IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Reexam of:	U.S. Pat. No. 10,601,780
Reexam Control No.:	90/015,746
Reexam Filing Date:	December 2, 2025
Patent Owner:	Croga Innovations Ltd.
Inventor:	Hoy, Robert B., et al.
Art Unit:	3992
Examiner:	Choi, Woo H.
Confirmation No.:	2365
Title:	INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS

PETITION FOR THE DIRECTOR TO SUSPEND THE RULES AND TERMINATE REEXAMINATION UNDER 35 U.S.C. § § 303(a) AND 325(d)

Mail Stop *Ex Parte* Reexam
Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Pursuant to 35 U.S.C. §§ 303(a) and 325(d), as well as 37 C.F.R. §§ 1.181(a)(3) and 1.182, Patent Owner Croga Innovations Ltd. ("Croga") petitions the Director to intervene and terminate the ongoing reexamination challenging the validity of U.S. Patent No. 10,601,780 ("the '780 Patent") because (1) the identical prior art and the argument were previously presented to the Office by the petition denied in IPR2025-00884 that was filed by the same requester, Amazon Web Services, Inc. (see 35 U.S.C. § 325(d)); and, alternatively, (2) Amazon's reexamination is an improper serial attack on the patent—the sixth attack on the '780 Patent lodged with the Office—coming on the heels of a fifth attack that was itself rejected because multiple serial attacks had already been filed against the patent (see *In re Vivint*, 14 F.4th 1342 (Fed. Cir. 2021)). Pursuant to 37 C.F.R. § 1.183, Croga requests that the Director suspend any rule that would prevent consideration of this petition (including but not limited to §§ 1.515, 1.530(a), and 1.540).

Patent Owner respectfully submits that under facts of this case, where the patent has been challenged six times through four petitions for IPR and two requests for reexamination, compounded by the aggravating factor that the request for reexamination set forth the very same prior art and very same argument presented by Amazon's earlier-rejected IPR petition, the Director should exercise his authority to terminate this proceeding under Section 325(d).

Croga requests that this petition be forwarded to the Director so that he may intervene pursuant to 37 C.F.R. § 1.183.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

PETITION DECISIONS

AGENCY DECISIONS

REGULATIONS

CONGRESSIONAL RECORD

PATENT OWNER'S EXHIBIT LIST

Ex. No.	Description
Ex. A	Complaint in *Croga Innovations Ltd. v. Amazon Web Services Inc.*, Case No. 1-24-cv-00398 (W.D. Tex.) Dkt. No. 1 (Apr. 16, 2024)
Ex. B	Request for reexamination by Amazon 90/019,638 for U.S. Pat. No. 10,601,780 (Aug. 28, 2024)
Ex. C	Petition for IPR by Amazon Web Services, IPR2025-00884 (Apr. 17, 2025)
Ex. D	Defense and Detection Strategies Against Internet Worms (Nazario)
Ex. E	U.S. Pat. Pub. No. 2010/0122343 (Ghosh)
Ex. F	Croga Request for Discretionary Denial, IPR2025-00884, Paper 6 (Jul. 21, 2025)
Ex. G	Amazon Response to Request for Discretionary Denial, IPR2025-00884, Paper 8 (Aug. 21, 2025)
Ex. H	Croga Patent Owner Preliminary Response, IPR2025-00884, Paper 7 (Aug. 20, 2025)
Ex. I	Director Denial of Petition, IPR2025-00884, Paper 9 (Sep. 3, 2025)
Ex. J	Petition for IPR by Cisco, IPR2024-01196, Paper 2 (Jul. 25, 2024)
Ex. K	Croga Patent Owner Preliminary Response, IPR2024-01196, Paper 6 (Nov. 20, 2024)
Ex. L	Order denying Petition, IPR2024-01196, Paper 7 (Feb. 13, 2025)
Ex. M	Petition for IPR by Fortinet, IPR2025-00086, Paper 1 (Oct. 24, 2024)
Ex. N	Croga Patent Owner Preliminary Response, IPR2025-00086, Paper 8 (Feb. 28, 2025)
Ex. O	Order denying Petition, IPR2025-00086, Paper 9 (Mar. 27, 2025)
Ex. P	Petition for IPR by IBM, IPR2025-00380, Paper 2 (Dec. 30, 2024)
Ex. Q	Croga Request for Discretionary Denial, IPR2025-00380, Paper 7 (Apr. 25, 2025)
Ex. R	Joint Motion to Terminate, IPR2025-00380, Paper 8 (May 27, 2025)

Ex. S	Order of Termination, IPR2025-00380, Paper 11 (June 2, 2025)
Ex. T	Notice of Proposed Rulemaking (Oct. 17, 2025)
Ex. U	USPTO Press Release on NPRM (Oct. 16, 2025)
Ex. V	Request for *Ex Parte* Reexamination by Amazon 90/019,638 (Aug. 28, 2024)
Ex. X	Reexamination Order 90/019,638 (Nov. 21, 2024)
Ex. Y	Final Office Action 90/019,638 (Aug. 1, 2025)
Ex. Z	After-Final Submission 90/019,638 (Dec. 9, 2025)
Ex. AA	Appeal Brief 90/019,638 (Jan. 16, 2026)
Ex. AB	Unified Patents Dispute Report 2025 (Jan. 13, 2026)
Ex. AC	PTAB Judges Alarmed by Squires' Moves to Limit Their Role (IPLaw360) (Oct. 27, 2025)
Ex. AD	Stewart Says New Patent Policies Aim To Bring Stability (IPLaw360) (Sep. 8, 2025)

I. Introduction

Croga Innovations Ltd. ("Croga" or "Patent Owner") is the owner of U.S. Pat. No. 10,601,780 ("the '780 Patent"). The '780 Patent has been the target of four petitions for IPR and now two requests for reexamination—six challenges to the same patent. This is the kind of abusive serial attack that was criticized by the Federal Circuit in *In re Vivint*, 14 F.4th 1342 (Fed. Cir. 2021) and that led to the Court ordering the Office to terminate that reexamination.

In this case, Amazon filed an IPR petition that was denied. Then Amazon reformatted the IPR petition into a request for reexamination and submitted it to the Office. For the sake of fairness and consistency, the Office should not grant a copycat request for reexamination submitted after the Office denied a substantively identical petition for IPR.

The Director should order this reexamination terminated pursuant to 35 U.S.C. § 325(d) because the same prior art and the same argument was previously presented to the Office, as admitted by Amazon in its request. See Request for Reexamination, 90/015,746, December 2, 2025 (hereinafter "the Request"), 4 ("The IPR was based on the same references relied on in this request for reexamination, Nazario and Ghosh."). The CRU examiner confirmed that Amazon's request was based on the very same prior art and argument Amazon presented to the Office in IPR2025-00884. Reexam Order, 9 ("A comparison between the current reexamination request and the prior Office post grant challenges indicates that current request presents the same prior art and arguments as were presented in the IPR2025-00884."). This is the kind of patent owner harassment that § 325(d) was designed to prevent, as reflected by the language of the statute and the legislative history. The Director should exercise his discretion to terminate this reexamination under § 325(d).

Alternatively, this reexamination should be terminated pursuant to *Vivint*. In *Vivint*, the patent had been subjected to three petitions for IPR and one request for reexamination—four

challenges to the patent. This case is more egregious because the '780 Patent has been the target of six challenges to the patent: four IPR petitions and two requests for reexamination including this one. Even before the request for reexamination was submitted for this proceeding, the Director criticized the Amazon's earlier-filed petition for IPR in IPR2025-00884: "However, this is the fourth petition for *inter partes* review" and, furthermore, an existing "*ex parte* reexamination has [already] been ordered." See Ex. I (Order denying Institution, IPR2025-00884), 2. The request for this new proceeding is all the more abusive because it is based on the very same prior art and very same argument as presented in the denied petition for IPR. Instituting a second reexamination when one reexamination is already ongoing, and where four prior petitions for IPRs failed, is a profoundly inappropriate use of the reexamination process. It is also a highly inefficient use of the resources of the Office. Under these circumstance, the Director should order that this reexamination be terminated.

II. Statement of Facts

A. The '780 Patent Has Been Subjected to a Serial Attack of Six Challenges Via IPRs and EPRs

The '780 Patent has been subjected to a serial attack consisting of six separate challenges: four petitions for IPR and two requests for *ex parte* reexamination ("EPR").

1. Challenge #1: Petition for IPR by Cisco in IPR2024-01196 Denied On Merits

Cisco filed a petition for IPR in IPR2024-01196 challenging Claims 1-20 based on two grounds: (1) Delco and Adams (Claims 1-7, 9-17, and 19-20), and (2) Delco, Adams, and Dadhia (Claims 8 and 18). See Ex. J (Petition, IPR2024-01196, 7/25/2024). Patent Owner's Preliminary Response ("POPR") explained that the Delco/Adams combination failed to meet the limitation in independent Claim 1 for "*an internal firewall [that] is configured to separate the host system*

from the virtual system in the computer system" and the similar limitation in independent Claim 11. See Ex. K (POPR, 11/20/2024), 3-10.

As set forth in Claim 1, the claimed networked "*computer system*" comprises "*a host system and a virtual system.*" The "*computer system*" is subject to three separate firewalls: (1) "*a network firewall … configured to implement network isolation between one or more untrusted network destinations and the networked computer system*," (2) "*a host-based firewall … configured to implement network isolation between the computer system and the network*," and (3) "*an internal firewall [] configured to separate the host system from the virtual system*." Ex. K, 4.

Patent Owner explained that Delco's packet filter 74 that filters incoming and outgoing packets from the network does not correspond to the claimed "*internal firewall*" that provides isolation between the "*host system*" and the "*virtual system*." Ex. K, 6-7. In other words, filter 74 provides ***network isolation*** for the computer for traffic from the network, not ***host system/virtual system isolation*** restricting communications between the host system and virtual system. Put another way, Delco's disclosure of packet filtering involves restricting communications of network traffic between the computer system and an external network, unlike the claimed "*internal firewall*" that restricts communications *within* the computer system between the "*host system*" and "*virtual system*." *Id.*, 8-9.

The Board agreed with Croga. The Board declined to institute Cisco's petition on the merits because Delco does not teach the claimed "*internal firewall*" limitation. See Ex. L (Order, 1/13/2025), 13. The Board found that Delco discloses a computer system executing a plurality of virtual machines. *Id.*, 12. Delco discloses that each virtual machine has a packet filter 74 that manages network communication with respect to external entities. *Id.* The packet filter 74 filters

"network packet traffic" for the guest operating system 58. Thus, packet filter 74 provides a network packet processing function to protect guest OS 58 from external network packets, not from communications with the host system. *Id.*, 16-17. The Board stated that its finding was confirmed by Figure 2 of Delco, which illustrates two firewalls, neither of which is positioned between the host system and a virtual machine. *Id.* Accordingly, the Board found that Delco does not teach or suggest the packet filter operating as the claimed "*internal firewall*" providing separation or isolation between the guest operating system and the host system, as would be required by the independent claims. *Id.*, 17-21.

The Board thus denied Cisco's challenge to Claims 1-20 on the merits.

2. Challenge #2: Petition for IPR by Fortinet in IPR2025-00086 Denied On Merits

Fortinet filed a petition for IPR in IPR2025-00086 challenged Claims 1-20 based on two grounds: (1) Claims 1-7, 9-17, and 19-20 based on Delco and Adams, and (2) Claims 8 and 18 based on Delco, Adams, and Dadhia. See Ex. M (Petition, 10/24/2024), 17. The challenge was very similar to that presented by Cisco. Ex. M, 17

Croga filed a POPR explaining that, as with Cisco's petition, Fortinet's petition failed to establish that Delco taught or suggested the claimed "*internal firewall*" of independent Claims 1 and 11. See Ex. N (POPR, 2/28/2025), 1-2. Croga explained that Delco's packet filter at best performed network isolation by filtering packets from the network (e.g., Internet), not an "*internal firewall*" providing isolation between the host system and the virtual system. *Id.*, 6-7. Croga pointed out that the distinction between network isolation and host system/virtual system separation is reflected in the claims, which recite the "*internal firewall*" (recited as providing separation between the host system and the virtual system) separately from the "*host-based firewall*" (recited as providing network isolation), and the "*network firewall*" (also recited as

providing network isolation). *Id.*, 6-7. Croga also pointed out that the "*internal firewall*" is not disclosed in the '780 Patent as a packet filter. *Id.*, 8. Croga also pointed out that Delco does not disclose that filter 74 limits guest OS access to the resources of the host operating system. *Id.*, 10.

The Board again agreed with Croga and denied institution of Fortinet's petition on the merits. See Ex. O (Decision, 3/17/2025). Based on reasoning similar to IPR2024-01196, the Board denied the petition because Delco failed to teach or suggest the claimed "*internal firewall*" limitations of Claims 1 and 11. *Id.*, 20-21.

3. Challenge #3: Petition for IPR by IBM in IPR2025-00380 Presenting Grounds Rejected On the Merits In IPR2024-01196 and IPR2025-00086

Another petition challenging the '780 Patent was filed by IBM challenging Claims 1-20 based on the same two grounds as in the Cisco and Fortinet IPRs, namely: (1) Claims 1-7, 9-17, and 19-20 based on Delco and Adams, and (2) Claims 8 and 18 based on Delco, Adams, and Dadhia. Ex. P (Petition, 12/30/2024), 19. The Petition made the same argument as Cisco's and Fortinet's failed petitions that Delco's packet filter 74 meets the "*internal firewall [] configured to separate the host system from the virtual system*." *Id.*, 39-42. IBM conceded that its petition was substantively the same as that presented by Cisco. *Id.*, 14-15.

Croga filed a request for discretionary denial of IPR2025-00380. See Ex. Q (Request, 4/25/2025). Croga pointed out that the prior art (Delco/Adams) and argument in IBM's petition were the same as that rejected by the Board two times on the merits for the petitions filed by Cisco and Fortinet. *Id.*, 1-2. Croga pointed out that just as in IPR2024-01196 and IPR2025-00086, the Delco art failed to teach or suggest the claimed "*internal firewall*." *Id.*, 16-23.

By the time Croga filed its request for discretionary denial, the Board had issued its two decisions declining to institute on the merits for Cisco in IPR2024-01196 and Fortinet in

IPR2025-00086. As a result, IBM agreed to terminate the IPR and settle the suit. *See Croga Innovations Ltd., v. International Business Machines Corp.*, Case No. 2:23-cv-00634-JRG (E.D. Tex.), Dkt. No. 49 (Joint Motion to Stay All Deadlines and Notice of Settlement, 4/15/2025). See Ex. R (Joint Motion to Terminate, IPR2025-00380, 5/27/2025), Ex. S (Order of Termination, IPR2025-00380, 6/2/2025).

4. Challenge #4: Request for Reexamination by Unified Patents in 90/019,638

Unified Patents filed a request for *ex parte* reexamination ("EPR") challenging Claims 1-20 based on Thomas and Garge. See Ex. V (Request, 8/28/2024), 10. In the proposed combination, Unified argued that the end point security facility 152 in Figure 2 of Thomas would "include network access control features allowing it to function as an internal firewall." *Id.*, 17. Requester Amazon conceded that Thomas was short on implementation details for end point security facility 152 and thus referred to Garge to try to fill the gap. *Id.*, 17-18. Garge allegedly describes a hypervisor configured to secure a point-to-point connection. *Id.*, 17.

The Office issued a Reexamination Order finding that a substantial new question of patentability ("SNQ") had been presented. See Ex. X (Reexam. Order, 90/019,638, 11/21/2024). The Examiner found that Thomas had not been previously considered and that it raised an SNQ. *Id.*, 6.

The Examiner issued two office actions finding that Thomas anticipates Claims 1-20. The second office action also asserted that new Claims 21-30 lacked written description support for the claim term "*a trusted local area network*." See Ex. Y (Office Action, 8/1/2025), 11-13.

An interview was conducted on December 3, 2025, with the undersigned counsel and the CRU examiner in attendance. The CRU examiner agreed to reopen prosecution if written description support was provided for "*a trusted local area network*" in an after-final paper.

Patent Owner provided such support in an After-Final Submission filed on December 9, 2025, which cited six passages from the specification providing literal, word-for-word support for the claimed "*trusted local area network.*" *See* '780 Patent, 3: 15-16 ("secure file exchange to transfer data between the Internet and the trusted hosts of the trusted LAN"), 7:17-20 ("The local system 1 includes a trusted local area network (LAN) 7"); 10:54-57 (the computer system is "on the trusted LAN network.). The '780 Patent also discloses the trusted local area network at 3:19-13, 4:63-5:15, and 12:11-16. See Ex. Z (After-Final Response), 23-24; Ex. AA (Appeal Brief), 29-31.

Despite the ample written description support provided by Patent Owner, the CRU examiner maintained the position that the claim term "*trusted local area network*" was not supported and refused to reopen prosecution. Patent Owner thus proceeded with its appeal to the Board. Patent Owner Croga filed its appeal brief challenging the written description and anticipation rejections on January 16, 2025. See Ex. AA (Appeal Brief, 90/019,638). Patent Owner is awaiting the Examiner's Answer.

5. Challenge #5: Petition for IPR by Amazon in IPR2025-00884 Denied by the Director

Amazon filed a petition challenging Claims 1, 3, 7, 10, 11, 13, 17, and 20 in IPR2025-00884 based on one ground: Nazario and Ghosh. See Ex. C (Petition, 4/17/2025), 13. See Ex. D (Nazario), Ex. E (Ghosh).

Nazario discloses a system with a computer running multiple virtual machines on a network with other computers. Nazario allegedly discloses a network with computer systems having various defenses against attacks, including a network-based firewall and a host-based firewall that acts as a "failover" if an attack penetrates the network-based firewall. Ex. C, 16-17.

It is alleged that a computer can run a virtual machine called a "virtual host" that can contain damage and prevent an attack from spreading to the rest of the computer. *Id.*, 16-17, 21.

