174648 to Wang et al. ("Wang") | September 18, 2003 |
| Appendix G | U.S. Patent No. 7,453,852 to Buddhikot et al. ("Buddhikot") | July 14, 2003 |
| Appendix G | U.S. Patent No. 6,496,935 to Fink et al ("Fink") | December 17, 2002 |
| Appendix G | U.S. Patent No. 7,032,031 to Jungck ("Jungck") | June 23, 2000 |
| H-1 | U.S. Patent No. 7,194,554 to Short et al. ("Short") | October 20, 2000 |
| H-2 | U.S. Patent Pub. No. 2003/0163581 to Moran et al. ("Moran") | June 25, 2002 |

| Chart(s) | Country/Patent Number | Publication/Filing Date |
|---|---|---|
| H-3 | U.S. Patent Pub. No. 7,257,640 to Callocchia et al. ("Callocchia") | April 16, 2002 |
| H-4 | U.S. Patent No. 6,324,184 to Hou et al. ("Hou") | September 4, 1998 |
| H-5 | U.S. Patent No. 6,427,174 to Sitaraman et al. ("Sitaraman") | November 12, 1998 |
| H-6 | U.S. Patent No. 7,433,943 to Ford et al. ("Ford") | December 20, 2001 |
| H-7 | U.S. Patent Pub. No. 2003/0061263 to Riddle ("Riddle") | September 26, 2001 |
| H-8 | U.S. Patent No. 7,073,055 to Freed et al. ("Freed") | February 22, 2001 |
| H-9 | U.S. Patent Pub. No. 2003/0152067 to Richmond et al. ("Richmond") | September 20, 2002 |
| I-1 | U.S. Patent Pub. No. 2008/0086773 to Tuvell et al. ("Tuvell") | April 10, 2008 |
| I-2 | U.S. Patent Pub. No. 2008/0056487 to Akyol et al. ("Akyol") | March 6, 2008 |
| I-3 | U.S. Patent No. 7,676,217 to Zhu et al. ("Zhu") | August 3, 2006 |
| I-4 | U.S. Patent No. 7,853,689 to Enderby ("Enderby") | December 18, 2008 |
| I-5 | U.S. Patent Pub. No. 2009/0328220 to Abdel-Aziz et al. ("Abdel-Aziz") | December 31, 2009 |
| I-6 | U.S. Patent Pub. No. 2003/0154399 to Zuk et al. ("Zuk") | August 14, 2003 |
| I-7 | U.S. Patent Pub. No. 2010/0161795 to Deridder et al. ("Deridder") | December 22, 2009 |
| I-8 | KR100765340B1 to Lee ("Lee") and Certified Translation | April 26, 2006 |

The following non-patent publications are prior art to the asserted patents under at least pre-AIA 35 U.S.C. §§ 102(a), (b), and/or (g).

| Chart(s) | Title | Publication Date | Author(s)/Publisher |
|---|---|---|---|
| A-1 | A Secure and Transparent Firewall Web Proxy | October 2003 | Crandell ("Crandell") |
| Appendix I | Request for Comments: 2616, Hyper Text Transfer Protocol – HTTP/1.1 | 1999 | ("RFC 2616") |
| Appendix I | p0f, v. 2.0.8, open source code | September 6, 2006 | ("p0f") |
| C-4 | Enterasys User Personalized Network White Paper | By 2001 | Enterasys Networks |

| Chart(s) | Title | Publication Date | Author(s)/Publisher |
|---|---|---|---|
| Appendix G | comp.os.linux.security FAQ, version 2.0, Released Canada Day 2002, Last updated Jun 29, 2002 | June 2002 | Daniel Swan ("Linux FAQ")[1] |
| Appendix G | IPTables Basics NHF[2] | December 2002 | Kenshi ("IPTables Basics NHF") |
| Appendix G | Firewalls and Internet Security, Second Edition | April 2003 | Cheswick et al. ("Cheswick") |

The following items, on information and belief, were publicly used, publicly known, offered for sale, and/or sold, and are therefore prior art to the Asserted Patents under at least pre-AIA 35 U.S.C. §§ 102(a), (b), and/or (g).

| Chart(s) | Title | Publication Date[3] | Author(s)/Publisher |
|---|---|---|---|
| A-2 | Cisco Subscriber Edge Services Manager Captive Portal | 2003 | Cisco |
| C-4 | Enterasys System / User Personalized Network | 2002 | Enterasys Networks |
| D-10 | Nortel Shasta | 1999 | Nortel |
| D-11 | Nomadix Service Engine / Universal Subscriber Gateway | 1999 | Nomadix |
| E-6 | Evidian Identity Management Software | 2005 | Evidian |
| E-7 | Azure Active Directory | 2004 | Microsoft |
| E-8 | Microsoft Identity Integration Server 2003 | 2003 | Microsoft |

[1] Available at https://web.archive.org/web/20021203032239/http://www.linuxsecurity.com/docs/colsfaq.html

[2] Available at https://web.archive.org/web/20021213024951/http://www.linuxnewbie.org/nhf/Security/IPtables_Basics.html

[3] Based on information and belief and publicly available information. Fortinet reserves all rights to amend these dates, including in light of information learned in discovery.

| Chart(s) | Title | Publication Date[3] | Author(s)/Publisher |
|---|---|---|---|
| E-9 | Oracle Identity Management | 2004 | Oracle |
| E-10 | Open Directory | 2006 | Apple |
| E-11 | iSeries Server (IBM Secure Identity Manager) | 2002 | IBM |
| H-10 | Nortel Shasta | 1999 | Nortel |
| H-11 | Nomadix Service Engine / Universal Subscriber Gateway | 1999 | Nomadix |

On information and belief, the Cisco Service Selection Gateway was available by 2002 and is invalidating prior art as to the '639, '983, and '153 patents. On information and belief, PortSentry was a firewall tool available by May 2003 and is invalidating prior art to the '282 patent. On information and belief, NoCatAuth was a captive portal solution available by 2002 and is invalidating prior art as to the '336 and '710 patents. For all prior art systems, Fortinet reserves the right to supplement these contentions as additional information becomes available during discovery, including information from third parties.

In addition, to the extent Netskope accuses of infringement Fortinet systems and products that pre-date the priority dates of one or more Asserted Patents, Netskope's Preliminary Infringement Contentions do not cite to technical documentation identifying the particular functionality accused of infringement—or how a multitude of varied products purportedly work together to infringe the claims. Fortinet denies that any of its products infringe any Asserted Claim, but to the extent that Netskope amends its contentions to include reference to specific functionality that allegedly practices the Asserted Claims, Fortinet reserves the right to demonstrate that any such functionality (or substantially similar functionality) was already present in the prior art versions of Fortinet's products.

Moreover, the following references illustrate the state of the art as of Plaintiff's claimed priority dates, along with any references cited or otherwise referred to in the Asserted Patents themselves, these

references or any applications (including provisional applications to which these references claim priority:

- U.S. Patent Pub. No. 2007/0061263 to Carter et al. ("Carter")
- U.S. Patent No. 7,681,229 to Ebrahimi et al. ("Ebrahimi 2")
- WO2004/061597 to Barrett ("Barrett")
- EP1089516 to Grandcolas et al. ("Grandcolas")
- U.S. Patent Pub. No. 2003/0005118 to Williams ("Williams")
- U.S. Patent Pub. No. 2005/0204148 to Mayo et al. ("Mayo")
- U.S. Patent No. 7,370,351 to Ramachadran et al. ("Ramachadran")
- U.S. Patent Pub. No. 2003/0046541 to Gerdes et al. ("Gerdes")
- U.S. Patent Pub. No. 2004/0054898 to Chao et al. ("Chao")
- U.S. Patent Pub. No. 2005/0050336 to Liang et al. ("Liang")
- U.S. Patent Pub. No. 2004/0117640 to Chu et al. ("Chu")
- U.S. Patent Pub. No. 2007/0204168 to Cameron et al. ("Cameron")
- U.S. Patent Pub. No. 2003/0163569 to Panasyuk et al. ("Panasyuk")
- EP0906593 to Gross et al. ("Gross")
- EP1631032 to Carter et al. ("Carter")
- Request for Comments: 2616, Hyper Text Transfer Protocol – HTTP/1.1, 1999 ("RFC 2616")
- Request for Comments: 793, Transmission Control Protocol, September 1981 ("RFC 793")
- A Robust Classifier for Passive TCP/IP Fingerprinting, by Beverly
- Index of _p0f3_releases_old_2.x, available at https://lcamtuf.coredump.cx/p0f3/releases/old/2.x/
- U.S. Patent No. 6,591,377 to Evoy et al. ("Evoy")
- U.S. Patent Pub. No.2002/0157035 to Wong et al. ("Wong")
- U.S. Patent No. 6,484,203 to Porras et al. ("Porras")

- U.S. Patent Pub. No. 2003/0139908 to Wegerich et al. ("Wegerich")

## III. P.R. 3-3(b): PRIOR ART THAT ANTICIPATES OR RENDERS OBVIOUS ONE OR MORE ASSERTED CLAIMS

Subject to Fortinet's reservation of rights, Fortinet identifies the prior art that anticipates the Asserted Claims in its Exhibits A-1 through I-8.

In the attached charts and below, Fortinet identifies the following combinations of prior art now known to Fortinet that render obvious one or more of the Asserted Claims under 35 U.S.C. § 103. Fortinet also discloses the motivation to combine such items. Fortinet reserves the right to assert that any of the identified prior art anticipates one or more of the Asserted Claims, any findings as to the priority date of the Asserted Claims, and/or positions that Plaintiff or its fact or expert witness(es) may take concerning claim construction, infringement, and/or invalidity issues. Furthermore, Fortinet incorporates by reference the motivation to combine and obviousness combinations from any petitions for *inter partes* review that are filed in the future.

### A. Motivations to Combine

The Asserted Claims do not represent innovation over the prior art but instead would be no more than the result of ordinary skill and common sense. No showing of a specific motivation is required to combine the prior art (including the references disclosed above), as each combination would not have produced unexpected results, and at most would simply represent a known alternative to a POSITA. *See KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398, 414-17 (2007). Indeed, the Supreme Court held that a POSITA is "a person of ordinary creativity, not an automaton," and "in many cases a person of ordinary skill in the art will be able to fit the teachings of multiple patents together like pieces of a puzzle." *Id.* at 420.

#### 1. Nature of the Problem Being Solved

For example, a POSITA would have been motivated to combine or modify the prior art (including to form the specific exemplary combinations identified below in Section III.B) based on the nature of the problem being solved, e.g., the problem of protecting a network from unauthorized access or allocating network bandwidth for users. To the extent additional relevant sources—such as the

Asserted Patents, the prosecution history, or testimony or documents provided by named inventors or companies involved in the development of the technology described in the Asserted Patents—identify additional problems that were allegedly being solved, Fortinet reserves the right to rely on such problems that were allegedly being solved.

**2. The Express, Implied, and Inherent Teachings of the Prior Art**

As another example, a POSITA would have been motivated to combine or modify the disclosed prior art (including to form the exemplary combinations identified below in Section III.B) based on the express, implied, and inherent teachings of the prior art, e.g., the benefits of protecting a network from unauthorized access or allocating network bandwidth for users. Fortinet also incorporates its claim charts (which specifically compare the teachings of the prior art to the limitations of the Asserted Claims) by reference. To the extent the prior art, including the prior art identified throughout these Invalidity Contentions, provides additional teachings, Fortinet reserves the right to rely on such teachings. Additionally, Fortinet reserves the right to rely on passages from the prior art beyond those explicitly quoted or cited below.

**3. The Knowledge of Persons of Ordinary Skill in the Art**

As another example, a POSITA would have been motivated to combine or modify any of the disclosed prior art (including to form the specific exemplary combinations identified below in Section III.B) because it was within such person's knowledge to combine or modify the prior art to include various features omitted from any single prior art reference or combination of references. Such features include, but are not limited to, the following: single sign-on, authentication methods, malware detection, automated computer support, anomaly detection, dynamic bandwidth allocation, firewalls, traffic shaping/throttling.

**4. The Predictable Results Obtained in Combining the Different Elements of the Prior Art According to Known Methods**

As another example, a POSITA would have been motivated to form combinations based on any of the disclosed prior art to include features omitted from any single prior art reference or combination of references because doing so would have generated predictable results and could have been

accomplished according to known methods. Such features include, but are not limited to, each of the features identified in Section III.A.3, above.

**5. The Predictable Results Obtained in Simple Substitution of One Known Element for Another**

As another example, a POSITA would have been motivated to combine or modify the prior art (including to form the specific exemplary combinations identified below in Section III.B) because doing so would have involved substituting one feature for another feature known in the art and would have generated predictable results. Such features that could have been added by substitution include, but are not limited to, each of the features identified in Section III.A.3., above.

**6. The Use of a Known Technique to Improve Similar Devices, Methods or Products in the Same Way**

As another example, a POSITA would have been motivated to combine or modify the prior art (including to form the specific exemplary combinations identified below in Section III.B) because doing so would have used known features to improve similar devices, methods, or products (including but not limited to devices, methods, or products in or related to the field of network access control) in the same way, and would have generated predictable results. Such features include, but are not limited to, each of the features identified in Section III.A.3, above.

**7. The Predictable Results Obtained in Applying a Known Technique to a Known Device, Method, or Product Ready for Improvement**

As another example, a POSITA would have been motivated to combine or modify the prior art (including to form the specific exemplary combinations identified below in Section III.B) because doing so would have involved applying a known technique to improve a known device, method, or product (including but not limited to devices, methods, or products in or related to the field of network access control), and would have generated predictable results. Such features include, but are not limited to, each of the features identified in Section III.A.3, above.

#### 8. The Finite Number of Identified Predictable Solutions that Had a Reasonable Expectation of Success

As another example, a POSITA would have been motivated to combine or modify the prior art (including to form the specific exemplary combinations identified below in Section III.B) because doing so would have been obvious to try. Specifically, a POSITA would have recognized that, within the field of network access control (for example), there were a finite number of identified, predictable potential features that could solve a recognized need or problem, and a POSITA would have pursued incorporating these known features with a reasonable expectation of success. Such features include, but are not limited to, each of the features identified in Section III.A.3, above.

#### 9. Known Work in Various Technological Fields that Could be Applied to the Same or Different Technological Fields Based on Design Incentives or Other Market Forces.

As another example, a POSITA would have been motivated to combine or modify the prior art (including to form the specific exemplary combinations identified below in Section III.B), including the prior art references, which are in the same field of the Asserted Patents and each other (such as network access control), or in a different field, to include various features because doing so would have been prompted by design incentives or market forces, variations or principles applying such features that were known in the prior art, and doing so would have generated predictable results. Such design incentives or market forces include, but are not limited to, those identified by the Asserted Patents themselves and the prior art (discussed above in Sections III.A.1–III.A.8). Such features include, but are not limited to, each of the features identified in Section III.A.3, above.

### B. Exemplary Combinations and Motivations to Combine

#### 1. Exemplary Combinations re the '336 Patent (Chart A-1)

- To the extent Subbiah does not expressly disclose "determining whether the second request contains an authentication token," a POSITA would have found it obvious and would have been motivated to apply the teachings of Crandell and/or Hinton. For example, each of these references is in the same general technological field of access control systems, and a POSITA would have understood that the combination would

yield predictable results. Hinton and Crandell each teach using authentication tokens (or cookies) to transmit information about the authentication status of a computer/user, and a POSITA would have recognized that such tokens (or cookies) would have improved Subbiah's access control system by providing a known and predictable mechanism for transmitting state information. A POSITA would have understood that Subbiah's existing teachings—which look to the state of a user's authentication attempts—would have benefited from the implementation details taught by Crandell and/or Hinton. And a POSITA would have had reasonable success in implementing Subbiah's system using Crandell's and/or Hinton's teachings. *See* Section III.A, above.

