

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

Fortinet, Inc.,

Petitioner,

v.

Netskope, Inc.,

Patent Owner.

---

Case No. 2026-0042

U.S. Patent 8,543,710

---

**PETITION FOR *INTER PARTES* REVIEW**

Mail Stop "PATENT BOARD"

Patent Trial and Appeal Board

U.S. Patent Trademark Office

P.O. Box 1450

Alexandria, VA 22313-1450

TABLE OF CONTENTS

|                                                                                                      | <u>Page</u> |
|------------------------------------------------------------------------------------------------------|-------------|
| TABLE OF ABBREVIATIONS .....                                                                         | vii         |
| EXHIBIT LIST .....                                                                                   | viii        |
| I. INTRODUCTION .....                                                                                | 1           |
| II. Requirements for inter partes review .....                                                       | 3           |
| A. GROUNDS FOR STANDING (37 C.F.R. §42.104(a)).....                                                  | 3           |
| B. Identification of Challenge.....                                                                  | 3           |
| 1. The Specific Art on Which the Challenge is Based.....                                             | 4           |
| 2. Roskind is Entitled To the 9/27/2004 Filing Date of the<br>Roskind Provisional .....              | 4           |
| 3. Statutory Grounds on Which the Challenge is Based.....                                            | 10          |
| 4. How the Challenged Claims are Unpatentable .....                                                  | 10          |
| III. THE PATENT AND STATE OF THE ART .....                                                           | 10          |
| A. The '710 Patent.....                                                                              | 10          |
| B. The Challenged Claims Are Not Entitled to Claim Priority To<br>The Provisional Application .....  | 11          |
| C. File History.....                                                                                 | 12          |
| D. POSITA.....                                                                                       | 13          |
| IV. Claim Construction.....                                                                          | 14          |
| A. "subordinate to" .....                                                                            | 14          |
| V. Grounds of Unpatentability .....                                                                  | 15          |
| A. Grounds 1 and 2 – Claims 1-20 Are Anticipated Or At<br>Minimum Rendered Obvious Over Roskind..... | 17          |

|     |                                                                                                                                                                                                                                                                                                                                         |    |
|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 1.  | Overview of Roskind .....                                                                                                                                                                                                                                                                                                               | 17 |
| 2.  | Independent Claim 1 .....                                                                                                                                                                                                                                                                                                               | 19 |
| 3.  | Claim [2]: "The method according to claim 1, 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." .....                                                                                       | 37 |
| 4.  | Claim [3]: "The method according to claim 1, further comprising: 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." .....                                                                                       | 39 |
| 5.  | Claim [4]: "The method according to claim 1, further comprising: filtering the network traffic emanating from the client device to limit network packet flow by the client device." .....                                                                                                                                               | 40 |
| 6.  | Claim [5]: "The method according to claim 1, further comprising: routing the network traffic emanating from the client device to limit network packet traversal by the client device." .....                                                                                                                                            | 41 |
| 7.  | Claim [6]: "The method according to claim 1, wherein the plurality of quarantine control functions further comprises: restricting all network traffic emanating from the client device to one or more network destination addresses in one or more network segments that are not in or subordinate to the first network segment." ..... | 42 |
| 8.  | Claim [7]: "The method according to claim 1, further comprising: performing all of the plurality of quarantine control functions over the client device." .....                                                                                                                                                                         | 42 |
| 9.  | Claims 8 and 15 .....                                                                                                                                                                                                                                                                                                                   | 43 |
| 10. | Claims 9-14 and 16-20.....                                                                                                                                                                                                                                                                                                              | 45 |

|    |                                                                                                                                                                                                                                                                                                                                                        |    |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| B. | Grounds 3 and 4 – Claims 1-20 Are Anticipated Or At<br>Minimum Rendered Obvious Over Gleichauf .....                                                                                                                                                                                                                                                   | 46 |
| 1. | Overview of Gleichauf.....                                                                                                                                                                                                                                                                                                                             | 46 |
| 2. | Independent Claim 1 .....                                                                                                                                                                                                                                                                                                                              | 49 |
| 3. | Claim [2]: "The method according to claim 1, wherein<br>the action requires the user to obtain and execute<br>abnormal behavior scanning software from a server<br>machine running at one of the one or more allowed<br>network destination addresses." .....                                                                                          | 60 |
| 4. | Claim [3]: "The method according to claim 1, further<br>comprising: evaluating network traffic emanating from<br>the client device after the client device has been scanned<br>and abnormal behavior has been removed, mitigated or<br>rendered inert." .....                                                                                          | 62 |
| 5. | Claim [4]: "The method according to claim 1, further<br>comprising: filtering the network traffic emanating from<br>the client device to limit network packet flow by the<br>client device." .....                                                                                                                                                     | 63 |
| 6. | Claim [5]: "The method according to claim 1, further<br>comprising: routing the network traffic emanating from<br>the client device to limit network packet traversal by the<br>client device." .....                                                                                                                                                  | 63 |
| 7. | Claim [6]: "The method according to claim 1, wherein<br>the plurality of quarantine control functions further<br>comprises: restricting all network traffic emanating from<br>the client device to one or more network destination<br>addresses in one or more network segments that are not<br>in or subordinate to the first network segment." ..... | 64 |
| 8. | Claim [7]: "The method according to claim 1, further<br>comprising: performing all of the plurality of quarantine<br>control functions over the client device." .....                                                                                                                                                                                  | 65 |
| 9. | Claims 8 and 15 .....                                                                                                                                                                                                                                                                                                                                  | 65 |

|       |                                                                                     |    |
|-------|-------------------------------------------------------------------------------------|----|
| 1.    | Claims 9-14 and 16-20.....                                                          | 67 |
| C.    | Grounds 5 and 6 – Grounds 1-4 in View of Short .....                                | 67 |
| VI.   | MANDATORY Notices Under 37 C.F.R. §42.8(a)(1) .....                                 | 72 |
| A.    | 37 C.F.R. §42.8(b)(1): Real Parties-In-Interest.....                                | 72 |
| B.    | 37 C.F.R. §42.8(b)(2): Related Matters .....                                        | 72 |
| C.    | 37 C.F.R. §42.8(b)(3)-(4): Lead And Back-Up Counsel And<br>Service Information..... | 72 |
| VII.  | FEES UNDER 37 C.F.R. §42.103 .....                                                  | 73 |
| VIII. | CONCLUSION .....                                                                    | 73 |

## TABLE OF AUTHORITIES

### Cases

|                                                                                                          |       |
|----------------------------------------------------------------------------------------------------------|-------|
| <i>Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.</i> ,<br>800 F.3d 1375 (Fed. Cir. 2015) .....          | 4, 9  |
| <i>In re Riggs</i> ,<br>131 F.4th 1377 (Fed. Cir. 2025) .....                                            | 9, 68 |
| <i>Intel Corp. v. Qualcomm Inc.</i> ,<br>21 F.4th 801 (Fed. Cir. 2021) .....                             | 15    |
| <i>Phillips v. AWH Corp.</i> ,<br>415 F.3d 1303 (Fed. Cir. 2005) .....                                   | 14    |
| <i>PowerOasis, Inc. v. T-Mobile USA, Inc.</i> ,<br>522 F.3d 1299 (Fed. Cir. 2008) .....                  | 12    |
| <i>Samsung Electronics America, Inc. v. Prisia Eng'g Corp.</i> ,<br>948 F.3d 1342 (Fed. Cir. 2020) ..... | 15    |

### Statutes

|                     |       |
|---------------------|-------|
| 35 U.S.C. §102..... | 10    |
| 35 U.S.C. §103..... | 10    |
| 35 U.S.C. §112..... | 4, 12 |
| 35 U.S.C. §311..... | 1     |

### Rules

|                            |    |
|----------------------------|----|
| 37 C.F.R. §42.103 .....    | 73 |
| 37 C.F.R. §42.104(b) ..... | 3  |

|                               |    |
|-------------------------------|----|
| 37 C.F.R. §42.104(b)(4) ..... | 10 |
| 37 C.F.R. §42.104(b)(5) ..... | 10 |
| 37 C.F.R. §42.21 .....        | 1  |
| 37 C.F.R. §42.8(a)(1) .....   | 72 |
| 37 C.F.R. §42.8(b)(1) .....   | 72 |
| 37 C.F.R. §42.8(b)(2) .....   | 72 |
| 37 C.F.R. §42.8(b)(3) .....   | 72 |
| 37 C.F.R. §42.8(b)(4) .....   | 72 |

**TABLE OF ABBREVIATIONS**

| <b>Abbreviation</b> | <b>Full Name</b>                    |
|---------------------|-------------------------------------|
| '710 Patent         | U.S. Patent No. 8,543,710           |
| Challenged Claims   | Claims 1-20 of the '710 Patent      |
| Patent Owner, PO    | Patent Owner Netskope, Inc.         |
| Petitioner          | Petitioner Fortinet, Inc.           |
| POSITA              | Person of Ordinary Skill In The Art |

**EXHIBIT LIST**

| <b>Exhibit No.</b> | <b>Document</b>                                                                              |
|--------------------|----------------------------------------------------------------------------------------------|
| 1001               | U.S. Patent No. 8,543,710 ("the '710 patent")                                                |
| 1002               | File History of the '710 patent                                                              |
| 1003               | Declaration of John R. Black                                                                 |
| 1004               | U.S. Provisional Patent Application No. 60/551,702 ("the '702 Provisional")                  |
| 1005               | U.S. Patent No. 9,398,037 to Roskind et al. ("Roskind")                                      |
| 1006               | U.S. Provisional Patent Application No. 60/613,909 to Roskind et al. ("Roskind Provisional") |
| 1007               | U.S. Patent Pub. 2003/0191966 to Gleichauf ("Gleichauf")                                     |
| 1008               | U.S. Patent No. 6,636,894 to Short et al. ("Short")                                          |

## I. INTRODUCTION

Petitioner Fortinet, Inc. ("Petitioner") respectfully petitions, under 35 U.S.C. §311 and 37 C.F.R. §42.21, for *inter partes* review ("IPR") of claims 1-20 ("the Challenged Claims") of U.S. Patent No. 8,543,710 ("the '710 patent") (EX1001) on the grounds below.<sup>1</sup>

The '710 patent generally relates to a method of "network access control" within a communications network. EX1001, 1:15-16. The alleged invention "make[s] use of network firewall rule technology" to confine users to particular networks and to the use of particular network protocols based on the access policies of the network and clients. *Id.*, 2:9-14; 3:48-55. The '710 patent refers to these measures of confining a computer to a particular network as a "quarantine." *See, id.*, 5:25-30.

But as demonstrated at least by the multiple rejections during prosecution, the only purported invention of the '710 patent is the restricting of network protocols during a so-called "quarantine." *Infra*, § III.C. As discussed herein, it was already well-known to "quarantine" computers—especially computers infected with a virus—to (a) disable communications other than ones necessary to remedy the virus; and (b) limit the use of network protocols other than those necessary to remedy the

---

<sup>1</sup> Unless otherwise noted, all emphases and annotations have been added.

virus.

For example, **Roskind** (EX1005) discloses a system and method for a gateway (or router) to "identify and intercept unauthorized, unwanted, and/or otherwise malicious communications." EX1005, 3:10-12. The gateway is "configured to provide and control access between a protected network and the Internet," and is used to "quarantine a local computer." EX1005, 11:63-67. This includes "restrict[ion] by the quarantine to certain classes of traffic, such as HTTP requests." *Id.*, 11:39-54. Similarly, **Gleichauf** discloses a method "for detecting an infective element in a network environment" that "allows for the quarantine of malicious traffic immediately after it is discovered within the network architecture." Gleichauf, [0020]. As part of this quarantine, the network management controller can "disable the communications" of an infected computer and disable any other "policies or services being provided to infected [computer]" until it is brought into compliance by visiting a remediator website using the allowed communication protocol, *e.g.*, TCP/IP. Gleichauf, [0006], [0008], [0058].

Thus, as further explained below, the prior art—none of which was before the Examiner—anticipates, and at minimum renders obvious, claims 1-20 of the '710 patent.

## **II. REQUIREMENTS FOR INTER PARTES REVIEW**

### **A. GROUNDS FOR STANDING (37 C.F.R. §42.104(a))**

Petitioner certifies that the '710 patent is available for IPR and that Petitioner is not barred or estopped from requesting IPR of the Challenged Claims on the grounds in this petition. The '710 patent issued more than 9 months ago, and Petitioner was served with the complaint alleging infringement of the '710 patent less than one year ago.

### **B. Identification of Challenge**

Pursuant to §42.104(b), Petitioner requests IPR of claims 1-20, and that the Board cancel the same as unpatentable. The '710 matured from U.S. Application 10/076,591 (filed 3/10/2005), and claims priority to U.S. Provisional Application 60/551,702 (filed 3/10/2004) ("the '702 Provisional"). However, the Challenged Claims of the '710 patent are not fully supported by the '702 Provisional and are therefore not entitled to its priority date. *Infra*, §III.B. Thus, for purposes of this proceeding, the priority date for the '710 patent is March 10, 2005. Even under the alleged March 10, 2004 priority date, however, the claims still would be unpatentable in view of the art and arguments set forth in Grounds 3-4, 6.