Notably, Nazario does not disclose a computer system having a "*host system*" and a "*virtual system*," as claimed, where there is an "*internal firewall*" that separates the "*host system*" from the "*virtual system*," and where the internal firewall is a protective firewall in addition to two other firewalls, which are the "*host-based firewall*" and the "*network firewall*."

Amazon's petition made a vague, high-level argument that Ghosh can fill the gaps in Nazario. Amazon broadly alleges that Ghosh teaches the use of "virtualization techniques" that can provide a "clean and isolated environment for instances of network applications" exposed to the Internet and susceptible to malicious attacks. Ex. C, 17. Croga's position was that Ghosh did not fill the gaps in Nazario to produce a viable combination meeting the claim limitations.

Croga filed a request for discretionary denial ("RDD") that explained, among other things, the weak merits of Amazon's ground based on Nazario and Ghosh. See Ex. F (RDD, 7/21/2025). Patent Owner Croga explained that the petition relied on "virtual machines" for the "*internal firewall*" limitation, an argument that had already been rejected twice for the petitions filed by Cisco and Fortinet denied on the merits in IPR2024-01196 and IPR2025-00086. *Id.*, 10. Patent Owner also pointed out that the '780 Patent had already been targeted by three earlier petitions for IPR and one ongoing EPR, and thus the patent was being subjected to serial attacks that are unfair to the Patent Owner.

Croga also filed a POPR that explained that Nazario/Ghosh failed to teach or suggest the "*an internal firewall . . . configured to separate the host system from the virtual system in the computer system*." Croga pointed out that Amazon's petition never identified where Nazario or

Ghosh or their combination has an "*internal firewall"* as claimed that separates the host system from the virtual system. Ex. H (POPR, IPR2025-00884, 8/20/2025), 8-9.

The Director denied institution in IPR2025-00884. See Ex. I (Denial of Institution, 9/3/2025). The Director found that various *Fintiv* factors were neutral: they "neither favor nor counsel against discretionary denial." *Id.*, 2.

The Director declined to institute the Amazon petition because it was part of an unfair serial attack on the '780 Patent. Specifically, Amazon's petition was the fourth in a sequence of IPR petitions and, additionally, there had already been a request for reexamination resulting in an ongoing EPR:

> **However, this is the fourth petition for *inter partes* review involving the challenged patent**. One petition was voluntarily dismissed prior to institution, and in the other two the Board denied institution on the merits. *See Fortinet v. Croga Innovations Ltd*., IPR2025-00086, Paper 9 at 20–21 (PTAB Mar. 27, 2025); *Cisco Sys., Inc. v. Croga Innovations Ltd*., IPR2024-01196, Paper 7 at 17, 21 (PTAB Feb. 13, 2025). Here, Petitioner states that its Petition "addresses the precise deficiency identified by the Board in denying the earlier petitions." DD Opp. 13. Petitioner's admission raises concerns of roadmaping and weighs in favor of discretionary denial.
>
> **Furthermore, an *ex parte* reexamination has been ordered on the challenged patent**, and the Office has issued a final rejection on the challenged claims. DD Opp. 2; Ex. 2003. **It is not an appropriate use of Office resources to review a patent in two separate, concurrent Office proceedings, especially when the reexamination is in an advanced stage**.

Denial of Institution, IPR2025-00884, Paper 9 at 2-3 (emph. added).

Accordingly, the Director rejected Amazon's petition for IPR because it was part of an unfair serial attack coming on the heels of multiple IPR petitions that were denied on the merits in addition to an ongoing reexamination. Notably, the Director's decision stated that all argument

and evidence presented by the parties had been considered, which includes the evidence and argument on the merits submitted by Croga and by Amazon in their papers. Ex. I (Decision), 2-3. See Ex. F (Croga Request), Ex. G (Amazon Response).

6. Challenge #6: Request for Reexamination by Amazon in 90/015,746

Three months after the Director rejected Amazon's petition for IPR, Amazon added to the serial attack by bringing forth a six challenge to the '780 Patent in the form of a request for EPR that presents the very same prior art and the very same arguments as Amazon's rejected IPR petition. Amazon concedes that its request for reexamination presents the same prior art (Nazario/Ghosh) and same argument that was presented in its rejected IPR petition. See Request, 90/015,746, December 2, 2025, 4 ("The IPR was based on the same references relied on in this request for reexamination, Nazario and Ghosh."); Reexam Order, 9 ("A comparison between the current reexamination request and the prior Office post grant challenges indicates that current request presents the **same prior art and arguments** as were presented in the IPR2025-00884.") (emph. added). Just as one example, the argument in the request for reexamination for limitation [1c] for the claimed "*internal firewall*" is a virtual cut-and-paste from the petition for IPR in IPR2025-00884. *Compare* Request, 52-56, *with* Ex. C (Petition), 27-32

On January 30, 2026, the Office granted the request for EPR in 90/015,746. Reexam Order, 6. The Reexamination Order evaluated whether to "reject the … request because, the same or substantially the same prior art or arguments were previously presented to the Office." *Id.* The CRU examiner recognized that four petitions for IPR had already been filed against the patent, as well as one request for EPR that resulted in an ongoing proceeding (90/019,638) that was on appeal. *Id*.

In analyzing the prior petition for IPR filed by Amazon in IPR2025-00884,[1] the CRU examiner conducted a cursory Section 325(d) analysis. That analysis was based on assertions that contradict the Director's statements in the order denying institution in IPR2025-00884, as discussed further below in Section IV.B.3. The analysis did not consider whether Requester Amazon had demonstrated a material error, nor did the CRU examiner consider the impact of the *Vivint* decision.

B. The Present Reexamination Is A Copycat Request That Presented The Same Prior Art and Same Argument As Amazon's Denied IPR Petition.

As discussed in Section A.6 above, the request for reexamination in 90/015,746 presents exactly the same prior art and argument as presented to the Office in Amazon's denied IPR petition in IPR2025-00884. See Request, 90/015,746, December 2, 2025, 4 ("The IPR was based on the same references relied on in this request for reexamination, Nazario and Ghosh."); Reexam Order, 9 ("A comparison between the current reexamination request and the prior Office post grant challenges indicates that current request presents the same prior art and arguments as were presented in the IPR2025-00884."). For example, in the request for reexamination the argument for limitation [1c] for the claimed "*internal firewall*" is a virtual cut-and-paste from the petition for IPR in IPR2025-00884. *Compare* Request, 52-56, *with* Ex. C (Petition), 27-32. The argument in the request for limitation [1d] for the claimed "*host-based firewall*" is literal cut-and-paste from the denied IPR petition. *Compare* Request, 60-62, *with* Ex. C (Petition), 32-34.

[1] The Order has a typo indicating that IPR2025-00884 was filed by "Cisco Systems, Inc." Reexam Order, 8. The -00884 petition was filed by Amazon, the same party requesting the instant reexamination in 90/015,746.

III. Applicable Law and Policy

A. The Director Has Authority To Terminate Reexaminations.

Congress granted the Director authority to decide whether to order reexamination. 35 U.S.C. § 303(a); *In re Vivint*, 14 F.4th 1342, 1349-50 (Fed. Cir. 2021). By rule, the Director has delegated that authority to the examining corps, see 37 C.F.R. § 1.515(a), but he may suspend "any requirement of the regulations ... which is not a requirement of the statutes" in "an extraordinary situation, when justice requires." 37 C.F.R. § 1.183. Delegation under Rule 515 is not a requirement of any statute, and, as explained below, justice requires that the Director suspend the Rule here and intervene to terminate the reexam under 35 U.S.C. § 325(d) and/or *Vivint*.

B. Section 325(d) Guards Against Serial Invalidity Challenges To A Patent Using Requests For Reexamination.

"Section 325(d) applies to both IPR petitions and requests for *ex parte* reexamination." *In re Vivint*, 14 F.4th at 1354. The statute authorizes the Director to terminate a reexamination if "the same or substantially the same prior art or arguments previously were presented to the Office." It reflects Congress's concern that the Patent Office was being "forced to accept many requests for *ex parte* ... reexamination that raise challenges that are cumulative to or substantially overlap with issues previously considered by the Office," without any prospect of finality. 157 Cong. Rec. S1376 (Mar. 8, 2011) (statement of Sen. Kyl). So strong was that concern that Congress enacted § 325(d) to fill gaps left by other statutory estoppel provisions in the IPR context (e.g., 35 U.S.C. § 315(e)(l)). Unlike those other provisions, § 325(d) can apply even if a prior IPR was denied and the ultimate issue of patentability was not reached, and even if the reexamination request raises a substantial new question of patentability. *Id*.; see *Vivint*, 14 F.4th at 1354.

In *Vivint*, the Federal Circuit explained that "[e]ven when an *ex parte* reexamination request presents a substantial new question of patentability, the Patent Office 'may ... reject the ... request because the same or substantially the same prior art or arguments previously were presented to' it." *In re Vivint,* 14 F.4th at 1350 (quoting 35 U.S.C. 325(d)). This is consistent with the legislative history of the Leahy-Smith America Invents Act:

> In the second sentence of section 325(d), the present bill also authorizes the Director to reject **any request for *ex parte* reexamination** or petition for post-grant or *inter partes* review on the basis that the same or substantially the same prior art or arguments previously were presented to the Office. This will prevent parties from **mounting attacks on patents that raise issues that are substantially the same as issues that were already before the Office** with respect to the patent. The Patent Office has indicated that **it currently is forced to accept many requests for *ex parte*** and *inter partes* reexamination that raise challenges that are cumulative to **or substantially overlap** with issues previously considered by the Office with respect to the patent.
>
> The second sentence of section 325(d) complements the **protections against abuse of *ex parte* reexamination** that are created by sections 315(e) and 325(e). The estoppels in subsection (e) will prevent *inter partes* and post-grant review petitioners from seeking *ex parte* reexamination of issues that were raised or could have been raised in the *inter partes* or post-grant review. The Office has generally declined to apply estoppel, however, to an issue that is raised in a request for i*nter partes* reexamination if the request was not granted with respect to that issue. **Under section 325(d), second sentence, however, the Office could nevertheless refuse a subsequent request for *ex parte* reexamination** with respect to such an issue, **even if it raises a substantial new question of patentability**, **because the issue previously was presented to the Office** in the petition for *inter partes* or post-grant review.

157 Cong. Rec. S1376 (2011) (emph. added).

The reason for the broad reach of § 325(d) is simple: "allowing similar, serial challenges to the same patent ... risks harassment of patent owners and frustration of Congress's intent in enacting the AIA." *Vivint,* 14 F.4th at 1353. "That is the heart of a § 325(d) analysis." *Id*. Indeed, the Office has denied or terminated reexamination under § 325(d) in scenarios like this one that recycle the same prior art and arguments that were previously presented to the Office. *See In re Bain*, No. 90/019,604, Decision on Petition, 7-8, 11 (Nov. 21, 2025) (Office exercising discretion to terminate under § 325(d) a reexamination presenting "grounds that are duplicative of each other and are composed of the same or substantially the same prior art" presented in earlier reexaminations); *In re Perisho*, No. 90/019,010, Decision on Petition (July 21, 2025) (Office exercising discretion to terminate a reexamination under § 325(d) where fifteen of the sixteen grounds had overlapping references with grounds previously presented in IPR petitions); *In re Haller*, No. 90/014,770, Decision on Petition, 12 (Feb. 10, 2022) (Office "exercis[ing] its discretion to reject" a request under § 325(d) where the claims had previously been upheld during reexam).

The policy concerns undergirding § 325(d) apply with equal force to both EPRs and IPRs. The Office has recognized that, to achieve stability in the patent system, we should encourage prompt patentability challenges and discourage serial challenges, and that logic holds regardless of whether the challenge is brought in an *ex parte* reexamination or an AIA trial proceeding. No matter the particular proceeding at issue, repeated "reconsideration of patent grants ... is the antithesis of stability." See Ex. AD (*Stewart Says New Patent Policies Aim to Bring Stability*, IPLaw360, 9/8/2025).

C. The Director's Framework For Exercising Discretion For IPRs Is Informative On Whether Discretion Should Be Exercised Under Section 325 (d) To Deny Or Terminate An EPR.

The policy concerns underlying Section 325(d) apply with equal force to EPRs and

IPRs. In light of their shared goals, the factors that are considered when determining whether to discretionarily deny IPR are at least informative for EPRs, and, accordingly, those factors should be considered in evaluating whether to exercise discretion to deny or terminate an EPR.

1. The *Advanced Bionics* Framework Is Applicable to EPRs.

The Consolidated Trial Practice Guide explains that the Office may "not necessarily consider" the same factors applicable in IPRs in evaluating the exercise of discretion under Section 325(d) for an EPR. CTG (Nov. 2019), 63. That said, the CTG does not rule out considering those factors for EPRs.

The framework for exercising discretion under Section 325(d) pursuant to *Advanced Bionics* for IPRs includes two inquiries:

(1) Whether the "same or substantially the same prior art or arguments" were previously presented to the Office. If so the burden shifts to the challenger to establish material error under (2);

(2) The challenger must establish that the examiner or other decision-maker made a material error in evaluating the prior art and/or arguments that were previously presented.

Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH, IPR2019-01469, Paper 6 (PTAB Feb. 13, 2020) (prec.), 8-10. The framework "reflects a commitment to defer to previous Office evaluations of the evidence of record unless material error is shown." *Id*., 9.

The objective of Section 325(d) for EPRs, as expressed by Congress, is to limit unfair serial challenges by providing "protection[] against abuse of *ex parte* reexamination" to "prevent parties from mounting attacks on patents that raise issues that are substantially the same as issues that were already before the Office" 157 Cong. Rec. S1376 (2011). This is the same objective as in the case of IPRs. Further, the need to provide protection to Patent Owners under Section

325(d) is greater because there is no estoppel protection for EPRs like there is for IPRs under Section 315(e)(1).

Accordingly, the framework for evaluating the application of discretion under Section 325(d) to deny an IPR is at least informative for evaluating the same inquiry for an EPR. This is particularly true given that, outside of a situation governed by the Federal Circuit's *Vivint* decision, there is no authoritative guidance governing the application of Section 325(d) in the context of EPRs in the regulations or in the MPEP.[2]

2. Other Discretionary Factors Should be Considered in Deciding Whether to Exercise Discretion to Deny an EPR.

Also informative are various factors that the Director considers when determining whether to exercise discretion to deny IPR petitions. *See Vivint*, 14 F.4th at 1353 (recognizing overlap between § 314(a) and§ 325(d) analysis). *General Plastic Indus. Co. v. Canon Kabushiki Kaisha*, IPR2016-01357, Paper 19, (PTAB Sept. 6, 2017) (prec.), 16-19 (factors to be evaluated under Section 314(a) and Section 325(d)). *See Ascentcare Dental Prods., Inc. v. Solmetex*, LLC, IPR2025-01020, Paper 11, 3 (PTAB Oct. 10, 2025) (denying IPR petition under both §§ 314(a) and 325(d)). Those factors include:

- Settled expectations of the parties, such as the length of time the patent has been in force;

[2] The MPEP indicates that if a request "includes issues involving" Section 325(d) "the examiner must bring such issues to the attention of the appropriate SPRS or the Director of the CRU." The MPEP does not provide guidance on what framework or standard should be applied in evaluating Section 325(d) for EPRs.

- Whether the challenger has used prior decisions as a roadmap to remedy prior, deficient challenges;
- The finite resources of the Office; and
- Any other considerations bearing on the Director's discretion.

Interim Processes for PTAB Workload Management, 2-3 (Mar. 26, 2025). These factors account for the "undue inequities and prejudices" to patent owners from the "the potential for abuse of the review process by repeated attacks on patents." *General Plastic*, IPR2016-01357, Paper 19, 17.

D. The Exercise Of Discretion Should Consider Whether Granting Reexamination Is An Efficient Use Of Office Resources.

In the IPR context, the Director has repeatedly issued decisions indicating that the exercise of discretion takes into account whether instituting the requested post-grant proceeding is an "appropriate use of Office resources." *See, e.g.*, *Dabico Airport Solutions, Inc. v. AXA Power Aps*, IPR2025-00408, Paper 21 (Director June 18, 2025) (informative). Indeed, in the case of Amazon's petition for IPR, that was one basis for the Director rejecting the petition because "[i]t is not an appropriate use of Office resources to review a patent in two separate, concurrent Office proceedings." See Ex. I, 2-3 (noting that the '780 Patent was already undergoing reexamination in 90/019,638).

The Director has a specific interest in managing the finite resources of the CRU for conducting *ex parte* reexaminations. The number of requests for EPRs filed each year has increased over 125% from 187 in 2018 to 425 in 2024. See https://www.uspto.gov/learning-and-resources/statistics/reexamination-information ("Reexamination Statistics"). The Office's Reexamination Statistics webpage indicates that 318 requests for EPR were filed in Q1-Q3 of 2025. Unified Patents reports that the number of requests for EPRs increased by 66% from 427

in 2024 to 726 in 2025. See Ex. AB (Unified Patents Dispute Report, 1/13/2026). Therefore, the CRU's workload has nearly doubled over the last several years, and it will continue to increase as the institution rate of IPRs drops.

Accordingly, the Director has a significant interest in managing the resources of the CRU. Because appeals in EPRs are conducted by the PTAB, granting requests for EPRs also implicates the limited resources of the PTAB. It has been widely reported that the number of APJs in the PTAB has fallen from about 230 in early 2025 to well under 200. See Ex. AC (IPLaw360, 10/27/2025).

Therefore, the Director should consider whether conducting an EPR proceeding is an appropriate use of Office resources when evaluating discretionary denial under Section 325(d).

IV. Argument

The Director has expressed significant concern that repeated challenges to patents can lead to strong patents being improperly invalidated, which can undermine the stability of the patent system. These concerns apply to repeated challenges to a patent from requests for EPRs and petitions for IPRs.