**2. Exemplary Combinations re the '710 Patent (Charts B-1 through B-3 and Appendix B)**

- To the extent Roskind, Gleichauf or Bauer do not expressly disclose "rendering a web page to display on the client device from the network access gateway device, wherein the web page contains an offer for a user of the client device to perform an action in order to obtain unrestricted access to the Internet responsive to implementation of one of the plurality of quarantine control function of the client device" and "wherein the action requires the user to obtain and execute abnormal behavior scanning software from a server machine running at one of the one or more allowed network destination addresses," a POSITA would have been motivated to apply the teachings of Jung. For example, each of these references is in the same general field of network access control, and a POSITA would have understood that the combination would yield predictable results. For example, Bauer discloses that a suspicious device may be partially or wholly shut down until the issue is resolved, and Roskind discloses the server providing remediation options for an infected computer that has been quarantined. Gleichauf similarly discloses directing an infected computer to a remediator's website to fix the infection. Jung discloses implementation details for resolving the issue to restore access, including retrieving software to resolve the issue from a server. A POSITA would have

recognized the benefits of incorporating these implementation details in Bauer's system and would have been motivated to do so. And a POSITA would have had reasonable success in implementing Bauer's system using these teachings. *See* Section III.A, above.

- To the extent Roskind, Gleichauf or Bauer do not each expressly disclose "rendering a web page to display on the client device from the network access gateway device," a POSITA would have been motivated to apply the teachings of any other of Roskind, Gleichauf, and Bauer and/or Hoffberg '078, Hoffberg '996, and/or Short '894. For example, each of these references is in the same general field of network access control, and a POSITA would have understood that the combination would yield predictable results. For example, Roskind, Bauer, and Gleichauf each disclose redirecting a user to, e.g., a remediation site when an infection is detected. Short '894 and Hoffberg '078/'996 each provide implementation details on servers embedded within a gateway device itself. In particular, Short '894 discloses authentication servers used to get access to a broader network that may be hosted within the gateway device itself. A POSITA would have recognized the benefits of incorporating these implementation details in the systems of Roskind, Bauer, and Gleichauf, and would have been motivated to do so. And a POSITA would have had reasonable success in implementing these systems using those teachings. *See* Section III.A., above.

**3. Exemplary Combinations re the '639 Patent (Charts C-1 through C-4 and Appendix C)**

- To the extent Richmond does not disclose "redirecting the user to a login web page that requests user credentials" or "using the user credentials received from the user to authenticate the user," it would have been obvious to a POSITA to combine that with the Enterasys System, the Enterasys User Personalized Network White Paper, Short, Fuh, Lerner, and/or Wood. For example, each of these references is in the same general technological field of network management, and a POSITA would have understood that the combination would yield predictable results. Moreover, Richmond provides an express statement that the Enterasys User Personalized Network White Paper (which

describes the prior art Enterasys System) should be consulted for further detail on the access control method. Richmond specifies that the user will provide credentials that the system will use to authenticate that user. The Enterasys System, the Enterasys User Personalized Network White Paper, Short, Fuh, Lerner, and Wood all use a webpage-based login system that requests credentials from the user. A POSITA would have recognized that the webpage-based login system would have been simple and easy to use, both from the perspective of the user (who was familiar with webpage login systems and could use their pre-existing web browser instead of installing new software) and from the perspective of the network administrator (who could use pre-existing webservers and web browsers instead of deploying custom servers and software). A combination thus would be a combination of known elements to achieve a predictable result, for which a POSITA would have had a reasonable expectation of success. *See* Section III.A, above.

- To the extent that Richmond, Short, Fuh, or the Enterasys System (including the publications that describe it, such as the Enterasys User Personalized Network White Paper) do not disclose "the traffic conditioning module further comprises an interface master queue for controlling a flow of network traffic over a particular network interface," it would have been obvious to combine those with Teraslinna and/or Kadambi. For example, each of these references is in the same general technological field of network management and a POSITA would have understood that the combination would yield predictable results. Richmond, Short, Fuh, the Enterasys System, and the Enterasys User Personalized Network White Paper disclose that network infrastructure devices will receive traffic from user devices and regulate the flow of traffic to a network, such as a corporate intranet or the Internet. Teraslinna and Kadambi provide efficient algorithms that utilizes an interface master queue for controlling the flow of traffic from a user over a network interface. A POSITA would have recognized that Teraslinna's and/or Kadambi's algorithm and associated queue

would provide an efficient means of implementing the regulation of traffic in the other references. Use of such queue would have been a straightforward implementation detail well within the skill of a POSITA to implement, as well as a straightforward combination of known elements to achieve a predictable result, with reasonable probability of success. *See* Section III.A, above.

**4. Exemplary Combinations re the '983 Patent (Charts D-1 through D-11)**

- To the extent any of Hou, Callocchia, or Riddle do not disclose "an authentication database storing user profiles," it would have been obvious to a POSITA to combine each of those references with any one of the other references and/or Moran, Sitaraman, or Freed. For example, each of these references is in the same general technological field of network management, and a POSITA would have understood that the combination would yield predictable results. Hou, Callocchia, and Riddle dynamically update bandwidth allocations. Moran, Sitaraman, and Freed expressly tie bandwidth allocations to users' profiles, where those profiles have a number of attributes. A POSITA would have recognized that the dynamic bandwidth allocating methods disclosed in Hou, Callocchia, and Riddle would have benefited from having associated with them user profiles with many different attributes. And a POSITA would have had reasonable success in using the teachings in Hou and Callocchia in the systems of Moran, Sitaraman, or Freed. *See* Section III.A, above.
- To the extent any of Moran, Sitaraman, Ford, or Freed do not disclose or render obvious on their own "determining a second network bandwidth limit for the first user based on the first network bandwidth limit associated with each of the users and the one or more attributes associated with the first user;" it would have been obvious to a POSITA to combine each of those references with any one of the other references and/or Hou, Callocchia, or Riddle. For example, each of these references is in the same general technological field of network management, and a POSITA would have understood that the combination would yield predictable results. Moran, Sitaraman, Ford, and Freed all

deal with assigning bandwidth limits to a user based on a user's profile. Hou, Callocchia, and Riddle further teach dynamic bandwidth allocation where the bandwidth limits change for certain reasons. A POSITA would have recognized that the bandwidth allocating systems disclosed in Moran, Sitaraman, Ford, or Freed would have benefited from the dynamic adjustments taught by Hou, Callocchia, or Riddle and would have been motivated to apply those teachings to make the bandwidth allocation more tailored to different users' needs and updated on the fly. And a POSITA would have had reasonable success in using the teachings in Hou, Callocchia, and Riddle in the systems of Moran, Sitaraman, Ford, or Free. *See* Section III.A, above.

- Similarly to the extent any of Moran, Sitaraman, Ford, or Freed do not anticipate or render obvious a system that operates in a "first state" and a "second state" as the claim requires, again, it would have been obvious to combine any of these references or to combine with Hou, Callocchia, and/or Riddle, to adjust bandwidth dynamically and thereby enter into a "second state." As discussed above, a POSITA would have recognized that the bandwidth allocating systems disclosed in Moran, Sitaraman, Ford, or Freed would have benefited from the dynamic adjustments taught by Hou, Callocchia, or Riddle and would have been motivated to apply those teachings to make the bandwidth allocation more tailored to different users' needs and updated on the fly and to thereby go from a "first state" to a "second state." And a POSITA would have had reasonable success in using the teachings in Hou and Callocchia in the systems of Moran, Sitaraman, Ford, or Free. *See* Section III.A, above.
- To the extent Hou, Callocchia, or Riddle do not disclose "a second user at the first device," a "second user profile for the second user associated with the first device," or a "third network bandwidth limit for the second user," it would have been obvious to a POSITA to combine each of those references with any one of the other references and/or Moran, Sitaraman, or Freed. For example, each of these references is in the same general technological field of network management, and a POSITA would have

understood that the combination would yield predictable results. Hou, Riddle, and Callocchia dynamically update bandwidth allocations. Moran, Sitaraman, and Freed expressly tie bandwidth allocations to users' profiles, where those profiles have a number of attributes, but do not tie a given user to a given device. A POSITA would have recognized that the dynamic bandwidth allocating methods disclosed in Hou, Riddle, and Callocchia would have benefited from having associated with them user profiles (and not devices) so that a user may login from different devices, and conversely so that different users could login from the same device. And a POSITA would have had reasonable success in using the teachings in Hou, Riddle, and Callocchia in the systems of Moran, Sitaraman, Ford, or Free. *See* Section III.A, above.

**5. Exemplary Combinations re the '426 Patent (Charts E-1 through E-11)**

- To the extent Ebrahimi 1, Gong, Evidian, Azure Active Directory, MIIS, Oracle Identity Management, Open Directory, iSeries Server, or Burch do not disclose or render obvious on their own "supplying, by the machine, an authentication message for use by an identity service on behalf of the principal, the authentication message serves as a new authentication request and as a new authentication response for single sign-on access of the principal to the identity service and other services external or internal to the identity service," it would have been obvious to combine each of those references with Hinton 1 or Hinton 2. For example, each of these references is in the same general technological field of single sign on systems and a POSITA would have understood that the combination would yield predictable results. Ebrahimi 1, Evidian, Azure Active Directory, MIIS, Oracle Identity Management, Open Directory, iSeries Server, or Gong disclose supplying authentication messages for a single sign-on access of a principal to an identity service, and Hinton 1 and Hinton 2 provide examples of the content that would be included in such a message, including in the claimed manner. A POSITA would have understood that there are many different ways in which an authentication message can be formatted, and it would have been obvious to check how others are formatted for interoperability purposes. And, a POSITA would have had a reasonable expectation of success

in implementing the Hinton 1 and Hinton 2 messages as part of the systems in Ebrahimi 1, Evidian, Azure Active Directory, MIIS, Oracle Identity Management, Open Directory, iSeries Server, or Gong because it would have been a straightforward application of including the information in the authentication message and is well within the skill of a POSITA and would be easy to implement. *See* Section III.A, above.

- To the extent Evidian, Azure Active Directory, MIIS, Oracle Identity Management, Open Directory, iSeries Server, Gong, or Burch do not disclose or render obvious on their own "the identity service acts as a proxy for access sessions to the other services on behalf of the principal, the principal's access sessions occur indirectly through the identity service and transparently to the principal" or "the principal believing interactions are with the external service, which is one of the other services that the identity service controls access to," it would have been obvious to combine each of those references with Hinton 1, Hinton 2, or Ebrahimi 1. For example, each of these references is in the same general technological field of single sign on systems and a POSITA would have understood that the combination would yield predictable results. Evidian, Azure Active Directory, MIIS, Oracle Identity Management, Open Directory, iSeries Server, Gong, or Burch disclose a single sign-on process, including an identity service, and Hinton 1, Hinton 2, or Ebrahimi 1provide specific ways of doing so using a proxy that is transparent to the user. A POSITA would have understood that proxies are used in many circumstances to improve efficiencies and make things more convenient for the user. And, a POSITA would have had a reasonable expectation of success in implementing the proxies in Hinton 1, Hinton 2, or Ebrahimi 1 as part of the systems in Evidian, Azure Active Directory, MIIS, Oracle Identity Management, Open Directory, iSeries Server, Gong, or Burch because proxies well within the skill of a POSITA and would be easy to implement. *See* Section III.A, above.
- To the extent Hinton 1, Hinton 2, Ebrahimi 1, Evidian, Azure Active Directory, MIIS, Oracle Identity Management, Open Directory, iSeries Server, or Gong do not disclose or render obvious on their own "and a determination as to whether to use a single interaction or multiple

interactions for authentication of the principal to the other services is automatically communicated in the new authentication response," it would have been obvious to combine each of those references with Burch. For example, each of these references is in the same general technological field of single sign-on systems, and a POSITA would have understood that the combination would yield predictable results. Hinton 1, Hinton 2, Ebrahimi 1, Evidian, Azure Active Directory, MIIS, Oracle Identity Management, Open Directory, iSeries Server, or Gong disclose single sign-on systems, and Burch provides a way to provide additional security for such systems. A POSITA would have understood that there are certain applications in which additional security would have been desired, even in single sign-on systems, and Burch provides such a system that allows for multi-factor authentication in single sign-on systems. A POSITA would have recognized that there would still be a benefit in such a system because the user would not have to retype the password and, instead, would only need to complete the additional means of authentication. A POSITA further would have recognized the benefits of the flexibility provided by the description in Burch. And, a POSITA would have had a reasonable expectation of success in implementing the multi-factor authentication in Burch as part of the systems in Hinton 1, Hinton 2, Ebrahimi 1, Evidian, Azure Active Directory, MIIS, Oracle Identity Management, Open Directory, iSeries Server, or Gong because the processes described in Burch are well within the skill of a POSITA and would be easy to implement. *See* Section III.A, above.

- To the extent Hinton 1, Hinton 2, Ebrahimi 1, Evidian, Azure Active Directory, MIIS, Oracle Identity Management, Open Directory, iSeries Server, or Gong do not disclose or render obvious on their own "wherein supplying further includes adding a second authentication to a second redirection of the principal, wherein the second authentication represents authentication of the principal to the identity service and wherein the second redirection directs the principal to request a target service that is to be proxied on behalf of the principal from the identity service," it would have been obvious to combine each of those references with Burch. For example, each of these references is in the same general technological field of single sign-on systems Hinton 1,

Hinton 2, Ebrahimi 1, Evidian, Azure Active Directory, MIIS, Oracle Identity Management, Open Directory, iSeries Server, or Gong disclose single sign-on systems, and Burch provides a way to provide additional security for such systems. A POSITA would have understood that there are certain applications in which additional security would have been desired, even in single sign-on systems, and Burch provides such a system that allows for multi-factor authentication in single sign-on systems. A POSITA would have recognized that there would still be a benefit in such a system because the user would not have to retype the password and, instead, would only need to complete the additional means of authentication. A POSITA further would have recognized the benefits of the flexibility provided by the description in Burch. And, a POSITA would have had a reasonable expectation of success in implementing the multi-factor authentication in Burch as part of the systems in Hinton 1, Hinton 2, Ebrahimi 1, Evidian, Azure Active Directory, MIIS, Oracle Identity Management, Open Directory, iSeries Server, or Gong because the processes described in Burch are well within the skill of a POSITA and would be easy to implement. *See* Section III.A, above.

- To the extent Evidian, Azure Active Directory, MIIS, Oracle Identity Management, Open Directory, iSeries Server, or Gong does not disclose or render obvious on their own "wherein supplying further includes representing the new authentication response as a first authentication token that informs the identity service that the principal is currently already properly authenticated to the processing associated with the method," it would have been obvious to combine each of those references with Hinton 1, Hinton 2, Ebrahimi, or Burch. For example, each of these references is in the same general technological field of single sign-on systems, and a POSITA would have understood that the combination would yield predictable results. Evidian, Azure Active Directory, MIIS, Oracle Identity Management, Open Directory, iSeries Server, or Gong discloses single sign-on using authentication messages, and Hinton 1, Hinton 2, Ebrahimi, or Burch explain that authentication tokens are often used for this purpose. A POSITA would have understood that there are many different ways in which an authentication message can be formatted, and it would have been obvious to check how others are formatted

for interoperability purposes. And, a POSITA would have had a reasonable expectation of success in implementing the tokens from Hinton 1, Hinton 2, Ebrahimi, or Burch as part of the system in Evidian, Azure Active Directory, MIIS, Oracle Identity Management, Open Directory, iSeries Server, or Gong because authentication tokens are well within the skill of a POSITA and would be easy to implement. *See* Section III.A, above.