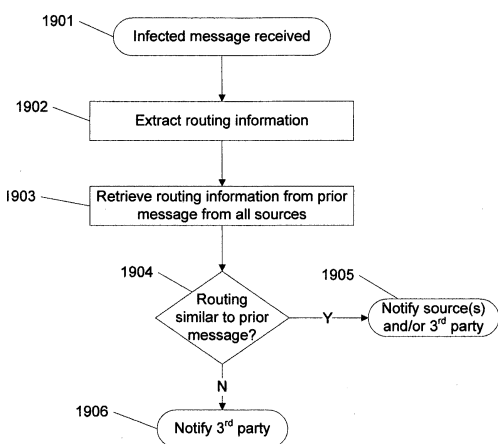
**1. The Specific Art on Which the Challenge is Based**

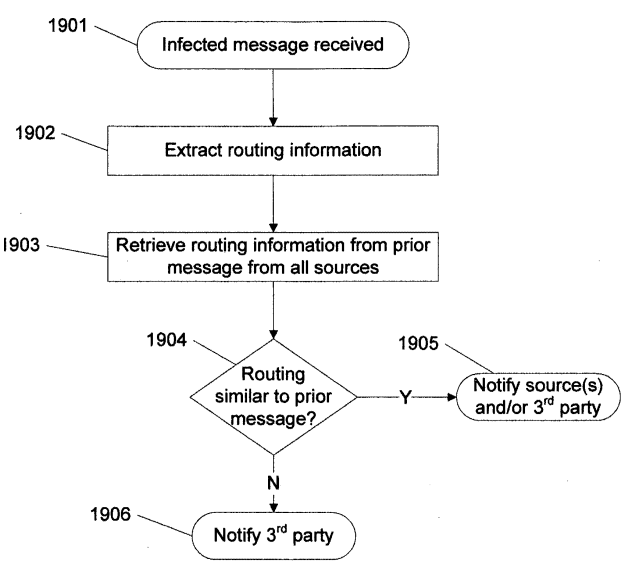
| Name      | Exhibit | Patent / Publication          | Filed      | Issued / Published | Prior art under at least |
|-----------|---------|-------------------------------|------------|--------------------|--------------------------|
| Roskind   | 1005    | U.S. 9,398,037                | 9/27/20050 | 7/19/2016          | §102(e)                  |
| Gleichauf | 1007    | U.S. Patent Pub. 2003/0191966 | 4/9/2002   | 10/9/2003          | §102(a)                  |
| Short     | 1008    | U.S. 6,636,894                | 12/8/1999  | 10/21/2003         | §102(a)                  |

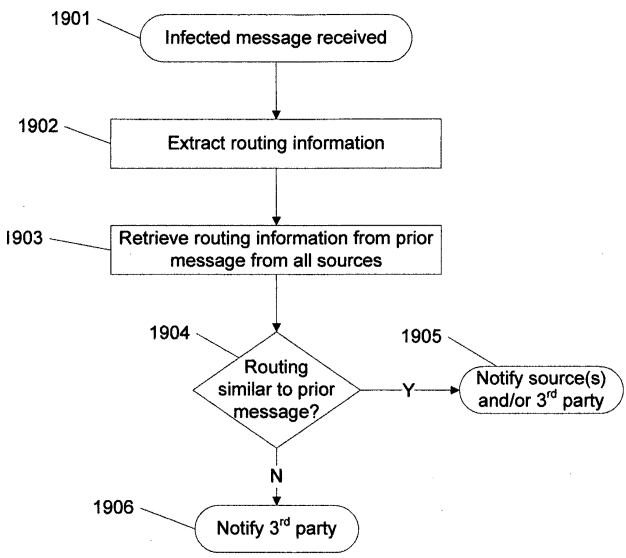
**2. Roskind is Entitled To the 9/27/2004 Filing Date of the Roskind Provisional**

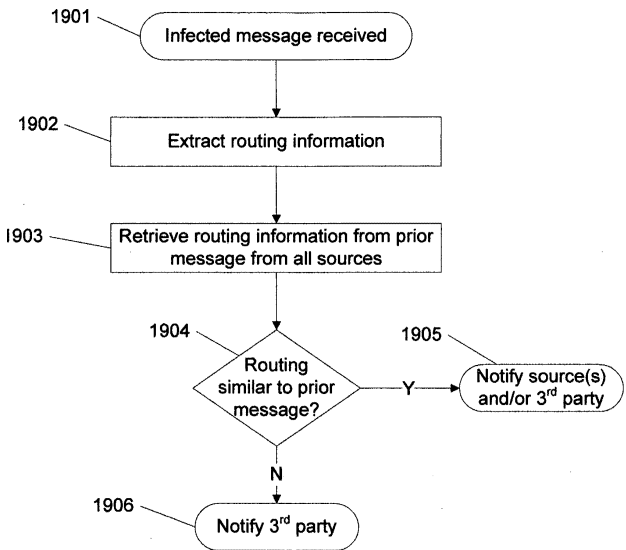
Roskind claims priority to a provisional application filed 9/27/2004, and is entitled to that date for purposes of this patentability challenge. EX1005. *See Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1382 (Fed. Cir. 2015) (quotation marks omitted) ("reference patent is only entitled to claim the benefit of the filing date of its provisional application if the disclosure of the provisional application provides support for the claims in the reference patent in compliance with § 112, ¶ 1"). Because the Roskind Provisional provides support to claim 1 of Roskind, as set forth in the chart below, Roskind is entitled to the 9/27/2004 priority date of the Roskind Provisional.

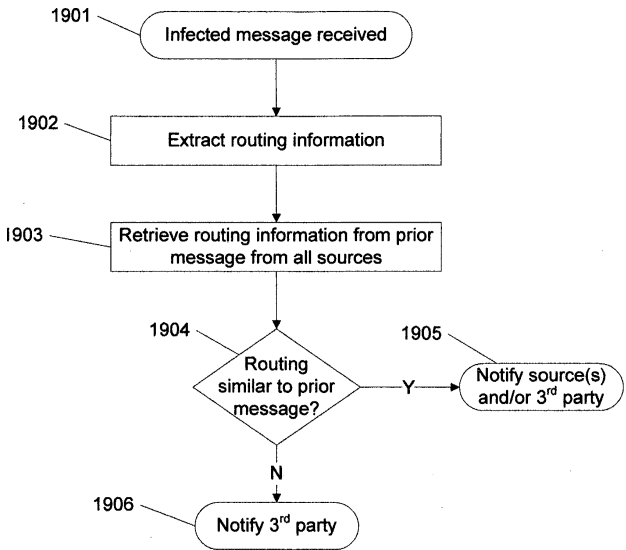
| Claim 1 of Roskind (EX1005)  | Roskind Provisional (EX1006)                      |
|------------------------------|---------------------------------------------------|
| [1.pre] A method, comprising | <b>4:1-5</b> (disclosing "a process").            |
| [1.1] determining that a     | <b>33:20-34:2</b> ("FIG 19 is a flow diagram of a |

| Claim 1 of Roskind (EX1005)                                                                                                                            | Roskind Provisional (EX1006)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| received network communication is classified by anti-contagion software as infected;                                                                   | method for notifying possible sources of infection according to some embodiments. In this example, an infected message is received (1901). An example of <i>an infected message</i> is <i>a message classified as such by anti-contagion software.</i> ")                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| [1.2] extracting first routing information from the received network communication;                                                                    | <b>34:1-7</b> (" <i>Routing information may be extracted from the message</i> (1902)....")                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| [1.3] determining whether second routing information from a prior network communication received previously matches the first routing information; and | <p><b>34:7-21</b> ("Routing information from previously received messages may be retrieved (1903).... <i>Routing information for the infected message may be compared with the retrieved routing information</i> (1904). <i>If no similarity with previous messages is found</i> (1904) then third party notification is optionally made.... <i>If a similarity is found with previous messages</i> (1904) then a notification may be sent (1905) in this example....")</p> <p><b>FIG 19 (1904):</b></p>  <pre> graph TD     1901([1901: Infected message received]) --&gt; 1902[1902: Extract routing information]     1902 --&gt; 1903[1903: Retrieve routing information from prior message from all sources]     1903 --&gt; 1904{1904: Routing similar to prior message?}     1904 -- Y --&gt; 1905([1905: Notify source(s) and/or 3rd party])     1904 -- N --&gt; 1906([1906: Notify 3rd party])     </pre> <p><b>Figure 19</b></p> |

| Claim 1 of Roskind<br>(EX1005)                                                                                                                                                                                                                                                                                                                | Roskind Provisional (EX1006)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>[1.4a] sending a notification that the received network communication was classified as infected,</p>                                                                                                                                                                                                                                      | <p><b>33:20-21</b> ("FIG 19 is a flow diagram of a method for <i>notifying possible sources of infection</i> according to some embodiments.")</p> <p><b>FIG 19</b> (1905, 1906):</p>  <pre> graph TD     1901([1901: Infected message received]) --&gt; 1902[1902: Extract routing information]     1902 --&gt; 1903[1903: Retrieve routing information from prior message from all sources]     1903 --&gt; 1904{1904: Routing similar to prior message?}     1904 -- Y --&gt; 1905([1905: Notify source(s) and/or 3rd party])     1904 -- N --&gt; 1906([1906: Notify 3rd party])     </pre> <p><b>Figure 19</b></p> |
| <p>[1.4b] wherein the notification is sent to a recipient selected from the group consisting of a sender associated with the prior network communication and a third party, wherein the third party is not a sender of the prior network communication and wherein the third party is not a sender of the received network communication,</p> | <p><b>34:12-35:7</b> ("If no similarity with previous message is found (1904) then <b>third party notification</b> is optionally made (1906) in this example. An example of a third party notification is sending notification to the ISP that provides network access to the message source. Another example of notifying a third party is notifying a viral clearinghouse of the apparent source of a viral message. Another example of a notifying a third party is notifying a collaborative filter service... [N]otification may be sent (1905) to one or more sources of the prior message(s) that best match the infected message, and/or to third</p>                                             |

| Claim 1 of Roskind<br>(EX1005)                                                                                                                                                                                 | Roskind Provisional (EX1006)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                | <p>parties...")</p> <p><b>FIG 19</b> (1905, 1906):</p>  <pre> graph TD     1901([Infected message received]) --&gt; 1902[Extract routing information]     1902 --&gt; 1903[Retrieve routing information from prior message from all sources]     1903 --&gt; 1904{Routing similar to prior message?}     1904 -- Y --&gt; 1905([Notify source(s) and/or 3rd party])     1904 -- N --&gt; 1906([Notify 3rd party])   </pre> <p><b>Figure 19</b></p> |
| <p>[1.4c] wherein the recipient is selected as the sender associated with the prior network communication if it is determined that the first routing information and the second routing information match,</p> | <p><b>34:13-35:3</b> ("Routing information for the infected message may be compared with the retrieved routing information (1904).... If <i>a similarity is found with previous message</i> (1904) then a notification may be sent (1905) in this example.... [N]otification may be sent (1905) to one or more sources of the prior message(s) that best match the infected message...")</p>                                                                                                                                          |

| Claim 1 of Roskind<br>(EX1005)                                                                                                                                              | Roskind Provisional (EX1006)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                             | <p><b>FIG 19 (1905):</b></p>  <pre> graph TD     1901([1901: Infected message received]) --&gt; 1902[1902: Extract routing information]     1902 --&gt; 1903[1903: Retrieve routing information from prior message from all sources]     1903 --&gt; 1904{1904: Routing similar to prior message?}     1904 -- Y --&gt; 1905([1905: Notify source(s) and/or 3rd party])     1904 -- N --&gt; 1906([1906: Notify 3rd party])     </pre> <p><b>Figure 19</b></p> |
| <p>[1.4d] and wherein the recipient is selected as the third party if it is not determined that the first routing information and the second routing information match.</p> | <p><b>34:13-15</b> ("Routing information for the infected message may be compared with the retrieved routing information (1904). <i>If no similarity with previous messages is found (1904) then third party notification is optionally made (1906) in this example.</i>")</p> <p><b>FIG 19 (1906):</b></p>                                                                                                                                                                                                                                      |

| Claim 1 of Roskind<br>(EX1005) | Roskind Provisional (EX1006)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                |  <pre> graph TD     1901([1901 Infected message received]) --&gt; 1902[1902 Extract routing information]     1902 --&gt; 1903[1903 Retrieve routing information from prior message from all sources]     1903 --&gt; 1904{1904 Routing similar to prior message?}     1904 -- Y --&gt; 1905([1905 Notify source(s) and/or 3rd party])     1904 -- N --&gt; 1906([1906 Notify 3rd party])     </pre> <p style="text-align: center;"><b>Figure 19</b></p> |

EX1003, ¶¶63-65. Roskind is therefore prior art under at least §102(e). See *Dynamic Drinkware*, 800 F.3d at 1382. Consistent with *In re Riggs*, 131 F.4th 1377 (Fed. Cir. 2025), the Roskind Provisional “also provide[s] written description support for the specific portions of the patent specification identified and relied on in the prior art rejection” and exemplary cites thereto will be included in the analysis below.

### 3. Statutory Grounds on Which the Challenge is Based

| Ground | Claims | Basis | Prior Art                  |
|--------|--------|-------|----------------------------|
| 1      | 1-20   | §102  | Roskind                    |
| 2      | 1-20   | §103  | Roskind                    |
| 3      | 1-20   | §102  | Gleichauf                  |
| 4      | 1-20   | §103  | Gleichauf                  |
| 5      | 1-20   | §103  | Roskind in view of Short   |
| 6      | 1-2    | §103  | Gleichauf in view of Short |

### 4. How the Challenged Claims are Unpatentable

Petitioner provides the information required under §§42.104(b)(4)-(5) in §V

## III. THE PATENT AND STATE OF THE ART

### A. The '710 Patent

The '710 patent generally relates to a method of "confining a network client's network access to a specific region of the network." EX1001, 1:58-60. The alleged invention "make[s] use of network firewall rule technology" to confine users to particular networks based on the access policies of the network and clients. *Id.*, 2:9-15. In addition, the alleged invention "may offer the technical advantages of a way to reduce the negative effects of virus and worm infections" on a network. *Id.*, 2:20-24. "Users can...be notified of computer infections and offered a means to seek resolution." *Id.*, 2:24-26. EX1003, ¶49.