The Director should intervene and terminate this reexamination under § 325(d) given that "the same or substantially the same prior art or arguments" in the request were previously presented to the Office in Amazon's failed petition in IPR2025-00884. In this case, the EPR presented exactly the same prior art and argument that had previously been presented to the Office in Amazon's rejected IPR petition, as conceded by Requester Amazon and acknowledged by the CRU examiner. Request, 90/015,746, Dec. 2, 2025, 4 ("The IPR was based on the same references relied on in this request for reexamination, Nazario and Ghosh."); Reexam Order, 9, Jan. 30, 2026 ("A comparison between the current reexamination request and the prior Office post grant challenges indicates that current request presents the same prior art and arguments as

were presented in the IPR2025-00884."). After considering Amazon's petition and the parties' arguments on the merits, the Director denied Amazon's petition. See Ex. I. The reasons set forth by the CRU examiner for not denying Amazon's follow-on request for reexamination contradict the reasoning set forth by the Director in denying the petition for IPR, as discussed in Section IV.B below.

Alternatively, the Director should intervene and terminate this reexamination pursuant to *Vivint*, where the Federal Circuit ordered the reexamination be vacated because it was part of a pattern of "undesirable, incremental" challenges made against the patent. *Vivint*, 14 F.4th at 1346. In *Vivint*, the patent had been subjected to three prior challenges via IPR petitions. When a fourth challenge requesting an EPR was filed, the Federal Circuit ordered that the reexamination be vacated because it reflected the same unfair challenge that was the basis for denying the petition for IPR. *Id.* at 1346-47, 1353-54. In the instant case, the '780 Patent has been subjected to four prior IPR challenges and two requests for EPR including the one being challenged here. The circumstances here call for termination under *Vivint.*

Justice requires that the Director intervene and terminate this reexamination. Under Rule 183, the Director may intervene to decide a reexamination request or to terminate a granted reexamination "[i]n an extraordinary situation, when justice requires." Such is the case here. The reexamination should have been denied pursuant to Section 325(d) because precisely the same prior art and the same argument were already presented to and considered by the Office. Also, the reexamination should have been rejected based on *Vivint*, where the Federal Circuit ruled that the Office could not deny a petition for IPR as being an abuse of the process, only to grant a follow-on request that repackaged the IPR arguments into a request for EPR that was a further abuse of the process.

A. The Director's Concern About Unfair Serial Attacks On Patents Applies To EPRs As Well As IPRs.

Director Squires and Deputy Director Stewart have criticized serial attacks on patents as unfair and undesirable. The October 17, 2025, Notice of Proposed Rulemaking ("NPRM"), while referencing AIA proceedings, expresses the underlying concern about the problem of multiple challenges to same patent. See Ex. T (NPRM). The NPRM states:

> [P]atents cannot serve their economic function if they are perpetually subject to *de novo* review. Consider a hypothetical patent claim where 70% of experienced patent practitioners would conclude that the claim was properly granted, and 30% would oppose that conclusion. Such a patent claim seems reliable, because a substantial majority of practitioners believe it is patentable and was properly issued. However, if the patent is subjected to repeated *de novo* patentability review each time it is enforced, it will no longer be reliable. For example, a patent with a 70% chance of surviving one de novo patentability review has less than a 50% chance of withstanding two or more de novo patentability challenges. Thus, even extremely strong patents depend on a presumption of validity for their survival."

NPRM, 3-4.

In the NPRM, the Director states that "[s]erial and parallel validity challenges remain a significant problem for the patent system." *Id.*, 4. "[S]erial and parallel patent challenges, including **challenges raising the same or substantially similar prior art and/or arguments**, remain a significant problem." *Id.*, 5 (emph. added). That is the scenario here where Amazon seeks a reexamination on the very same prior art and argument presented in its failed IPR petition.

The concerns expressed by the Director in the NPRM about serial challenges are readily applicable to the '780 Patent, which has been subjected to four IPR petitions and now two requests for reexamination. This kind of serial attack is what the Director had in mind in stating:

> The Office is concerned that **even extremely strong patents become unreliable** when **subject to serial or parallel challenges**. … And repeated challenges do not benefit the patent system.

See Ex. U (USPTO Press Release, Oct. 16, 2025) (emph. added).

Deputy Director Stewart has stated that "to have a stable economy, we need a stable patent system [and] [r]epeated and expedited reconsideration of patent grants under the low preponderance of evidence standard is the antithesis of stability." Remarks, IPO Annual Mtg., (Sept. 8, 2025). She explained that "it's only a matter of simple math that if you challenge the same claim over and over again, you will increase the odds that it will be determined to be unpatentable…" *Id.* The Deputy Director explained that "on-demand, limitless reviews of IP rights are not good for the system and not fair." Remarks at the Intellectual Property Business Congress (IPBC) Global 2025 (June 10, 2025).

Accordingly, the statements from the Director indicate that discretionary decisions on post-grant proceedings, which would include evaluating requests for EPRs under Section 325(d), should disfavor a new proceeding when the patent has already been subjected to "undesirable, incremental" serial challenge. *See Vivint*, 14 F.4th at 1346.

B. The Reexamination Should Be Terminated Under § 325(d).

1. Amazon's Petition in IPR2025-00884 Presented Nazario and Gosh.

Under § 325(d), the Director may deny a request for reexamination if "the same or substantially the same prior art or arguments previously were presented to the Office." As outlined in Section II.A above, the '780 Patent has been targeted with six challenges to its validity—four petitions for IPR and two requests for EPR including the one at issue here.

In the fifth challenge, which was the petition in IPR2025-00884, Amazon asserted that Claims 1, 3, 7, 10, 11, 13, and 17 of the '780 Patent are unpatentable based on one ground:

Nazario combined with Ghosh. Ex. C (Petition, 4/17/2025), 13. See Ex. D (Nazario), Ex. E (Ghosh). See Section II.A.5 above.

Nazario discloses a system with a computer running multiple virtual machines on a network with other computers. Nazario allegedly discloses computer systems having multiple defenses against attacks, including a network-based firewall and a host-based firewall that acts as a "failover" if an attack penetrates the network-based firewall. Ex. C, 16-17. It is alleged that a computer may run a virtual machine called a "virtual host" that can contain damage and prevent an attack from spreading to the rest of the computer. *Id.*, 16-17, 21.

However, Nazario does not disclose a computer system having a "*host system*" and a "*virtual system*," as claimed in independent Claims 1 and 11, where there is an "*internal firewall*" that separates the "*host system*" from the "*virtual system*," and where the internal firewall is a protective firewall in addition to two other firewalls, namely, the "*host-based firewall*" and the "*network firewall*."

Croga filed a request for discretionary denial ("RDD") that explained, among other things, the weak merits of Amazon's ground based on Nazario and Ghosh. See Ex. F (RDD, 7/21/2025). Patent Owner Croga explained that the petition relied on "virtual machines" for the "*internal firewall*" limitation, an argument that had already been rejected twice for the petitions filed by Cisco and Fortinet that were denied on the merits in IPR2024-01196 and IPR2025-00086. *Id.*, 10. See Section II.A.1-2 above.

Patent Owner also pointed out that the '780 Patent had already been targeted by three earlier petitions for IPR and one ongoing EPR, and thus the patent was being subjected to unfair serial attacks. Instituting a fourth petition for IPR would not be an efficient use of the resources of the Office, particularly under these circumstances where there already was an ongoing

reexamination. *Dabico Airport Solutions, Inc. v. AXA Power ApS*, IPR2025-00408, Paper 21 (Director June 18, 2025) (informative) (denying review as not "an appropriate use of Office resources").

Croga also filed a POPR that explained that Nazario/Ghosh failed to teach or suggest the "*an internal firewall . . . configured to separate the host system from the virtual system in the computer system*." Croga pointed out that Amazon never identified where Nazario or Ghosh or their combination has an "*internal firewall"* as claimed that separates the host system from the virtual system. Ex. H (POPR, IPR2025-00884, 8/20/2025), 8-9.

The Director denied institution in IPR2025-00084. See Ex. I (Denial of Institution, 9/3/2025). The Director found that the various *Fintiv* factors were neutral: they "neither favor nor counsel against discretionary denial." *Id.*, 2. Instead, the Director rejected the IPR petition because it was the fourth IPR challenge in an unfair serial attack on the '780 Patent. The Director also pointed out that there already was an ongoing EPR proceeding, and thus instituting an IPR would result in overlapping proceedings that would be inefficient for the Office, as further discussed below. See Ex. I, 2-3.

2. Amazon's Request for EPR Was a Copycat Challenge That Again Presented Nazario and Gosh and the Same Argument.

Three months after the Director rejected Amazon's petition for IPR, Amazon added to the serial attack by bringing forth a six challenge to the '780 Patent in the form of a request for EPR that presents the very same prior art and the very same argument from Amazon's rejected IPR petition. Amazon conceded that it was presenting the very same prior art (Nazario/Ghosh) and very same argument in the request for EPR as contained in its rejected IPR petition. See Request, 90/015,746, December 2, 2025, 4 ("The IPR was based on the same references relied on in this request for reexamination, Nazario and Ghosh."); Reexam Order, 9 ("A comparison between the

current reexamination request and the prior Office post grant challenges indicates that current request presents the **same prior art and arguments** as were presented in the IPR2025-00884.") (emph. added).

The request for reexamination simply copied the arguments from the denied IPR petition and resubmitted them in a request for EPR. For example, in the request for reexamination the argument for limitation [1c] for the claimed "*internal firewall*" is a virtual cut-and-paste from the petition for IPR in IPR2025-00884. *Compare* Request, 52-56, *with* Ex. C (Petition), 27-32. The argument in the request for limitation [1d] for the claimed "*host-based firewall*" is a cut-and-paste from the denied IPR petition. *Compare* Request, 60-62, *with* Ex. C (Petition), 32-34.

On January 30, 2026, the Office granted the request for EPR in 90/015,746. Reexam Order, 6.

3. Amazon's Request for EPR Should Be Terminated Pursuant To Section 325(d).

It defies logic and basic notions of fairness that a party who files a petition for IPR that is denied can simply turn around and reformat that paper into a request for reexamination that is granted by the Office.

The Reexamination Order issued by the CRU examiner addressed Section 325(d) as to whether to "reject the … request because, the same or substantially the same prior art or arguments previously were presented to the Office."[3] Reexam Order, 6. The CRU examiner

[3] Based on Patent Owner's research, the Office of Patent Legal Administration (OPLA) has granted petitions to deny/terminate reexamination under Section 325(d) only three times. OPLA has denied requests to deny/terminate reexamination under Section 325(d) over one-hundred and

recognized that four petitions for IPR had already been filed against the patent, as well as one request for EPR that resulted in an ongoing proceeding that was on appeal. Reexam Order, 6 (recognizing ongoing 90/019,638).

The CRU examiner concluded that the statutory threshold for Section 325(d) is met because: "A comparison between the current reexamination request and the prior Office post grant challenges indicates that current request **presents the same prior art and arguments** as were presented in the IPR2025-00884." Reexam Order, 9 (emph. added). However, the CRU examiner declined to exercise discretion to deny the request for several reasons.

First, the CRU examiner asserted that the petition in IPR2025-00884 by Amazon[4] was discretionarily denied because of the "current litigation and the expected trial date." Reexam Order, 8. That is not correct. In the order denying institution of Amazon's IPR petition (see Ex. I), the Director stated that those factors were neutral and that the denial was based on the petition being a serial, fourth petition for IPR lodged on top of the ongoing EPR, as explained further below.

Second, the CRU Examiner stated that the "Director did not address … the merits of the IPR2025-00884 petition" and thus "[t]he prior IPR petition (IPR2025-00884) in which the same prior art grounds were presented was discretionarily denied without [] substantive consideration

---

fifty times. As for the CRU, Patent Owner has not been able to locate any decision by a CRU examiner denying a request for reexamination on the basis of Section 325(d).

[4] The Order has a typo indicating that IPR2025-00884 was filed by "Cisco Systems, Inc." Reexam Order, 8. The petition in -00884 was filed by Amazon, the same party requesting the instant reexamination in 90/015,746. See Section II.A.5 above.

of the prior art and arguments presented in that petition." Reexam Order, 8-9. This is not correct. The Director's decision denying institution of Amazon's IPR petition considered the arguments and evidence presented by the parties, which included the evidence and argument on the merits:

> After considering the parties' arguments and the record, and in view of all relevant considerations, discretionary denial of institution is appropriate in this proceeding. This determination is based on the totality of the evidence and arguments the parties have presented. … Although certain arguments are highlighted above, the determination to exercise discretion to deny institution is based on a holistic assessment of all of the evidence and arguments presented.

Ex. I (Order denying institution), 2-3. Thus, contrary to the CRU examiner's assertion, the Director did consider the merits arguments on the Nazario/Ghosh prior art that had been presented by Croga (see Ex. F, RDD, 9-12) and the merits arguments on that prior art presented by Amazon (see Ex. G, Response to RDD, 11-13). In short, contrary to the CRU examiner's assertion, the Director did substantively consider the merits of the ground.

Next, the CRU examiner justified refusing to exercise discretion under Section 325(d) to deny the reexamination request because "[t]here is no evidence that the Requester of the current reexam has engaged in abusive post grant challenges to the '780 patent." Reexam Order, 9. Patent Owner respectfully disagrees. The Director denied the IPR petition because the '780 Patent had been subjected—at that time—to four petitions for IPR on top of an ongoing EPR proceeding. Ex. I (Decision denying institution, IPR2025-00884), 2-3 (exercising discretion to deny because "this [petition for IPR] is the fourth petition for *inter partes* review involving the challenged patent," "[f]urthermore, an *ex parte* reexamination has been ordered on the challenged patent," and "[i]t is not an appropriate use of Office resources to review a patent in two separate, concurrent Office proceedings, especially when the reexamination is in an advanced stage.").

The CRU examiner's Section 325(d) analysis did not acknowledge those reasons the Director cited in denying the IPR2025-00884 petition, let alone apply those considerations to the request for EPR filed by Amazon on the heels of its denied IPR petition. Applying those considerations should have resulted in the denial of the request for EPR that Amazon copied from its denied IPR petition. The filing of the request for EPR constituted the sixth challenge to the '780 Patent. If five challenges to the '780 Patent was reason to exercise discretion under Section 325(d) to deny institution of the IPR, then the filing of a sixth challenge provides even more reason to exercise discretion to reject a subsequent copycat request for EPR. See Ex. I, 2 ("this [petition for IPR] is the fourth petition for *inter partes* review involving the challenged patent").

Additionally, the Director exercised discretion not to institute the IPR petition because a first EPR was already ongoing: "It is not an appropriate use of Office resources to review a patent in two separate, concurrent Office proceedings, especially when the reexamination is in an advanced stage." Ex. I, 2-3. Here, the CRU examiner's grant of a second request for EPR filed by Amazon results in just what the Director said should not occur: "two separate, concurrent Office proceedings, especially when the reexamination is in an advanced stage" that constitute an inappropriate use of Office resources. *Id.* If discretion under Section 325(d) called for non-instituting Amazon's petition for IPR to avoid overlapping proceedings, then discretion under Section 325(d) requires denying the second request for reexam for the very same reason.

Additionally, application of the rule under *Advanced Bionics* requires that discretion be exercised to terminate this EPR. It is undisputed that the same prior art and argument were presented in the request for EPR in 90/015,746 as presented in Amazon's petition for IPR2025-00884. Accordingly, the burden shifts to Amazon to establish that the Office committed material

error. *Advanced Bionics*, IPR2019-01469, Paper 6 at 8-10. But Amazon's request for EPR does not assert, let alone establish, material error.

In sum, the EPR process should not allow a party who files a petition for IPR that is denied to then turn around and copy that paper into a request for reexamination that is granted by the Office. That would violate basic notions of fairness to the Patent Owner. It would also be an abuse of process that will become standard practice for IPR petitioners if it is permitted here.

Patent Owner Croga reiterates its request that the Director terminate and this reexamination proceeding pursuant to Section 325(d).

4. Other Factors Weigh in Favor of Terminating this EPR Proceeding.

The Office's decision as to whether to grant a request for EPR that presents prior art or arguments that were previously presented is a matter of discretion. As discussed in Section III.C.2, this discretionary decision should consider relevant considerations.

First, the '780 Patent issued on March 24, 2020. The patent has been in force nearly six years and thus is entitled to a presumption of settled expectations that weighs in favor of discretionary denial of the request for EPR. *See, e.g., Kahoot! AS v. Interstellar, Inc.*, IPR2025-00696, Paper 12 (Director July 31, 2025).

Second, the Director considers whether the challenger used prior decisions as a roadmap to remedy prior, deficient challenges. *Vivint*, 14 F.4th at 1353 (observing that the requester "'used prior Board decisions as a roadmap to correct past deficiencies'" in its earlier-filed IPR petition). In the present case, the Director found that Amazon's petition presented issues of improper roadmaping. Ex. I, 2 ("Petitioner's admission raises concerns of roadmaping and weighs in favor of discretionary denial.").

Third, considerations about the appropriate use of the Office's resources weighs in favor of terminating this reexamination. As discussed in Section II.D above, implementing a second

reexamination on top of an existing reexamination is not an efficient use of the resources of the Office.

C. Amazon's Request for EPR Should Be Terminated Pursuant to *Vivint*.

As best Patent Owner can discern, OPLA has never terminated a reexamination based on *Vivint* since that decision issued in 2021. However, the facts of this case are even more egregious. If any case warrants termination based on *Vivint*, it is this one.

In *Vivint*, the Federal Circuit held that it was arbitrary and capricious for the Office to grant a request for reexamination after it had declined to institute an earlier-filed IPR petition applying substantially the same prior art where the petition was part of an "undesirable, incremental" attack on the patent. *Vivint*, 14 F.4th at 1353-54. The Court reasoned:

> The government argues that, because IPR and *ex parte* reexamination involve different procedures and policies, the Patent Office is free to grant an "undesirable, incremental" *ex parte* reexamination request even after it denies a nearly identical IPR petition that was deemed "a case of undesirable, incremental petitioning." We do not agree. … Section 325(d) applies to both IPR petitions and requests for *ex parte* reexamination. Thus, the Patent Office, when applying § 325(d), cannot deny institution of IPR based on abusive filing practices then grant a nearly identical reexamination request that is even more abusive. We see no difference between the IPR and *ex parte* reexamination processes that would justify such conduct and nothing short of termination of the reexamination would be appropriate.