- To the extent Hinton 1, Hinton 2, Ebrahimi 1, Evidian, Azure Active Directory, MIIS, Oracle Identity Management, Open Directory, iSeries Server, or Gong do not disclose or render obvious on their own "wherein supplying further includes representing the new authentication response as an instruction to the identity service to enforce its own independent authentication with the principal before considering the principal authenticated to the identity service," it would have been obvious to combine each of those references with Burch. Hinton 1, Hinton 2, Ebrahimi 1, Evidian, Azure Active Directory, MIIS, Oracle Identity Management, Open Directory, iSeries Server, or Gong disclose single sign-on systems, and Burch provides a way to provide additional security for such systems. A POSITA would have understood that there are certain applications in which additional security would have been desired, even in single sign-on systems, and Burch provides such a system that allows for multi-factor authentication in single sign-on systems. A POSITA would have recognized that there would still be a benefit in such a system because the user would not have to retype the password and, instead, would only need to complete the additional means of authentication. A POSITA further would have recognized the benefits of the flexibility provided by the description in Burch. And, a POSITA would have had a reasonable expectation of success in implementing the multi-factor authentication in Burch as part of the systems in Hinton 1, Hinton 2, Ebrahimi 1, Evidian, Azure Active Directory, MIIS, Oracle Identity Management, Open Directory, iSeries Server, or Gong because the processes described in Burch are well within the skill of a POSITA and would be easy to implement. *See* Section III.A, above.
- To the extent Evidian, Azure Active Directory, MIIS, Oracle Identity Management, Open Directory, iSeries Server, Ebrahimi 1, or Gong do not disclose or render obvious on their own

"comprising, interacting, by the machine, with the principal via a World-Wide Web (WWW) browser over the Internet using at least one of a Security Assertion Markup Language (SAML), a Liberty Alliance markup language, and Web Services (WS) Foundation markup language," it would have been obvious to combine each of those references with Hinton 1, Hinton, 2, or Burch. For example, each of these references is in the same general technological field of single sign-on systems, and a POSITA would have understood that the combination would yield predictable results. Evidian, Azure Active Directory, MIIS, Oracle Identity Management, Open Directory, iSeries Server, Ebrahimi 1, or Gong disclose single sign on systems in which security measures are exchanged between different devices, and Hinton 1, Hinton, 2, or Burch provide a specific means of doing that exchange using SAML, which was a well-known standard for exchanges like these. A POSITA would have understood that there are many different ways in which an authentication message can be formatted, and it would have been obvious to check how others are formatted for interoperability purposes. And, a POSITA would have had a reasonable expectation of success in implementing SAML as part of the systems in Evidian, Azure Active Directory, MIIS, Oracle Identity Management, Open Directory, iSeries Server, Ebrahimi 1, or Gong because SAML is well within the skill of a POSITA and would be easy to implement. *See* Section III.A, above.

**6. Exemplary Combinations re the '936 Patent (Charts F-1 through F-5 and Appendix F)**

- To the extent McCallam, Eastman, or Lieblich do not disclose or render obvious on their own "receiving snapshots from a plurality of computers within a population of computers, wherein individual snapshots include data indicating a state of a respective computer," it would have been obvious to combine each of those references with Honig, Vinberg, or Evoy. For example, each of these references is in the same general technological field of anomaly detection and automated computer support and a POSITA would have understood that the combination would yield predictable results. McCallam, Eastman, or Lieblich disclose using certain data from multiple machines in a network to help identify anomalies, and Honig, Vinberg, or Evoy provide specific

examples of the type of data that would be helpful, including the claimed snapshots. A POSITA would have understood that additional information would be helpful in detecting anomalies and would have understood that the data in Honig, Vinberg, and Evoy could be efficiently collected and used. And, a POSITA would have had a reasonable expectation of success in implementing the snapshots in Honig, Vinberg, and Evoy as part of the systems in McCallam, Eastman, or Lieblich because collecting data from computers in a network is well within the skill of a POSITA and would be easy to implement. *See* Section III.A, above.

- To the extent McCallam, Eastman, Vinberg, or Lieblich do not disclose or render obvious on their own "wherein individual snapshots include data associated with at least one of: system files, application files, a registry entry, a performance counter, a process, a communication port, a hardware configuration, a log file, a running task, services, and network connections," it would have been obvious to combine each of those references with Honig or Evoy. McCallam, Eastman, Vinberg, or Lieblich disclose using certain data from multiple machines in a network to help identify anomalies, and Honig or Evoy provide specific examples of the type of data that would be helpful, including a snapshot as claimed. A POSITA would have understood that additional information would be helpful in detecting anomalies and would have understood that the data in Honig and Evoy could be efficiently collected and used. And, a POSITA would have had a reasonable expectation of success in implementing the snapshots in Honig and Evoy as part of the systems in McCallam, Eastman, Vinberg, or Lieblich because collecting data from computers in a network is well within the skill of a POSITA and would be easy to implement. *See* Section III.A, above.
- To the extent Honig or Vinberg do not disclose or render obvious on their own "wherein the adaptive reference model is generated to include a value layer that determines whether an asset value contained in a snapshot is anomalous," it would have been obvious to combine each of those references with Eastham, McCallam, Evoy, or Lieblich. For example, each of these references is in the same general technological field of anomaly detection and automated computer support, and a POSITA would have understood that the combination would yield

predictable results. Honig and Vinberg disclose anomaly detection systems with a comparison between a snapshot and an adaptive reference model, and Eastham, McCallam, Evoy, or Lieblich provide different types of comparisons and models. It would have been obvious to a POSITA to check other comparisons and models that are used in the industry to ensure that the system works efficiently and eliminates as many false positives and false negatives as possible And, a POSITA would have had a reasonable expectation of success in implementing the Eastham, McCallam, Evoy, or Lieblich techniques as part of the systems in Vinberg and Honig because data comparisons and models are well within the skill of a POSITA and would be easy to implement. *See* Section III.A, above.

- To the extent Honig or Vinberg do not disclose or render obvious on their own "wherein the adaptive reference model is generated to include a cluster layer that tracks relationships between assets and identifies an anomaly in response to an asset being unexpectedly absent from or present in a set of assets in a snapshot," it would have been obvious to combine each of those references with Eastham, McCallam, Evoy, or Lieblich. For example, each of these references is in the same general technological field of anomaly detection and automated computer support, and a POSITA would have understood that the combination would yield predictable results. Honig and Vinberg disclose anomaly detection systems with a comparison between a snapshot and an adaptive reference model, and Eastham, McCallam, Evoy, or Lieblich provide different types of comparisons and models. It would have been obvious to a POSITA to check other comparisons and models that are used in the industry to ensure that the system works efficiently and eliminates as many false positives and false negatives as possible. And, a POSITA would have had a reasonable expectation of success in implementing the Eastham, McCallam, Evoy, or Lieblich techniques as part of the systems in Vinberg and Honig because data comparisons and models are well within the skill of a POSITA and would be easy to implement. *See* Section III.A, above.
- To the extent Honig or Vinberg do not disclose or render obvious on their own "wherein the adaptive reference model is generated to include a profile layer that identifies anomalies in

response to violation of relationships of clusters of assets in a snapshot," it would have been obvious to combine each of those references with Eastham, McCallam, Evoy, or Lieblich. For example, each of these references is in the same general technological field of anomaly detection and automated computer support, and a POSITA would have understood that the combination would yield predictable results. Honig and Vinberg disclose anomaly detection systems with a comparison between a snapshot and an adaptive reference model, and Eastham, McCallam, Evoy, or Lieblich provide different types of comparisons and models. It would have been obvious to a POSITA to check other comparisons and models that are used in the industry to ensure that the system works efficiently and eliminates as many false positives and false negatives as possible. And, a POSITA would have had a reasonable expectation of success in implementing the Eastham, McCallam, Evoy, or Lieblich techniques as part of the systems in Vinberg and Honig because data comparisons and models are well within the skill of a POSITA and would be easy to implement. *See* Section III.A, above.

- To the extent Honig, Eastham, Lieblich, Vinberg, or McCallam do not disclose or render obvious on their own "comparing the anomaly to a recognition filter to diagnose a trouble condition on the at least one of the computers; and in the event of a trouble condition, generating an automated response to the trouble condition," it would have been obvious to combine each of those references with Oliphant, Oliphant Provisional, Largman, or Gertner. For example, each of these references is in the same general technological field of anomaly detection and automated computer support, and a POSITA would have understood that the combination would yield predictable results. Honig, Eastham, Lieblich, Vinberg, or McCallam discloses methods for detecting malware or anomalies in devices within a managed network and, when identified, raising an alert or an alarm. A POSITA would have understood or found obvious that the alert or alarm in these systems would trigger the expectation that some action be taken in response to the alert, or else there would be no point to the alert. For example, a POSITA would have been motivated to take further remediation steps in response to the alert to prevent any further damage to the network and prevent propagation of the malware to other computers. A POSITA,

therefore, would have been motivated to look for other real-time detection systems to see what remediation steps could be taken. A POSITA would have understood that a network administrator could take multiple different actions in response to the alert, including, for example, limit network access of the device causing the alert or install security patches to address the problem. Oliphant, Oliphant Provisional, Largman, or Gertner provide different remediation techniques that would have been obviously beneficial to implement in the systems in Honig, Eastham, Lieblich, Vinberg, or McCallam. A POSITA would have recognized that it would have been beneficial to combine the remediation techniques disclosed in Oliphant, Oliphant Provisional, Largman, or Gertner with the detection system disclosed in Honig, Eastham, Lieblich, Vinberg, or McCallam to prevent any further damage to the network and prevent propagation of the malware to other computers. In other words, the combinations disclose a system that generates alerts in response to detected anomalies and a remediation system that responds to those alerts by taking appropriate action. And a POSITA would have had a reasonable expectation of success in doing so. A POSITA would have understood that, once an attack is detected by the system in Honig, Eastham, Lieblich, Vinberg, or McCallam, the attack could be looked up in the remediation database disclosed in Oliphant, Oliphant Provisional, Largman, or Gertner to determine what remediation techniques are available for that particular attack. It would have been obvious to a POSITA that the attacks detected by Honig, Eastham, Lieblich, Vinberg, or McCallam are often linked to vulnerabilities as well. It would further have been obvious to a POSITA to try to determine what vulnerability is targeted by a detected attack. *See* Section III.A, above.

- To the extent Honig, Eastham, Lieblich, Vinberg, or McCallam do not disclose or render obvious on their own "wherein the automated response is a generic response not specific to a particular asset of the at least one computer, and wherein the method further comprises: sending the generic response and a set of anomalies found in the snapshot to the at least one computer, the set of anomalies indicating assets of the at least one computer whose states are anomalous; and applying the generic response to the anomalous assets to correct the trouble condition," it would

have been obvious to combine each of those references with Oliphant, Oliphant Provisional, Largman, or Gertner. For example, each of these references is in the same general technological field of anomaly detection and automated computer support, and a POSITA would have understood that the combination would yield predictable results. Honig, Eastham, Lieblich, Vinberg, or McCallam discloses methods for detecting malware or anomalies in devices within a managed network and, when identified, raising an alert or an alarm. A POSITA would have understood or found obvious that the alert or alarm in these systems would trigger the expectation that some action be taken in response to the alert, or else there would be no point to the alert. For example, a POSITA would have been motivated to take further remediation steps in response to the alert to prevent any further damage to the network and prevent propagation of the malware to other computers. A POSITA, therefore, would have been motivated to look for other real-time detection systems to see what remediation steps could be taken. A POSITA would have understood that a network administrator could take multiple different actions in response to the alert, including, for example, limit network access of the device causing the alert or install security patches to address the problem. Oliphant, Oliphant Provisional, Largman, or Gertner provide different remediation techniques that would have been obviously beneficial to implement in the systems in Honig, Eastham, Lieblich, Vinberg, or McCallam. A POSITA would have recognized that it would have been beneficial to combine the remediation techniques disclosed in Oliphant, Oliphant Provisional, Largman, or Gertner with the detection system disclosed in Honig, Eastham, Lieblich, Vinberg, or McCallam to prevent any further damage to the network and prevent propagation of the malware to other computers. In other words, the combinations disclose a system that generates alerts in response to detected anomalies and a remediation system that responds to those alerts by taking appropriate action. And a POSITA would have had a reasonable expectation of success in doing so. A POSITA would have understood that, once an attack is detected by the system in Honig, Eastham, Lieblich, Vinberg, or McCallam, the attack could be looked up in the remediation database disclosed in Oliphant, Oliphant Provisional, Largman, or Gertner to determine what remediation techniques are

available for that particular attack. It would have been obvious to a POSITA that the attacks detected by Honig, Eastham, Lieblich, Vinberg, or McCallam are often linked to vulnerabilities as well. It would further have been obvious to a POSITA to try to determine what vulnerability is targeted by a detected attack. *See* Section III.A, above.

- To the extent Honig, Eastham, Lieblich, Vinberg, or McCallam do not disclose or render obvious on their own " wherein the generic response includes at least one of: installing a missing software component, removing an undesirable software component, and restoring an incorrect registry setting," it would have been obvious to combine each of those references with Oliphant, Oliphant Provisional, Largman, or Gertner. For example, each of these references is in the same general technological field of anomaly detection and automated computer support, and a POSITA would have understood that the combination would yield predictable results. Honig, Eastham, Lieblich, Vinberg, or McCallam discloses methods for detecting malware or anomalies in devices within a managed network and, when identified, raising an alert or an alarm. A POSITA would have understood or found obvious that the alert or alarm in these systems would trigger the expectation that some action be taken in response to the alert, or else there would be no point to the alert. For example, a POSITA would have been motivated to take further remediation steps in response to the alert to prevent any further damage to the network and prevent propagation of the malware to other computers. A POSITA, therefore, would have been motivated to look for other real-time detection systems to see what remediation steps could be taken. A POSITA would have understood that a network administrator could take multiple different actions in response to the alert, including, for example, limit network access of the device causing the alert or install security patches to address the problem. Oliphant, Oliphant Provisional, Largman, or Gertner provide different remediation techniques that would have been obviously beneficial to implement in the systems in Honig, Eastham, Lieblich, Vinberg, or McCallam. A POSITA would have recognized that it would have been beneficial to combine the remediation techniques disclosed in Oliphant, Oliphant Provisional, Largman, or Gertner with the detection system disclosed in Honig, Eastham, Lieblich, Vinberg, or McCallam to prevent

any further damage to the network and prevent propagation of the malware to other computers. In other words, the combinations disclose a system that generates alerts in response to detected anomalies and a remediation system that responds to those alerts by taking appropriate action. And a POSITA would have had a reasonable expectation of success in doing so. A POSITA would have understood that, once an attack is detected by the system in Honig, Eastham, Lieblich, Vinberg, or McCallam, the attack could be looked up in the remediation database disclosed in Oliphant, Oliphant Provisional, Largman, or Gertner to determine what remediation techniques are available for that particular attack. It would have been obvious to a POSITA that the attacks detected by Honig, Eastham, Lieblich, Vinberg, or McCallam are often linked to vulnerabilities as well. It would further have been obvious to a POSITA to try to determine what vulnerability is targeted by a detected attack. *See* Section III.A, above.