As the '710 patent specification teaches, the system may use these standard firewall techniques "to 'quarantine' certain clients...to particular walled garden(s)...while simultaneously allowing other clients...unhindered access to the

internet." EX1001, 5:25-31. This may be implemented to control a "computer...infected with a worm" whereby the "gateway 11 notices the abusive traffic and 'quarantines' [the] client" by, for example, restricting the client's ability to communicate with destinations outside the walled garden. *Id.*, 5:54-64. EX1003, ¶50.

Once restricted, "[t]he quarantined client may then attempt to browse a web page on the Internet. In response to this attempt, the gateway redirects the web request to a cooperating web server...[which] renders a web page informing the client of its perceived infection and offering links to self-help documents and to the websites of anti-virus vendors and the client's OS vendor." EX1001, 5:65-6:7. EX1003, ¶51.

**B. The Challenged Claims Are Not Entitled to Claim Priority To The Provisional Application**

All the Challenged Claims recite "quarantine control functions" to be performed by the network access gateway device, including "restricting all network traffic emanating from the client device to an allowed network destination address *to selected one or more network protocols*." As the specification explains, controlling a network may involve "limit[ing] the network segments or routes available, as well as the network protocol traffic permitted...where a network *client may be constrained in terms of the types of network protocols* (and applications) *that they are permitted....*" EX1001, 3:48-55; *see also id.*, 6:17-24 ("...all network

requests from a client in network protocols other than HTTP are denied if they emanate from a constrained client...). The '710 patent purports to claim priority to the '702 Provisional, but the priority application does not disclose or in any way discuss limiting network traffic to a select one or more network protocols. *See generally*, EX1004. Thus, because the '702 Provisional fails to disclose every element of any Challenged Claim—including elements added to overcome the prior art (*infra* § III.C), the earliest priority date to which the Challenged Claims are entitled is 3/10/2005, the filing date of the application leading to the '710 patent. *PowerOasis, Inc. v. T-Mobile USA, Inc.*, 522 F.3d 1299, 1306 (Fed. Cir. 2008) (“It is elementary patent law that a patent application is entitled to the benefit of the filing date of an earlier filed application only if the disclosure of the earlier application provides support for the claims of the later application, as required by 35 U.S.C. § 112.”). EX1003, ¶¶54-56.

### **C. File History**

U.S. Patent Application No. 11/076,591, which matured into the '710 patent, was filed 3/10/2005. The original application had only 3 claims, all of which were rejected as anticipated in an initial 8/13/2008 Office Action. EX1002, 409-415. In response, Applicant amended the claims to require restricting the client to a "walled garden...in a network outside the network access gateway" and added 17 more claims. EX1002. 461-467. In a 2/13/2009 Final Office Action, the Examiner again

rejected all the pending claims as obvious over the prior art, finding the prior art already disclosed "walled gardens," including ones outside the network access gateway. EX1002, 596-620.

After three more rejections (on 8/06/2009, 2/2/2010, 7/20/2010) (EX1002), Applicant cancelled all pending claims and submitted 20 new claims for consideration. EX1002, 861-869. These twenty claims were again rejected as anticipated by, and obvious over, the prior art. EX1002, 994-1004. In response, Applicant further amended the independent claims to require the underlined additions (1) "restricting all network traffic emanating from the client device to the allowed network destination address to selected one or more network protocols"; and (2) that the web page rendering be "responsive to the implementation of one of the plurality of quarantine control function[s] of the client device." EX1002, 1054. With that amendment, the claims were allowed. EX1002, 1069-1074. EX1003, ¶53.

#### **D. POSITA**

The relevant art for the '710 patent is the field of computer science generally, and specifically computer networking and security. A person of ordinary skill in that art, as of August 2004, would have been an individual with either (1) at least a bachelor's degree in computer science or computer engineering or an equivalent field plus at least one year of experience working on computer networking and/or computer security, or (2) at least 3 years of experience working on computer

networking and/or computer security, even without a formal degree. EX1003, ¶¶16-20.

#### IV. CLAIM CONSTRUCTION

A claim is construed "using the same claim construction standard that would be used to construe the claim in a civil action," 37 C.F.R. § 42.100(b), which is governed by *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005). Under the standard set out in *Phillips*, this petition applies the plain and ordinary meaning to each term in the '936 Patent, which is "the meaning that the term would have to a [POSITA] in question at the time of the invention." *Id.* at 1313.

##### A. "subordinate to"

All the independent claims require "restricting all network traffic...to one or more network destination addresses that are not *in or subordinate to* the first network segment" but the specification never explains what it means for an address to be "subordinate to the first network segment." *See*, EX1001, *generally*. Indeed, the term "subordinate to" never appears in the specification and a POSITA would not have reasonable certainty as to full bounds of this term—namely, in which scenarios an address would *not* be in a network segment but still *would* be subordinate to that network segment. Nonetheless, indefiniteness here does not preclude finding the claims unpatentable in view of the prior art because—like the examples in the '710 patent—the grounds herein rely on disclosures and arguments

for restricting communications to Internet destinations which are unambiguously neither within the local network nor subordinate to the local network in any fashion. See *Intel Corp. v. Qualcomm Inc.*, 21 F.4th 801, 813 (Fed. Cir. 2021) (citing *Samsung Electronics America, Inc. v. Prisia Eng'g Corp.*, 948 F.3d 1342, 1353 (Fed. Cir. 2020)) ("it is not always impossible to adjudicate a prior-art challenge, one way or the other, just because some aspect of a claim renders the claim indefinite," rather indefiniteness "precludes a patentability determination only when the indefiniteness renders it logically impossible for the Board to reach such a decision"). In particular, while the full bounds of the term are not reasonably certain, a POSITA would understand from the specification that, at minimum, a general Internet website is not a network address "subordinate to" the first network segment. EX1003, ¶24.

Petitioner respectfully submits that no other constructions are required for purposes of this petition.

## **V. Grounds of Unpatentability**

The '710 patent is directed to a method and system for controlling network access using so-called "quarantine control functions."

Independent claim 1 (representative of the other independent claims) recites:

A method of network traffic quarantine control, comprising:

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;

at the network access gateway device, performing a plurality of quarantine control functions over the client device, wherein the plurality of quarantine control functions comprises:

a) 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;

b) restricting all network traffic emanating from the client device to an allowed network destination address to selected one or more network protocols; and

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.

At their core, the claims are directed to (1) restricting communications from a computer to only specific destinations; and (2) limiting those communications to only specific allowable communications protocols (*e.g.*, TCP/IP). The claimed features are anticipated and, at minimum, obvious in view of the prior art, as explained below. EX1003, ¶¶52, 76.

Specifically, as explained within the grounds below the cited prior art renders the Challenged Claims of the '710 patent unpatentable.

Grounds 1 and 2 demonstrate the unpatentability of the challenged claims as anticipated by (Ground 1) and obvious over (Ground 2) **Roskind**. Roskind claims priority to a provisional application filed before the effective filing date of the

application leading to the '710 patent and is therefore prior art under at least pre-AIA §102(e).<sup>2</sup> In addition, Ground 5 demonstrates the obviousness of the claims over **Roskind** in view of **Short**.

Even should the Board find that the '710 Patent is entitled to its earlier priority date despite the '702 Provisional failing to disclose key limitations, the Challenged Claims still are anticipated by (Ground 3) and obvious over (Ground 4) **Glechauf**. In addition, Ground 6 demonstrates the obviousness of the claims over **Glechauf** in view of **Short**.

This Petition is supported by the Declaration of John R. Black, Jr., which describes the scope and content of the prior art at the time of the alleged invention of the '710 patent. EX1003, §§VI-XII.

**A. Grounds 1 and 2 – Claims 1-20 Are Anticipated Or At Minimum Rendered Obvious Over Roskind**

**1. Overview of Roskind**

**Roskind** discloses a gateway (or router) that "identif[ies] and intercept[s] unauthorized, unwanted, and/or otherwise malicious communications." EX1005, 3:10-13. The gateway is "configured to provide and control access between a protected network and the Internet" and to "quarantine a local computer." EX1005, 11:63-66, 14:27-32. EX1003, ¶57.

---

<sup>2</sup> As discussed above, the '710 patent is not entitled to the filing date of the '702 Provisional. *Supra* § III.B.

**Roskind** discloses "a method for identifying and remedying problems....

After a detection of a problem, *a computer or network containing the problem is quarantined....*" EX1005, 11:15-28. As disclosed, "quarantining includes preventing unauthorized communications from being sent from the quarantined computer" (EX1005, 11:27-35) while allowing "access to remediation services [which] includes or may include allowing connections to servers providing security patches or advisories, for example allowing connections to a vendor's server...[or] direct access to vendor sites known to provide remediation assistance, such as to Microsoft's Windows Update service, where security patches may be obtained." EX1005, 11:39-54. In addition, **Roskind** discloses that "access to vendor sites is restricted by the quarantine to certain classes of traffic, such as HTTP requests, certain port access, such as port 80 or port 443...." *Id.* EX1003, ¶58.

Similar to the '710 patent, **Roskind** discloses that, responsive to the infected computer being quarantined, unauthorized network requests are redirected to "a special quarantine server (1407), such as an ISP web server that provides information and links to assist in remediation." EX1005, 14:66-15:1; *see also id.*, 15:57-16:43 ("the server responds with a quarantine notification page (1604)...a web page that provides notification that the computer is quarantined, and/or provides links to remediation sites appropriate to the quarantine, such as a link to a site that provides anti-contagion software for removing a virus..."). This is similar to the

'710 patent's disclosure of redirecting a user to "a cooperating web server...[which] renders a web page informing the client of its perceived infection and offering links to self-help documents and to the websites of anti-virus vendors and the client's OS vendor." EX1001, 5:65-6:4. EX1003, ¶¶59-60; 62.

Finally, **Roskind** discloses continuously monitoring network traffic to identify malicious activity (EX1005, 13:10-53) and monitoring individual computers for infestation. EX1005, 13:54-14:26. As part of monitoring computers for infestation, **Roskind** discloses that the "query for cleanliness" to a computer "may be responded to by anti-contagion software, such as antivirus software, with assertions about the currency of a scan...wherein a sufficiently updated software and/or scan may act as a cleanliness assertion." *Id.* In other words, a POSITA would have understood **Roskind** to disclose providing remediation access to anti-contagion software in response to a quarantine (*e.g.*, as disclosed in FIGs. 10 and 14 and related discussion) and allowing the user to remediate the infection (and thereby resolve the need for quarantine controls) by running an up-to-date scan and making a "cleanliness assertion" (as described in FIG. 13 and related discussion). EX1003 ¶¶61-62.

## 2. Independent Claim 1

- (a) Claim [1pre]: "A method of network traffic quarantine control, comprising:"

**Roskind discloses a method of network traffic quarantine control.**

EX1003, ¶78.

**Roskind** discloses a system and "a process" for "identify[ing] and intercept[ing] unwanted, unauthorized, and/or...malicious traffic" and "quarantining" communications accordingly. *E.g.*, Roskind, 2:47-52 ("The invention can be implemented in numerous ways, including as *a process...*"), Abstract ("Analyzing *routing information* to identify and intercept unauthorized, unwanted, and/or otherwise malicious communications is disclosed."), 11:15-39 ("FIG. 10A is a flow diagram of *a method for identifying and remedying problems....* After a detection of a problem, *a computer or network containing the problem is quarantined....* Examples of quarantining activities are illustrated in FIGS. 14 and 15."). As Roskind explains, "[u]nwanted and/or malicious network communications...burden affected networks with unauthorized and/or undesired traffic." Roskind, 1:14–19. To mitigate these harms, Roskind therefore teaches "[a]nalyzing routing information to identify and intercept unauthorized, unwanted, and/or otherwise malicious communications." *Id.*, Abstract. Figures 14 and 15 further illustrate methods for quarantining a computer:

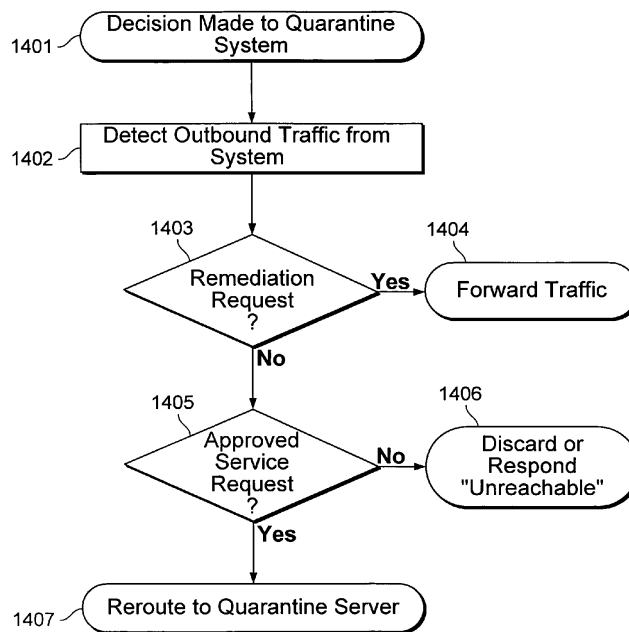


FIG. 14

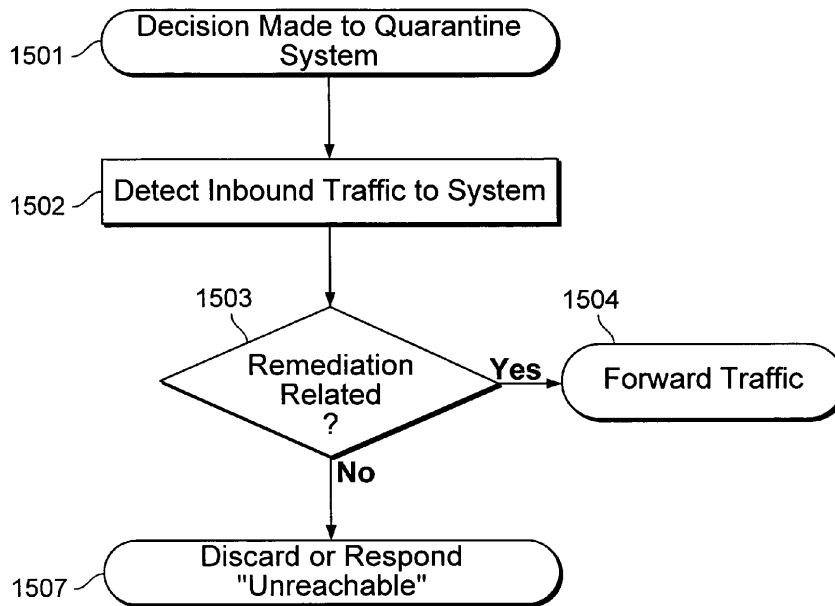


FIG. 15

Roskind, FIGs. 14-15; *see also*, EX1006, 4:1-5, 18:7-19:3. EX1003, ¶¶79-80.