Id.

In *Vivint*, the challenger had filed three petitions for IPR followed by a fourth challenge that was a request for reexamination. In this case, the facts are more egregious because the '780 Patent has been subjected to six challenges—four petitions for IPR and two requests for EPR including the present one. Further, Amazon's request for reexamination submitted the exact same prior art and argument as its denied IPR petition, making it worse than *Vivint* where the requester

at least included two new grounds.[5] Under these circumstances, the reexamination should be terminated because Amazon's "*ex parte* reexamination request was a more egregious abuse than [] [Amazon's denied IPR] petition under the same considerations already analyzed" by the Office which found that it was "the [fourth] filing in a string of 'undesirable, incremental petitioning' practices." *Id.* at 1353. Thus, Amazon's "*ex parte* reexamination request was another iteration" of the "abuse of process" and it was legal error for the Office to come to a different result under Section 325(d) for the reexamination request than it did for the IPR petition. *Id.*

Accordingly, Patent Owner Croga respectfully requests that 90/015,746 reexamination be terminated pursuant to *Vivint.*

[5] In *Vivint*, the Federal Circuit noted that the Office declined to institute the earlier-filed IPR because the challenger had engaged in inappropriate roadmaping. *Id.* In this case, the Director declined to institute Amazon's IPR2025-00884 in part because of concerns about roadmaping. See Ex. I, 2 ("Petitioner's admission raises concerns of roadmaping").

V. Conclusion

Patent Owner respectfully requests that the Director terminate this reexamination for the aforementioned reasons.

The Commissioner is hereby authorized to charge to Deposit Account No. 60-0202 (131-10686) any additional fees under 37 C.F.R. §§ 1.16 and 1.17 that may be required by this paper and to credit any overpayment to that Account. If any extension of time is required in connection with the filing of this paper and has not been separately requested, such extension is hereby requested.

A certificate of service on the Third Party Requester is being filed with this response.

Respectfully submitted,

Date: February 6, 2025

By: /Stephen T. Schreiner/

Stephen T. Schreiner
Reg. No. 43,097
Attorney for Patent Owner
CARMICHAEL IP, PLLC
8607 Westwood Center Drive,
Suite 270
Tysons Corner, VA 22182
Telephone: (703) 646-9255
schreiner@carmichaelip.com

EXHIBIT A

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

CROGA INNOVATIONS LTD., Plaintiff, v. AMAZON WEB SERVICES, INC., Defendant.	Case No. 1:24-cv-398 **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT AGAINST AMAZON WEB SERVICES, INC.

This is an action for patent infringement arising under the Patent Laws of the United States of America, 35 U.S.C. § 1 *et seq.*, in which Plaintiff Croga Innovations Limited ("Plaintiff" or "Croga") makes the following allegations against Defendant Amazon Web Services, Inc. ("Defendant" or "AWS"):

INTRODUCTION

1. This complaint arises from AWS' unlawful infringement of the following United States patent owned by Plaintiff, which relates to improvements in computer networking systems: United States Patent No. 10,601,780 ("the '780 Patent" or the "Asserted Patent").

PARTIES

2. Plaintiff Croga Innovations Limited is a private company limited by shares organized and existing under the laws of Ireland, with its principal place of business at The Hyde Building, Suite 23, The Park, Carrickmines, Dublin 18, Ireland. Croga is the sole owner by assignment of all rights, title, and interest in the Asserted Patent, including the right to recover damages for past, present, and future infringement.

3. On information and belief, Defendant Amazon Web Services, Inc. is a Delaware corporation with its principal place of business at 410 Terry Avenue North, Seattle, WA 98109-5210, U.S.A. AWS is registered to do business in the State of Texas and may be served through its registered agent Corporation Service Company dba CSC – Lawyers Incorporating Service Company, 211 E. 7th Street, Suite 620, Austin, Texas 78701.

JURISDICTION AND VENUE

4. This action arises under the patent laws of the United States, Title 35 of the United States Code. This Court has original subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

5. This Court has personal jurisdiction over AWS in this action because AWS has committed acts within this District giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over AWS would not offend traditional notions of fair play and substantial justice. AWS maintains several places of business within the State, including at 11501 Alterra Pkwy, Austin, Texas 78758. AWS, directly and through subsidiaries or intermediaries, has committed and continues to commit acts of infringement in this District by, among other things, importing, offering to sell, and selling products that infringe the Asserted Patent. AWS is registered to do business in the State of Texas, and has appointed as their registered agent, Corporation Service Company d/b/a CSC – Lawyers Incorporating Service Company, 211 E. 7th Street, Suite 620, Austin, Texas 78701, for service of process.

6. Venue is proper in this District under 28 U.S.C. §§ 1391 and 1400(b). AWS is registered to do business in Texas, and upon information and belief, AWS has transacted business in this District and has committed acts of direct and indirect infringement in this District by, among other things, making, using, offering to sell, selling, and importing products that infringe the

Asserted Patent. AWS has regular and established places of business in this District, including at 11501 Alterra Pkwy, Austin, Texas 78758.

COUNT I

INFRINGEMENT OF U.S. PATENT NO. 10,601,780

7. Plaintiff realleges and incorporates by reference the foregoing paragraphs as if fully set forth herein.

8. Plaintiff owns by assignment all rights, title, and interest, including the right to recover damages for past, present, and future infringement, in U.S. Patent No. 10,601,780, titled "Internet isolation for avoiding internet security threats." The '780 Patent was duly and legally issued by the United States Patent and Trademark Office on March 24, 2020. A true and correct copy of the '780 Patent is attached as Exhibit 1.

9. On information and belief, Defendant has and continues to make, use, offer for sale, sell, and/or import certain products and services, including without limitation AWS VPC, AWS EC2, and AWS Network Firewall ("Accused Products"), that directly infringe, literally and/or under the doctrine of equivalents, one or more claims of the '780 Patent. Identification of the Accused Products will be provided in Plaintiff's infringement contentions disclosed pursuant to the Court's scheduling order.

10. The Accused Products satisfy all claim limitations of one or more claims of the '780 Patent. A claim chart comparing exemplary independent claim 11 of the '780 Patent to representative Accused Products is attached as Exhibit 2.

11. By making, using, offering for sale, selling and/or importing into the United States the Accused Products, AWS has injured Plaintiff and are liable for infringement of the '780 Patent pursuant to 35 U.S.C. § 271.

12. AWS also knowingly and intentionally induces infringement of one or more claims of the '780 Patent in violation of 35 U.S.C. § 271(b). At least as of the filing and service of this complaint, AWS has knowledge of the '780 Patent and the infringing nature of the Accused Products through, for example, the '780 Patent claim chart served therewith. Despite this knowledge of the '780 Patent, AWS continues to actively encourage and instruct its customers and end users (for example, through user manuals and online instruction materials on its website and materials cited in Exhibit 2) to use the Accused Products in ways that directly infringe the '780 Patent. For example, AWS advertises the benefits of its network firewall functionality. *See* Ex. 3 (https://docs.aws.amazon.com/network-firewall/latest/developerguide/how-it-works.html); Ex. 4 (https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html). Further, AWS provides its users with instructions explaining how to configure the Accused Products in an infringing manner. *Id*. AWS provides these instructions, user manuals, and other materials knowing and intending (or with willful blindness to the fact) that its customers and end users will commit these infringing acts. AWS also continues to make, use, offer for sale, sell, and/or import the Accused Products, despite its knowledge of the '780 Patent, thereby specifically intending for and inducing its customers to infringe the '780 Patent through the customers' normal and customary use of the Accused Products.

13. AWS has also infringed, and continues to infringe, one or more claims of the '780 Patent by selling, offering for sale, or importing into the United States, the Accused Products, knowing that the Accused Products constitute a material part of the inventions claimed in the '780 Patent, are especially made or adapted to infringe the '780 Patent, and are not staple articles or commodities of commerce suitable for non-infringing use. At least as of the filing and service of this complaint, AWS has knowledge of the '780 Patent and the infringing nature of the Accused

Products through, for example, the ’780 Patent claim chart served therewith. AWS has been, and currently is, contributorily infringing the ’780 Patent in violation of 35 U.S.C. §§ 271(c) and/or (f). For example, accused functionality supplied by AWS constitutes a material part of the inventions claimed in the ’780 Patent, are especially made or adapted to infringe the ’780 Patent, and are not staple articles or commodities of commerce suitable for non-infringing use, as demonstrated by the evidence in Exhibit 2.

14. On information and belief, Plaintiff (including its predecessors and any licensees) complied with 35 U.S.C. § 287 because Plaintiff, any predecessor assignees to the ’780 Patent, and any licensees did not make, offer for sale, or sell products that practice(d) the ’780 Patent during the relevant time period or were not otherwise required to mark during the relevant time period.

15. As a result of AWS’ direct infringement of the ’780 Patent, Plaintiff is entitled to monetary damages (past, present, and future) in an amount adequate to compensate for AWS’ infringement, but in no event less than a reasonable royalty for the use made of the invention by AWS, together with interest and costs as fixed by the Court.

16. As a result of AWS’ indirect infringement of the ’780 Patent, Plaintiff is entitled to monetary damages (present and future) in an amount adequate to compensate for AWS’ infringement, but in no event less than a reasonable royalty for the use made of the invention by AWS, together with interest and costs as fixed by the Court, accruing as of the time AWS obtained knowledge of the ’780 Patent.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that this Court enter:

a. A judgment in favor of Plaintiff that AWS has infringed, either literally and/or

under the doctrine of equivalents, the ’780 Patent;

b. A judgment and order requiring AWS to pay Plaintiff its damages (past, present, and future), costs, expenses, and pre-judgment and post-judgment interest for AWS’ infringement of the ’780 Patent;

c. A judgment and order requiring AWS to pay Plaintiff compulsory ongoing licensing fees, as determined by the Court in equity.

d. A judgment and order requiring AWS to provide an accounting and to pay supplemental damages to Plaintiff, including without limitation, pre-judgment and post-judgment interest and compensation for infringing products released after the filing of this case that are not colorably different from the accused products;

e. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiff its reasonable attorneys’ fees against AWS; and

f. Any and all other relief as the Court may deem appropriate and just under the circumstances.

DEMAND FOR JURY TRIAL

Plaintiff, under Rule 38 of the Federal Rules of Civil Procedure, requests a trial by jury of any issues so triable by right.

Dated: April 16, 2024

Respectfully submitted,

By: */s/ Brett E. Cooper*

Brett E. Cooper (NY SBN 4011011)
bcooper@bclgpc.com
Seth Hasenour (TX SBN 24059910)
shasenour@bclgpc.com
Jonathan Yim (TX SBN 24066317)
jyim@bclgpc.com
Drew B. Hollander (NY SBN 5378096)
dhollander@bclgpc.com

BC LAW GROUP, P.C.
200 Madison Avenue, 24th Floor
New York, NY 10016
Phone: 212-951-0100

Attorneys for Plaintiff Croga Innovations Limited

EXHIBIT B

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent of Hoy *et al.*		§	Attorney Docket No.: UP-EPR-10601780
		§	
U.S. Patent:	10,601,780	§	
		§	
Issue Date:	March 24, 2020	§	Customer No.: 25962
		§	
Filing Date:	March 2, 2018	§	
		§	
For:	Internet Isolation for Avoiding Internet Security Threats	§	

REQUEST FOR *EX PARTE* REEXAMINATION OF U.S. PATENT 10,601,780

Mail Stop "*Ex Parte* Reexam"
Attn: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

Pursuant to the provisions of 35 U.S.C. §§ 301-307, Unified Patents, LLC ("Requester") hereby requests an *ex parte* reexamination of claims 1-20 (the "Challenged Claims") of U.S. Patent 10,601,780 (the "'780 Patent," Ex. 1001), which issued on March 24, 2020, to Robert B. Hoy *et al.* from U.S. Patent Application 15/910,734 (the "'734 Application," Ex. 1002), filed on March 2, 2018, which claims priority to U.S. Patent Application 13/981,896 (the "'896 Application," Ex. 1003), filed as application no. PCT/US2012/013027, on January 27, 2012, and issued as U.S. Patent No. 9,942,198, and which claims priority to U.S. Provisional Application 61/436,932 (the "'932 Provisional," Ex. 1004), filed on January 27, 2011. The '780 Patent is currently assigned to Croga Innovations Limited ("Croga" or "Patent Owner"). The assignment is recorded in the U.S. Patent and Trademark Office ("USPTO") at reel/frame 065999/0444.

Requester submits that this Request presents prior art references and analyses that are noncumulative of the prior art that was before the Examiner during the original prosecution of the '780 Patent and that the Challenged Claims are invalid over these references. Requester therefore requests that an order for reexamination and an Office Action rejecting claims 1-20 be issued.

Ex Parte Patent Reexamination Filing Requirements

Pursuant to 37 C.F.R. § 1.510(b)(1), statements pointing out at least one substantial new question of patentability based on material, non-cumulative reference patents and printed publications for the Challenged Claims of the '780 Patent are provided in Section I of this Request.

Pursuant to 37 C.F.R. § 1.510(b)(2), reexamination of the Challenged Claims of the '780 Patent is requested, and a detailed explanation of the pertinence and manner of applying the cited references to the Challenged Claims is provided in Section II of this Request.

Pursuant to 37 C.F.R. § 1.510(b)(3), copies of every patent or printed publication relied upon or referred to in the statements pointing out each substantial new question of patentability or in the detailed explanation of the pertinence and manner of applying the cited references are provided as Exhibits 1001-1004 and 1006-1012 of this Request.

Pursuant to 37 C.F.R. §1.510(b)(4), a copy of the '780 Patent is provided as Exhibit 1001 of this Request, along with a copy of any disclaimer, certificate of correction, and reexamination certificate issued corresponding to the patent.

Pursuant to 37 C.F.R. § 1.510(b)(5), the attached Certificate of Service indicates that a copy of this Request, in its entirety, has been served on Patent Owner at the following addresses of record for Patent Owner, in accordance with 37 C.F.R. § 1.33(c):

199393 - Atlantic IP
c/o Lombard Geliebter LLP
1325 Avenue of the Americas
28th Floor
New York, NY 10019
UNITED STATES

Furthermore, the undersigned has also served a courtesy copy of the Request via email on the current assignee of record:

Croga Innovations Limited
The Hyde Building, Suite 23
The Park, Carrickmines
Dublin, Ireland 18

Additionally, the undersigned has also served courtesy copies of the Request via email on lead counsel for Croga Innovations Limited in the co-pending litigations:

BC Law Group, P.C.
Brett E. Cooper
Drew B. Hollander

Jonathan R. Yim
Seth R. Hasenour
bcooper@bc-lawgroup.com
shasenour@bc-lawgroup.com
jyim@bc-lawgroup.com
dhollander@bc-lawgroup.com

200 Madison Avenue, 24th Floor
New York, NY 10016
Telephone: (212) 951-0100

Also submitted herewith is the fee set forth in 37 C.F.R. § 1.20(c)(2).

Pursuant to 37 C.F.R. § 1.510(b)(6), Requester hereby certifies that the statutory estoppel provisions of 35 U.S.C. § 315(e)(1) and 35 U.S.C. § 325(e)(1) do not prohibit Requester from filing this *ex parte* patent reexamination request.

TABLE OF CONTENTS

TABLE OF EXHIBITS

Exhibit	Description
Ex. 1001	U.S. Patent 10,601,780
Ex. 1002	File History for U.S. Patent Application 15/910,734
Ex. 1003	File History for U.S. Patent Application 13/981,896
Ex. 1004	File History for U.S. Provisional Patent Application 61/436,932
Ex. 1005	*Reserved*
Ex. 1006	U.S. Publication 2009/0241194 ("Thomas")
Ex. 1007	U.S. Publication 2006/0206300 ("Garg")
Ex. 1008	Expert Declaration of Dr. Seth James Nielson in Support of the Request for *Ex Parte* Reexamination of U.S. Patent 10,601,780
Ex. 1009	U.S. Patent 8,250,641 ("Morgan")
Ex. 1010	Tal Garfinkel et al., A Virtual Machine Introspection Based Architecture for Intrusion Detection, Ndss. Vol. 3. No. 2003, 2003 ("Garfinkel")
Ex. 1011	U.S. Patent 8,966,312 ("Gupta")
Ex. 1012	U.S. Patent 8,151,337 ("Crowell")

I. SUBSTANTIAL NEW QUESTIONS OF PATENTABILITY

Prior to describing the substantial new questions of patentability presented in this Request, provided below is an overview of the '780 Patent, a discussion of claim construction, and an overview of the prior art being discussed in this Request. Support for the overview of the '780 Patent can also be found in Dr. Nielson's declaration. *See, e.g.*, Ex. 1008, ¶¶ 67-72. Dr. Nielson's background and qualifications are outlined in paragraphs 1-28 of Exhibit 1008.

A. U.S. Patent 10,601,780

1. Overview

The '780 Patent is directed to "the protection of computer systems from injurious software that can be encountered while browsing or accessing the Internet, and also to the protection of local [area] networks (LANS) that have access to the [Internet]." Ex. 1001, 1:17-21. "FIG. 1 is a diagram of an exemplary system on a local area network using the Internet isolation system of the present invention." Ex. 1001, 6:65-67. FIG. 1 is reproduced below for convenience.