- To the extent Honig, Eastham, Lieblich, Vinberg, or McCallam do not disclose or render obvious on their own "wherein the recognition filter comprises a particular pattern of anomalies that indicates the presence of a particular root cause condition or a generic class of conditions," it would have been obvious to combine each of those references with Oliphant, Oliphant Provisional, Largman, or Gertner. For example, each of these references is in the same general technological field of anomaly detection and automated computer support and a POSITA would have understood that the combination would yield predictable results. Honig, Eastham, Lieblich, Vinberg, or McCallam discloses methods for detecting malware or anomalies in devices within a managed network and, when identified, raising an alert or an alarm. A POSITA would have understood or found obvious that the alert or alarm in these systems would trigger the expectation that some action be taken in response to the alert, or else there would be no point to the alert. For example, a POSITA would have been motivated to take further remediation steps in response to the alert to prevent any further damage to the network and prevent propagation of the malware to other computers. A POSITA, therefore, would have been motivated to look for other real-time detection systems to see what remediation steps could be taken. A POSITA would have understood that a network administrator could take multiple different actions in

response to the alert, including, for example, limit network access of the device causing the alert or install security patches to address the problem. Oliphant, Oliphant Provisional, Largman, or Gertner provide different remediation techniques that would have been obviously beneficial to implement in the systems in Honig, Eastham, Lieblich, Vinberg, or McCallam. A POSITA would have recognized that it would have been beneficial to combine the remediation techniques disclosed in Oliphant, Oliphant Provisional, Largman, or Gertner with the detection system disclosed in Honig, Eastham, Lieblich, Vinberg, or McCallam to prevent any further damage to the network and prevent propagation of the malware to other computers. In other words, the combinations disclose a system that generates alerts in response to detected anomalies and a remediation system that responds to those alerts by taking appropriate action. And a POSITA would have had a reasonable expectation of success in doing so. A POSITA would have understood that, once an attack is detected by the system in Honig, Eastham, Lieblich, Vinberg, or McCallam, the attack could be looked up in the remediation database disclosed in Oliphant, Oliphant Provisional, Largman, or Gertner to determine what remediation techniques are available for that particular attack. It would have been obvious to a POSITA that the attacks detected by Honig, Eastham, Lieblich, Vinberg, or McCallam are often linked to vulnerabilities as well. It would further have been obvious to a POSITA to try to determine what vulnerability is targeted by a detected attack. *See* Section III.A, above.

- To the extent Honig, Eastham, Lieblich, Vinberg, or McCallam do not disclose or render obvious on their own "comparing a plurality of anomalies associated with a particular snapshot with a recognition filter to diagnose a trouble condition; and diagnosing a trouble condition on the at least one of the computers in response to at least a subset of the plurality of anomalies matching information in the recognition filter," it would have been obvious to combine each of those references with Oliphant, Oliphant Provisional, Largman, or Gertner. For example, each of these references is in the same general technological field of anomaly detection and automated computer support, and a POSITA would have understood that the combination would yield predictable results. Honig, Eastham, Lieblich, Vinberg, or McCallam discloses methods for

detecting malware or anomalies in devices within a managed network and, when identified, raising an alert or an alarm. A POSITA would have understood or found obvious that the alert or alarm in these systems would trigger the expectation that some action be taken in response to the alert, or else there would be no point to the alert. For example, a POSITA would have been motivated to take further remediation steps in response to the alert to prevent any further damage to the network and prevent propagation of the malware to other computers. A POSITA, therefore, would have been motivated to look for other real-time detection systems to see what remediation steps could be taken. A POSITA would have understood that a network administrator could take multiple different actions in response to the alert, including, for example, limit network access of the device causing the alert or install security patches to address the problem. Oliphant, Oliphant Provisional, Largman, or Gertner provide different remediation techniques that would have been obviously beneficial to implement in the systems in Honig, Eastham, Lieblich, Vinberg, or McCallam. A POSITA would have recognized that it would have been beneficial to combine the remediation techniques disclosed in Oliphant, Oliphant Provisional, Largman, or Gertner with the detection system disclosed in Honig, Eastham, Lieblich, Vinberg, or McCallam to prevent any further damage to the network and prevent propagation of the malware to other computers. In other words, the combinations disclose a system that generates alerts in response to detected anomalies and a remediation system that responds to those alerts by taking appropriate action. And a POSITA would have had a reasonable expectation of success in doing so. A POSITA would have understood that, once an attack is detected by the system in Honig, Eastham, Lieblich, Vinberg, or McCallam, the attack could be looked up in the remediation database disclosed in Oliphant, Oliphant Provisional, Largman, or Gertner to determine what remediation techniques are available for that particular attack. It would have been obvious to a POSITA that the attacks detected by Honig, Eastham, Lieblich, Vinberg, or McCallam are often linked to vulnerabilities as well. It would further have been obvious to a POSITA to try to determine what vulnerability is targeted by a detected attack. *See* Section III.A, above.

#### 7. Exemplary Combinations re the '282 Patent (Charts G-1 through G-4 and Appendix G)

- To the extent any of Joyce, Villa, Coss, and/or Swander does not explicitly disclose "wherein the set of firewall rules is dynamically self-configurable during runtime without operator interaction," "wherein the set of firewall rules comprises a plurality of chains of rules forming various paths through a hierarchical structure, and wherein the hierarchical structure comprises defined places for dynamically updating the set of firewall rules during runtime," "wherein dynamically updating the set of firewall rules during runtime further comprises, during runtime, adding a rule to the set of firewall rules, deleting a rule from the set of firewall rules, or modifying a rule in the set of firewall rules without operator interaction," and/or "dynamically updating the set of firewall rules during runtime without operator interaction," a POSITA would have been motivated to combine each of those reference with any other of Joyce, Villa, Coss, Swander, Haberlan, Wang, Buddhikot, Linux FAQ, Iptables Basics NHF, Cheswick, and/or Jungck. Each of these references is in the same general field of endeavor, processing packets through a firewall, and each discloses known implementation details on structuring rules, for example, as hierarchical chains, and dynamically updating rules during runtime. Further, these references also teach the use of iptables and ipchains—known prior art implementations in Linux—that form Applicant Admitted Prior Art and confirm that the structuring of rules as hierarchical structures with defined places to insert/delete rules was known in the art. A POSITA would have recognized the benefits of incorporating these implementation details into each of Joyce, Villa, Coss, and/or Swander, and would have been motivated to do so. And a POSITA would have had reasonable success in implementing each of these systems using the respective teachings of the prior art. *See* Section III.A, above.
- To the extent any of Joyce, Villa, Coss, and/or Swander does not explicitly disclose "conditioning the packet based on the set of firewall rules" and/or "rewriting a portion of a network packet header associated with the packet," a POSITA would have been motivated to combine each of those references with any of Coss, Jungck, and/or Fink. Each of these references is in the same general field of endeavor, processing packets through a firewall, and

Coss, Jungck, and Fink each disclose implementation details for modifying packet headers when a firewall accepts, re-routes, etc., an incoming or outgoing packet. A POSITA would have recognized the benefits of these implementation details and would have been motivated to do so with a reasonable expectation of success. *See* Section III.A, above.

**8. Exemplary Combinations re the '153 Patent (Charts H-1 through H-11)**

- To the extent any of Hou, Riddle, or Callocchia do not disclose "wherein the user bandwidth allocation profile contains an arbitrary number of attributes specifying bandwidth limitations for the first user," it would have been obvious to a POSITA to combine each of those references with any one of the other references and/or Moran, Freed, or Sitaraman. For example, each of these references is in the same general technological field of network management, and a POSITA would have understood that the combination would yield predictable results. Hou, Riddle, and Callocchia dynamically update bandwidth allocations. Moran, Freed, and Sitaraman expressly tie bandwidth allocations to users' profiles, where those profiles have a number of attributes. A POSITA would have recognized that the dynamic bandwidth allocating methods disclosed in Hou, Riddle and Callocchia would have benefited from having associated with them user profiles with many different attributes. And a POSITA would have had reasonable success in using the teachings in Hou, Riddle, and Callocchia in the systems of Moran, Sitaraman, or Freed. *See* Section III.A, above.
- To the extent any of Moran, Sitaraman, Ford, or Freed do not disclose or render obvious on their own "dynamically updating the network bandwidth for said first user utilizing said at least one traffic control rule associated with said first user" it would have been obvious to a POSITA to combine each of those references with any one of the other references and/or Hou, Reed, or Callocchia. For example, each of these references is in the same general technological field of network management, and a POSITA would have understood that the combination would yield predictable results. Moran, Sitaraman, Ford, and Freed all deal with assigning bandwidth limits to a user based on a user's

profile. Hou, Riddle, and Callocchia further teach dynamic bandwidth allocation, where the bandwidth limits change for certain reasons. A POSITA would have recognized that the bandwidth allocating systems disclosed in Moran, Sitaraman, Ford, or Freed would have benefited from the dynamic adjustments taught by Hou, Riddle, or Callocchia and would have been motivated to apply those teachings to make the bandwidth allocation more tailored to different users' needs and updated on the fly. And a POSITA would have had reasonable success in using the teachings in Hou, Riddle, and Callocchia in the systems of Moran, Sitaraman, Ford, or Freed. *See* Section III.A, above.

- To the extent any of Hou, Riddle, or Callocchia do not disclose "indexing said user specific rules utilizing," "filling in missing attribute values with default values," or "mapping attributes in said user bandwidth allocation profile for said first user of at least one traffic control rule" it would have been obvious to a POSITA to combine each of those references with any one of the other references and/or Moran, Freed, or Sitaraman. For example, each of these references is in the same general technological field of network management, and a POSITA would have understood that the combination would yield predictable results. Hou, Riddle, and Callocchia dynamically update bandwidth allocations. Moran, Freed, and Sitaraman expressly tie bandwidth allocations to users' profiles, where those profiles have a number of attributes. A POSITA would have recognized that the dynamic bandwidth allocating methods disclosed in Hou, Riddle, and Callocchia would have benefited from having associated with them user profiles with many different attributes. And a POSITA would have had reasonable success in using the teachings in Hou, Riddle, and Callocchia in the systems of Moran, Sitaraman, or Freed. *See* Section III.A, above.

#### 9. Exemplary Combinations re the '697 Patent (Charts I-1 through I-8 and Appendix I)

- To the extent Deridder do not disclose or render obvious on their own "a method of network based malware detection in a service provider network," "a system for network based malware

detection in a service provider network," or "a computer readable memory containing instructions for network based malware detection in a service provider network," it would have been obvious to combine Deridder with Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, and/or Lee. For example, each of these references is in the same general technological field of malware and intrusion detection, and a POSITA would have understood that the combination would yield predictable results. Deridder actually discloses that its system would be useful in services "such as network monitoring, targeted advertising, ***malware detection*** etc." Deridder, ¶ 22. In doing so, Deridder recognizes that a POSITA would commonly add malware detection services to the service provider side of the NAT. When this happens, Deridder further recognizes that its technique of OS fingerprinting would be helpful to identify the computer connecting through the NAT with specificity, since all devices connecting through the NAT will have the same network address on the service provider side. It would therefore have been obvious to a POSITA to add malware detection to the service provider's network and use the OS fingerprinting in Deridder based upon Deridder's explicit recognition of this. Deridder, ¶ 22; And, since Deridder does not detail how to set up such a malware detection system, a POSITA would have turned to references in that field. Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, and/or Lee are examples of these types of references. Furthermore, a POSITA would have had a reasonable expectation of success implementing these malware detection systems in the NAT-based system disclosed in Deridder for multiple reasons. For example, like the traffic inspection device in Deridder, the systems operate on network components that see all of the traffic passing through a network as part of a service provider network. The traffic inspection device in Deridder similarly inspects traffic passing through the NAT in a service provider network. A POSITA, therefore, would have known that the malware detection systems in Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, and/or Lee could be combined with the NAT-based system in Deridder with only trivial modifications to identify devices in the local area network. Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, and/or Lee all operate on a service provider network or the equivalent. And, a POSITA would have been motivated to use both OS fingerprinting and the User-Agent field as a

cross-check to ensure that the OS ID of the mobile device is properly identified. A POSITA would know that each method could be prone to errors or failure. And a POSITA would understand the importance of correctly identifying the OS because it would have been obvious that malware may only infect certain operating systems. *See* Section III.A, above.

- To the extent Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, and/or Lee do not disclose or render obvious on their own "receiving one or more transmission control protocol (TCP) packets originating from an access device coupled to the service provider network, the one or more TCP packets defining a TCP session between a computing device coupled to the access device, and a destination coupled to the service provider network," it would have been obvious to combine each of those references with Deridder. For example, each of these references is in the same general technological field of malware and intrusion detection, and a POSITA would have understood that the combination would yield predictable results. Although certain references disclose and/or render obvious extracting the OS type from the User-Agent field, a POSITA would have understood, however, that clients may sometimes not include OS information in the User-Agent field and would have been motivated to look for other methods of obtaining the OS type, especially where it is not included in the User-Agent field. OS fingerprinting was one well-known way to do so that was readily known to a POSITA since the 1990s. Deridder discloses performing OS fingerprinting using, for example, "IP and TCP header fields from the initial TCP synchronization (SYN) packet of a connection to provide a unique signature or 'fingerprint' of the OS that generated the packet." Deridder, ¶ 31. Deridder even mentions that this could be useful in services "such as network monitoring, targeted advertising, malware detection etc." *Id.*, ¶ 22. In other words, Deridder explicitly teaches using its OS fingerprinting technique in the exact systems Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, and/or Lee. Furthermore, a POSITA would have been motivated to use both OS fingerprinting and the User-Agent field as a cross-check to ensure that the OS ID of the mobile device is properly identified. A POSITA would know that each method could be prone to errors or failure. And a POSITA would

understand the importance of correctly identifying the OS because it would have been obvious that malware may only work on certain OS. *See* Section III.A, above.

- To the extent Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, or Zuk do not disclose or render obvious on their own "determining an operating system identifier (OS ID) associated with the TCP session and the computing device," it would have been obvious to combine each of those references with Lee, Deridder, and/or RFC 2616. For example, each of these references is in the same general technological field of malware and intrusion detection, and a POSITA would have understood that the combination would yield predictable results. For example, each of these references is in the same general technological field of malware and intrusion detection and a POSITA would have understood that the combination would yield predictable results. A POSITA would have been motivated to combine the system in Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, or Zuk with that in Lee, Deridder, and/or RFC 2616 because Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, or Zuk teach or render obvious tying malware to a specific OS. E.g., Tuvell, ¶ 49. A POSITA would also have understood that OS type is useful information to link with the virus name because viruses commonly target only specific operating systems. A POSITA further would have been motivated to determine the OS type without receiving it from the mobile device in the network to reduce network traffic and make the network analyzer less dependent upon client input. In other words, a POSITA would have been motivated to look for ways to determine the OS type. A POSITA further would have recognized that it would be beneficial to determine the OS type based on the network traffic. A POSITA, therefore, would have been motivated to look for a system that determines the OS based upon the network traffic, and Lee, Deridder, and/or RFC 2616 disclose such systems. And, because a POSITA would have had a general familiarity with the HTTP specification, a POSITA would have understood that the OS information can be extracted from the User-Agent field, in which clients disclose their OS type.
- Although certain references disclose and/or render obvious extracting the OS type from the User-Agent field, a POSITA would have understood, however, that clients may sometimes not include

OS information in the User-Agent field and would have been motivated to look for other methods of obtaining the OS type, especially where it is not included in the User-Agent field. OS fingerprinting was one well-known way to do so that was readily known to a POSITA since the 1990s. Deridder discloses performing OS fingerprinting using, for example, "IP and TCP header fields from the initial TCP synchronization (SYN) packet of a connection to provide a unique signature or 'fingerprint' of the OS that generated the packet." Deridder, ¶ 31. Deridder even mentions that this could be useful in services "such as network monitoring, targeted advertising, malware detection etc." *Id.*, ¶ 22. In other words, Deridder explicitly teaches using its OS fingerprinting technique in the exact systems Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, and/or Lee. Furthermore, a POSITA would have been motivated to use both OS fingerprinting and the User-Agent field as a cross-check to ensure that the OS ID of the mobile device is properly identified. A POSITA would know that each method could be prone to errors or failure. And a POSITA would understand the importance of correctly identifying the OS because it would have been obvious that malware may only work on certain OS. *See* Section III.A, above. *See* Section III.A, above.