- (b) Claim [1a]: "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;"

**Roskind discloses, or at minimum renders obvious, at a network access gateway device (e.g., "router") between a local network (e.g., "LAN") and the Internet, selecting (e.g., "deciding to quarantine") a client device (e.g., "host", "local computer") in a first network segment of the network (e.g., "LAN").** EX1003, ¶81.

**Roskind discloses a "gateway 1028...configured to provide and control access between a protected network and the Internet," which includes a "router." E.g., Roskind, 11:57-12:3 ("FIG. 10B is a block diagram illustrating *a network environment in which infected hosts and/or networks are quarantined.... A plurality of hosts* 1 to "m", represented in FIG. 10B by hosts 1020, 1022, and 1024, *connect via a router 1026 and a gateway 1028 to the Internet 1030.... [R]outer 1026 is omitted or included in the gateway 1028.... [G]ateway 1028 comprises a gateway, router, firewall, or other device configured to provide and control access between a protected network and the Internet....").***

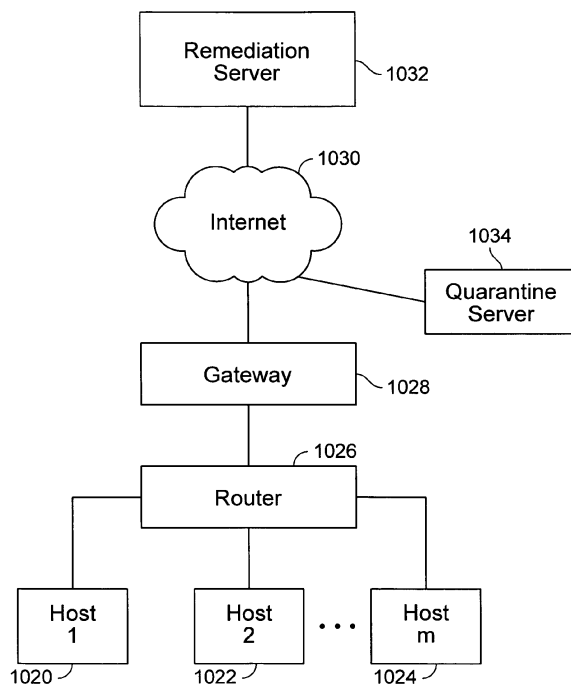


FIG. 10B

Roskind, FIG. 10B. EX1003, ¶82.

The quarantine process begins with a "firewall or router for a LAN deciding to quarantine a local computer." Roskind, 14:27-32 ("FIG. 14 is a flow diagram of a method for quarantining a computer.... In this example, a *decision has been made to quarantine a computer (1401)*, such as...*a firewall or router for a LAN deciding to quarantine a local computer.*"); see also EX1006, 24:13-17 (same). Further, Roskind Provisional discloses a "router for a LAN deciding to quarantine a local computer" and a quarantine "restricting internet connections," confirming the router is a gateway between the LAN and the Internet. EX1006, 24:13-17, 27:4-10 ("a configuration based quarantine...may be automatically setup...that establishes a

quarantine, for example restricting internet connections..."). A POSITA would have thus understood Roskind Provisional discloses, and at minimum renders obvious, a router as a network access gateway device between a local network and the Internet. EX1003, ¶¶83-84. Figure 14 illustrates the flow diagram once the router has "decid[ed] to quarantine a local computer"—*e.g.*, a computer in the first network segment, namely the LAN:

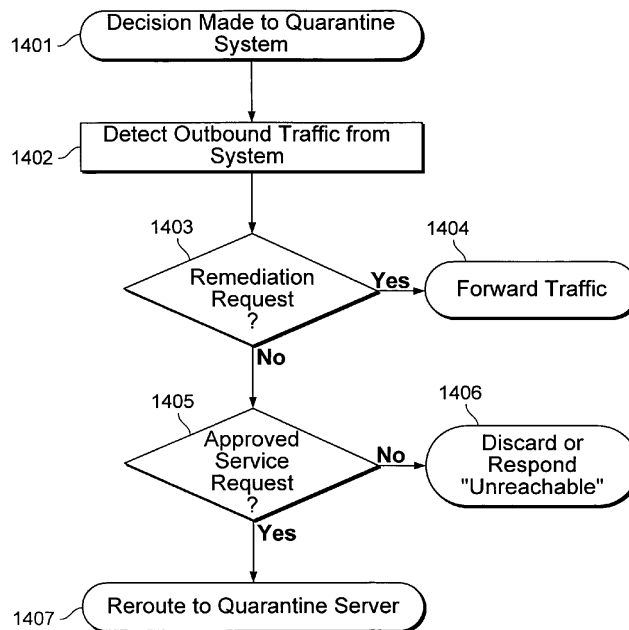


FIG. 14

Roskind, FIG. 14. EX1003, ¶85.

- (c) Claim [1b]: "at the network access gateway device, performing a plurality of quarantine control functions over the client device, wherein the plurality of quarantine control functions comprises:"

**Roskind discloses at the network access gateway device (e.g., "router"),**

**performing a plurality of quarantine control functions over the client device**(e.g., "quarantining a computer"), **wherein the plurality of quarantine control functions comprises [ [1b(a)]-[1b(b)]]**. EX1003, ¶86.

Roskind discloses a "router, firewall, or other network component" detecting a vulnerability or infestation and, in response, the "firewall or router for a LAN decid[es] to quarantine [the] local computer" containing the problem. *E.g.*, Roskind, 11:15-39 ("FIG. 10A is a flow diagram of a method for identifying and remedying problems...*detection may be made by a router, firewall, or other network component....* After a detection of a problem, *a computer or network containing the problem is quarantined* (1002). In some embodiments, *quarantining includes preventing unauthorized communications from being sent* from the quarantined computer ..., *or efforts to communicate data without authorization,....* In some embodiments, *quarantining includes preventing undesired communications from reaching the quarantined computer*, such as control messages or infectious messages. *Examples of quarantining activities are illustrated in FIGS. 14 and 15.*"), 14:27-50 ("FIG. 14 is a flow diagram of *a method for quarantining a computer....* [A] decision has been made to quarantine a computer (1401), such as...*a firewall or router for a LAN deciding to quarantine a local computer.*"). EX1003, ¶87.

For example, Figure 10A illustrates "a method for identifying and remedying

problems," resulting in "[e]xamples of quarantining activities [as] illustrated in FIGs.

14 and 15":

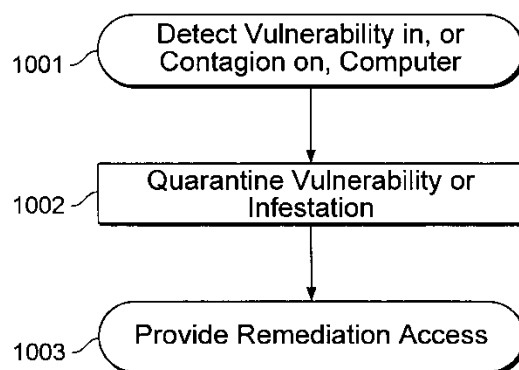


**FIG. 10A**

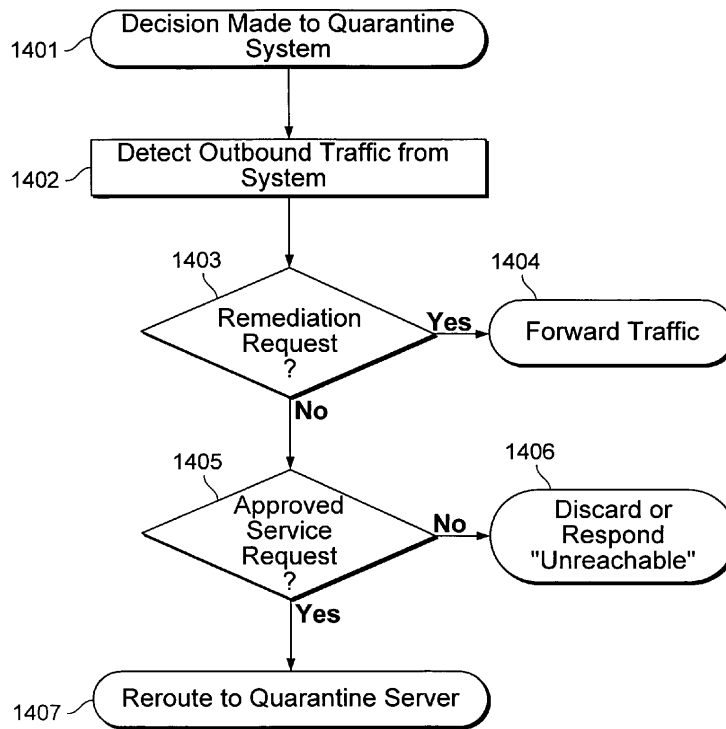


FIG. 14

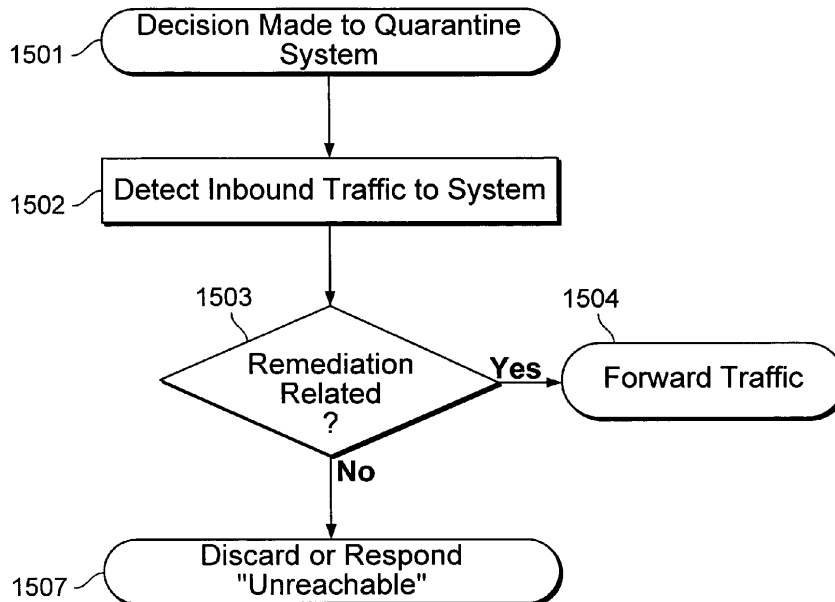


FIG. 15

Roskind, 11:15-39, FIGs. 10A, 14, 15; *see also* EX1006, 24:13-17, 18:7-18:3.

EX1003, ¶¶88-89.

- (d) Claim [1b(a)]: "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;"

**Roskind discloses, or at minimum renders obvious, restricting all network traffic emanating from the client device (e.g., "preventing unauthorized communications from being sent from the quarantined computer") to one or more network destination addresses that are not in or subordinate to the first network segment (e.g., restricting "outbound traffic" not "associated with a remediation request").** EX1003, ¶90.