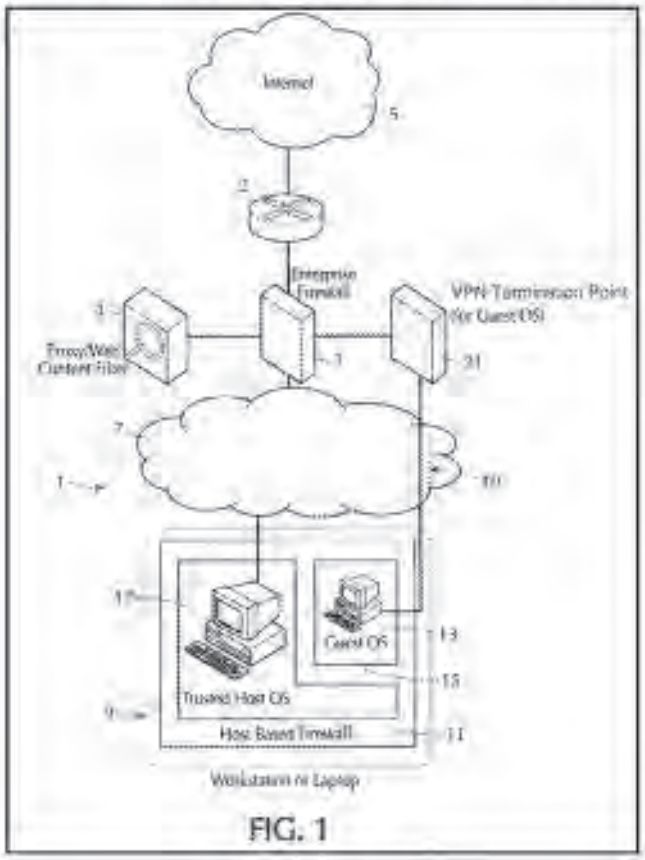


FIG. 1

'780 Patent, FIG. 1

FIG. 1 illustrates a networked computer system 1 that is linked to the Internet 5 via a firewall 3 and a router 2 of conventional configuration that is well-known in the art and a proxy/web-content filter 4 that is connected with and cooperates with the firewall hardware 3. *See* Ex. 1001, 7:7-11. "The local system 1 includes a trusted local area network (LAN) 7 that transmits electrical data signals between a plurality or large number (not shown) of computer systems each identified by a unique LAN address." Ex. 1001, 7:17-20. One such computer system 9 is illustrated in FIG. 1. Ex. 1001, 7:20-24.

The computer system 9 includes "a host-based firewall 11 that provides restrictive egress from the computer [system] 9." Ex. 1001, 7:42-45. The host-based firewall 11 is intended to provide a barrier to access of the Internet 5 from the computer system 9. *See* Ex. 1001, 7:60-62. Communications between the host OS 17 and the Internet 5 are selectively enabled by the host-based firewall 11 "provided that the websites being accessed are on a whitelist of predetermined trusted sites with which the host OS 17 is permitted to communicate with." Ex. 1001, 10:26-32.

The computer system 9 also "stores data defining software that when executed creates a hypervisor on the computer system 9," and "the hypervisor effectively creates a virtual machine [virtual guest OS 13] operating on the host computer that has a virtual configuration different from the real hardware and software configuration of the computer [system] 9." Ex. 1001, 7:63-8:12. The hypervisor also provides an additional internal host-supported firewall 15 that separates and restricts interaction between the virtual guest OS 13 and the trusted host OS 17 running the computer system 9. *See* Ex. 1001, 8:13-20. "Communications between the trusted host OS 17 and the guest OS 13 pass through the hypervisor firewall 15." Ex. 1001, 8:20-22.

The '780 Patent also provides for situations in which the computer system 9 is disconnected from the LAN 7 and connected with a different network. Ex. 1001, 10:38-42. In this case, the "host based firewall 11 (HBFW) remains on the computer system 9, but performs multiple predetermined functions based on whether the computer 9 is 'home' (attached to the LAN) or 'roaming' (disconnected from the LAN and connected via a non-secure network to the Internet)." Ex. 1001, 10:42-47. More specifically, "when the host is 'home' on the trusted LAN network," the virtual guest OS 13 is allowed only to egress the network through a specified IP address, and the trusted host OS 17 is only allowed to communicate to other LAN resources or whitelisted sites as previously discussed. *See* Ex. 1001, 10:48-64. On the other hand, when the host is roaming, or off the trusted network, the virtual guest OS 13 is allowed "to freely communicate on whatever

network it is connected to." *See* Ex. 1001, 10:65-11:4. On the contrary, the trusted host OS 17, "when roaming on a nonsecure network, has all egress blocked by the HBFW" 11. Ex. 1001, 11:5-6.

In summary, with reference to FIG. 1, the '780 Patent teaches a networked computer system (1) that includes a network (7), at least one computer system (9) configured to connect to the network (7), the computer system (9) comprising a host system (17) and a virtual system (13), wherein the virtual system (13) is a separate operating system or a software module operating on the computer system (9), wherein an internal firewall (15) is configured to separate the host system (17) from the virtual system (13) in the computer system (9), and a host-based firewall (11) executed on the computer system (9) is configured to implement network isolation between the computer system (9) and the network (7), and at least one device (3, 4) configured to implement at least one of a network firewall or a web proxy, wherein the device (3, 4) comprises a processor and a memory configured to implement network isolation between one or more untrusted network destinations (5) and the networked computer system (1).

2. Claim Index

Copies of the '780 Patent, its file history, and the file histories of its priority applications are provided as Exhibits 1001-1004, respectively. For the sake of reference, the claims for which reexamination is requested are reproduced below. Claims 1 and 11 are the independent claims, while the remaining challenged claims depend directly or indirectly from these claims.

1. A networked computer system comprising:

a network;

at least one computer system configured to connect to the network, the computer system comprising a host system and a virtual system, wherein the virtual system is a separate operating system or a software module operating on the computer system, wherein an internal firewall is configured to separate the host system from the virtual system in the computer system, and a host-based firewall executed on the computer system is configured to implement network isolation between the computer system and the network; and

at least one device configured to implement at least one of a network firewall or a web proxy, wherein the device comprises a processor and a memory configured to implement network isolation between one or more untrusted network destinations and the networked computer system.

2. The networked computer system of claim 1, wherein the internal firewall is configured to prevent data from being communicated between the virtual system and the host system without an explicit user input.

3. The networked computer system of claim 1, wherein the host system is configured to store data in a host memory space and the virtual system is configured to store data in a virtual memory space that is segregated from the host memory space.

4. The networked computer system of claim 1, wherein malware introduced to the computer system is prevented from moving to another computer system of the networked computer system.

5. The networked computer system of claim 1, wherein the computer system is configured to:

communicate with the one or more untrusted network destinations via a first communication connection,

communicate with one or more trusted network destinations via a second communication connection; and

enforce separation of the first communication connection from the second communication connection.

6. The networked computer system of claim 1, wherein the host-based firewall is configured to prevent lateral communication and movement of malware between the computer system and other devices on the networked computer system.

7. The networked computer system of claim 1, wherein the device is configured to prevent unauthorized communication between the computer system and the one or more untrusted network destinations.

8. The networked computer system of claim 1, wherein the host-based firewall is configured to implement a first policy when the computer system is connected to the network and a second policy when the computer system is connected to another network, wherein the first policy permits one or more communications between the host system of the computer system and one or more resources on the network and the second policy blocks communications egressing from the host system of the computer system but allows communications egressing from the virtual system.

9. The networked computer system of claim 1, wherein one or more applications or processes are configured to run in the virtual system, and wherein the one or more applications or processes running in the virtual system are configured to communicate with the one or more untrusted network destinations.

10. The networked computer system of claim 1, wherein one or more applications or processes are configured to run in the host system, and wherein the one or more applications or processes running in the host system are configured to communicate with one or more devices on the network.

11. A method of network isolation in a networked computer system, the method comprising:

providing a network and at least one computer system that is configured to connect to the network, the computer system comprising a host system and a virtual system, wherein the virtual system is a separate operating system or a software module operating on the computer system;

separating the host system from the virtual system using an internal firewall executed on the computer system;

implementing network isolation between the computer system and the network using a host-based firewall executed on the computer system;

providing at least one device configured to implement a network firewall or a web proxy; and

implementing network isolation, between one or more untrusted network destinations and the networked computer system, via the at least one device.

12. The method of claim 11, wherein the internal firewall is configured to prevent data from being communicated between the virtual system and the host system without an explicit user input.

13. The method of claim 11, further comprising:

the host system storing data in a host data storage; and

the virtual system storing data in a virtual data storage.

14. The method of claim 11, further comprising preventing malware introduced to the computer system from moving to another computer system of the networked computer system.

15. The method of claim 11, further comprising:

communicating with the one or more untrusted network destinations via a first communication connection;

communicating with one or more trusted network destinations via a second communication connection; and

enforcing separation of the first communication connection from the second communication connection.

16. The method of claim 11, further comprising preventing, via the host-based firewall, lateral communication and movement of malware between the computer system and other devices on the networked computer system.

17. The method of claim 11, further comprising the at least one device preventing unauthorized communication between the computer system and the one or more untrusted network destinations.

18. The method of claim 11, further comprising:

implementing a first policy for the host-based firewall when the computer system is connected to the network, the first policy for the host-based firewall permitting one or more communications between the host system of the computer system and one or more resources on the network; and

implementing a second policy for the host-based firewall when the computer system is connected to another network, the second policy for the host-based firewall blocking communications egressing from the host system of the computer system but allowing communications egressing from the virtual system.

19. The method of claim 11, further comprising running one or more applications or processes in the virtual system that are configured to communicate with the one or more untrusted network destinations.

20. The method of claim 11, further comprising running one or more applications or processes in the host system that are configured to communicate with one or more devices on the network.

3. Prosecution History of the '734 Application

The '734 Application was originally filed on March 2, 2018, with claims 1-27 being cancelled and claims 28-47 being added by Preliminary Amendment, in which claims 28 and 38 were independent. Ex. 1002, pp. 2-9.

A first Office Action was issued on June 5, 2018, rejecting all of claims 28-47 under 35 U.S.C. § 103 as being unpatentable over U.S. Publication No. 2007/0260873 ("Hatfalvi") in view of "A Survey on Virtual Machine Security" ("Reuben"). Ex. 1002, pp. 88-100. This rejection was made by Examiner Wayne An, the same examiner who examined the parent '896 Application. *See id.*; *see also* Ex. 1003. The Applicant filed a response on December 4, 2018, without any amendments to the specification or claims. Ex. 1002, pp. 110-114. The Applicant specifically argued, "Reuben does not contemplate the [virtual machine] being installed on a host machine that is located on a network with other devices" and thus "Reuben does not contemplate isolation of the host machine and virtual machines from a network on which the host machine is located." *Id.*, p. 112.

A second Office Action, which was made final, was thereafter issued by Examiner An on March 19, 2019, maintaining the prior rejection of claims 28-47 under Hatfalvi and Reuben. *Id.*, pp. 126-140. Following an Examiner Interview with a newly assigned Examiner, Examiner Thanhnga B Truong, on June 13, 2019 (*see id.*, p. 166), the Applicant filed a Response with a Request for Continued Examination (RCE) on June 19, 2019, again without any amendments to the specification or claims. *Id.*, pp. 154-160. In this response, the Applicant argued that the prior art failed to "teach or suggest three distinct methods of isolation through a combination of an internal firewall, a host-based firewall, and a network firewall or web proxy as claimed." *Id.*, pp. 155-156. Once again, the Applicant focused primarily on the features related to the host-based firewall, stating, "For example, none of the references teach or suggest that ***a host-based firewall executed on the computer system*** is configured to ***implement network isolation between the computer system and the network***." *Id.*, pp. 155-159 (emphasis in original).

A third Office Action was issued by Examiner Truong on July 25, 2019, obviating without comment the previous prior art rejections and issuing a nonstatutory obviousness-type double patenting rejection of claims 28-47 over claims 1-23 of U.S. Patent No. 9,942,198 (the '734 Application's parent). *Id.*, pp. 161-165. Applicant thereafter filed a Reply with Terminal Disclaimer on August 30, 2019. *Id.*, pp. 333-334 and 340-341. A Notice of Allowance was issued on November 8, 2019, allowing claims 28-47. *Id.*, pp. 344-350. In the accompanying Notice of Allowability, the Examiner highlighted each of: (1) the network firewall, (2) the host-based firewall, and (3) the internal firewall. Specifically, Examiner Truong stated the prior art of record did not disclose the specific limitations of "separating the host system from the virtual system

using an internal firewall executed on the computer system; implementing network isolation between the computer system and the network using a host-based firewall executed on the computer system; providing at least one device configured to implement a network firewall or web proxy; and implementing network isolation, between one or more untrusted network destinations and the networked computer system, via the at least one device." *Id.*, p. 349. Following payment of the issue fee on February 7, 2020, the '734 Application issued on March 24, 2020. *Id.*, pp. 514 and 519.

B. Claim Construction

Because this Request relates to an unexpired patent, the claims should be construed under their broadest reasonable interpretation. Therefore, all claim terms addressed herein have been construed according to their ordinary and customary meaning, as a POSITA would have understood them in the context of the '780 Patent. Requester reserves the right to advocate a different claim interpretation in any other forum if necessary.

C. Listing of Prior Art Patents and Printed Publications

Reexamination of the Challenged Claims is requested in view of the following references, which due to the earliest possible priority date of January 27, 2011, are applied under pre-AIA 35 U.S.C. § 102:

- **Ex. 1006 ("Thomas")**: U.S. Publication 2009/0241194 to Thomas was filed on March 21, 2008, and later published on September 24, 2009. Thomas is prior art at least under 35 U.S.C. §§ 102(a), (b), and (e). It is prior art under § 102(a) because it was published in this country prior to January 27, 2011; it is prior art under § 102(b) because that publication was more than one year prior to January 27, 2011; and it is prior art under § 102(e) because it is a publication of an application for patent that was applied for in this country prior to January 27, 2011.
- **Ex. 1007 ("Garg")**: U.S. Publication 2006/0206300 to Garg *et al.* was filed on March 11, 2005, and later published on September 14, 2006. Garg is prior art at least under 35 U.S.C. §§ 102(a), (b), and (e). It is prior art under § 102(a) because it was published in this country prior to January 27, 2011; it is prior art under § 102(b) because that publication was more than one year prior to January 27, 2011; and it is prior art under § 102(e) because it is a publication of an application for patent that was applied for in this country prior to January 27, 2011.

None of the references listed above were cited during prosecution of the '780 Patent. A Form SB-08 and copies of the cited references are submitted herewith. This request is also

supported by the declaration of Dr. Seth James Nielson, Ph.D. (Ex. 1008). Copies of additional references discussed in Dr. Nielson's declaration are provided in Exhibits 1009-1012 and are included on Form SB-08.

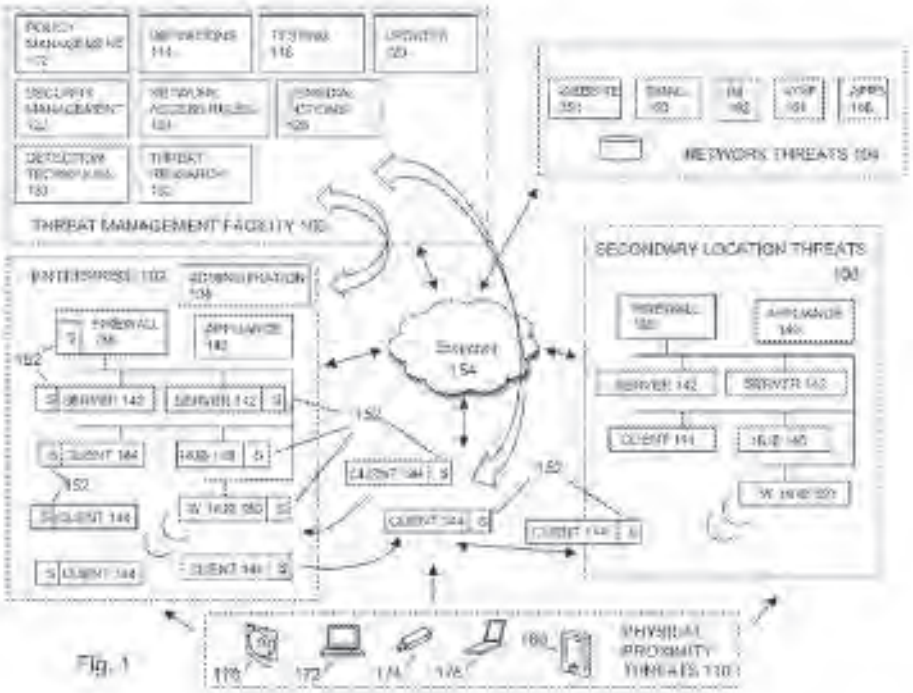
As shown below, Requester submits that the prior art references raise new "substantial question[s] of patentability" because "the teaching of the (prior art) patents and printed publications is such that a reasonable examiner would consider the teaching to be important in deciding whether or not the claim is patentable." *See* MPEP § 2242 (emphasis in original). For example, the references discussed below, when considered as an ordered combination, teach each element of the Challenged Claims, including the idea of "providing computer security using three separate firewalls, including an internal firewall, a host-based firewall, and a device configured as a network firewall or a web proxy," which the Examiner seemingly believed was missing in the art during the original prosecution. Further, the references are new; the "same question of patentability as to the claim[s] has not been decided by the Office in an earlier concluded examination or review of the patent" at least because none of the art referenced in this Request was before the Office during prosecution of the '780 Patent or during a prior post-grant proceeding challenging any claim of the '780 Patent (any of which that are known to Requester have been listed in Section IV of this Request). *See id.*

D. Ground 1: Claims 1-20 Are Obvious over Thomas in Combination with Garg

1. Overview of Thomas

Thomas (Ex. 1006, U.S. Publication 2009/0241194) relates to a "computer configuration, and more specifically to the sharing of information between virtual machines." Ex. 1006, ¶ [0002]. More specifically, Thomas is directed to providing protection to devices on a networked computer-based infrastructure from computer-based malware, including viruses, spyware, adware, Trojans, intrusion, spam, policy abuse, uncontrolled access, etc. *Id.*, ¶ [0026]. The system and method of Thomas can be understood with reference to Figures 1 and 2 of Thomas (reproduced and discussed in turn below). These figures demonstrate Thomas' teachings of a system that implements (1) firewall 138 (a network firewall), (2) host computer security facility 152A (a host-based firewall), and (3) a virtual computing machine monitor 208 having the same network access control features (i.e., a computer security facility 152) to function as an internal firewall between the virtual computing machines 204A and 204B (the internal firewall). Thomas also teaches the use of proxy server facility 142 (a web proxy) as an alternative to or in combination with firewall 138.