- To the extent Deridder do not disclose or render obvious on their own "determining if malware is present in the TCP session and an associated malware ID by comparing a malware signature to the one or more TCP packets," it would have been obvious to combine each of those references with Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, and/or Lee. For example, each of these references is in the same general technological field of malware and intrusion detection, and a POSITA would have understood that the combination would yield predictable results. Deridder actually discloses that its system would be useful in services "such as network monitoring, targeted advertising, ***malware detection*** etc." Deridder, ¶ 22. In doing so, Deridder recognizes that a POSITA would commonly add malware detection services to the service provider side of the NAT. When this happens, Deridder further recognizes that its technique of OS fingerprinting would be helpful to identify the computer connecting through the NAT with specificity, since all devices connecting through the NAT will have the same network address on the service provider

side. It would therefore have been obvious to a POSITA to add malware detection to the service provider's network and use the OS fingerprinting in Deridder based upon Deridder's explicit recognition of this. Deridder, ¶ 22; And, since Deridder does not detail how to set up such a malware detection system, a POSITA would have turned to references in that field. Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, and/or Lee are examples of these types of references. Furthermore, a POSITA would have had a reasonable expectation of success implementing these malware detection systems in the NAT-based system disclosed in Deridder for multiple reasons. For example, like the traffic inspection device in Deridder, the systems operate on network components that see all of the traffic passing through a network as part of a service provider network. The traffic inspection device in Deridder similarly inspects traffic passing through the NAT in a service provider network. A POSITA, therefore, would have known that the malware detection systems in Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, and/or Lee could be combined with the NAT-based system in Deridder with only trivial modifications to identify devices in the local area network. Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, and/or Lee all operate on a service provider network or the equivalent. And, a POSITA would have been motivated to use both OS fingerprinting and the User-Agent field as a cross-check to ensure that the OS ID of the mobile device is properly identified. A POSITA would know that each method could be prone to errors or failure. And a POSITA would understand the importance of correctly identifying the OS because it would have been obvious that malware may only infect certain operating systems. *See* Section III.A, above.

- To the extent Deridder does not disclose or render obvious on its own "generating an alert identifying a network address associated with the access device, the malware ID and the OS ID associated with TCP session that generated the alert," it would have been obvious to combine that reference with Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, and/or Lee. For example, each of these references is in the same general technological field of malware and intrusion detection, and a POSITA would have understood that the combination would yield predictable results. For example, each of these references is in the same general technological field of

malware and intrusion detection, and a POSITA would have understood that the combination would yield predictable results. Deridder actually discloses that its system would be useful in services "such as network monitoring, targeted advertising, ***malware detection*** etc." Deridder, ¶ 22. In doing so, Deridder recognizes that a POSITA would commonly add malware detection services to the service provider side of the NAT. When this happens, Deridder further recognizes that its technique of OS fingerprinting would be helpful to identify the computer connecting through the NAT with specificity, since all devices connecting through the NAT will have the same network address on the service provider side. It, therefore, would have been obvious to a POSITA to add malware detection to the service provider's network and use the OS fingerprinting in Deridder based upon Deridder's explicit recognition of this. Deridder, ¶ 22; And, since Deridder does not detail how to set up such a malware detection system, a POSITA would have turned to references in that field. Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, and/or Lee are examples of these types of references. Furthermore, a POSITA would have had a reasonable expectation of success implementing these malware detection systems in the NAT-based system disclosed in Deridder for multiple reasons. For example, like the traffic inspection device in Deridder, the systems operate on network components that see all of the traffic passing through a network as part of a service provider network. The traffic inspection device in Deridder similarly inspects traffic passing through the NAT in a service provider network. A POSITA, therefore, would have known that the malware detection systems in Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, and/or Lee could be combined with the NAT-based system in Deridder with only trivial modifications to identify devices in the local area network. Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, and/or Lee all operate on a service provider network or the equivalent. And, a POSITA would have been motivated to use both OS fingerprinting and the User-Agent field as a cross-check to ensure that the OS ID of the mobile device is properly identified. A POSITA would know that each method could be prone to errors or failure. And a POSITA would understand the importance of correctly identifying the OS because it would have been obvious that malware may only infect certain operating systems. *See* Section III.A, above.

- To the extent Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, and/or Lee do not disclose or render obvious on their own "determining a protocol associated with the TCP packets and matching an OS fingerprint from one or more protocol parameters if present in the TCP packets to determine a first operating system identifier (ID)" or "wherein determining the first OS ID is performed by comparing one or more protocol parameters of the one or more TCP packets having a SYN flag associated with the session, wherein the OS fingerprints identify the protocol parameters of the SYN flagged packet and the OS ID associated with parameters," it would have been obvious to combine each of those references with Deridder. For example, each of these references is in the same general technological field of malware and intrusion detection, and a POSITA would have understood that the combination would yield predictable results. For example, each of these references is in the same general technological field of malware and intrusion detection, and a POSITA would have understood that the combination would yield predictable results. A POSITA would have been motivated to combine the system in Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, or Zuk with that in Deridder because Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, or Zuk teach or render obvious tying malware to a specific OS. *E.g.*, Tuvell, ¶ 49. A POSITA would also have understood that OS type is useful information to link with the virus name because viruses commonly target only specific operating systems. A POSITA further would have been motivated to determine the OS type without receiving it from the mobile device in the network to reduce network traffic and make the network analyzer less dependent upon client input. In other words, a POSITA would have been motivated to look for ways to determine the OS type. A POSITA would have further recognized that it would be beneficial to determine the OS type based on the network traffic. A POSITA, therefore, would have been motivated to look for a system that determines the OS based upon the network traffic, and Deridder discloses such a system. *See* Section III.A, above.
- To the extent Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, and/or Deridder do not disclose or render obvious on their own "determining an application parameter associated with the TCP session if present, and identifying a second OS ID from the application parameter" or "wherein

determining the application parameter associated with the session and identifying the second OS ID from the application parameter by inspecting an HTTP user agent string to determine the second OS ID," it would have been obvious to combine each of those references with Lee and/or RFC 2616. For example, each of these references is in the same general technological field of malware and intrusion detection, and a POSITA would have understood that the combination would yield predictable results. For example, each of these references is in the same general technological field of malware and intrusion detection, and a POSITA would have understood that the combination would yield predictable results. A POSITA would have been motivated to combine the system in Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, or Zuk with that in Lee and/or RFC 2616 because Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, or Zuk teach or render obvious tying malware to a specific OS. E.g., Tuvell, ¶ 49. A POSITA would also have understood that OS type is useful information to link with the virus name because viruses commonly target only specific operating systems. A POSITA further would have been motivated to determine the OS type without receiving it from the mobile device in the network to reduce network traffic and make the network analyzer less dependent upon client input. In other words, a POSITA would have been motivated to look for ways to determine the OS type. A POSITA further would have recognized that it would be beneficial to determine the OS type based on the network traffic. A POSITA, therefore, would have been motivated to look for a system that determines the OS based upon the network traffic, and Lee and/or RFC 2616 disclose such systems. And, because a POSITA would have had a general familiarity with the HTTP specification, a POSITA would have understood that the OS information can be extracted from the User-Agent field, in which clients disclose their OS type. *See* Section III.A, above.

- To the extent Deridder does not disclose or render obvious on its own "wherein the OS ID in the alert comprises one of the first OS ID or second OS ID associated with one or more computing devices coupled to the access device," it would have been obvious to combine that reference with Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, RFC 2616, and/or Lee. For example, each of these references is in the same general technological field of malware and intrusion detection and

a POSITA would have understood that the combination would yield predictable results. Deridder actually discloses that its system would be useful in services "such as network monitoring, targeted advertising, ***malware detection*** etc." Deridder, ¶ 22. In doing so, Deridder recognizes that a POSITA would commonly add malware detection services to the service provider side of the NAT. When this happens, Deridder further recognizes that its technique of OS fingerprinting would be helpful to identify the computer connecting through the NAT with specificity, since all devices connecting through the NAT will have the same network address on the service provider side. It would therefore have been obvious to a POSITA to add malware detection to the service provider's network and use the OS fingerprinting in Deridder based upon Deridder's explicit recognition of this. Deridder, ¶ 22; And, since Deridder does not detail how to set up such a malware detection system, a POSITA would have turned to references in that field. Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, RFC 2616, and/or Lee are examples of these types of references. Furthermore, a POSITA would have had a reasonable expectation of success implementing these malware detection systems in the NAT-based system disclosed in Deridder for multiple reasons. For example, like the traffic inspection device in Deridder, the systems operate on network components that see all of the traffic passing through a network as part of a service provider network. The traffic inspection device in Deridder similarly inspects traffic passing through the NAT in a service provider network. A POSITA, therefore, would have known that the malware detection systems in Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, RFC 2616, and/or Lee could be combined with the NAT-based system in Deridder with only trivial modifications to identify devices in the local area network. Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, RFC 2616, and/or Lee all operate on a service provider network or the equivalent. And, a POSITA would have been motivated to use both OS fingerprinting and the User-Agent field as a cross-check to ensure that the OS ID of the mobile device is properly identified. A POSITA would know that each method could be prone to errors or failure. A POSITA would understand the importance of correctly identifying the OS because it would have been obvious that malware may only infect certain operating systems. And, a POSITA would

have understood that the malware detection systems should raise some sort of alert or alarm when malware is detected, as disclosed in these references. *See* Section III.A, above.

- To the extent Deridder does not disclose or render obvious on its own "sending a notification to a subscriber associated with the network address associated with the access device, the notification identifying a remediation portal to remove the determined malware in the alert," it would have been obvious to combine that reference with Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, and/or Lee. For example, each of these references is in the same general technological field of malware and intrusion detection, and a POSITA would have understood that the combination would yield predictable results. Deridder actually discloses that its system would be useful in services "such as network monitoring, targeted advertising, ***malware detection*** etc." Deridder, ¶ 22. In doing so, Deridder recognizes that a POSITA would commonly add malware detection services to the service provider side of the NAT. When this happens, Deridder further recognizes that its technique of OS fingerprinting would be helpful to identify the computer connecting through the NAT with specificity, since all devices connecting through the NAT will have the same network address on the service provider side. It would therefore have been obvious to a POSITA to add malware detection to the service provider's network and use the OS fingerprinting in Deridder based upon Deridder's explicit recognition of this. Deridder, ¶ 22; And, since Deridder does not detail how to set up such a malware detection system, a POSITA would have turned to references in that field. Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, and/or Lee are examples of these types of references. Furthermore, a POSITA would have had a reasonable expectation of success implementing these malware detection systems in the NAT-based system disclosed in Deridder for multiple reasons. For example, like the traffic inspection device in Deridder, the systems operate on network components that see all of the traffic passing through a network as part of a service provider network. The traffic inspection device in Deridder similarly inspects traffic passing through the NAT in a service provider network. A POSITA, therefore, would have known that the malware detection systems in Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, and/or Lee could be combined with the NAT-based system in

Deridder with only trivial modifications to identify devices in the local area network. Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, and/or Lee all operate on a service provider network or the equivalent. And, a POSITA would have been motivated to use both OS fingerprinting and the User-Agent field as a cross-check to ensure that the OS ID of the mobile device is properly identified. A POSITA would know that each method could be prone to errors or failure. A POSITA would understand the importance of correctly identifying the OS because it would have been obvious that malware may only infect certain operating systems. And, a POSITA would have understood that the malware detection systems should raise some sort of alert or alarm when malware is detected, as disclosed in these references. *See* Section III.A, above.

- To the extent Deridder does not disclose or render obvious on its own "identifying at the remediation portal the subscriber accessing the remediation portal, identifying the OS associated with the computing device used by the subscriber to access the remediation portal, comparing the OS associated with the computing device to the at least one of the first OS ID or second OS ID identified in the alert, and providing malware remediation to the computing device when the at least one of the first OS ID or second OS ID matches the OS associated with the computing device," it would have been obvious to combine that reference with Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, RFC 2616, and/or Lee. For example, each of these references is in the same general technological field of malware and intrusion detection, and a POSITA would have understood that the combination would yield predictable results. Deridder actually discloses that its system would be useful in services "such as network monitoring, targeted advertising, ***malware detection*** etc." Deridder, ¶ 22. In doing so, Deridder recognizes that a POSITA would commonly add malware detection services to the service provider side of the NAT. When this happens, Deridder further recognizes that its technique of OS fingerprinting would be helpful to identify the computer connecting through the NAT with specificity, since all devices connecting through the NAT will have the same network address on the service provider side. It would therefore have been obvious to a POSITA to add malware detection to the service provider's network and use the OS fingerprinting in Deridder based upon Deridder's explicit

recognition of this. Deridder, ¶ 22; And, since Deridder does not detail how to set up such a malware detection system, a POSITA would have turned to references in that field. Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, RFC 2616, and/or Lee are examples of these types of references. Furthermore, a POSITA would have had a reasonable expectation of success implementing these malware detection systems in the NAT-based system disclosed in Deridder for multiple reasons. For example, like the traffic inspection device in Deridder, the systems operate on network components that see all of the traffic passing through a network as part of a service provider network. The traffic inspection device in Deridder similarly inspects traffic passing through the NAT in a service provider network. A POSITA, therefore, would have known that the malware detection systems in Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, RFC 2616, and/or Lee could be combined with the NAT-based system in Deridder with only trivial modifications to identify devices in the local area network. Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, RFC 2616, and/or Lee all operate on a service provider network or the equivalent. A POSITA would have been motivated to use both OS fingerprinting and the User-Agent field as a cross-check to ensure that the OS ID of the mobile device is properly identified. A POSITA would know that each method could be prone to errors or failure. And a POSITA would understand the importance of correctly identifying the OS because it would have been obvious that malware may only infect certain operating systems. *See* Section III.A, above.

- To the extent Deridder does not disclose or render obvious on its own "wherein if the OS of the computing device is not the at least one of the first OS ID or second OS ID identified in the alert an indication is provided to the subscriber to connect to the remediation portal with another computing device connected to the access device," it would have been obvious to combine that reference with Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, RFC 2616, and/or Lee. For example, each of these references is in the same general technological field of malware and intrusion detection, and a POSITA would have understood that the combination would yield predictable results. Deridder actually discloses that its system would be useful in services "such as network monitoring, targeted advertising, ***malware detection*** etc." Deridder, ¶ 22. In doing

so, Deridder recognizes that a POSITA would commonly add malware detection services to the service provider side of the NAT. When this happens, Deridder further recognizes that its technique of OS fingerprinting would be helpful to identify the computer connecting through the NAT with specificity, since all devices connecting through the NAT will have the same network address on the service provider side. It would therefore have been obvious to a POSITA to add malware detection to the service provider's network and use the OS fingerprinting in Deridder based upon Deridder's explicit recognition of this. Deridder, ¶ 22; And, since Deridder does not detail how to set up such a malware detection system, a POSITA would have turned to references in that field. Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, RFC 2616, and/or Lee are examples of these types of references. Furthermore, a POSITA would have had a reasonable expectation of success implementing these malware detection systems in the NAT-based system disclosed in Deridder for multiple reasons. For example, like the traffic inspection device in Deridder, the systems operate on network components that see all of the traffic passing through a network as part of a service provider network. The traffic inspection device in Deridder similarly inspects traffic passing through the NAT in a service provider network. A POSITA, therefore, would have known that the malware detection systems in Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, RFC 2616, and/or Lee could be combined with the NAT-based system in Deridder with only trivial modifications to identify devices in the local area network. Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, RFC 2616, and/or Lee all operate on a service provider network or the equivalent. And, a POSITA would have been motivated to use both OS fingerprinting and the User-Agent field as a cross-check to ensure that the OS ID of the mobile device is properly identified. A POSITA would know that each method could be prone to errors or failure. And a POSITA would understand the importance of correctly identifying the OS because it would have been obvious that malware may only infect certain operating systems. *See* Section III.A, above.