**Roskind discloses that once a computer or network is quarantined, unauthorized communications are blocked while limited access is provided to specified "remediation" services:**

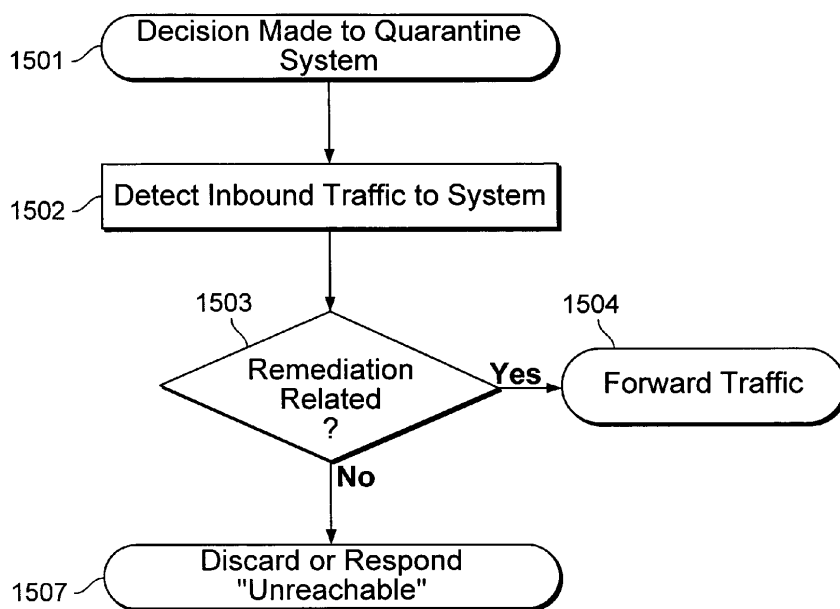


**FIG. 15**

Roskind, FIG. 15. Roskind teaches that “quarantining includes preventing unauthorized communications from being sent from the quarantined computer, such as efforts to infect, probe, or harass other computers, or efforts to communicate data without authorization.” Roskind, 11:27–35. In some embodiments, “no communications are authorized” at all. *Id.* EX1003, ¶¶91-92.

In this way, Roskind discloses restricting all network traffic emanating from the client device to allow only communications directed at "remediation" services. Specifically, Roskind explains that “the quarantined computer is provided access to remediation services (1003)... [A]ccess to remediation includes or may include allowing connections to servers providing security patches...such as to Microsoft’s Windows Update service, where security patches may be obtained.” *Id.*, 11:39–50.

Roskind further specifies that “access to vendor sites is restricted by the quarantine to...certain content requests, such as specific URLs.” *Id.*, 11:50–54. These remediation servers—such as “an appropriate anti-contagion software distributor, or...security patch update provider”—are necessarily located on different network segments than the quarantined client device (i.e., on the Internet, rather than on the local network) and, insofar as they are on the general Internet, also are not subordinate to the local network. *See id.*, 14:50–15:12; *see also* EX1001, 5:35-52 (restricting "Client 4" to Internet "Site 'S'" only), FIG. 1 (40). EX1003, ¶93.

Roskind further discloses filtering traffic during the quarantine to ensure only authorized remediation-related communications are allowed. For example, Figure 14 depicts a flow where “outbound traffic is detected (1402)...[and] tested...to see if it is associated with a remediation request (1403), such as contact with an appropriate anti-contagion software distributor, or contact with a security patch update provider.” Roskind, 14:50–57.

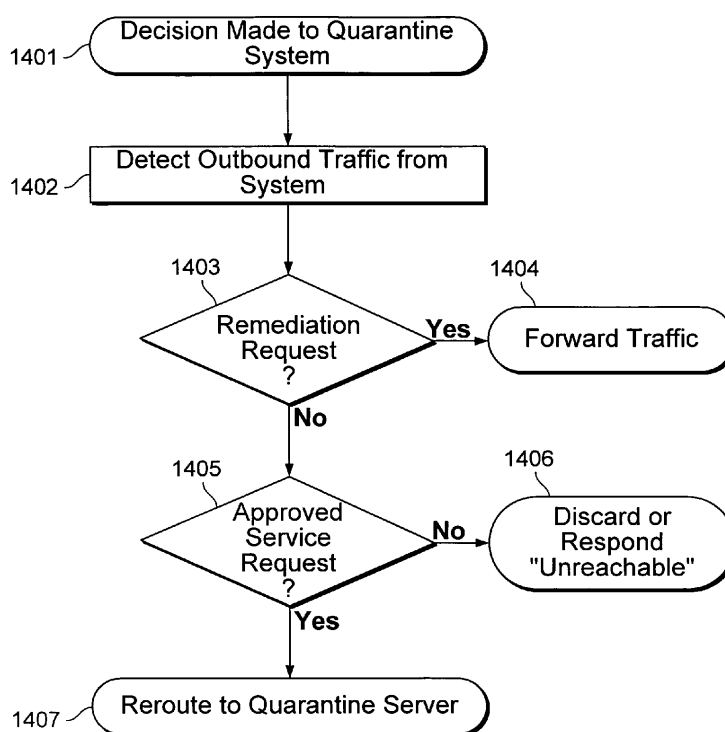


FIG. 14

Roskind, FIG. 14. If the traffic is not associated with remediation, it is further tested to determine whether it is an “approved service request (1405), such as a request for a web page.” *Id.*, 14:59-65. If the request is for an approved service, “the request is re-routed to a special quarantine server (1407),” thereby restricting the quarantined computer’s access to the actual service. *Id.*, 14:59–67. If the request is not for an approved service, “the outbound traffic is discarded or responded to with [an] indication that the desired traffic destination is unreachable.” *Id.*, 15:9-12. EX1003, ¶¶94-95. Accordingly, Roskind expressly discloses a quarantine mechanism that (i) blocks unauthorized communications, (ii) permits access only to remediation

services defined by a specific set of URLs associated with security patch providers, and (iii) restricts or discards all other outbound traffic, including requests to otherwise approved services. *See also* EX1006, 25:8-26:8, 19:4-15, 18:16-22.

- (e) Claim [1b(b)]: "restricting all network traffic emanating from the client device to an allowed network destination address to selected one or more network protocols; and"

**Roskind discloses, or at minimum renders obvious, restricting all network traffic emanating from the client device** (e.g., "preventing unauthorized communications from being sent from the quarantined computer") **to an allowed network destination address** (e.g., "vendor sites") **to selected one or more network protocols** (e.g., "HTTP requests"). EX1003, ¶96.

**Roskind** discloses that, even when a quarantined computer is allowed access to remediation services (e.g., "vendor sites"), that access is further restricted to only "certain classes of traffic, such as HTTP requests." *E.g.*, Roskind, 11:39-56 ("[T]he quarantined computer is provided access to remediation services (1003)... [A]ccess to remediation includes...allowing connections to servers providing security patches or advisories, for example...a vendor's server.... [A]ccess to remediation includes allowing direct access to vendor sites known to provide remediation assistance...where security patches may be obtained. In some embodiments, *access to vendor sites is restricted by the quarantine to certain classes of traffic, such as HTTP requests*, certain port access, such as port 80 or port 443, ...."); EX1006,

19:14-15. Thus, all other classes of traffic (*i.e.*, other network protocols) are blocked. EX1003, ¶97.

- (f) Claim [1c]: "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."

**Roskind discloses, or at minimum renders obvious, rendering a web page** (*e.g.*, "quarantine notification 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** (*e.g.*, "information and links to assist in remediation"; "remediation information", "notification that the computer is quarantined[ and] links to remediation sites appropriate to the quarantine") **responsive to implementation of one of the plurality of quarantine control function of the client device** (*e.g.*, "web page...[or]...remediation sites appropriate to the quarantine"). EX1003, ¶98.

**Roskind discloses and at minimum renders obvious rendering a web page to display on the client device from the network access gateway device.** Specifically, **Roskind** discloses re-routing a quarantined computer, via its browser, to a "quarantine server." Roskind, 7:2-13 ("[t]he client system 420 further includes...*browser software used to navigate the World Wide Web*, *e.g.*, to

send/receive data to/from a website"), 14:66-15:1 ("the request is re-routed to a *special quarantine server (1407)*, such as an ISP web *server that provides information and links to assist in remediation*"); *see also id.*, 6:63-7:23 ("FIG. 4B is a block diagram of a client system configured to obtain an update...the update agent/browser 424 comprises browser software used to navigate the World Wide Web, e.g., to send/receive data to/from a website from which an update is available for download..."). EX1003, ¶99.

The quarantine server "respond[s] to requests...with a quarantine notification page (1604)...a web page that provides notification that the computer is quarantined, and/or provides links to remediation sites appropriate to the quarantine, such as a link to a site that provides anti-contagion software for removing a virus that the quarantined computer is believed to contain." Roskind, 15:57-16:43. Roskind further discloses that the quarantine server "resides on the router...and/or gateway." Roskind, 11:57-12:13. Likewise, Roskind discloses the "special quarantine server" is "an ISP web server." Roskind, 14:65-15:1. At minimum, a POSITA would have understood, and found it an obvious choice to place the quarantine server within the gateway so as to better control infected traffic while restricting the quarantined computer from communicating with unauthorized hosts. EX1003, ¶100. For example, Roskind's teaching to use an ISP web server as the quarantine server—i.e., having the entity controlling Internet access as the entity providing the quarantine

server—suggests this very benefit to an organization protecting its own network. EX1003, ¶100. Likewise, to the extent "rendering" of the web page requires graphical production of the complete web page at the server (rather than rendering on the local browser), this too is a simple design choice with only two options—either rendering at the server or rendering on the client device—which would have been obvious in view of **Roskind's** disclosures of having the quarantine server "respond to requests...with a web page that provides notification that the computer is quarantined." Roskind, 15:57-16:43. "Rendering" is neither the focus of the invention here nor an aspect that is described in any detail in the '710 specification, and either option would have been known and obvious. EX1003, ¶100.

**Roskind further discloses and at minimum renders obvious 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.**

**Roskind** further explains that "re-rout[ing] to a special quarantine server" is performed as part of the "method for quarantining a computer"—*i.e.*, responsive to the gateway restricting traffic to any sites beyond the remediation sites—and that the server "provides information and links to assist in remediation." Roskind, 14:27–15:12, FIG. 14. Figure 16 provides additional details on the "quarantine server []

respond[ing] to requests" including that the server "responds with a quarantine notification page (1604)"—a web page "that provides notification that the computer is quarantined, and/or provides links to remediation sites appropriate to the quarantine, *such as a link to a site that provides anti-contagion software for removing a virus that the quarantined computer is believed to contain.*" Roskind, 15:57-16:7; *see also id.*, 11:41-50 ("[A]ccess to remediation includes or may include allowing connections to *servers providing security patches or advisories*, for example allowing connections to a vendor's server, or providing virus and worm disinfecting tools, such as focused removal tools...."). In addition, Roskind discloses, and at minimum renders obvious that directing users to these patches is an offer to perform an action—*i.e.*, to install the patch—to obtain unrestricted access to the Internet following an infestation and quarantine. EX1003, ¶¶101-102. This is supported, for example, by Roskind's further disclosure of "monitoring a computer for infestation" and "assertions about the cleanliness (e.g., infestation status)" of a computer after installing a patch. *E.g.*, Roskind, 14:19-26 ("In some embodiments, an operating system may respond with information associated with its patch level, wherein *a sufficiently recent patch level may be interpreted as an assertion of cleanliness*. If a computer asserts it is clean (1303) then monitoring is complete (1305) in this example."). In other words, a POSITA would have understood that the purpose of providing information on "patches" for an infestation is to allow the

user to access and install the patch so as to void the quarantine. EX1003, ¶¶101-102.

*See also* EX1006, 19:5-9, 25:20-23, 27:20-28:14, 24:7-12.

3. **Claim [2]: "The method according to claim 1, 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."**

**Roskind discloses, or at minimum renders obvious, the method according to claim 1, wherein the action requires the user to obtain and execute abnormal behavior scanning software (e.g., "anti-contagion software") from a server machine running at one of the one or more allowed network destination addresses (e.g., "a site that provides anti-contagion software", "appropriate anti-contagion software distributor").** EX1003, ¶103.

As discussed in [1c], **Roskind** teaches that a quarantined computer may be redirected to a quarantine notification page that instructs the user to perform remediation steps before normal communications are restored. *Supra*, §V.A.2(f). For example, Roskind describes “a web page that provides notification that the computer is quarantined, and/or provides links to remediation sites appropriate to the quarantine, such as a link to a site that provides anti-contagion software for removing a virus that the quarantined computer is believed to contain.” Roskind, 16:2–7. EX1003, ¶104.

Roskind further discloses that remediation requests may include contacting “an appropriate anti-contagion software distributor, or...a security patch update provider,” and that such requests are routed to their destination while other traffic is blocked. Roskind, 14:53–61. In addition, Roskind teaches that the quarantined client may include “an agent associated with anti-contagion software installed on the client system 420.” Roskind, 6:63–7:23. A POSITA would have understood from these disclosures that Roskind requires the user of the quarantined computer to obtain anti-contagion software from a permitted remediation site and execute that software in order to remediate the infection. For example, Roskind also expressly ties remediation to a subsequent “assertion of cleanliness.” Specifically, Roskind teaches that “the query for cleanliness (1302) may be responded to by anti-contagion software, such as antivirus software, with assertions about the currency of a scan...wherein a sufficiently updated software and/or scan may act as a cleanliness assertion.” Roskind, 14:12–19. Thus, Roskind discloses, and at minimum renders obvious, that the required action for a quarantined user includes obtaining and executing anti-contagion software from an approved remediation server and running a scan before the computer can make an assertion of cleanliness and restore unrestricted communications. EX1003, ¶105.

*See also*, EX1006, 28:7-11, 25:11-18, 23:2-7.

4. **Claim [3]: "The method according to claim 1, further comprising: 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."**

**Roskind discloses or at minimum renders obvious the method according to claim 1, further comprising: 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.** EX1003, ¶106.