FIG. 1 illustrates a threat management facility 100 that provides protection to an enterprise facility 102, which is any entity with a networked computer-based infrastructure. *Id.*, ¶¶ [0023]-[0026]; FIG. 1 (reproduced below). "The threat management facility 100 may include a plurality of functions, such as security management facility 122, policy management facility 112, update facility 120, definitions facility 114, network access rules facility 124, remedial action facility 128, detection techniques facility 130, testing facility 118, threat research facility 132, and the like." *Id.*, ¶ [0026]. The enterprise facility 102 "may include a plurality of networked components, such as client facility 144, server facility 142, administration facility 134, firewall 138, gateway, hubs 148, routers, threat management appliance 140, desktop users, mobile users, and the like." *Id.*, ¶ [0050]. One or more of the networked components of the enterprise facility may have access to the Internet 154. *Id.*, ¶ [0056]. For example, Thomas teaches, "Interactions between the threat management facility 100 and the components of the enterprise facility 102, including mobile client facility 144 extensions of the enterprise facility 102, may ultimately be connected through the internet 154." *Id.*, ¶ [0059].



Thomas, FIG. 1

The enterprise facility 102 also includes firewall 138, i.e., a network firewall, which "may be a hardware or software device that may be configured to permit, deny, or proxy data through a computer network that has different levels of trust in its source of data through a computer network

that has different levels of trust in its source of data." *Id.*, ¶ [0056]. Thomas further discloses the hardware of the firewall 138 may include a general-purpose computer and/or dedicated computing device and its processes may be realized in one or more microprocessors, microcontrollers, embedded microcontrollers, programmable digital signal processors or other programmable device, along with internal and/or external memory." *Id.*, ¶ [0100]. In addition, Thomas discloses the enterprise facility 102 "may include … proxy servers 142." *Id.*, ¶ [0052].

Thomas discloses end-point computer security facility 152, e.g., an application, is located on a computer's desktop and provides threat protection to a user and the associated enterprise facility 102. *Id.*, ¶ [0050]. Thomas explains that "the term end-point may refer to a computer system that may source data, receive data, evaluate data, buffer data, or the like, such as a user's desktop computer as an end-point computer, a firewall as a data evaluation end-point computer system, a laptop as a mobile end-point computer, a PDA as a hand-held end-point computer. In embodiments, end-point may refer to a source or destination for data, including such components where the destination is characterized by an evaluation point for data, and where the data may be sent to a subsequent destination after evaluation." *Id.* The threat management facility 100 and associated end-point computer security facilities 152 may provide seamless threat protection to the plurality of clients 144 across the enterprise facility 102. *Id.*, ¶ [0051]. Thus, Thomas teaches that the end-point computer security facility 152 may be located on any number of devices and components within the enterprise facility 102, such that each instance of the end-point computer security facility 152 may operate as, for example, an internal firewall or a host-based firewall depending on the installation location.

With reference to Figures 1 and 2, Thomas explains that the physical computing machine 202 of FIG. 2 may be a client facility 144. *Id.*, ¶ [0067]; FIG. 2 (reproduced below). The physical computing machine 202 may be connected to a network either through a wired connection or a wireless connection, and it may include hardware, software, software applications, etc. *Id.* The physical computing machine 202 may include a virtual computing machine 204A and a plurality of virtual computing machines 204B, each of which may be a software implementation of a machine on a computer that may execute processes like a real computer. *Id.* Thomas discloses, "In order to maintain isolation amongst these virtual machines 204, there is typically no sharing of information or software resources between the virtual computing machines 204." *Id.*, ¶ [0064].

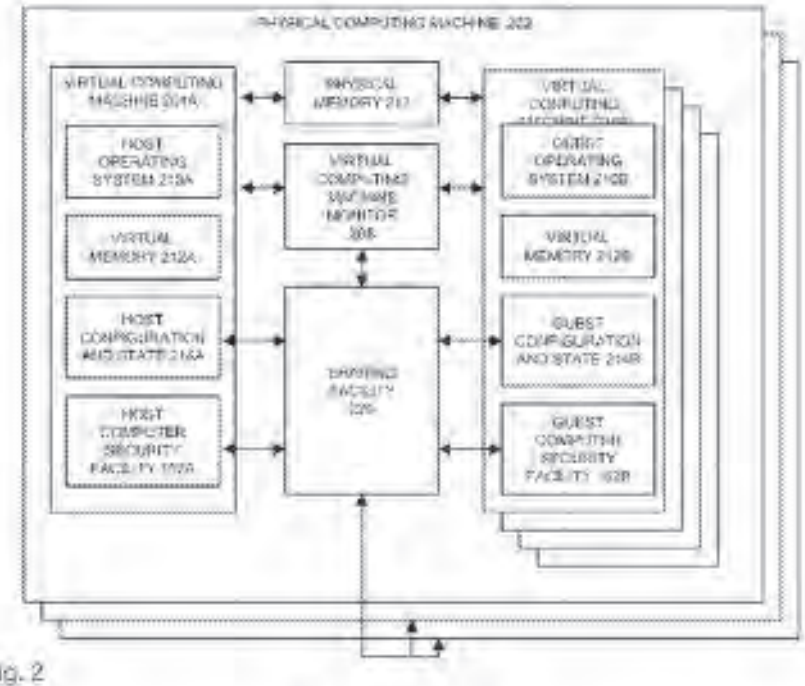


Fig. 2

Thomas, FIG. 2

As further illustrated in Figure 2, the virtual computing machine 204A may include a host operating system 210A, a virtual memory 212A, a host configuration and state 214A, and a host computer security facility 152A. *Id.*, ¶ [0067]. Likewise, the virtual computing machine 204B may include a guest operating system 210B, a virtual memory 212B, a guest configuration and state 214B, and a guest computer security facility 152B. *Id.*, ¶ [0069]. The guest operating system 210B may run a different operating system with respect to the host operating system 210A. *Id.*, ¶ [0070]. The computer security facilities 152A and 152B may be associated with network access control related to securing the virtual computing machines 204A and 204B prior to a network connection. *Id.*, ¶ [0080]. For example, the network access control may verify access rights for client facilities 144 from within the network or may verify access rights of computer facilities from external networks. *Id.*, ¶ [0043]. Thomas describes the network access control "may provide control over network connections," "may stop unauthorized, guest, or non-compliant systems from accessing networks, and may control network traffic that may not be bypassed from the client level," and "may control access to virtual private networks (VPN), where VPNs may be a communications network tunneled through another network, establishing a logical connection acting as a virtual network." *Id.*, ¶ [0029]. Accordingly, the host computer security facility 152A functions as a host-based firewall.

Figure 2 further illustrates that the physical computing machine 202 also includes a virtual computing machine monitor 208 that provides a software layer for the virtual computing machines 204A and 204B. *Id.*, ¶ [0071]. The virtual computing machine monitor 208 may be a hypervisor. *Id.*, ¶ [0073]. As explained above, based on the teachings of Thomas, a POSITA would understand that an end-point computer security facility 152, having the same network access control features described above for computer security facilities 152A and 152B, may be present on the virtual computing machine monitor 208 to function as an internal firewall between the virtual computing machines 204A and 204B. Ex. 1008, ¶ 79.

Thomas further describes the different ways in which the threat management facility 100 may operate to protect the client facilities 144 that are connected to the enterprise facility 102 network and those that are connected outside the enterprise facility 102. *Id.*, ¶¶ [0058]-[0060].

Thomas is analogous art to the '780 Patent. As noted in Section I.A of this Request, the field of endeavor of the '780 Patent includes "the protection of computer systems from injurious software that can be encountered while browsing or accessing the Internet, and also to the protection of local [area] networks (LANS) that have access to the [Internet]." Ex. 1001, 1:17-21. Like the '780 Patent, Thomas is in this field; for example, it relates to "protecting computer assets from many threats, both computer generated threats and user generated threats." Ex. 1006, ¶ [0023]. Further, Thomas is reasonably pertinent to problems concerning the inventors of the '780 Patent, such as providing protection for a computer network by controlling communications between the various parts including the host computer, virtual machines running on the host computer, other computers on the network, and both trusted and untrusted sites. *See, e.g.*, Ex. 1001, 3:6-28 and Ex. 1006, ¶ [0025]; *see also* Ex. 1008, ¶ 81.

Requester also cites the testimony of Dr. Nielson, who provides background knowledge regarding the state of the art and discusses possible variations of Thomas' disclosure that would have been apparent to a POSITA, as discussed in greater detail below. *See, e.g.*, Ex. 1008, ¶¶ 50-66.

2. Overview of Garg

Garg (Ex. 1007, U.S. Publication 2006/0206300) relates to "traffic monitoring and filtering of virtual machine (VM) network data on a host computer." Ex. 1007, ¶ [0001]. The system and method of Garg can be understood with reference to Figures 2B and 3 of Garg (reproduced and

discussed in turn below). These figures demonstrate Garg's teachings of implementation details for virtual computing machines including a virtual ethernet NIC ("VNIC") 80 (internal firewall).

FIG. 2B illustrates a virtualized computing system that includes physical computer hardware 62 and a host operating system (OS) software layer 64 running directly above the physical computer hardware 62. *Id.*, ¶ [0044]; FIG. 2B (reproduced below). The host OS 64 provides access to the resources of the physical computer hardware 62 by exposing interfaces that are the same as the hardware the host OS is emulating (or 'virtualizing'). *Id.* To perform the emulation, the host OS 64 may be a standard operating system with an incorporated hypervisor component for performing the emulation. *Id.*

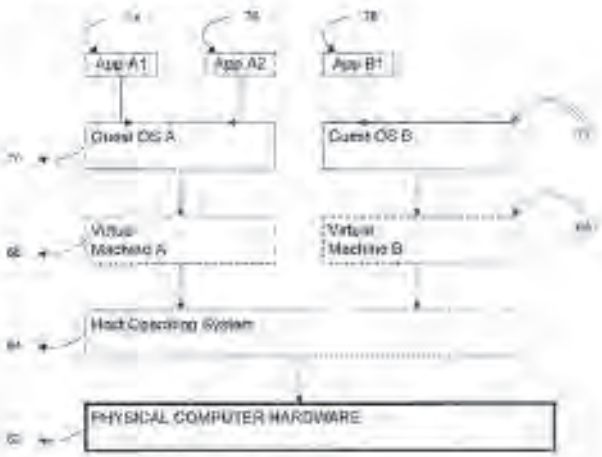


FIG. 2B

Garg, FIG. 2B

More generally, Garg describes its virtualizer program as follows:

> The virtualizer program acts as the interchange between the hardware architecture of the host machine and the instructions transmitted by the software (e.g., operating systems, applications, etc.) running within the emulated environment. This virtualizer program may be a host operating system (HOS), which is an operating system running directly on the physical computer hardware (and which may comprise a hypervisor). Alternately, the emulated environment might also be a virtual machine monitor (VMM) which is a software layer that runs directly above the hardware, perhaps running side-by-side and working in conjunction with the host operating system, and which can virtualize all the resources of the host machine (as well as certain virtual resources) by exposing interfaces that are the same as the hardware the VMM is virtualizing.

Id., ¶ [0039].

Turning to Figure 3, Garg illustrates a host OS 20 and a guest OS 30 corresponding to the host OS 64 and the guest OS A 70 of Figure 2B, respectively. *See id.*, ¶ [0049]; FIG. 3 (reproduced below). As illustrated in Figure 3, a virtual Ethernet NIC ("VNIC") 32 is inside the guest OS 30 and enables communication with the host OS 20. *Id.* A VNIC 80 is provided in the host OS 20 and corresponds to the VNIC 32. *Id.* In addition, the host OS 20 also includes NDIS IM drivers 82, which "provide features such as firewall, quality of service, IP security, and the like by monitoring and filtering the incoming and outgoing network traffic" (*id.*, ¶ [0002]) and which "bind themselves on top of the host VNIC and effectively place themselves as a filter on the point to point connection" (*id.*, abstract), which is described further below.

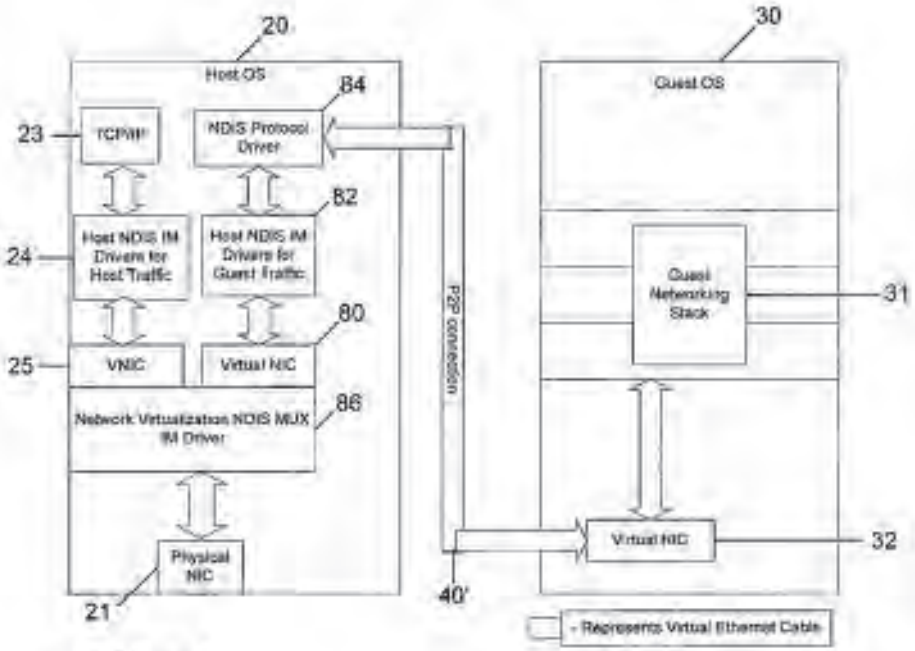


FIGURE 3

Garg, FIG. 3

Garg teaches that "a point to point connection 40' is created between the VNIC 32 of the guest OS 30 and the VNIC 80 of the host OS 20." *Id.*, ¶ [0049]. As noted above, the NDIS IM drivers 82 bind themselves on top of the host VNIC 80 on the side of the host OS 20 and effectively place themselves as a filter, i.e., an internal firewall, on this point to point connection, i.e., the point to point connection 40'. *See id.*, ¶ [0050] and abstract. In other words, a virtual Ethernet cable 40' is created between the VNIC 32 and the VNIC 80, and the NDIS IM drivers 82 bind themselves to the host VNIC 80 thus placing themselves as a filter on the virtual Ethernet cable 40' between the host OS 20 and the guest OS 30. *Id.* That is, all outgoing network traffic from the guest OS 30

goes over the virtual Ethernet cable 40' to the VNIC 80 on the host OS 20 and all the incoming network traffic to the guest OS 30 first goes to the VNIC 80 on the host OS 20 before being sent to the guest OS 30 over the virtual Ethernet cable 40'. *Id.*

Garg is analogous art to the '780 Patent. As noted in Section I.A of this Request, the field of endeavor of the '780 Patent includes "the protection of computer systems from injurious software that can be encountered while browsing or accessing the Internet, and also to the protection of local [area] networks (LANS) that have access to the [Internet]." Ex. 1001, 1:17-21. Like the '780 Patent, Garg is in this field; for example, it relates to making virtualized operating systems "less susceptible to Internet viruses, and worms, network denial of service (DOS) attacks, and the like." Ex. 1007, Abstract. Further, Garg is reasonably pertinent to problems concerning the inventors of the '780 Patent, such as providing protection for a computer network by controlling communications between the various parts including the host computer, virtual machines running on the host computer, other computers on the network, and both trusted and untrusted sites. *See, e.g.*, Ex. 1001, 3:6-28 and Ex. 1007, ¶ [0008]; *see also* Ex. 1008, ¶ 87.

Requester also cites the testimony of Dr. Nielson, who provides background knowledge regarding the state of the art and discusses possible variations of Garg's disclosure that would have been apparent to a POSITA, as discussed in greater detail below. *See, e.g.*, Ex. 1008, ¶¶ 50-66.