- To the extent Deridder does not disclose or render obvious on their own "wherein the alert is cleared when all computing devices associated with the access device and the computing device

having the at least one of the first OS ID or second OS ID have accessed the remediation portal," it would have been obvious to combine each of that reference with Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, RFC 2616 and/or Lee. For example, each of these references is in the same general technological field of malware and intrusion detection, and a POSITA would have understood that the combination would yield predictable results. Deridder actually discloses that its system would be useful in services "such as network monitoring, targeted advertising, ***malware detection*** etc." Deridder, ¶ 22. In doing so, Deridder recognizes that a POSITA would commonly add malware detection services to the service provider side of the NAT. When this happens, Deridder further recognizes that its technique of OS fingerprinting would be helpful to identify the computer connecting through the NAT with specificity, since all devices connecting through the NAT will have the same network address on the service provider side. It would therefore have been obvious to a POSITA to add malware detection to the service provider's network and use the OS fingerprinting in Deridder based upon Deridder's explicit recognition of this. Deridder, ¶ 22; And, since Deridder does not detail how to set up such a malware detection system, a POSITA would have turned to references in that field. Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, RFC 2616, and/or Lee are examples of these types of references. Furthermore, a POSITA would have had a reasonable expectation of success implementing these malware detection systems in the NAT-based system disclosed in Deridder for multiple reasons. For example, like the traffic inspection device in Deridder, the systems operate on network components that see all of the traffic passing through a network as part of a service provider network. The traffic inspection device in Deridder similarly inspects traffic passing through the NAT in a service provider network. A POSITA, therefore, would have known that the malware detection systems in Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, RFC 2616, and/or Lee could be combined with the NAT-based system in Deridder with only trivial modifications to identify devices in the local area network. Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, RFC 2616, and/or Lee all operate on a service provider network or the equivalent. And, a POSITA would have been motivated to use both OS fingerprinting and the User-Agent field as a

crosscheck to ensure that the OS ID of the mobile device is properly identified. A POSITA would know that each method could be prone to errors or failure. And a POSITA would understand the importance of correctly identifying the OS because it would have been obvious that malware may only infect certain operating systems. *See* Section III.A, above.

- To the extent Deridder does not disclose or render obvious on their own "verifying the first OS ID against the second OS ID, wherein if the second OS ID does not match the first OS ID the session is identified by the OS ID identified as a more reliable OS ID," "verifying the first OS ID against the second OS ID, wherein if the second OS ID matches the first OS ID either OS ID is used," or "verifying the first OS ID against the second OS ID, wherein if the second OS ID matches the first OS ID but the second OS ID provides additional information, the second OS ID is used," it would have been obvious to combine that reference with Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, RFC 2616, and/or Lee. For example, each of these references is in the same general technological field of malware and intrusion detection, and a POSITA would have understood that the combination would yield predictable results. Deridder actually discloses that its system would be useful in services "such as network monitoring, targeted advertising, ***malware detection*** etc." Deridder, ¶ 22. In doing so, Deridder recognizes that a POSITA would commonly add malware detection services to the service provider side of the NAT. When this happens, Deridder further recognizes that its technique of OS fingerprinting would be helpful to identify the computer connecting through the NAT with specificity, since all devices connecting through the NAT will have the same network address on the service provider side. It would therefore have been obvious to a POSITA to add malware detection to the service provider's network and use the OS fingerprinting in Deridder based upon Deridder's explicit recognition of this. Deridder, ¶ 22; And, since Deridder does not detail how to set up such a malware detection system, a POSITA would have turned to references in that field. Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, RFC 2616, and/or Lee are examples of these types of references. Furthermore, a POSITA would have had a reasonable expectation of success implementing these malware detection systems in the NAT-based system disclosed in Deridder

for multiple reasons. For example, like the traffic inspection device in Deridder, the systems operate on network components that see all of the traffic passing through a network as part of a service provider network. The traffic inspection device in Deridder similarly inspects traffic passing through the NAT in a service provider network. A POSITA, therefore, would have known that the malware detection systems in Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, RFC 2616, and/or Lee could be combined with the NAT-based system in Deridder with only trivial modifications to identify devices in the local area network. Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, RFC 2616, and/or Lee all operate on a service provider network or the equivalent. And, a POSITA would have been motivated to use both OS fingerprinting and the User-Agent field as a cross-check to ensure that the OS ID of the mobile device is properly identified. A POSITA would know that each method could be prone to errors or failure. And a POSITA would understand the importance of correctly identifying the OS because it would have been obvious that malware may only infect certain operating systems. *See* Section III.A, above.

- To the extent Deridder does not disclose or render obvious on their own "wherein sending the notification to the subscriber associated with the access device further comprises replacing the network address of the access device with a subscriber ID," it would have been obvious to combine each of those references with Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, RFC 2616, and/or Lee. For example, this reference is in the same general technological field of malware and intrusion detection, and a POSITA would have understood that the combination would yield predictable results. Deridder actually discloses that its system would be useful in services "such as network monitoring, targeted advertising, ***malware detection*** etc." Deridder, ¶ 22. In doing so, Deridder recognizes that a POSITA would commonly add malware detection services to the service provider side of the NAT. When this happens, Deridder further recognizes that its technique of OS fingerprinting would be helpful to identify the computer connecting through the NAT with specificity, since all devices connecting through the NAT will have the same network address on the service provider side. It would therefore have been obvious to a POSITA to add malware detection to the service provider's network and use the OS

fingerprinting in Deridder based upon Deridder's explicit recognition of this. Deridder, ¶ 22; And, since Deridder does not detail how to set up such a malware detection system, a POSITA would have turned to references in that field. Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, RFC 2616, and/or Lee are examples of these types of references. Furthermore, a POSITA would have had a reasonable expectation of success implementing these malware detection systems in the NAT-based system disclosed in Deridder for multiple reasons. For example, like the traffic inspection device in Deridder, the systems operate on network components that see all of the traffic passing through a network as part of a service provider network. The traffic inspection device in Deridder similarly inspects traffic passing through the NAT in a service provider network. A POSITA, therefore, would have known that the malware detection systems in Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, RFC 2616, and/or Lee could be combined with the NAT-based system in Deridder with only trivial modifications to identify devices in the local area network. Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, RFC 2616, and/or Lee all operate on a service provider network or the equivalent. And, a POSITA would have been motivated to use both OS fingerprinting and the User-Agent field as a cross-check to ensure that the OS ID of the mobile device is properly identified. A POSITA would know that each method could be prone to errors or failure. And a POSITA would understand the importance of correctly identifying the OS because it would have been obvious that malware may only infect certain operating systems. *See* Section III.A, above.

- To the extent Deridder does not disclose or render obvious on their own "wherein sending the notification to the subscriber associated with the access device further comprises aggregating one or more detailed alerts having the subscriber ID into a single alert summary associated with the subscriber ID," it would have been obvious to combine this reference with Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, RFC 2616, and/or Lee. For example, each of these references is in the same general technological field of malware and intrusion detection, and a POSITA would have understood that the combination would yield predictable results. Deridder actually discloses that its system would be useful in services "such as network monitoring, targeted

advertising, ***malware detection*** etc." Deridder, ¶ 22. In doing so, Deridder recognizes that a POSITA would commonly add malware detection services to the service provider side of the NAT. When this happens, Deridder further recognizes that its technique of OS fingerprinting would be helpful to identify the computer connecting through the NAT with specificity, since all devices connecting through the NAT will have the same network address on the service provider side. It would therefore have been obvious to a POSITA to add malware detection to the service provider's network and use the OS fingerprinting in Deridder based upon Deridder's explicit recognition of this. Deridder, ¶ 22; And, since Deridder does not detail how to set up such a malware detection system, a POSITA would have turned to references in that field. Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, RFC 2616, and/or Lee are examples of these types of references. Furthermore, a POSITA would have had a reasonable expectation of success implementing these malware detection systems in the NAT-based system disclosed in Deridder for multiple reasons. For example, like the traffic inspection device in Deridder, the systems operate on network components that see all of the traffic passing through a network as part of a service provider network. The traffic inspection device in Deridder similarly inspects traffic passing through the NAT in a service provider network. A POSITA, therefore, would have known that the malware detection systems in Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, RFC 2616, and/or Lee could be combined with the NAT-based system in Deridder with only trivial modifications to identify devices in the local area network. Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, RFC 2616, and/or Lee all operate on a service provider network or the equivalent. And, a POSITA would have been motivated to use both OS fingerprinting and the User-Agent field as a cross-check to ensure that the OS ID of the mobile device is properly identified. A POSITA would know that each method could be prone to errors or failure. And a POSITA would understand the importance of correctly identifying the OS because it would have been obvious that malware may only infect certain operating systems. *See* Section III.A, above.

- To the extent Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, and/or Lee do not disclose or render obvious on their own "wherein the one or more computing devices are coupled to the

access device through a local area network (LAN), the access device providing network address translation (NAT) or is coupled to NAT device to share the network address of the access device," it would have been obvious to combine each of those references with Deridder. For example, each of these references is in the same general technological field of malware and intrusion detection, and a POSITA would have understood that the combination would yield predictable results. Deridder actually discloses that its system would be useful in services "such as network monitoring, targeted advertising, ***malware detection*** etc." Deridder, ¶ 22. In doing so, Deridder recognizes that a POSITA would commonly add malware detection services to the service provider side of the NAT. When this happens, Deridder further recognizes that its technique of OS fingerprinting would be helpful to identify the computer connecting through the NAT with specificity, since all devices connecting through the NAT will have the same network address on the service provider side. It would therefore have been obvious to a POSITA to add malware detection to the service provider's network and use the OS fingerprinting in Deridder based upon Deridder's explicit recognition of this. Deridder, ¶ 22; And, since Deridder does not detail how to set up such a malware detection system, a POSITA would have turned to references in that field. Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, and/or Lee are examples of these types of references. Furthermore, a POSITA would have had a reasonable expectation of success implementing these malware detection systems in the NAT-based system disclosed in Deridder for multiple reasons. For example, like the traffic inspection device in Deridder, the systems operate on network components that see all of the traffic passing through a network as part of a service provider network. The traffic inspection device in Deridder similarly inspects traffic passing through the NAT in a service provider network. A POSITA, therefore, would have known that the malware detection systems in Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, and/or Lee could be combined with the NAT-based system in Deridder with only trivial modifications to identify devices in the local area network. Tuvell, Akyol, Zhu, Enderby, Abdel-Aziz, Zuk, and/or Lee all operate on a service provider network or the equivalent. *See* Section III.A, above.

- To the extent Deridder, Akyol, Zhu, Enderby, or Lee do not disclose or render obvious on their own "a plurality of network sensors coupled to the service provider network," it would have been obvious to combine each of those references with Tuvell, Abdel-Aziz, and/or Zuk. For example, each of these references is in the same general technological field of malware and intrusion detection, and a POSITA would have understood that the combination would yield predictable results. Deridder, Akyol, Zhu, Enderby, or Lee disclose malware or anomaly detection systems on a network, and Tuvell, Abdel-Aziz, and/or Zuk disclose alternative means of implementing such systems. A POSITA would have understood that it may have been desirable to distribute collection agents around a network, particularly for large networks, so there is not a single bottleneck and/or point of failure. And, a POSITA would have had a reasonable expectation of success in implementing the plurality of network sensors of Tuvell, Abdel-Aziz, and/or Zuk as part of the systems in Deridder, Akyol, Zhu, Enderby, or Lee because distributing network sensors is well within the skill of a POSITA and would be easy to implement. *See* Section III.A, above.

## IV. P.R. 3-3(c): CLAIM CHARTS

Pursuant to Local Rule P.R. 3-3(c), and subject to Fortinet's reservation of rights contained herein, the invalidity claim charts, attached hereto as Exhibits A-1 through I-8, identify where in each item of prior art each element of each asserted claim is found for the Asserted Claims.

The cited portions of the prior art references are examples and representative of the content of the prior art references, and should be understood in the context of the reference as a whole, as understood by one of ordinary skill in the art. To the extent any cited prior art reference fails to explicitly teach or suggest one or more limitations of that claim, the limitation would nonetheless have been inherent in and/or implied by the reference and/or obvious to one of ordinary skill in the art at the time of the alleged invention(s), either alone or by the combination of the cited prior art references with any of the other listed references and/or common knowledge disclosing the missing claim limitations. Non-limiting examples of certain combinations are outlined above. It should be understood that

citations within each exhibit are exemplary, not exhaustive, and should not be construed as the sole evidentiary support in the reference.

## V. P.R. 3-3(d): INVALIDITY BASED ON SECTION 101, INDEFINITENESS, LACK OF ENABLEMENT, AND LACK OF WRITTEN DESCRIPTION

Pursuant to Local P.R. 3-3(d), and subject to Fortinet's reservation of rights, Fortinet includes below the grounds on which Fortinet contends the Asserted Claims are invalid based on 35 U.S.C. § 101, indefiniteness, lack of written description, and/or lack of enablement under 35 U.S.C. § 112.

As noted above, Plaintiff has not yet provided a claim construction for any of the terms and phrases that Fortinet anticipates will be in dispute. Fortinet, therefore, cannot provide a complete list of its indefiniteness, lack of written description, and lack of enablement defenses because Fortinet does not know whether Plaintiff will proffer a construction for certain terms and phrases that would be broader than, or inconsistent with, a construction supportable by the disclosure set forth in the specification. Accordingly, Fortinet reserves the right, to the extent permitted by the Court and the applicable statutes and rules, to supplement, amend, and/or modify these indefiniteness, lack of written description, and lack of enablement defenses as discovery progresses and in accordance with Plaintiff's claim construction, infringement, and validity disclosures.

### A. Section 101

Each and every asserted claim of the Asserted Patents is invalid as patent-ineligible under 35 U.S.C. § 101. Plaintiff has not identified any factual issue or potential claim construction that would preclude judgment as a matter of law regarding the § 101 defense, and Fortinet contends there is none. To the extent Plaintiff (or the Court) identifies any such issue, Fortinet reserves the right to amend this contention to address such factual issue or claim construction.

### B. Indefiniteness

Pre-AIA 35 U.S.C. § 112, ¶ 2 contains two requirements: "first, [the claim] must set forth what the applicant regards as his invention and second, it must do so with sufficient particularity and distinctness, i.e., the claim must be sufficiently definite." *Allen Eng'g Corp. v. Bartell Indus., Inc.*, 299 F.3d 1336, 1348 (Fed. Cir. 2002) (internal quotes removed) (quoting *Solomon v. Kimberly-Clark Corp.*,

216 F.3d 1372, 1377 (Fed. Cir. 2000)). "A determination of whether a claim recites the subject matter which the applicant regards as his invention and is sufficiently definite, so as to satisfy the requirements of 35 U.S.C. § 112, ¶ 2, is a legal conclusion." *Allen Eng'g*, 299 F.3d at 1343. Under the first requirement of pre-AIA § 112, ¶ 2, a court must hold a claim invalid "[w]here it would be apparent to one of skill in the art, based on the specification, that the invention set forth in [the] claim is not what the patentee regarded as his invention." *Id*. at 1349. Under the second requirement of pre-AIA § 112, ¶ 2, a claim is sufficiently definite only if, viewed in light of the specification and prosecution history, it informs those skilled in the art about the scope of the invention with reasonable certainty. *Nautilus, Inc. v. Biosig Instruments, Inc*., 572 U.S. 898 (2014).