**Roskind** discloses monitoring network traffic "for anomalous traffic" and that such "monitoring...may be continuous." *E.g.*, Roskind, 13:10-53 ("FIG. 12 is a flow diagram of a method for identifying an infestation.... [A] device near a computer, such as a firewall on a LAN or an ISP's router, is used in some embodiments to monitor a computer for infestation (1201). *Network traffic is monitored for anomalous traffic* volume, port, or IP destination (1202).... If an anomaly is detected (1203) then an apparent infestation is noted (1204).... [A] response to infestation may include quarantining of the computer or network containing the computer, for example as discussed in conjunction with FIGS. 14, 15, and 16. In some embodiments, a response to infestation may include an attempt to remediate the problem, for example by inoculation, such as discussed in conjunction with FIG. 17.... In some embodiments, *monitoring for anomalous traffic may be continuous.*" *E.g.*, Roskind, 13:10-53; *see also id.*, 13:54-14:26 ("FIG. 13 is a flow

*diagram of a method for monitoring one or more computers for infestation....* In

some embodiments, *the query for cleanliness (1302) may be responded to by anti-contagion software, such as antivirus software, with assertions about the currency of a scan...wherein a sufficiently updated software and/or scan may act as a cleanliness assertion...[or] wherein a sufficiently recent patch level may be interpreted as an assertion of cleanliness....*"). A POSITA would have understood that, insofar as the monitoring is "continuous," traffic from the computer would have been evaluated before, during, and after an infestation is identified and mitigated using a security patch or anti-contagion software. *See* [1c], [2], above. EX1003, ¶¶107-108.

*See also* EX1006, 21:19-22:20, 23:7-24:12

5. **Claim [4]: "The method according to claim 1, further comprising: filtering the network traffic emanating from the client device to limit network packet flow by the client device."**

**Roskind discloses or at minimum renders obvious the method according to claim 1, further comprising: filtering the network traffic emanating from the client device (e.g., "preventing unauthorized communications from being sent from the quarantined computer") to limit network packet flow by the client device. *See* [1b(a)], [1b(b)]. EX1003, ¶109.**

A POSITA would have understood that quarantining an infected computer to "prevent[] unauthorized communications from being sent" from the quarantined

computer, as discussed above in [1b(a)] discloses or at minimum renders obvious filtering the network traffic emanating from the client device (e.g., allowing authorized communications while preventing unauthorized communications), which would result in limiting the network packet flow from by the client device. EX1003, ¶110.

6. **Claim [5]: "The method according to claim 1, further comprising: routing the network traffic emanating from the client device to limit network packet traversal by the client device."**

**Roskind discloses or at minimum renders obvious the method according to claim 1, further comprising: routing the network traffic emanating from the client device to limit network packet traversal by the client device. See [1b(a)], [1b(b)]. EX1003, ¶111.**

A POSITA would have understood that quarantining an infected computer to "prevent[] unauthorized communications from being sent" from the quarantined computer, as discussed above in [1b(a)] discloses or at minimum renders obvious routing the network traffic emanating from the client device to only specifically allowed servers or sites (e.g., "a site that provides anti-contagion software" or an "appropriate anti-contagion software distributor"), which limit network packet traversal by the client device by blocking traffic to any non-approved computer. EX1003, ¶112.

7. **Claim [6]: "The method according to claim 1, wherein the plurality of quarantine control functions further comprises: restricting all network traffic emanating from the client device to one or more network destination addresses in one or more network segments that are not in or subordinate to the first network segment."**

**Roskind discloses, or at minimum renders obvious, the method according to claim 1, wherein the plurality of quarantine control functions further comprises: restricting all network traffic emanating from the client device to one or more network destination addresses in one or more network segments that are not in or subordinate to the first network segment. See [1b(a)]. EX1003, ¶113.**

As discussed in [1b(a)], **Roskind** discloses limiting traffic from the quarantined computer to allow access to only remediation sites. A POSITA would have understood that such remediation sites—*i.e.*, Internet web sites—are not in or subordinate to the first network segment. EX1003, ¶114.

8. **Claim [7]: "The method according to claim 1, further comprising: performing all of the plurality of quarantine control functions over the client device."**

**Roskind discloses, or at minimum renders obvious, the method according to claim 1, further comprising: performing all of the plurality of quarantine control functions over the client device. EX1003, ¶115.**

As discussed above in [1b(a)] and [1b(b)], **Roskind** discloses restricting network traffic for the quarantined computer to only certain allowed websites (e.g.,

only "allowing connections to a vendor's server" as set forth in [1b(a)]) and restricting communications to those same sites using only certain protocols (e.g., "access to vendor sites is restricted by the quarantine to certain classes of traffic, such as HTTP requests," as set forth in [1b(b)]. *See, e.g.*, EX1005, 11:15-56. EX1003, ¶116. *See also* [1b(a)], [1b(b)].

## 9. Claims 8 and 15

Claims 8 and 15 are substantively similar to claim 1, other than the preambles and preliminary limitations. Claim 8 recites "a computer program product" for implementing a method substantively similar to the claim 1, while claim 15 recites a "network access gateway device" (also recited in claim 1) programmed in the same manner. Petitioner addresses the claim 8 preamble below. The other limitations are invalid for the same reasons set forth in claim 1 (or 8), as detailed in the mapping below. The analysis from claim 1 is incorporated by reference. EX1003, ¶117.

- (a) **Claims [8pre]: "A computer program product comprising at least one non-transitory computer readable medium storing instructions translatable by at least one processor to perform:"; [15a] "at least one processor"; and [15b] "at least one non-transitory computer readable medium storing instructions translatable by the at least one processor to perform:"**

**Roskind discloses, or at minimum renders obvious, a computer program product comprising at least one non-transitory computer readable medium storing instructions translatable by at least one processor.** EX1003, ¶1118.

See, claim 1, above. Further, Roskind discloses that its "invention can be implemented in numerous ways, including as...*a computer readable medium such as a computer readable storage medium or a computer network wherein program instructions are sent over optical or electronic communication links. ...A component such as a processor or a memory described as being configured to perform a task includes both a general component that is temporarily configured to perform the task at a given time and a specific component that is manufactured to perform the task.*"; E.g., Roskind, 2:47-60. EX1006, 4:2-9. EX1003, ¶119.

(b) Claim [15pre]: "A network access gateway device, comprising:"

See claim [1a]; 8[pre]. EX1003, ¶120.

(c) Remaining Limitations

| Claim 8                                                                                                                                                                                                                                                                                                                                                    | Claim 15                                                                                                                                                                                                                                                                                                                                                    | Claim 1     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| [8a]: "a plurality of quarantine control functions over a client device coupled to the network access gateway device, wherein the network access gateway device is between a local network and the Internet, wherein the client device is in a first network segment of the network, and wherein the plurality of quarantine control functions comprises:" | [15c]: "a plurality of quarantine control functions over a client device coupled to the network access gateway device, wherein the network access gateway device is between a local network and the Internet, wherein the client device is in a first network segment of the network, and wherein the plurality of quarantine control functions comprises:" | [1a], [1b]. |

|                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                    |          |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| [8a(a)]: "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;                                                                                                                                                                                  | [15c(a)]: "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;"                                                                                                                                                                             | [1b(a)]. |
| [8a(b)]: "restricting all network traffic emanating from the client device to an allowed network destination address to selected one or more network protocols; and"                                                                                                                                                                                                  | [15c(b)]: "restricting all network traffic emanating from the client device to an allowed network destination address to selected one or more network protocols; and"                                                                                                                                                                                              | [1b(b)]. |
| [8b]: "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 the implementation of one of the plurality of quarantine control function of the client device." | [15d]: "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." | [1c].    |

See EX1003, §X.C.3.

#### 10. Claims 9-14 and 16-20

The remaining dependent system and device claims are substantively the same as the corresponding method claims already addressed and are invalid for the reasons

set forth above based upon the following mapping. The analysis from the method claims are incorporated herein by reference. EX1003, ¶121.

| Computer Program Product Dependent Claim | System Dependent Claim | Method Dependent Claim |
|------------------------------------------|------------------------|------------------------|
| 9                                        | 16                     | 2                      |
| 10                                       | 17                     | 3                      |
| 11                                       | 18                     | 4                      |
| 12                                       | 19                     | 5                      |
| 13                                       | 20                     | 6                      |
| 14                                       |                        | 7                      |

**B. Grounds 3 and 4 – Claims 1-20 Are Anticipated Or At Minimum Rendered Obvious Over Gleichauf**

**1. Overview of Gleichauf**

**Gleichauf** discloses a system and method "for detecting an infective element in a network environment" that relies on community monitoring within a communication system to only a selected number of peers within the network need to be properly configured to identify a rogue element within the system. Gleichauf, Abstract, ¶20. This "community monitoring approach allows for the quarantine of malicious traffic immediately after it is discovered within the network architecture. This is particularly critical in network security systems where time is of the essence in containing damaging information" once an infection is discovered. Gleichauf, [0020]. EX1003, ¶66.

In particular, **Gleichauf** discloses the quarantining is facilitated by a "network

management controller" which "allows for the quarantine of malicious traffic immediately after it is discovered within the network architecture." Gleichauf, [0006]. Specifically, network management controller "may respond to the identification of infective element [] with any number of appropriate remedies...in order to prohibit infective element [] from permeating through the system being threatened." Gleichauf, [0020]. This includes (a) "immediately disabl[ing] the communications capability of a rogue (or an infected computer)" thereby "prohibit[ing] the rogue [computer] from communicating to a next computer or to another destination, which may infect additional elements within the network[,]" while "direct[ing the infected computer] to a remediator website in order to comply with a network security enforcement protocol" (Gleichauf, [0006], [0008]); and (b) enforcing "policies" set in a "policies node [] in order to disable one or more of those policies or services being provided to infected [computer] 18 until it properly complies with the requisite security parameters." Gleichauf, [0058]. In this way, like the '710 patent, **Gleichauf** discloses both restricting all network traffic emanating from the infected to computer to only the remediator website and, in doing so (and shutting down all other services), restricting all network traffic to only the network protocol used to contact the remediator website (e.g., TCP/IP). To the extent it is argued that remediator website is not in a network "not in or subordinate to the first network segment" where the infected computer resides, a POSITA would

have understood that the placement of the remediator website in an internal or external network is a simple design choice that would have been easily implemented and, therefore, would have been obvious. Indeed, insofar as the "internal network" may be any of a LAN, WAN, or MAN, a POSITA would have recognized that the remediator *website* residing on the Internet is not in the same network as, for example, infected computer in a home network or accessing a LAN remotely. EX1003, ¶¶67-68.

Further, **Gleichauf** discloses transmitting a "signal" to identify the presence of the infected computer (*e.g.*, Gleichauf, [0005]), that a signal may be transmitted to or from the network management controller (*e.g.*, *id.*, [0007]), that the signal may be transmitted "directly to infected computer" (*e.g.*, *id.*, [0045]), and that the signal "includes numerous pieces of information that relate to the presence of infective element 12. For example, the signal may include...information relating to the type of damaging element that has entered the system. Also, the signal may include information for remedial measures for coping with or for combating the damaging element. For example, certain damaging elements may be eliminated from the system by a simple deletion instruction, whereas others may need more complex instructions for how to combat their presence. Alternatively, the signal...may include any other suitable information that offers some guidance in handling the presence or harmful affects of infective element 12." Gleichauf, [0048]. A POSITA

reading these disclosures would have understood Gleichauf's "signal" containing that much detailed information to refer, for example, to a web page or something similar that is transmitted to recipients as necessary. EX1003, ¶¶69-70. Further, a POSITA would have recognized the benefits and would have found it obvious for such a "signal" (*e.g.*, an informational webpage) to be transmitted from the network management controller to the infected computer in response to the end user's attempts to navigate to other network locations. *Id.* Indeed, to the extent **Gleichauf** discloses disabling all communications from the infected computer, it would be advantageous to notify an end user of the computer as to why network communication attempts are unsuccessful and how to remedy the infection to restore communications. Such a modification would have been advantageous and easily implemented by a POSITA in that timeframe and would render the limitations of the Challenged Claims, as detailed below. *Id.*

## 2. Independent Claim 1

- (a) Claim [1pre]: "A method of network traffic quarantine control, comprising:"

**Gleichauf discloses, or at minimum renders obvious, a method of network traffic quarantine control.** EX1003, ¶122.

**Gleichauf** explains that “a network management controller is provided that operates to immediately disable the communications capability of a rogue (or an infected computer) that contains an infective element.” Gleichauf, [0006]. “This

prohibits the rogue from communicating to a next computer or to another destination, which may infect additional elements within the network.” *Id.* Gleichauf emphasizes that this process “*allows for the quarantine of malicious traffic*” immediately after it is discovered within the network architecture.” *Id.* EX1003, ¶123

Likewise, Gleichauf teaches that “network management controller 14 may then disable a communicating capability of infected computer 18 such that the infective element 12 may not be communicated to a next destination.” Gleichauf, [0019]. In addition, the controller “may also implement other suitable actions...in order to sandbox, siderail, isolate, or otherwise disable infected computer 18 from communicating further.” *Id.* “This community monitoring approach *allows for the quarantine of malicious traffic* immediately after it is discovered within the network architecture,” which is “particularly critical in network security systems where time is of the essence in containing damaging information...once a security breach has occurred.” Gleichauf, [0020]. EX1003, ¶124.

- (b) Claim [1a]: "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;"

**Gleichauf discloses, or at minimum renders obvious, at a network access gateway device (e.g., "network management controller") between a local network (e.g., "internal network") and the Internet (e.g., "external network," "Internet"),**

**selecting** (e.g., in response to "a signal...that identifies infected computer") **a client device** (e.g., "infected computer") **in a first network segment of the network** (e.g., "internal network"). EX1003, ¶125.