3. The Proposed Combination of Thomas in view of Garg

As detailed above, Thomas provides disclosure of firewall functionality being provided throughout enterprise facility 102 by end point security facilities 152. *See* Ex. 1008, ¶ 88. Thomas describes an arrangement in which virtual computing machine monitor 208 may be present between host virtual computing machine 204A and guest virtual computing machine 204B and teaches that the virtual computing machine monitor 208 may be a hypervisor. *See id.* Though not explicitly stated in Thomas, a POSITA would understand from the teachings of Thomas that an end point security facility 152 would be present on the virtual computing machine monitor 208 as it is an "end point" location as defined by Thomas, and a POSITA would further understand that the end point security facility 152 on the virtual computing machine monitor 208 would include network access control features allowing it to function as an internal firewall. *See id.* Nevertheless, to the extent a POSITA would have required specific implementation details of an internal firewall on the virtual computing machine monitor 208, Garg provides those details with its emulation program, e.g., a hypervisor of the host operating system (analogous to the virtual computing

machine monitor 208 of Thomas), that is configured to secure a point to point connection, i.e., the virtual Ethernet cable 40', that is created between the VNIC 32 of the guest OS 30 and the VNIC 80 of the host OS 20 (analogous to the virtual computing machines 204A and 204B, respectively, of Thomas). *See id.*

A POSITA would have been motivated to incorporate Garg's teachings (including the NDIS IM drivers 82 bound to the host VNIC 80) with Thomas' teachings (of improving security between host and guest systems). First, Thomas provides teachings and motivations to include a virtual machine monitor in its system but it does not provide many implementation details for such a system. So motivated by Thomas' suggestion to include such a virtual machine monitor, a POSITA would have turned to Garg for implementation details to arrive at the claimed combination. *Id.*, ¶ 89; *see* MPEP § 2143(I)(G) (citing *KSR*, 550 U.S. at 416, 82 USPQ2d at 1395). Specifically, a POSITA would have been motivated to look to Garg to explain a specific implementation of separating Thomas' host virtual computing machine 204A and guest virtual computing machine 204B using Thomas' virtual computing machine monitor 208. A POSITA would have turned to Garg, in particular, at least because of the overlap in technologies. Ex. 1008, ¶ 89. For example, Garg, like Thomas, describes techniques for securing virtual machines. *Id.* This overlap in technologies would have provided a POSITA with a reasonable expectation of success in the combination. *Id.*

Additionally, the proposed combination merely amounts to the simple substitution of one known element (i.e., Garg's host operating system with a hypervisor component) for another (i.e., Thomas' host operating system with a hypervisor component) to obtain predictable results (i.e., a hypervisor with firewall functionalities that enhances security between host and guest operating systems). *Id.*, ¶ 90; *see* MPEP § 2143(I)(A) (citing *KSR*, 550 U.S. at 416, 82 USPQ2d at 1395). Furthermore, the proposed combination merely amounts to combining prior art elements (i.e., Garg's network traffic filtering in Thomas' hypervisor) according to known methods (i.e., binding an NDIS IM driver to a VNIC) to yield predictable results (i.e., a hypervisor with firewall functionalities that enhances security between host and guest operating systems). Ex. 1008, ¶ 90; *see* MPEP § 2143(I)(A) (citing *KSR*, 550 U.S. at 416, 82 USPQ2d at 1395). A POSITA reading Thomas would have looked for known ways to configure an existing hypervisor component to enhance security between host and guest operating systems to further protect the host computer and the network. Ex. 1008, ¶ 90. A POSITA would have understood that incorporating Garg's host

operating system with a hypervisor component including the NDIS IM drivers 82 bound to the host VNIC 80 with Thomas' host operating system with a hypervisor component would have been a beneficial modification to Thomas, so that greater security is achieved within the host and guest systems as well as within the networked computer. *Id.*

4. Thomas in view of Garg Presents Substantial New Questions of Patentability

As shown below, Thomas in view of Garg renders obvious each of claims 1-20. For this reason, Thomas in view of Garg presents substantial new questions of patentability. A reasonable examiner would consider the teachings of Thomas in combination with Garg important in determining whether claims 1-20 are patentable because they teach every element of these claims, and the combination is new: neither Thomas nor Garg was cited or otherwise considered during prosecution. Section II.A of this Request provides greater detail regarding how Thomas in view of Garg renders obvious each and every element of claims 1-20.

II. DETAILED APPLICATION OF THE PRIOR ART TO EVERY CLAIM FOR WHICH REEXAMINATION IS REQUESTED

Requester requests *ex parte* reexamination based on the following ground:

Ground	Claims	Statute	Prior Art
1	1-20	§ 103	Thomas and Garg

This challenge is based on pre-AIA statutory grounds.

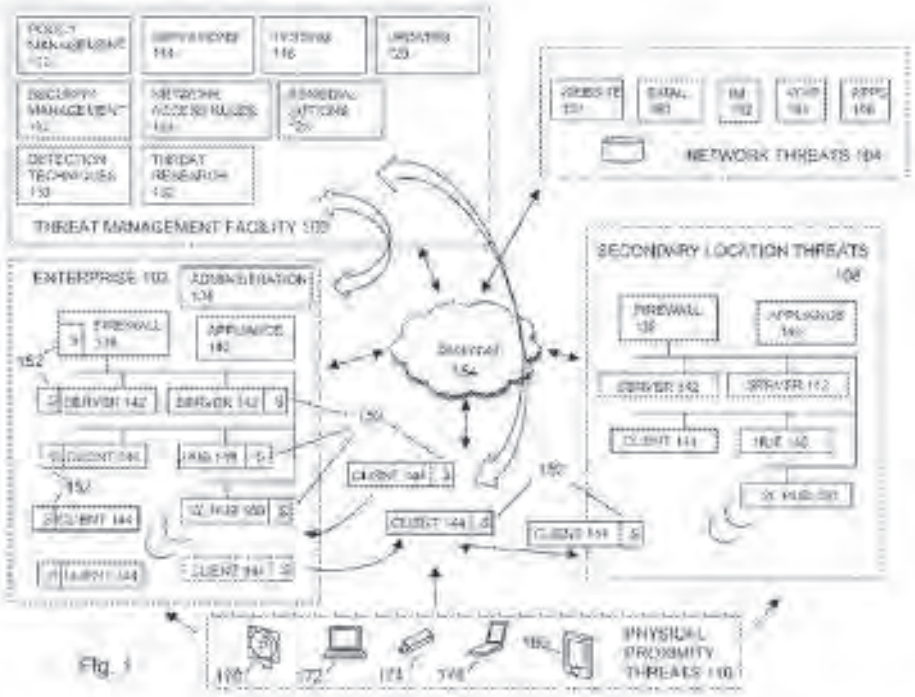
A. Ground 1: Thomas in view of Garg (§ 103)

1. Claim 1

1pre. A networked computer system comprising:

To the extent the preamble is limiting, Thomas teaches a networked computer system (**e.g., the enterprise facility 102 and the threat management facility 100**).

For example, regarding FIG. 1, Thomas teaches an enterprise facility 102, which "may be any entity with a networked computer-based infrastructure." Ex. 1006, ¶ [0026].



Thomas, FIG. 1

Thomas explains that "the enterprise facility 102 may include a plurality of networked components, such as client facility 144, server facility 142, administration facility 134, firewall 138, gateway, hubs 148, routers, threat management appliance 140, desktop users, mobile users, and the like." *Id.*, ¶ [0050]. In addition, Thomas states, "Interactions between the threat management facility 100 and the components of the enterprise facility 102, including mobile client facility 144 extensions of the enterprise facility 102, may ultimately be connected through the internet 154." *Id.*, ¶ [0059].

In view of the foregoing, Thomas renders obvious a networked computer system (**e.g., the enterprise facility 102 and the threat management facility 100**).

1A. a network;

Thomas teaches a network (**e.g., the enterprise facility 102**).

In general terms, Thomas teaches an enterprise facility 102, which may be any entity with a networked computer-based infrastructure. *See id.*, ¶ [0026]; *see also id.*, FIG. 1. More specifically, Thomas discloses, "The enterprise facility 102 may be corporate, commercial, educational, governmental, or the like, and the enterprise facility's 102 computer network may be distributed amongst a plurality of facilities, and in a plurality of geographical locations." *Id.*, ¶ [0026]. Thomas further teaches that "the enterprise facility 102 may include a plurality of

networked components, such as client facility 144, server facility 142, administration facility 134, firewall 138, gateway, hubs 148, routers, threat management appliance 140, desktop users, mobile users, and the like." *Id.*, ¶ [0050].

In view of the foregoing, Thomas renders obvious a network (**e.g., the enterprise facility 102**).

1B. at least one computer system configured to connect to the network,

Thomas teaches at least one computer system (**e.g., the physical computing machine 202 corresponding to the client 144**) configured to connect to the network (**e.g., the enterprise facility 102**).

For example, Thomas teaches the enterprise facility 102 is associated with client facilities 144. *See id.*, ¶ [0033]. Thomas provides further details about the clients 144 in FIG. 2: "In embodiments, referring to FIG. 2 the physical computing machine 202 is illustrated. The physical computing machine may be a client 144." *Id.*, ¶ [0067].

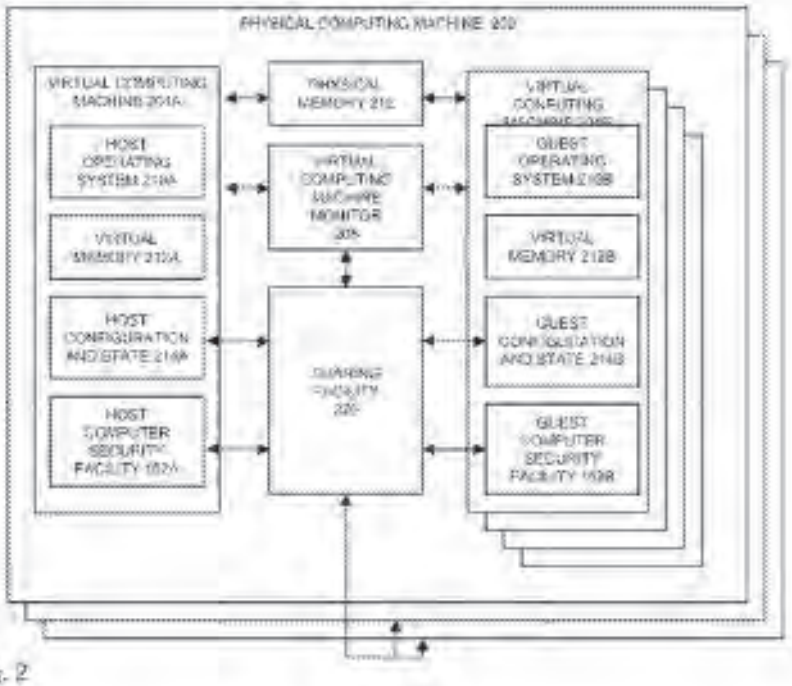


Fig. 2

Thomas, FIG. 2

Furthermore, Thomas explains "The physical computing machine 202 may be connected to a network either through a wired or a wireless connection. Further, those skilled in art would appreciate that the physical computing machine 202 may include hardware, software, software

applications, processes, procedure, in embodiments, described herein." *Id.*, ¶ [0067] (emphasis added); FIG. 2.

In view of the foregoing, Thomas renders obvious at least one computer system (**e.g., the physical computing machine 202 corresponding to the client 144**) configured to connect to the network (**e.g., the enterprise facility 102**).

1C. the computer system comprising a host system and a virtual system,

Thomas teaches the computer system (**e.g., the physical computing machine 202 corresponding to the client 144**) comprising a host system (**e.g., host operating system 210A operating on virtual computing machine 204A**) and a virtual system (**e.g., guest operating system 210B operating on virtual computing machine 204B**).

As illustrated in Figure 2, the physical computing machine 202 includes virtual computing machine 204A and virtual computing machine 204B. *Id.*, ¶ [0067]; FIG. 2. Thomas teaches, "The virtual computing machine 204A and the virtual computing machine 204B may be a software implementation of a machine on a computer that may execute process like a real computer. The virtual computing machine 204A may include a host operating system 210A, a virtual memory 212A and a host configuration and state 214A." *Id.*

Thomas further teaches, "The physical computing machine 202 may include another different virtual computing machine 204B that may run a guest operating system 210B. It may be noted that the virtual computing machine 204B may include one or more guest operation systems as shown in FIG. 2." *Id.*, ¶ [0069].

In view of the foregoing, Thomas renders obvious the computer system (**e.g., the physical computing machine 202 corresponding to the client 144**) comprising a host system (**e.g., host operating system 210A operating on virtual computing machine 204A**) and a virtual system (**e.g., guest operating system 210B operating on virtual computing machine 204B**).

1D. wherein the virtual system is a separate operating system or a software module operating on the computer system,

Thomas teaches wherein the virtual system (**e.g., virtual computing machine 204B**) is a separate operating system (**e.g., guest operating system 210B**) or a software module (**e.g., a software implementation of a machine**) operating on the computer system (**e.g., the physical computing machine 202 corresponding to the client 144**).

Requester notes the '780 Patent states that a hypervisor for creating the virtual system may be "software that executes directly as a separate operating system on the hardware of computer 9" or "a software module that operates based on the underlying operating system, e.g., Windows 7, of the computer 9." Ex. 1001, 7:66-8:2. Thus, it is either the "separate operating system" or the "software module" which is "operating on the computer system." Notably, although only one option is required to operate "on the computer system" to render this element obvious, Thomas discloses both options.

For example, Thomas teaches, "The guest operating system 210B may run a different operating system with respect to host operating system 210A." *Id.*, ¶ [0070]; *see also id.*, ¶ [0064] (stating "each virtual computing machine 20 runs its own operating system 210"). In addition, Thomas teaches that "the virtual computing machine 204B may be a software implementation of a machine on a computer that may execute process like a real computer." *Id.*, ¶ [0067]; *see also id.*,]0098] (teaching the elements depicted in the flow charts and block diagrams throughout the figures and their functions may be implemented as standalone software modules).

In view of the foregoing, Thomas renders obvious wherein the virtual system (**e.g., virtual computing machine 204B**) is a separate operating system (**e.g., guest operating system 210B**) or a software module (**e.g., a software implementation of a machine**) operating on the computer system (**e.g., the physical computing machine 202 corresponding to the client 144**).

1E. wherein an internal firewall is configured to separate the host system from the virtual system in the computer system, and

Thomas in view of Garg teaches wherein an internal firewall (**e.g., Thomas' virtual computing machine monitor 208 as modified by Garg's NDIS IM drivers 82**) is configured to separate the host system (**e.g., Thomas' host operating system 210A operating on virtual computing machine 204A**) from the virtual system (**e.g., Thomas' guest operating system 210B operating on virtual computing machine 204B**) in the computer system (**e.g., Thomas' physical computing machine 202 corresponding to the client 144**).

Thomas teaches, "In embodiments, the virtual computing machine 204A and the virtual computing machine 204B may be associated with the virtual computing machine monitor 208. The virtual computing machine monitor 208 may provide a software layer which may implement virtualization for running multiple virtual computing machines. For example, the virtual

computing machine monitor 208 may provide the software layer for the virtual computing machine 204A and the virtual computing machine 204B." *Id.*, ¶ [0071].

Thomas further teaches that "the virtual computer machine monitor 208 may be a hypervisor." *Id.*, ¶ [0073]. As explained in Thomas, the end-point computer security facility 152 is present at end-points throughout its system and "may provide threat protection in a plurality of network infrastructure locations" including at "the desktop of client facility 144 computers." *Id.*, ¶ [0056]. More specifically, Thomas explains, "the term end-point may refer to a computer system that may source data, receive data, evaluate data, buffer data, or the like, such as a user's desktop computer as an end-point computer, a firewall as a data evaluation end-point computer system, a laptop as a mobile end-point computer, a PDA as a hand-held end-point computer. In embodiments, end-point may refer to a source or destination for data, including such components where the destination is characterized by an evaluation point for data, and where the data may be sent to a subsequent destination after evaluation." *Id.*, ¶ [0050]. Thus, a POSITA in reading Thomas would understand that Thomas teaches the end-point computer security facility 152 (e.g., an internal firewall) is present on "end-points throughout its system" including the virtual computer machine monitor (hypervisor) 208 of the computer system (e.g., client 144). Ex. 1008, ¶ 113.

To the extent a POSITA would have required specific implementation details of an internal firewall on the virtual computing machine monitor 208 of Thomas, a POSITA would have been motivated to look to Garg to explain a specific implementation of separating the host virtual computing machine 204A and the guest virtual computing machine 204B using the hypervisor 208 of Thomas. *See id.*, ¶ 114. That is, Thomas contemplates a host operating system with a hypervisor component (e.g., hypervisor 208) and end point security facilities 152 distributed throughout the networked computer system. *See id.* Garg provides specific implementation details for the hypervisor 208 of Thomas with details of Garg's emulation program, e.g., the program running on a hypervisor of the host operating system (analogous to the virtual computing machine monitor 208 of Thomas), in which Garg's system is configured to secure a point to point connection between Garg's VNIC 32 of guest OS 30 and VNIC 80 of host OS 20 (analogous to the virtual computing machines 204A and 204B, respectively, of Thomas). *See id.*

In detail, Garg teaches that FIG. 2B illustrates a virtualized computing system that includes physical computer hardware 62 and a host operating system (OS) software layer 64 running

directly above the physical computer hardware 62. Ex. 1007, ¶ [0044]; FIG. 2B. The host OS 64 provides access to the resources of the physical computer hardware 62 by exposing interfaces that are the same as the hardware the host OS is emulating (or "virtualizing"). *Id.* To perform the emulation, the host OS 64 may be a standard operating system with an incorporated hypervisor component for performing the emulation. *Id.*

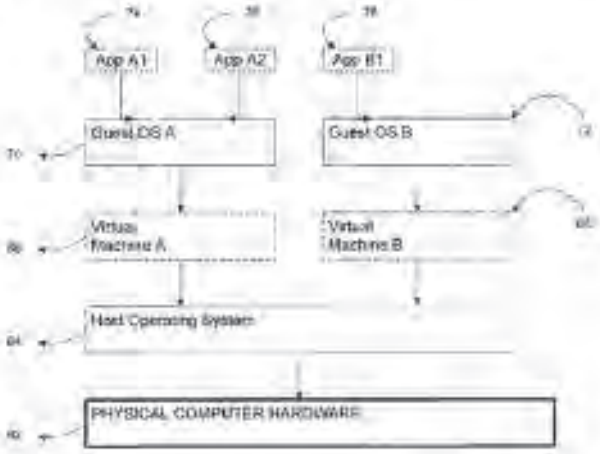


FIG. 2B

Garg, FIG. 2B

In Figure 3, Garg illustrates a host OS 20 and a guest OS 30 corresponding to the host OS 64 and the guest OS A 70 of Figure 2B, respectively. *See id.*, ¶ [0049]; FIG. 3 (reproduced below). As illustrated in Figure 3, a virtual Ethernet NIC ("VNIC") 32 is inside the guest OS 30 and enables communication with the host OS 20. *Id.* A VNIC 80 is provided in the host OS 20 and corresponds to the VNIC 32. *Id.* In addition, the host OS 20 also includes NDIS IM drivers 82, which "provide features such as firewall, quality of service, IP security, and the like by monitoring and filtering the incoming and outgoing network traffic" (*id.*, ¶ [0002]) and which "bind themselves on top of the host VNIC and effectively place themselves as a filter on the point to point connection" (*id.*, abstract), which is described further below.