Various Asserted Claims identified below do not comply with the requirements pre-AIA 35 U.S.C. § 112, ¶ 2, for failing to particularly point out and distinctly claim "the subject matter which the applicant regards as his invention" for the following reasons. For example, as demonstrated either individually or collectively by the claim elements addressed below, various Asserted Claims fail to inform those skilled in the art about the scope of the invention with reasonable certainty, rendering those claims (and any claims depending therefrom) invalid as indefinite. The following chart identifies the claims in which the identified terms and phrases explicitly appear, although those identified terms and phrases are also incorporated into additional dependent Asserted Claims. Fortinet's contentions as to indefiniteness also include those dependent claims. Additionally, to the extent any Asserted Claim containing the identified limitations or phrases or substantially identical limitations or phrases is not specifically identified in the table below, Fortinet still identifies such a claim based on its inclusion of such term or phrase.

| Patent | Claim(s) | Indefinite Term and/or Phrase |
|---|---|---|
| '336 | 1, 9 | "intercepting at [a/the] network access controller a request to access a network resource from a browser application running on a client device within the shared network associated with an anonymous user"; |
| '336 | 16 | "intercepting a request to access a network resource from a browser application running on a client device within the |

| Patent | Claim(s) | Indefinite Term and/or Phrase |
|---|---|---|
| | | shared network coupled to the apparatus, wherein the client device is associated with an anonymous user" |
| '336 | 5, 12, 19 | "intercepting at the network access controller a second request from the browser application running on the client device associated with the anonymous user to access a second network resource that is not in the set of network destinations" |
| '710 | 1 | "at a network access gateway device between a local network and the Internet, selecting a client device in a first network segment of the network" |
| '710 | 1, 6, 8, 12, 15, 20 | "restricting all network traffic emanating from the client device to one or more network destination addresses that are not in or subordinate to the first network segment" |
| '710 | 1, 8, 15 | "rendering a web page to display on the client device from the network access gateway device" |
| '710 | 1, 8, 15 | "responsive to[the] implementation of one of the plurality of quarantine control function of the client device" |
| '710 | 2, 9, 16 | "wherein the action requires the user to obtain and execute abnormal behavior scanning software from a server machine running at one of the one or more allowed network destination addresses" |
| '710 | 7, 14 | "perform[ing] all of the plurality of quarantine control functions over the client device" |
| '639 | 4, 13, 20, 22, 23 | “provisioning module” |
| '639 | 13, 20, 21 | “traffic conditioning model [for user specific allocation of bandwidth]” |
| '639 | 22 | “firewall module for associating the packet with the user specific firewall rules.” |
| '639 | 23 | “authentication module for authenticating the user.” |
| '983 | 1, 4, 7 | "first state" |
| '983 | 1, 4, 7 | "first network communication" |
| '983 | 1, 4, 7 | "wherein the first user profile comprises one or more attributes associated with the first user" |
| '983 | 1, 4, 7 | "determining a second network bandwidth limit for the first user based on the first network bandwidth limit associated with each of the users" |

| Patent | Claim(s) | Indefinite Term and/or Phrase |
|---|---|---|
| '983 | 1, 4, 7 | "dynamically updating at least one of the first network bandwidth limits associated with the plurality of users based on the second network bandwidth limit" |
| '983 | 1, 4, 7 | "including configuring the access control device to operate in a second state," |
| '983 | 1, 4, 7 | "wherein operation of the access control device in the second state comprises regulating network bandwidth usage for each of the plurality of users based on the first network bandwidth limits" |
| '983 | 2, 5, 8 | "second user at the first user device" |
| '983 | 2, 5, 8 | "determining a third network bandwidth limit for the second user based on the one or more attributes of the second user profile and the first user device" |
| '983 | 3, 6, 9 | "dynamically updating at least one of the first network bandwidth limits based on the second network bandwidth limit comprises dynamically updating the first network bandwidth associated with the first user to the second network bandwidth" |
| '426 | 1 | "receiving, by the machine, an authentication request from a principal, the request directed by the principal to an external service and intercepted by the method for receipt" |
| '426 | 1 | "the authentication message serves as a new authentication request and as a new authentication response for single sign-on access of the principal to the identity service and other services external or internal to the identity service" |
| '426 | 1 | "the identity service acts as a proxy for access sessions to the other services on behalf of the principal" |
| '426 | | "the principal's access sessions occur indirectly through the identity service and transparently to the principal" |
| '426 | 1 | "wherein the authentication message includes the new authentication request made on behalf of the principal and the authentication message also includes a new authentication response that satisfies the new authentication request" |
| '426 | 1 | "that response vouches for authentication of the principal to the identity service for the single sign-on access of the principal" |

| Patent | Claim(s) | Indefinite Term and/or Phrase |
|---|---|---|
| '426 | 1 | "which is one of the other services that the identity service controls access to" |
| '426 | 1 | "a determination as to whether to use a single interaction or multiple interactions for authentication of the principal to the other services is automatically communicated in the new authentication response" |
| '426 | 2 | "making, by the machine, a target service available to interactions between the principal and an external service" |
| '426 | 2 | "the target service is directly accessible from an environment of the identity service" |
| '426 | 4 | "the principal is currently already properly authenticated to the processing associated with the method" |
| '426 | 5 | "supplying further includes adding a second authentication to a second redirection of the principal, wherein the second authentication represents authentication of the principal to the identity service and wherein the second redirection directs the principal to request a target service that is to be proxied on behalf of the principal from the identity service" |
| '426 | 6 | "representing the new authentication response as an instruction to the identity service to enforce its own independent authentication with the principal before considering the principal authenticated to the identity service" |
| '936 | 1 | "abnormal system states in computers" |
| '936 | 1, 12 | "snapshots" |
| '936 | 1, 12 | "data indicating a state of a respective computer" |
| '936 | 1, 12 | "adaptive reference model comprising a rule set customized to characteristics of the population of computers" |
| '936 | 1, 12 | "the rule set being developed by identifying patterns among the snapshots from the plurality of computers such that the adaptive reference model is indicative of normal states in the computers within the population" |
| '936 | 1, 12 | "anomaly" |
| '936 | 2, 13 | "recognition filter" |
| '936 | 2, 13 | "trouble condition" |
| '936 | 3, 14 | "generic response not specific to a particular asset of the at least one computer" |

| Patent | Claim(s) | Indefinite Term and/or Phrase |
|---|---|---|
| '936 | 3, 14 | "send[ing] the generic response and a set of anomalies found in the snapshot to the at least one computer, the set of anomalies indicating assets of the at least one computer whose states are anomalous" |
| '936 | 5, 16 | "wherein the recognition filter comprises a particular pattern of anomalies that indicates the presence of a particular root cause condition or a generic class of conditions" |
| '936 | 6, 20 | "comparing a plurality of anomalies associated with a particular snapshot with a recognition filter to diagnose a trouble condition" |
| '936 | 9, 17 | "wherein the adaptive reference model is generated to include a value layer that determines whether an asset value contained in a snapshot is anomalous" |
| '936 | 10, 18 | "wherein the adaptive reference model is generated to include a cluster layer that tracks relationships between assets and identifies an anomaly in response to an asset being unexpectedly absent from or present in a set of assets in a snapshot" |
| '282 | 1 | "accepting or denying the packet based on the set of firewall rules, wherein the set of firewall rules is dynamically self-configurable during runtime without operator interaction, wherein the set of firewall rules comprises a plurality of chains of rules forming various paths through a hierarchical structure, and wherein the hierarchical structure comprises defined places for dynamically updating the set of firewall rules during runtime" |
| '282 | 2 | "wherein dynamically updating the set of firewall rules during runtime further comprises, during runtime, adding a rule to the set of firewall rules, deleting a rule from the set of firewall rules, or modifying a rule in the set of firewall rules without operator interaction" |
| '282 | 3 | "wherein associating the set of firewall rules with the at least one node further comprises associating a first subset of the set of firewall rules with the first node" |
| '282 | 4 | "wherein the at least one node further comprises at least two nodes including a second node, further comprising associating a second subset of the set of firewall rules with the second node" |

| Patent | Claim(s) | Indefinite Term and/or Phrase |
|---|---|---|
| '282 | 5 | "wherein the first subset of firewall rules is the same as or at least partially different from the second subset of firewall rules" |
| '282 | 6, 17, 30 | "wherein [one of /either] the first subset of firewall rules or second subset of firewall rules equals the entire set of firewall rules" |
| '282 | 12 | "a first computer readable storage medium storing a set of firewall rules, wherein the set of firewall rules is dynamically self-configurable during runtime without operator interaction, wherein the set of firewall rules comprises a plurality of chains of rules forming various paths through a hierarchical structure, and wherein the hierarchical structure comprises defined places for dynamically updating the set of firewall rules during runtime without operator interaction" |
| '282 | 12 | "when a packet is received at one of the two or more network interfaces associated with the at least one node, accept or deny the packet based on a review of the set of firewall rules" |
| '282 | 14, 27 | "wherein the [data controlling computer program code /computer instructions] [is/are] further executable to: associate a first subset of the set of firewall rules with the first node; and if the packet is received at the first node, apply the first subset of the set of firewall rules associated with the first node" |
| '282 | 15, 28 | "wherein the at least one node further comprises at least two nodes including a second node, and wherein the data controlling computer program code is further executable to: associate a second subset of the set of firewall rules with the second node; and if the packet is received at the second node, apply the second subset of the set of firewall rules associated with the second node" |
| '282 | 16, 29 | "wherein the first subset of the set of firewall rules is the same as or different from the second subset of the set of firewall rules" |
| '282 | 22, 35 | "wherein each of the plurality of network interfaces is physically connected to every other network interface of the plurality of network interfaces and wherein physical connection between the plurality of network interfaces comprises indirect physical connection between the plurality of network interfaces" |

| Patent | Claim(s) | Indefinite Term and/or Phrase |
|---|---|---|
| '282 | 23 | "wherein the data controlling computer program code is further executable to dynamically update the set of firewall rules during runtime without operator interaction" |
| '282 | 24 | "wherein the data controlling computer program code is further executable to dynamically update the set of firewall rules during runtime without operator interaction." |
| '282 | 24 | "accept or deny the packet based on a review of the set of firewall rules, wherein the set of firewall rules is dynamically self-configurable during runtime without operator interaction" |
| '153 | 1, 10, 15 | "first network" |
| '153 | 1, 10, 15 | "second network" |
| '153 | 1, 10 | "said user bandwidth allocation profile is stored local or remote to said control device" |
| '153 | 1, 10 | "wherein the user bandwidth allocation profile contains an arbitrary number of attributes specifying bandwidth limitations for the first user" |
| '153 | 1, 10 | "wherein said control device is located between said user device and said first network" |
| '153 | 1, 10, 15 | "user specific rules and conditions" |
| '153 | 1, 10 | "information identifying said user device" |
| '153 | 1, 10 | "said at least one traffic control rule" |
| '153 | 1 | "considering said information identifying said user device" |
| '153 | 1, 10 | "utilizing said at least one traffic control rule associated with said first user" |
| '153 | 2, 11 | "indexing said user specific rules" |
| '153 | 3, 12 | "filling in missing attribute values with default values" |
| '153 | 4, 12 | "local to or remote from said control device" |

| Patent | Claim(s) | Indefinite Term and/or Phrase |
|---|---|---|
| '153 | 5 | "a network communication" |
| '153 | 6 | "mapping said attributes in said user bandwidth allocation profile" |
| '153 | 6, 13 | "tracking said control session by said user credentials, one or more addresses of said user device, an identifier, or a combination" |
| '153 | 7, 14, 24 | "a programmatic user" |
| '153 | 8, 9 | "mapping attributes in said user bandwidth allocation profile for said first user of at least one traffic control rule stored on said control device" |
| '153 | 15 | "based on the arbitrary number of attributes in each user profile, establish user specific rules and conditions that are bound to each user" |
| '153 | 15 | "associate each of said user specific rules with said first user based on an arbitrary identifier associated with a user device" |
| '153 | 16 | "attributes governing upload and download bandwidth allocations to said user" |
| '153 | 17 | "map said priorities to a user specific traffic control rule" |
| '153 | 22 | "session monitoring module operable to perform bandwidth metering" |
| '697 | 1, 15, 24 | "receiving one or more transmission control protocol (TCP) packets originating from an access device coupled to the service provider network" |
| '697 | 1, 15, 24 | "the one or more TCP packets defining a TCP session between a computing device coupled to the access device" |
| '697 | 1, 15, 24 | "generating an alert identifying a network address associated with the access device, the malware ID and the OS ID associated with TCP session that generated the alert" |
| '697 | 2, 16 | "determin[ing] a protocol associated with the TCP packets and matching an OS fingerprint from one or more protocol parameters if present in the TCP packets to determine a first operating system identifier (ID)" |

| Patent | Claim(s) | Indefinite Term and/or Phrase |
|---|---|---|
| '697 | 2, 16 | "determin[ing] an application parameter associated with the TCP session if present, and identifying a second OS ID from the application parameter" |
| '697 | 3, 17 | "a notification to a subscriber associated with the network address associated with the access device, the notification identifying a remediation portal to remove the determined malware in the alert" |
| '697 | 4, 25 | "identifying at the remediation portal the subscriber accessing the remediation portal" |
| '697 | 4, 25 | "identifying the OS associated with the computing device used by the subscriber to access the remediation portal" |
| '697 | 4, 25 | "comparing the OS associated with the computing device to the at least one of the first OS ID or second OS ID identified in the alert" |
| '697 | 4, 25 | "providing malware remediation to the computing device when the at least one of the first OS ID or second OS ID matches the OS associated with the computing device" |
| '697 | 5 | "wherein if the OS of the computing device is not the at least one of the first OS ID or second OS ID identified in the alert an indication is provided to the subscriber to connect to the remediation portal with an other computing device connected to the access device" |
| '697 | 6 | "wherein the alert is cleared when all computing devices associated with the access device and the computing device having the at least one of the first OS ID or second OS ID have accessed the remediation portal" |
| '697 | 7, 19 | "determin[ing] the first OS ID is performed by comparing one or more protocol parameters of the one or more TCP packets having a SYN flag associated with the session, wherein the OS fingerprints identify the protocol parameters of the SYN flagged packet and the OS ID associated with parameters" |
| '697 | 9, 21 | "a more reliable OS ID" |
| '697 | 11, 23 | "the second OS ID provides additional information" |
| '697 | 12, 18 | "send[ing] the notification to the subscriber associated with the access device further comprises replacing the network address of the access device with a subscriber ID" |
| '697 | 13 | "detailed alerts" |

The above limitations of the Asserted Claims, even when read in light of the specification and prosecution history, fail to inform with reasonable certainty one of ordinary skill in the art about the scope of the invention. For example, to one skilled in the art, at least the terms identified above are not adequately defined in the specifications of the Asserted Patents. Their lack of reasonably ascertainable scope is compounded by Plaintiff's overbroad and vague infringement contentions. Thus, the Asserted Claims fail to distinctly claim the subject matter that the applicant regards as the invention and are invalid under the second paragraph of pre-AIA 35 U.S.C. § 112. *See Nautilus*, 572 U.S. at 907–911.

**C. Lack of Written Description and Enablement**

Various Asserted Claims are invalid for failure to comply with the written description requirement under pre-AIA 35 U.S.C. § 112, ¶ 1. To satisfy the written description requirement, the description must "clearly allow persons of ordinary skill in the art to recognize that [the inventor] invented what is claimed." *Ariad Pharms., Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010). In other words, the test for sufficiency is whether the disclosure of the application relied upon reasonably conveys to those skilled in the art that the inventor had possession of the claimed subject matter as of the filing date. *Id*.

Various Asserted Claims are invalid for failure to comply with the enablement requirement pre-AIA 35 U.S.C. § 112, ¶ 1. To satisfy the enablement requirement, the disclosure "must teach those skilled in the art how to make and use the full scope of the claimed invention without 'undue experimentation.'" *Sitrick v. Dreamworks, LLC*, 516 F.3d 993, 999 (Fed. Cir. 2008). Moreover, "[i]t is the specification, not the knowledge of one skilled in the art that must supply the novel aspects of the invention in order to constitute adequate enablement." *Genentech, Inc. v. Novo Nordisk A/S*, 108 F.3d 1361, 1366 (Fed. Cir. 1997). The Federal Circuit has enumerated several factors to consider in determining whether a disclosure would require "undue experimentation": (1) the quantity of experimentation necessary; (2) the amount of direction or guidance presented; (3) the presence or absence of working examples; (4) the nature of the invention; (5) the state of the prior art; (6) the relative skill of those in the art; (7) the predictability or unpredictability of the art; and (8) the breadth of the claims. *In re Wands*, 858 F.2d 731, 737 (Fed. Cir. 1988).