**Gleichauf** describes that “FIG. 1 is a block diagram of a communication system 10 for detecting an infective element 12.... *Communication system 10 includes a network management controller 14, multiple computers 16a-16d, an infected computer 18, an external network 22, and an internal network 24.*”

Gleichauf, [0017]. The network management controller is "coupled to" or "inclusive of" a router "positioned at a gateway or at a communications interface." Gleichauf, [0035]. "Router [] may receive data packets from computers...and communicate those packets to [the] external network." *Id.* EX1003, ¶126.

Gleichauf further explains: “a signal may be generated and transmitted...to network management controller [] such that a source associated with infective element [] is identified. This signal may include an address associated with infected computer 18.... *Based on this signal, network management controller [] may then disable a communicating capability of [the] infected computer.*” Gleichauf, [0019]. Thus, based on this identification, the network management controller selects the infected computer for quarantine control actions. EX1003, ¶127.

- (c) Claim [1b]: "at the network access gateway device, performing a plurality of quarantine control functions over the client device, wherein the plurality of quarantine control functions comprises:"

**Gleichauf discloses, or at minimum renders obvious, at the network access gateway device (e.g., "network management controller"), performing a plurality of quarantine control functions over the client device(e.g., "the quarantine of malicious traffic"), wherein the plurality of quarantine control functions comprises [limitations [1b(a)]-[1b(b)]].** EX1003, ¶128.

*Gleichauf discloses that "a network management controller is provided that operates to immediately disable the communications capability of a rogue (or an infected computer) that contains an infective element.... This prohibits the rogue from communicating to a next computer or to another destination, which may infect additional elements within the network. The network management controller allows for the quarantine of malicious traffic immediately after it is discovered within the network architecture. This is important because time is a critical element in containing infective elements once they have penetrated the corresponding security system." Gleichauf, [0006]. As Gleichauf explains, "allow[ing] for the quarantine of malicious traffic immediately after it is discovered...is particularly critical in network security systems where time is of the essence in containing damaging information...once a security breach has occurred[.]" Gleichauf, [0020]; see also Gleichauf [0032] ("Network management controller 14 may implement this and other appropriate remedial procedures in order to prohibit infected computer 18 from communicating infective element 12 to a next destination.*

*Network management controller 14 may also direct infected computer 18 to remediator website 30.").* EX1003, ¶129.

- (d) Claim [1b(a)]: "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;"

**Gleichen** discloses, or at minimum renders obvious, restricting all network traffic emanating from the client device (e.g., "disabl[ing] the communications capability of a rogue (or an infected computer)") to one or more network destination addresses that are not in or subordinate to the first network segment (e.g., permitting infected computer only "to communicate with the remediator website"). EX1003, ¶130.

**Gleichen** discloses the network management controller "immediately disabl[ing] the communications capability of a rogue (or an infected computer)...prohibit[ing] the rogue from communicating to a next computer or to another destination," thereby blocking all traffic except as expressly permitted. Gleichen, [0006]; *see also id.*, [0019] ("network management controller 14 may then disable a communicating capability of infected computer 18 such that infective element 12 may not be communicated to a next destination. Network management controller 14 may also implement other suitable actions...in order to sandbox, siderail, isolate, or otherwise disable infected computer 18 from communicating further"), [0031] ("network management controller 14 may respond to the signal by

employing sandboxing or siderailing techniques on the associated infected device or unit. In addition, network management controller 14 may position an infected device or unit on an island or suitably disable the infected device or unit "), [0061] ("a communicating capability of infected computer 18 may be disabled.... Alternatively,...infected computer 18 may be disabled by employing sandboxing, constraining, isolating, or siderailing techniques.... Network management controller 14 may also execute any number of other actions in order to prohibit infected computer 18 from further communications."). EX1003, ¶131.

In addition to disabling regular communications, **Gleichauf**'s further discloses the network management controller "direct[ing the computer containing an infected element] to a remediator website in order to comply with a network security enforcement protocol," in which case, the computer "may continue to communicate with the remediator website until it removes the infective element...at which time it may be permitted to resume communications with other network components." Gleichauf, [0008]; *see also id.*, [0052] ("Remediator website 30 is a security element designed to facilitate the removal of infective element 12 from infected computer 18 in accordance with one embodiment of the present invention. Remediator website 30 is coupled to internal network 24 and infected computer 18, and may receive a communication from infected computer 18 after it has been identified as a rogue, i.e. inclusive of a damaging element. Infected computer 18 may be shunted or otherwise

directed to remediator website 30 until the proper software or configurations are downloaded or until infective element 12 is removed from infected computer 18."). In this way, **Gleichauf** discloses restricting all traffic emanating from the client device to only the remediator's website. EX1003, ¶132.

Additionally, the remediator's website is "coupled to"—but not necessarily in the "internal network" (Gleichauf, [0052]), which may be any of a "LAN, MAN, WAN, or any other architecture system that facilitates communications in a network environment." *Id.*, [0050]. To the extent it is argued, however, that being "coupled to internal network 24 and infected computer 18" means it is in or subordinate to the same network as the infected computer, a POSITA would have at minimum found it obvious that remediator's website could also be placed in an external network, such as the Internet. EX1003, ¶133. Placement of the remediator's website on the internal or external network is a simple design choice and a POSITA would have known and found obvious either of the two options. *Id.*

- (e) Claim [1b(b)]: "restricting all network traffic emanating from the client device to an allowed network destination address to selected one or more network protocols; and"

**Gleichauf discloses, or at minimum renders obvious, restricting all network traffic emanating from the client device (e.g., "disabl[ing] the communications capability of a rogue (or an infected computer)") to an allowed network destination address (e.g., "remediator websites") to selected one or more**

**network protocols** (*e.g.*, "TCP/IP"). EX1003, ¶134.

As discussed in [1b(a)], **Gleichauf** discloses disabling all communications from an infected computer aside from communications with a "remediator website." *E.g.*, Gleichauf, [0008] ("[A] computer containing an infective element may be directed to a remediator website in order to comply with a network security enforcement protocol."), [0032] ("***Network management controller 14 may implement...appropriate remedial procedures in order to prohibit infected computer 18 from communicating infective element 12 to a next destination. Network management controller 14 may also direct infected computer 18 to remediator website 30.*** Infected computer 18 may then communicate with remediator website 30 until infective element 12 is removed or until infected computer 18 is otherwise brought in compliance with suitable networking security protocols.") EX1003, ¶135.

**Gleichauf** further discloses that communications on the internal network and external network are implemented using "TCP/IP communication language protocol." Gleichauf, [0050], [0049]. And Gleichauf discloses a "policies node" that "includes protocols that dictate what may be accessed and run by elements within [the] communication system" and include policies on "any other suitable network enhancement or communications feature." Gleichauf, [0057]. Network management controller may use these policies "in order to disable one or more of

those policies or services being provided to infected [computer] 18 until it properly complies with the requisite security parameters." Gleichauf, [0058]; *see also id.*, [0061] ("network management controller 14 may access policies node 38 in order to restrict some service offered to infected computer 18..."). A POSITA would have understood, or at minimum found obvious, that restricting policies in this manner (*i.e.*, "disabl[ing] one or more of those policies or services being provided...until it properly complies with the requisite security parameters") would include restricting the use of network protocols other than TCP/IP needed to access the remediator's website. This would ensure that only the authorized traffic—TCP/IP traffic to the remediation website—is allowed while all other potentially harmful traffic is restricted. EX1003, ¶136.

- (f) Claim [1c]: "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."

**Gleichauf discloses, or at minimum renders obvious, rendering a web page to display on the client device from the network access gateway device (e.g., "signal", "broadcast signal", "alert signal"), 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 (e.g., communications blocked "until the proper**

software or configurations are downloaded or until infective element [] is removed from infected computer") **responsive to implementation of one of the plurality of quarantine control function of the client device.** EX1003, ¶137.

**Gleichauf** discloses a "web browser" on the infected computer that can be used to "view pages." Gleichauf, [0027]. Gleichauf further discloses once an infection is detected on an infected computer, "communication protocol shim" may generate a signal that is transmitted to the network management controller and to other computers that "may signal the presence of infective element [] at infected computer." Gleichauf, [0044] ("*Communication protocol shim 42 may be configured such that once infected element 12 is identified, a signal is generated and sent to network management controller 14.... Communication protocol shim 42 may signal the presence of infective element 12 at infected computer 18 in any number of ways...*"). This includes "send[ing] a signal directly to infected computer 18 that signifies that infective element 12 is within its internal structure" and, in response, infected computer may "communicat[e] with the remediator website [], or alternatively [] perform[] some cleaning or security check." Gleichauf, [0045]. In addition, **Gleichauf** discloses that the network management controller may "broadcast an alert signal to components within communication system." Gleichauf, [0061]; *see also id.* [0060]. This "alert signal may include information such as...the type of damaging element present in the network, or remedial measures." Gleichauf,

[0032]; *see also id.* [0047] ("**broadcast signal may** include the type of damaging element present...and **further provide remedial measures to be taken** if the damaging element is subsequently encountered"), [0048] ("the **signal may include information for remedial measures** for coping with or for combating the damaging element...[or] include any other suitable information that offers some guidance in handling the presence or harmful affects of infective element"), [0060] ("**signal may include...the remedial measures to be taken** when encountering infective element 12, or any other suitable information relating to the presence of infective element 12. **The signal may be communicated directly to infected computer 18...**"). EX1003, ¶138.

A POSITA would have thus understood, or at minimum found it obvious, that the network management controller could, like the communication protocol shim, broadcast an alert "signal directly to infected computer" identifying the "damaging element...[and] remedial measures" for dealing with it. EX1003, ¶139; Gleichauf, [0032], [0047], [0048]. A POSITA further would have understood that—because the "signal" includes information such as "remedial measures for coping with or for combating the damaging element," it would have been an obvious design choice to implement the signal in a form easily usable by an end-user, such as a web page from the network management controller informing the user of the infection and ways to remediate it, including by visiting a remediation website. EX1003, ¶139. A

POSITA would have understood that, by sending a web page from the controller to the infected computer, the controller could easily and quickly inform a user of the infected computer of the reason why its communications are being blocked and how to remediate the issue to restart regular communications, such as by visiting a "remediator website" to install "software...that facilitates the removal of infective element" as discussed in [2]. This would have been easily implemented by a POSITA in that timeframe and would have yielded expected results. *Id.* Further, that the "alert" also is broadcast to all other devices within the network suggests, and at minimum renders obvious, that the web-page implementation would be graphically rendered at the server and transmitted in an easily accessible format to quickly and cleanly ensure the information is received accordingly. *Id.*

3. **Claim [2]: "The method according to claim 1, 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."**

**Glechauf discloses, or at minimum renders obvious, the method according to claim 1, wherein the action requires the user to obtain and execute abnormal behavior scanning software (e.g., "hardware, software, or any other object or element that combats or that facilitates the removal of infective element", "virus detection element") from a server machine running at one of the one or more allowed network destination addresses (e.g., "remediator website").**

EX1003, ¶140.

*See [1c].* In addition, a POSITA would have understood that **Gleichauf's** disclosure of quarantining an infected computer and blocking all communications other than to a remediator website "until the proper software or configurations are downloaded" (Gleichauf, [0052]) discloses, and at minimum renders obvious, requiring the user to download and execute virus scanning software, or something similar, in order restore normal communications. EX1003, ¶141; *see also* Gleichauf [0032] (allowing only "communicat[ions] with remediator website 30 until infective element 12 is removed or until infected computer 18 is otherwise brought in compliance").

Further, a POSITA would understand that **Gleichauf** discloses, or at minimum renders obvious the remediator website providing an updated "virus detection element" as an example of software "that combats or that facilitates the removal of infective element." EX1003, ¶142. Specifically, **Gleichauf** discloses that the remediator website, which includes "software...that combats or that facilitates the removal of infective element" will "evaluate infected computer 18 and determine that it is in proper security compliance," which discloses, or at minimum renders obvious, scanning the infected computer for abnormalities. Gleichauf, [0052]; EX1003, ¶142. Likewise, Gleichauf describes a "virus detection element" as "any hardware, *software*, or elements *operable to detect a damaging element*,

such as infective element 12, present in communication system 10. *Virus detection element 40 may also be a desktop firewall product, such as those produced by Symantec Inc., Network Associates, or Computer Associates that perform some (potentially routine) security screening in insuring that a corresponding element is clean of potential harmful elements.* Virus detection element 40 may also be capable of identifying a particular type of damaging element, such as a Trojan, a worm, or a virus, for example...." Gleichauf, [0042]. Further, **Gleichauf** discloses that computers without a "virus detection element" are "not in compliance with any security protocol." Gleichauf, [0041]. A POSITA thus would have understood that bringing such a computer into compliance (*i.e.*, an infected computer without a virus detection element) would have required downloading and executing a valid "virus detection element" on the infected computer. EX1003, ¶143.

4. **Claim [3]: "The method according to claim 1, further comprising: 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."**

**Gleichauf discloses or at minimum renders obvious the method according to claim 1, further comprising: evaluating network traffic (*e.g.*, "routines or programs that execute pattern matching, looking for specific or systematic traffic behavior") emanating from the client device after the client device has been scanned and abnormal behavior has been removed, mitigated or rendered**

**inert.** EX1003, ¶144.

**Gleichauf** discloses using the "virus detection element" to "execute pattern matching, looking for specific or systematic traffic behavior." Gleichauf, [0042]. A POSITA would have understood that **Gleichauf** therefore discloses, or at minimum renders obvious, performing such traffic pattern matching for communications from all computers—including the infected computer—before, during, and after an infection has been identified and mitigated. *See* [1c], [2], above. EX1003, ¶145.

5. **Claim [4]: "The method according to claim 1, further comprising: filtering the network traffic emanating from the client device to limit network packet flow by the client device."**

**Gleichauf discloses the method according to claim 1, further comprising: filtering the network traffic emanating from the client device (e.g., "disabl[ing] the communications capability of a rogue (or an infected computer)") to limit network packet flow by the client device.** EX1003, ¶146.

*See* [1b(a)], [1b(b)]. A POSITA would have understood that quarantining an infected computer to "disable the communications capability of a rogue (or an infected computer)" as discussed above in [1b(a)] discloses or at minimum renders obvious filtering the network traffic emanating from the client device (e.g., allowing authorized communications while preventing unauthorized communications), which would result in limiting the network packet flow by the client device. EX1003, ¶147.

6. **Claim [5]: "The method according to claim 1, further**

**comprising: routing the network traffic emanating from the client device to limit network packet traversal by the client device."**

**Glechauf discloses the method according to claim 1, further comprising: routing the network traffic emanating from the client device (e.g., "shunt[] or otherwise direct[ traffic] to remediator website") to limit network packet traversal by the client device. EX1003, ¶148.**

*See [1b(a)], [1b(b)].* A POSITA would have understood that quarantining an infected computer such that it is "shunted or otherwise directed to remediator website 30" until the problem is fixed, as discussed above in [1b(a)] discloses or at minimum renders obvious routing the network traffic emanating from the client device to only specifically allowed servers or sites (e.g., "remediator website"), which limit network packet traversal by the client device by blocking traffic to any non-approved computer. EX1003, ¶149.

7. **Claim [6]: "The method according to claim 1, wherein the plurality of quarantine control functions further comprises: restricting all network traffic emanating from the client device to one or more network destination addresses in one or more network segments that are not in or subordinate to the first network segment."**

**Glechauf discloses, or at minimum renders obvious, the method according to claim 1, wherein the plurality of quarantine control functions further comprises: restricting all network traffic emanating from the client device to one or more network destination addresses in one or more network**

**segments that are not in or subordinate to the first network segment.**

EX1003, ¶150.

**See [1b(a)].** As discussed in [1b(a)], **Glechauf** discloses limiting traffic from the quarantined computer to allow access to only remediator websites. A POSITA would have understood that such remediation sites—*i.e.*, Internet web sites—are not in the first network segment. EX1003, ¶151.

**8. Claim [7]: "The method according to claim 1, further comprising: performing all of the plurality of quarantine control functions over the client device."**

**Glechauf discloses, or at minimum renders obvious, the method according to claim 1, further comprising: performing all of the plurality of quarantine control functions over the client device.** EX1003, ¶152.

As discussed above in [1b(a)] and [1b(b)], **Glechauf** discloses restricting network traffic for the quarantined computer to only certain allowed websites (e.g., only "remediator website" as set forth in [1b(a)]) and restricting communications to those same sites using only certain protocols (e.g., limiting services but allowing TCP/IP connection to remediator website) as set forth in [1b(b)]. *See, e.g.*, EX1005, 11:15-56. EX1003, ¶153.

*See also* [1b(a)], [1b(b)].

**9. Claims 8 and 15**

As with Ground 1, Petitioner addresses the differences in claims 8 and 15 and

provides a mapping for the remaining claim limitations that are substantively similar to claim 1 limitations addressed above. EX1003, ¶154.

- (a) **Claims [8pre]: "A computer program product comprising at least one non-transitory computer readable medium storing instructions translatable by at least one processor to perform:"; [15a] "at least one processor"; and [15b] "at least one non-transitory computer readable medium storing instructions translatable by the at least one processor to perform:"**

**Glechauf discloses, or at minimum renders obvious, a computer program product comprising at least one non-transitory computer readable medium storing instructions translatable by at least one processor.** EX1003, ¶155.

*See*, claim 1, above. **Glechauf** further discloses a "[n]etwork management controller" that "may include any hardware, software, object, or elements" to perform the disclosed methods. Glechauf, [0030]. To the extent not explicit, a POSITA would have understood that a computer "hardware" and "software" programmed to carry out the disclosed invention discloses, and at minimum renders obvious, some form of a processor and non-transitory computer readable medium storing [software] instructions. EX1003, ¶156.

- (a) **Claim [15pre]: "A network access gateway device, comprising:"**

*See* claim [1a]; 8[pre]. EX1003, ¶157.

- (b) **Remaining Limitations**

As with Grounds 1 and 2, the remaining limitations of claims 8 and 15 are already addressed with respect to claim 1 and are invalid for the same reasons. *Supra* § V.A.9(c). The same mapping of limitations from the prior grounds applies equally to these grounds. *Id.* EX1003, §XI.C.3.

**1. Claims 9-14 and 16-20**

The remaining dependent system and device claims are substantively the same as the corresponding method claims already addressed and are invalid for the reasons set forth above based upon the same claim mapping set forth in Grounds 1 and 2. *Supra*, § V.A.10. The Grounds 3-4 analysis from the method claims are incorporated herein by reference. EX1003, ¶158.

**C. Grounds 5 and 6 – Grounds 1-4 in View of Short**

As discussed above, §§V.A-V.B, **Roskind** and **Gleichenhauf** each discloses, and at minimum, renders obvious, all the limitations of Challenged Claims 1-20. With respect to Claim 1's requirement of "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" (element [1c]), **Roskind** discloses a "browser" on the client computer that is redirected to a "quarantine server [] configured to provide a notice and other information and/or instructions to a user of

the quarantined host" and a POSITA would have understood that browsers are used to render web pages. Roskind further discloses that the quarantine server "resides on the router...and/or gateway," EX1005, 12:11-13; §V.A. To the extent it is argued that **Roskind** is not entitled to its 9/27/2004 priority date for this disclosure,<sup>3</sup> **Short** discloses such a server residing on a gateway device. *E.g.*, Short, 4:13-21. EX1003, ¶159.

Likewise, **Gleichauf** discloses transmitting a "signal" containing detailed information about the presence of, and how to remedy, an infection, and a POSITA would have found it obvious to implement this signal as a web page transmitted from the network management controller to the infected computer. §V.B. But to the extent further disclosure is required for such a web page transmitted from a server residing on a router/gateway, a POSITA would have found it obvious to implement such teachings from **Short**. EX1003, ¶160.

**Short** discloses a gateway device which "serves as an interface connecting [a] user to a number of networks or other online services. For example, the gateway device can serve as a gateway to the Internet, the enterprise network, or other networks and/or on-line services." Short, 2:5-9. In addition, the gateway allows

---

<sup>3</sup> Even if not considered prior art for this specific disclosure, Roskind "constitutes prior art for all that it teaches as of its earliest accorded filing date." *In re Riggs*, 131 F.4th at 1385.

"Internet Service Providers (ISPs) [and] enterprise network (such as a LAN established by an entity such as a hotel) providers [to] permit a wide variety of users simple and transparent user access to their networks and to other online services." In doing so, the providers or ISPs may "redirect users to portal pages that [they]...wish the user to access or view." Short, 2:45-53. The portal pages include a "login page, so that the user may enter login information to be authenticated and authorized access on the network." Short, 3:9-12. Further, **Short** discloses that "[t]he portal page of the system can also be maintained *on a server local to the gateway device*." Short, 5:32-34; *see also id.*, 4:13-21 ("the method can include the step of establishing *a login page on a webserver local to the gateway device* prior to redirecting the user to the login page. The method can also include *accepting user information at the login page which is thereafter utilized by the gateway device to authorize the user access to the destination network*."); 4:54-55 ("login page is maintained local to the gateway device"). By locating the web server within the gateway device, "the redirection will be efficient and fast." Short, 9:5-15. **Short** further discloses that this redirection to a locally-hosted web server can be limited to certain types of traffic, *i.e.*, "redirecting web pages only, rather than all traffic, including E-mails, FTPs, or any other traffic." Short, 9:26-48. In addition, "the portal page can be a webpage containing any information whatsoever, and can be created by the ISP, enterprise network administrator or user. The portal page can

contain information specific to the user accessing the network." Short, 8:20-30. This includes offers for services, including for the network connection, from the network service provider. *See* Short, 10:5-19; *see also id.*, 3:54-59 ("users are directed to a login page in which the users must input user information so that the users can obtain access to networks"). As **Short** explains, the login page on the webserver local to the gateway device "accept[s] user information...which is thereafter utilized by the gateway device to authorize the user access to the destination network...which can be an Internet destination address." Short, 4:16-25. Thus, **Short** discloses "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." EX1003, ¶¶72-76, 161-163.

A POSITA would have been motivated to apply these teachings to the quarantine control systems of **Roskind** and **Gleichauf**. EX1003, ¶164. Like Roskind and Gleichauf, **Short** is in the same field as the '710 patent—controlling access to networks—and is reasonably pertinent to the '710 patent's alleged problems, including implementing a gateway to control access to networks by unauthorized computers. *See, e.g.*, EX1005, 3:10-23 (disclosed invention involved "[a]nalyzing routing information to identify and intercept unauthorized...communications"); Gleichauf, [0006] ("allows for the quarantine of

malicious traffic immediately after it is discovered within the network architecture");

Short, 4:17-20 ("method can also include accepting user information...utilized by the gateway device to authorize the user access to the destination network.").

**Roskind** and **Gleichauf** already teach methods of quarantining communications to restrict unauthorized computers and actors from utilizing protected network resources, including redirection of quarantined computers to an ISP web page on a quarantine server or a "remediator website." See §§V.A.1, **Error! Reference source not found.** ([1b], [1b(a)], [1b(b)], [1(c)]), V.B.1, **Error! Reference source not found.** ([1b], [1b(a)], [1b(b)], [1(c)]). Thus, a POSITA would have been motivated to look to references, including **Short**, for well-understood implementation details such as hosting the quarantine server local to the gateway for efficient and fast redirection, as well as offers to the user for gaining (or re-gaining) access to network services, including the Internet. EX1003, ¶¶164-165. Modifying these quarantine control system—which already performs redirection responsive to the quarantine control functions—to include these teachings from **Short** yields a method that renders 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, rendering obvious claims 1-20. *Id.* A POSITA would have had reasonable

expectation of success modifying **Roskind** and **Gleichen** with **Short's** teachings because these locally-hosted web servers are well-understood and are used for their intended purposes. *Id.*

# **VI. MANDATORY NOTICES UNDER 37 C.F.R. §42.8(a)(1)**

## **A. 37 C.F.R. §42.8(b)(1): Real Parties-In-Interest**

Petitioner is the real party-in-interest.

## **B. 37 C.F.R. §42.8(b)(2): Related Matters**

The '710 patent is asserted against Petitioner in *Netskope, Inc. v. Fortinet, Inc.*, No. 3:25-cv-2360 (N.D. Cal.).

## **C. 37 C.F.R. §42.8(b)(3)-(4): Lead And Back-Up Counsel And Service Information**

Designated Counsel for Petitioner and service information is below:

| Lead Counsel                                                                                                                                                             | Back-Up Counsel                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Andrew D. Gish (Reg. # 67,562)</b><br/> GISH PLLC<br/> 41 Madison Avenue<br/> New York, New York 10010<br/> Telephone: (212) 518-7380<br/> andrew@gishpllc.com</p> | <p><b>Ryan Iwahashi (Reg. # 63,378)</b><br/> GISH PLLC<br/> 50 California Street, Suite 1500<br/> San Francisco, CA 94111<br/> Telephone: (415) 630-8960<br/> ryan@gishpllc.com</p> <p><b>Josef B. Schenker</b> (<i>pro hac forthcoming</i>)<br/> 41 Madison Avenue<br/> New York, New York 10010<br/> Telephone: (212) 518-7380<br/> Josef.schenker@gishpllc.com</p> |

Petitioner consents to service by email at the addresses above.

**VII. FEES UNDER 37 C.F.R. §42.103**

Petition and Post-Institution fees totaling \$51,875.00 have been paid by electronic funds transfer.

**VIII. CONCLUSION**

Petitioner requests the Board institute IPR of the Challenged Claims and cancel them.

Respectfully Submitted,

Dated: October 13, 2025

/s/Andrew Gish

Andrew Gish (Reg. #67,562)

ATTORNEY FOR PETITIONER

**CERTIFICATE OF WORD COUNT UNDER 37 C.F.R. §42.24(a)**

I, the undersigned, do hereby certify that the attached petition contains 13,844 words, as measured by the Word Count function of Microsoft Word. This is less than the limit of 14,000 words as specified by 37 C.F.R. §42.24(a)(i).

Dated: October 13, 2025

/s/ Andrew Gish

Andrew Gish (Reg. # 67,562)

ATTORNEY FOR PETITIONER

**CERTIFICATION OF SERVICE**

The undersigned certifies service pursuant to 37 C.F.R. §§42.6(e) and 42.105 on the Patent Owner of a copy of this Petition for *Inter Partes* Review and supporting materials via FedEx at the following correspondence address of record:

25883 - MUNCK WILSON MANDALA L.L.P  
2000 McKinney Ave Ste 1900  
Dallas, TX  
UNITED STATES

Dated: October 13, 2024

/s/ Andrew Gish

Andrew Gish (Reg. # 67,562)

ATTORNEY FOR PETITIONER