Various Asserted Claims identified below do not comply with the requirements of pre-AIA 35 U.S.C. § 112, ¶ 1, for failing to satisfy the written description or enablement requirements. For example, as demonstrated either individually or collectively by the claim elements addressed below, the specification fails to convey that the inventor had possession of that subject matter, and the specification fails to teach how to make and use the full scope of the invention without undue experimentation. The following chart identifies the claims in which the identified terms and phrases explicitly appear, although those identified terms and phrases are also incorporated into additional dependent Asserted Claims. Fortinet's contentions as to written description and enablement also include those dependent claims. Additionally, to the extent any Asserted Claim containing the identified limitations or phrases or substantially identical limitations or phrases is not specifically identified in the table below, Fortinet still identifies such a claim based on its inclusion of such term or phrase.

| Patent | Claim(s) | Term and/or Phrase Lacking Written Description and/or Enablement |
|---|---|---|
| '710 | 1, 8, 15 | "rendering a web page to display on the client device from the network access gateway device, wherein the web page contains an offer for a user of the client device to perform an action in order to obtain unrestricted access to the Internet responsive to implementation of one of the plurality of quarantine control function of the client device" |
| '710 | 2, 9, 16 | "wherein the action requires the user to obtain and execute abnormal behavior scanning software from a server machine running at one of the one or more allowed network destination addresses" |
| '710 | 3, 10, 17 | "evaluating network traffic emanating from the client device after the client device has been scanned and abnormal behavior has been removed, mitigated or rendered inert" |
| '639 | 1, 10, 17, 27 | "applying the user specific traffic control rules and the user specific firewall rules to the packet as governed by at least one user specific class of service rule associated with the user on the user device in the first network" |
| '639 | 21 | "an interface master queue for controlling a flow of network traffic over a particular network interface" |
| '983 | 1, 4, 7 | "wherein the first user profile comprises one or more attributes associated with the first user" |

| Patent | Claim(s) | Term and/or Phrase Lacking Written Description and/or Enablement |
|---|---|---|
| '983 | 1, 4, 7 | "determining a second network bandwidth limit for the first user based on the first network bandwidth limit associated with each of the users" |
| '983 | 1, 4, 7 | "dynamically updating at least one of the first network bandwidth limits associated with the plurality of users based on the second network bandwidth limit" |
| '983 | 1, 4, 7 | " configuring the access control device to operate in a second state," |
| '983 | 1, 4, 7 | "wherein operation of the access control device in the second state comprises regulating network bandwidth usage for each of the plurality of users based on the first network bandwidth limits" |
| '983 | 2, 5, 8 | "determining a third network bandwidth limit for the second user based on the one or more attributes of the second user profile and the first user device" |
| '983 | 3, 6, 9 | "dynamically updating at least one of the first network bandwidth limits based on the second network bandwidth limit comprises dynamically updating the first network bandwidth associated with the first user to the second network bandwidth" |
| '426 | 1 | "receiving, by the machine, an authentication request from a principal, the request directed by the principal to an external service and intercepted by the method for receipt" |
| '426 | 1 | "the authentication message serves as a new authentication request and as a new authentication response for single sign-on access of the principal to the identity service and other services external or internal to the identity service" |
| '426 | 1 | "the identity service acts as a proxy for access sessions to the other services on behalf of the principal" |
| '426 | | "the principal's access sessions occur indirectly through the identity service and transparently to the principal" |
| '426 | 1 | "wherein the authentication message includes the new authentication request made on behalf of the principal and the authentication message also includes a new authentication response that satisfies the new authentication request" |

| Patent | Claim(s) | Term and/or Phrase Lacking Written Description and/or Enablement |
|---|---|---|
| '426 | 1 | "that response vouches for authentication of the principal to the identity service for the single sign-on access of the principal" |
| '426 | 1 | "which is one of the other services that the identity service controls access to" |
| '426 | 1 | "a determination as to whether to use a single interaction or multiple interactions for authentication of the principal to the other services is automatically communicated in the new authentication response" |
| '426 | 2 | "making, by the machine, a target service available to interactions between the principal and an external service" |
| '426 | 2 | "the target service is directly accessible from an environment of the identity service" |
| '426 | 4 | "the principal is currently already properly authenticated to the processing associated with the method" |
| '426 | 5 | "supplying further includes adding a second authentication to a second redirection of the principal, wherein the second authentication represents authentication of the principal to the identity service and wherein the second redirection directs the principal to request a target service that is to be proxied on behalf of the principal from the identity service" |
| '426 | 6 | "representing the new authentication response as an instruction to the identity service to enforce its own independent authentication with the principal before considering the principal authenticated to the identity service" |
| '936 | 1, 12 | "data indicating a state of a respective computer" |
| '936 | 1, 12 | "snapshot" |
| '936 | 1, 12 | "adaptive reference model comprising a rule set customized to characteristics of the population of computers" |
| '936 | 1, 12 | "the rule set being developed by identifying patterns among the snapshots from the plurality of computers such that the adaptive reference model is indicative of normal states in the computers within the population" |
| '936 | 3, 14 | "generic response not specific to a particular asset of the at least one computer" |
| '936 | 3, 14 | "send[ing] the generic response and a set of anomalies found in the snapshot to the at least one computer, the set of |

| Patent | Claim(s) | Term and/or Phrase Lacking Written Description and/or Enablement |
|---|---|---|
| | | anomalies indicating assets of the at least one computer whose states are anomalous" |
| '936 | 5, 16 | "wherein the recognition filter comprises a particular pattern of anomalies that indicates the presence of a particular root cause condition or a generic class of conditions" |
| '936 | 6, 20 | "comparing a plurality of anomalies associated with a particular snapshot with a recognition filter to diagnose a trouble condition" |
| '936 | 9, 17 | "wherein the adaptive reference model is generated to include a value layer that determines whether an asset value contained in a snapshot is anomalous" |
| '936 | 10, 18 | "wherein the adaptive reference model is generated to include a cluster layer that tracks relationships between assets and identifies an anomaly in response to an asset being unexpectedly absent from or present in a set of assets in a snapshot" |
| '282 | 1 | "accepting or denying the packet based on the set of firewall rules, wherein the set of firewall rules is dynamically self-configurable during runtime without operator interaction, wherein the set of firewall rules comprises a plurality of chains of rules forming various paths through a hierarchical structure, and wherein the hierarchical structure comprises defined places for dynamically updating the set of firewall rules during runtime" |
| '282 | 2 | "wherein dynamically updating the set of firewall rules during runtime further comprises, during runtime, adding a rule to the set of firewall rules, deleting a rule from the set of firewall rules, or modifying a rule in the set of firewall rules without operator interaction" |
| '282 | 3 | "wherein associating the set of firewall rules with the at least one node further comprises associating a first subset of the set of firewall rules with the first node" |
| '282 | 4 | "wherein the at least one node further comprises at least two nodes including a second node, further comprising associating a second subset of the set of firewall rules with the second node" |
| '282 | 5 | "wherein the first subset of firewall rules is the same as or at least partially different from the second subset of firewall rules" |

| Patent | Claim(s) | Term and/or Phrase Lacking Written Description and/or Enablement |
|---|---|---|
| '282 | 6, 17, 30 | "wherein [one of /either] the first subset of firewall rules or second subset of firewall rules equals the entire set of firewall rules" |
| '282 | 12 | "a first computer readable storage medium storing a set of firewall rules, wherein the set of firewall rules is dynamically self-configurable during runtime without operator interaction, wherein the set of firewall rules comprises a plurality of chains of rules forming various paths through a hierarchical structure, and wherein the hierarchical structure comprises defined places for dynamically updating the set of firewall rules during runtime without operator interaction" |
| '282 | 12 | "when a packet is received at one of the two or more network interfaces associated with the at least one node, accept or deny the packet based on a review of the set of firewall rules" |
| '282 | 14, 27 | "wherein the [data controlling computer program code /computer instructions] [is/are] further executable to: associate a first subset of the set of firewall rules with the first node; and if the packet is received at the first node, apply the first subset of the set of firewall rules associated with the first node" |
| '282 | 15, 28 | "wherein the at least one node further comprises at least two nodes including a second node, and wherein the data controlling computer program code is further executable to: associate a second subset of the set of firewall rules with the second node; and if the packet is received at the second node, apply the second subset of the set of firewall rules associated with the second node" |
| '282 | 16, 29 | "wherein the first subset of the set of firewall rules is the same as or different from the second subset of the set of firewall rules" |
| '282 | 22, 35 | "wherein each of the plurality of network interfaces is physically connected to every other network interface of the plurality of network interfaces and wherein physical connection between the plurality of network interfaces comprises indirect physical connection between the plurality of network interfaces" |

| Patent | Claim(s) | Term and/or Phrase Lacking Written Description and/or Enablement |
|---|---|---|
| '282 | 23 | "wherein the data controlling computer program code is further executable to dynamically update the set of firewall rules during runtime without operator interaction" |
| '282 | 24 | "wherein the data controlling computer program code is further executable to dynamically update the set of firewall rules during runtime without operator interaction." |
| '282 | 24 | "accept or deny the packet based on a review of the set of firewall rules, wherein the set of firewall rules is dynamically self-configurable during runtime without operator interaction" |
| '153 | 1, 10 | "wherein the user bandwidth allocation profile contains an arbitrary number of attributes specifying bandwidth limitations for the first user" |
| '153 | 1, 10 | "at least one traffic control rule" |
| '153 | 1 | "considering said information identifying said user device" |
| '153 | 1, 10 | "utilizing said at least one traffic control rule associated with said first user" |
| '153 | 2, 11 | "indexing said user specific rules" |
| '153 | 3, 12 | "filling in missing attribute values with default values" |
| '153 | 6 | "mapping said attributes in said user bandwidth allocation profile" |
| '153 | 6, 13 | "tracking said control session by said user credentials, one or more addresses of said user device, an identifier, or a combination" |
| '153 | 8, 9 | "mapping attributes in said user bandwidth allocation profile for said first user of at least one traffic control rule stored on said control device" |
| '153 | 15 | "based on the arbitrary number of attributes in each user profile, establish user specific rules and conditions that are bound to each user" |

| Patent | Claim(s) | Term and/or Phrase Lacking Written Description and/or Enablement |
|---|---|---|
| '153 | 15 | "associate each of said user specific rules with said first user based on an arbitrary identifier associated with a user device" |
| '153 | 17 | "map said priorities to a user specific traffic control rule" |
| '153 | 22 | "session monitoring module operable to perform bandwidth metering" |
| '697 | 1, 15, 24 | "receiving one or more transmission control protocol (TCP) packets originating from an access device coupled to the service provider network" |
| '697 | 1, 15, 24 | "the one or more TCP packets defining a TCP session between a computing device coupled to the access device" |
| '697 | 1, 15, 24 | "generating an alert identifying a network address associated with the access device, the malware ID and the OS ID associated with TCP session that generated the alert" |
| '697 | 2, 16 | "determin[ing] a protocol associated with the TCP packets and matching an OS fingerprint from one or more protocol parameters if present in the TCP packets to determine a first operating system identifier (ID)" |
| '697 | 2, 16 | "determin[ing] an application parameter associated with the TCP session if present, and identifying a second OS ID from the application parameter" |
| '697 | 3, 17 | "a notification to a subscriber associated with the network address associated with the access device, the notification identifying a remediation portal to remove the determined malware in the alert" |
| '697 | 4, 25 | "identifying at the remediation portal the subscriber accessing the remediation portal" |
| '697 | 4, 25 | "identifying the OS associated with the computing device used by the subscriber to access the remediation portal" |
| '697 | 4, 25 | "comparing the OS associated with the computing device to the at least one of the first OS ID or second OS ID identified in the alert" |
| '697 | 4, 25 | "providing malware remediation to the computing device when the at least one of the first OS ID or second OS ID matches the OS associated with the computing device" |
| '697 | 5 | "wherein if the OS of the computing device is not the at least one of the first OS ID or second OS ID identified in the alert an indication is provided to the subscriber to |

| Patent | Claim(s) | Term and/or Phrase Lacking Written Description and/or Enablement |
|---|---|---|
| | | connect to the remediation portal with an other computing device connected to the access device" |
| '697 | 6 | "wherein the alert is cleared when all computing devices associated with the access device and the computing device having the at least one of the first OS ID or second OS ID have accessed the remediation portal" |
| '697 | 7, 19 | "determin[ing] the first OS ID is performed by comparing one or more protocol parameters of the one or more TCP packets having a SYN flag associated with the session, wherein the OS fingerprints identify the protocol parameters of the SYN flagged packet and the OS ID associated with parameters" |
| '697 | 9, 21 | "a more reliable OS ID" |
| '697 | 11, 23 | "the second OS ID provides additional information" |
| '697 | 12, 18 | "send[ing] the notification to the subscriber associated with the access device further comprises replacing the network address of the access device with a subscriber ID" |
| '697 | 13 | "detailed alerts" |

## VI. P.R. 3-4: DISCLOSURES AND PRODUCTIONS

Alongside these contentions, Fortinet makes a production in compliance with the Patent Local Rules of this District.

### A. Technical Documents

Fortinet has produced technical documents showing the operation of its products, including the Accused Products, in accordance with P.R. 3-4(a). Discovery is ongoing, and Fortinet reserves the right to supplement this production as additional information is discovered in accordance with the Local Rules of this District, the Federal Rules, and any other applicable statute or rules.

### B. Prior Art Documents

Fortinet has produced prior art documents, including the above-cited prior art patents and publications, in accordance with P.R. 3-4(b). Discovery is ongoing, and Fortinet reserves the right to supplement this production as additional information is discovered in accordance with the Local Rules of this District, the Federal Rules, and any other applicable statute or rules.

### C. Comparable Agreements and Agreements Supporting Damages Case

Fortinet has produced agreements in accordance with Patent Local Rules 3-4(c), and 3-4(e) that may be related to the accused instrumentalities, that may be comparable, and/or that Fortinet may rely on in connection with its damages case. This production should not be taken as an admission that any such agreement is comparable. Fortinet will disclose its damages contentions in compliance with the local rules. Discovery is ongoing, and Fortinet reserves the right to supplement this production as additional information is discovered in accordance with the Local Rules of this District, the Federal Rules, and any other applicable statutes or rules.

### D. Financial Documents

Fortinet has produced financial information in accordance with Patent Local Rule 3-4(d). Discovery is ongoing, and Fortinet reserves the right to supplement this production as additional information is discovered in accordance with the Local Rules of this District, the Federal Rules, and any other applicable statutes or rules.

Dated: August 15, 2025

Respectfully submitted,

*/s/ Andrew D. Gish*

Ryan Iwahashi (CA SBN 284766)
ryan@gishpllc.com
**GISH PLLC**
50 California Street, Suite 1500
San Francisco, CA 94111
Phone: (415) 630-2000

Andrew D. Gish (NY SBN 4918454) *(pro hac vice)*
andrew@gishpllc.com
Christopher Gerson (NY SBN 4595708) *(pro hac vice)*
Chris.Gerson@gishpllc.com
**GISH PLLC**
41 Madison Avenue, Floor 31
New York, NY 10010
Phone: (212) 518-7380

*Attorneys for Fortinet, Inc.*

.

**CERTIFICATE OF SERVICE**

The undersigned hereby certifies that counsel of record has been served August 15, 2025, with a copy of the foregoing document via email.

*/s/Hilary C. Efron*