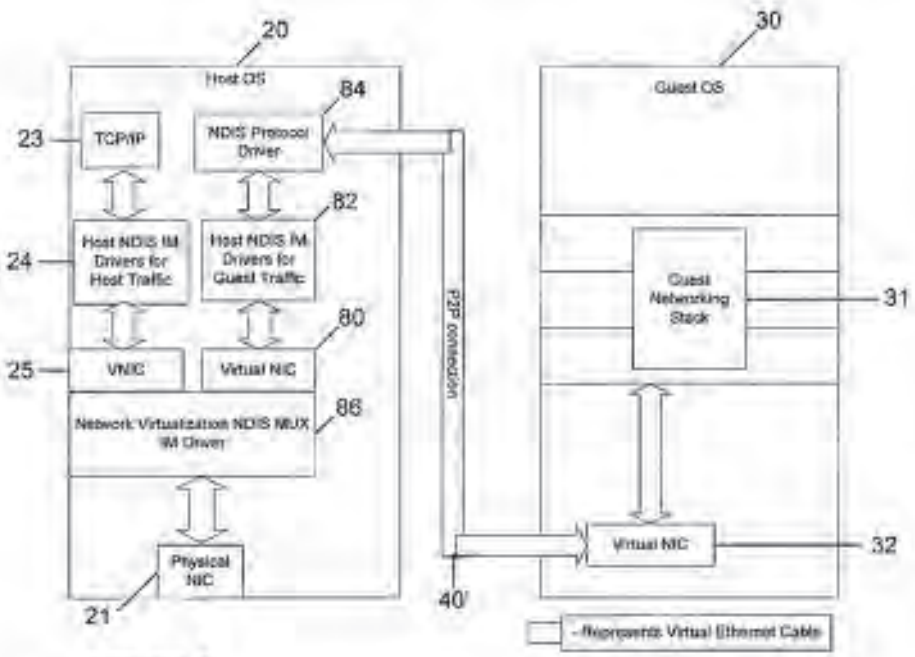


FIGURE 3

Garg, FIG. 3

Garg teaches that "a point to point connection 40' is created between the VNIC 32 of the guest OS 30 and the VNIC 80 of the host OS 20." *Id.*, ¶ [0049]. As noted above, the NDIS IM drivers 82 bind themselves on top of the host VNIC 80 on the side of the host OS 20 and effectively place themselves as a filter, i.e., an internal firewall, on this point to point connection, i.e., the point to point connection 40'. *See id.*, ¶ [0050] and abstract. In other words, a virtual Ethernet cable 40' is created between the VNIC 32 and the VNIC 80, and the NDIS IM drivers 82 bind themselves to the host VNIC 80 thus placing themselves as a filter on the virtual Ethernet cable 40' between the host OS 20 and the guest OS 30. *Id.* That is, all outgoing network traffic from the guest OS 30 goes over the virtual Ethernet cable 40' to the VNIC 80 on the host OS 20 and all the incoming network traffic to the guest OS 30 first goes to the VNIC 80 on the host OS 20 before being sent to the guest OS 30 over the virtual Ethernet cable 40'. *Id.*

The NDIS IM drivers 82 bound to the host VNIC 80 are incorporated into (and thus internal to) the hypervisor component of Garg's host OS. Furthermore, they are acting as a firewall between the host OS 20 and the guest OS 30 by virtue of filtering the data communicated between them over the virtual Ethernet cable 40'. It was well known by a POSITA at the time of the invention of the '780 Patent that packet filtering is a known function of a firewall. *See, e.g.*, Ex. 1008, ¶¶ 118 and 50-66 (citing, *inter alia*, Ex. 1012, 1:28-40). The '780 Patent itself also recognizes a function

of a firewall is to filter data packets. *See, e.g.*, Ex. 1001, 9:66-10:4; Ex. 1008, ¶ 118. Thus, Garg's filtering of data communicated over the virtual Ethernet cable teaches an "internal firewall" between the host OS 20 and the guest OS 30. Ex. 1008, ¶ 118.

Firewalls have been around for decades now and are being used extensively for packet filtering purposes as a means of monitoring the flow of network communication, whether it be internal between VMs or external from a physical host to the internet. *Id.*, ¶ 119. Moreover, including firewall functionality with a hypervisor would help with the filtering of data flow. *Id.*

It would have been obvious to include Garg's filtering of data communicated over the virtual Ethernet cable implemented by Garg's host operating system having a hypervisor component with Thomas' host operating system having a hypervisor component so as to separate the host virtual computing machine 204A and the guest virtual computing machine 204B of Thomas. *Id.*, ¶ 120.

A POSITA would have been motivated to incorporate Garg's teachings (including the NDIS IM drivers 82 bound to the host VNIC 80) with Thomas' teachings (of improving security between host and guest systems) for the reasons provided here and detailed in Section I.D.3. *See id.*, ¶ 121.

In view of the foregoing, Thomas in view of Garg renders obvious wherein an internal firewall (**e.g., Thomas' virtual computing machine monitor 208 as modified by Garg's NDIS IM drivers 82**) is configured to separate the host system (**e.g., Thomas' host operating system 210A operating on virtual computing machine 204A**) from the virtual system (**e.g., Thomas' guest operating system 210B operating on virtual computing machine 204B**) in the computer system (**e.g., Thomas' physical computing machine 202 corresponding to the client 144**).

IF, a host-based firewall executed on the computer system is configured to implement network isolation between the computer system and the network; and

Thomas teaches a host-based firewall (**e.g., an end-point computer security facility 152**) executed on the computer system (**e.g., the physical computing machine 202 corresponding to the client 144**) is configured to implement network isolation (**e.g., network access control**) between the computer system (**e.g., the physical computing machine 202 corresponding to the client 144**) and the network (**e.g., the enterprise facility 102**).

For example, Thomas states that "the end-point computer security facility 152, located on a computer's desktop" may "provide threat protection to a user." Ex. 1006, ¶ [0050].

Thomas further teaches, "The end-point computer security facility 152 may be an application loaded onto the computer platform or computer support component, where the application may accommodate the plurality of computer platforms and/or functional requirements of the component. For instance, a client facility 144 computer may be one of a plurality of computer platforms, such as Windows, Macintosh, Linux, and the like, where the end-point computer security facility 152 may be adapted to the specific platform, while maintaining a uniform product and product services across platforms." *Id.*, ¶ [0050]. Thomas also explains, "In embodiments, the threat management facility 100, and associated end-point computer security facility 152, may provide seamless threat protection to the plurality of clients 144, and client facility 144 types, across the enterprise facility 102." *Id.*, ¶ [0051]. Thomas further teaches, "In embodiments, the most effective location for threat detection may be at the user's computer desktop end-point computer security facility 152." *Id.*, ¶ [0056].

Moreover, the end-point computer security facility can be configured with network access rules that limit network connections, thus creating network isolation. Thomas teaches, "In embodiments, the computer security facility 152 may be associated with network access control. The network access control may be related to securing the [host] 204A… prior to a network connection." *Id.*, ¶ [0080]. In addition, Thomas teaches that "the network access control may verify access rights for client facilities 144 from within the network or may verify access rights of computer facilities from external networks." *Id.*, ¶ [0043]. Thomas describes the network access control "may provide control over network connections," "may stop unauthorized, guest, or non-compliant systems from accessing networks, and may control network traffic that may not be bypassed from the client level," and "may control access to virtual private networks (VPN), where VPNs may be a communications network tunneled through another network, establishing a logical connection acting as a virtual network." *Id.*, ¶ [0029]. Based on the detailed disclosures in Thomas of the purpose and functionality of the end-point security facility 152, a POSITA would have understood the end-point security facility 152 is a firewall. Ex. 1008, ¶ 127.

In view of the foregoing, Thomas renders obvious a host-based firewall (**e.g., an end-point computer security facility 152**) executed on the computer system (**e.g., the physical computing machine 202 corresponding to the client 144**) is configured to implement network isolation (**e.g., network access control**) between the computer system (**e.g., the physical computing machine 202 corresponding to the client 144**) and the network (**e.g., the enterprise facility 102**).

1G. at least one device configured to implement at least one of a network firewall or a web proxy,

Thomas teaches at least one device (**e.g., the firewall 138 or the proxy server 142**) configured to implement at least one of a network firewall (**e.g., the firewall 138**) or a web proxy (**e.g., the proxy server 142**). Specifically, Thomas states that the firewall 138 "may be a hardware or software device that may be configured to permit, deny, or proxy data through a computer network that has different levels of trust in its source of data." Ex. 1006, ¶ [0056]. Thus, Thomas discloses the firewall 138 may be a network firewall or a web proxy. Furthermore, the firewall 138 is described as representing "boundaries between threat levels" and controlling "the flow of threats." *Id.* These statements teach the firewall 138 implements network isolation between untrusted network destinations and the networked computer system.

In addition, Thomas further teaches that the enterprise facility 102 may include a proxy server 142. *Id.*, ¶ [0052]. As is well known to a POSITA, proxy server is another term for a web proxy. Ex. 1008, ¶ 129. Accordingly, Thomas also teaches a separate device from the firewall 138 that is configured to implement a web proxy. *Id.*

In view of the foregoing, Thomas renders obvious at least one device (**e.g., the firewall 138 or the proxy server 142**) configured to implement at least one of a network firewall (**e.g., the firewall 138**) or a web proxy (**e.g., the proxy server 142**).

1H. wherein the device comprises a processor and a memory configured to implement network isolation between one or more untrusted network destinations and the networked computer system.

Thomas teaches wherein the device (**e.g., the firewall 138 or the proxy server 142**) comprises a processor and a memory configured to implement network isolation between one or more untrusted network destinations (**e.g., the Internet 154**) and the networked computer system (**e.g., the enterprise facility 102 and the threat management facility 100**).

Specifically, Thomas states that the firewall 138 "may be a hardware or software device that may be configured to permit, deny, or proxy data through a computer network that has different levels of trust in its source of data." Ex. 1006, ¶ [0056]. Also, Thomas discloses devices including proxy servers 142. *Id.*, ¶ [0052]. Relevant to both, Thomas states, "The methods or processes described above, and steps thereof, may be realized in hardware, software, or any combination of these suitable for a particular application. The hardware may include a general-

purpose computer and/or dedicated computing device. The processes may be realized in one or more microprocessors, microcontrollers, embedded microcontrollers, programmable digital signal processors or other programmable device, along with internal and/or external memory." *Id.*, ¶ [0100].

In view of the foregoing, Thomas renders obvious wherein the device (**e.g., the firewall 138 or the proxy server 142**) comprises a processor and a memory configured to implement network isolation between one or more untrusted network destinations (**e.g., the Internet 154**) and the networked computer system (**e.g., the enterprise facility 102 and the threat management facility 100**).

2. Claim 2

2. The networked computer system of claim 1, wherein the internal firewall is configured to prevent data from being communicated between the virtual system and the host system without an explicit user input.

Thomas in combination with Garg teaches wherein the internal firewall (**e.g., the end-point computer security facility 152 installed on the virtual computing machine monitor 208 or the virtual computing machine monitor 208 of Thomas as modified by Garg**) is configured to prevent data from being communicated between the virtual system (**e.g., the guest operating system 210B operating on virtual computing machine 204B**) and the host system (**e.g., the host operating system 210A operating on virtual computing machine 204A**) without an explicit user input (**e.g., user-input access rights through network access control**).

Thomas' guest computer security facility 152B can restrict communications over a network between the virtual system and the host system. Thomas teaches, "In embodiments, the computer security facility 152 may be associated with network access control. The network access control may be related to securing the [host] 204A and the virtual computing machine 204B prior to a network connection." *Id.*, ¶ [0080].

In addition, Thomas teaches that "the network access control may verify access rights for client facilities 144 from within the network or may verify access rights of computer facilities from external networks." *Id.*, ¶ [0043]. Thomas describes the network access control "may provide control over network connections," "may stop unauthorized, guest, or non-compliant systems from accessing networks, and may control network traffic that may not be bypassed from the client level," and "may control access to virtual private networks (VPN), where VPNs may be a

communications network tunneled through another network, establishing a logical connection acting as a virtual network." *Id.*, ¶ [0029]. Accordingly, the configurable access rights associated with the guest computer security facility 152B are explicit user inputs allowing and/or disallowing data from being communicated between systems in the networked computer system. Once configured by the user, the configurable access rights provide control over network traffic without further user input, until explicitly re-configured by the user. Ex. 1008, ¶ 136.

In view of the foregoing, Thomas in combination with Garg renders obvious wherein the internal firewall (**e.g., the end-point computer security facility 152 installed on the virtual computing machine monitor 208 or the virtual computing machine monitor 208 of Thomas as modified by Garg**) is configured to prevent data from being communicated between the virtual system (**e.g., the guest operating system 210B operating on virtual computing machine 204B**) and the host system (**e.g., the host operating system 210A operating on virtual computing machine 204A**) without an explicit user input (**e.g., user-input access rights through network access control**).

3. Claim 3

3. The networked computer system of claim 1, wherein the host system is configured to store data in a host memory space and the virtual system is configured to store data in a virtual memory space that is segregated from the host memory space.

Thomas teaches wherein the host system (**e.g., the host operating system 210A operating on virtual computing machine 204A**) is configured to store data in a host memory space (**e.g., the virtual memory 212A**) and the virtual system (**e.g., the guest operating system 210B operating on virtual computing machine 204B**) is configured to store data in a virtual memory space (**e.g., the virtual memory 212B**) that is segregated (**e.g., separately allocated**) from the host memory space (**e.g., the virtual memory 212A**).

For example, Thomas teaches, "The virtual computing machine 204A may include a host operating system 210A, a virtual memory 212A and a host configuration and state 214A." Ex. 1006, ¶ [0067]; FIG. 2.

Thomas further teaches, "The host operating system 210A may be associated with the virtual memory 212A. The virtual memory 212A may hold instructions related to host operating system 210A. The virtual memory 212A may also hold information related to host configuration and state information 214A. The host configuration and state information 214A may store the

information related to configuration such as operating system configuration information, firewall configuration, information application, configuration information, and the like." *Id.*, ¶ [0068]. Thomas further teaches, "The virtual computing machine 204B may include a guest operating system 210B, a virtual memory 212B, a guest configuration and state 214B and a guest computer security facility 152B, and the like." *Id.*, ¶ [0069]; FIG. 2. Thomas further teaches, "In addition, the guest operating system 210B may be store program instruction specific to it in the virtual memory 212B. The virtual memory 212B may store configuration and state information specific to the virtual computing machine 204B. In addition, the virtual memory 212B may be associated with the guest configuration and state facility 214B." *Id.*, ¶ [0070]. Thomas additionally teaches "The memory may be a physical memory, which may be allocated to the virtual memory 212A or to the virtual memory 212B." *Id.*, ¶ [0078].

In view of the foregoing, Thomas renders obvious wherein the host system (**e.g., the host operating system 210A operating on virtual computing machine 204A**) is configured to store data in a host memory space (**e.g., the virtual memory 212A**) and the virtual system (**e.g., the guest operating system 210B operating on virtual computing machine 204B**) is configured to store data in a virtual memory space (**e.g., the virtual memory 212B**) that is segregated (**e.g., separately allocated**) from the host memory space (**e.g., the virtual memory 212A**).

4. Claim 4

4. The networked computer system of claim 1, wherein malware introduced to the computer system is prevented from moving to another computer system of the networked computer system.

Thomas teaches wherein malware introduced to the computer system (**e.g., the physical computing machine 202 corresponding to the client 144**) is prevented from moving to another computer system (**e.g., the physical computing machine 202 corresponding to the server 142**) of the networked computer system (**e.g., the enterprise facility 102 and the threat management facility 100**).

Specifically, Thomas teaches providing "one of the plurality of virtual computing machine 204B as a protected environment. The protected environment may be used to isolate suspicious files that may have malware associated with them. For example, the protected environment provided by the virtual computing machine 204B may be used to isolate suspicious files from the virtual computing machine 204A and other guest virtual computing machines." *Id.*, ¶ [0093]. "In

addition, the network access control may secure the virtual computing machine 204A and the virtual computing machine 204B prior to making a network connection." *Id.*, ¶ [0087]. That is, the protected environment and/or the network access control may be used to prevent malware introduced to a virtual machine on the physical computing machine 202 from moving to another physical computing machine 202 associated, for example, with another client 144 or a server 142 of the enterprise 102.

In view of the foregoing, Thomas renders obvious wherein malware introduced to the computer system (**e.g., the physical computing machine 202 corresponding to the client 144**) is prevented from moving to another computer system (**e.g., the physical computing machine 202 corresponding to the server 142**) of the networked computer system (**e.g., the enterprise facility 102 and the threat management facility 100**).

5. Claim 5

5p. The networked computer system of claim 1, wherein the computer system is configured to:

See claim 1 above.

5A. communicate with the one or more untrusted network destinations via a first communication connection,

Thomas teaches wherein the computer system (**e.g., the physical computing machine 202 corresponding to the client 144**) is configured to: communicate with the one or more untrusted network destinations (**e.g., the Internet 154**) via a first communication connection (**e.g., through the threat management facility 100**).

For example, Thomas teaches that "if the mobile client facility 144 [were] to attempt to connect into an unprotected connection point, such as at a secondary location 108 that is not a part of the enterprise facility 102, the mobile client facility 144 may be required to request network interactions through the threat management facility 100, where contacting the threat management facility 100 may be performed prior to any other network action." *Id.*, ¶ [0060].

In view of the foregoing, Thomas renders obvious wherein the computer system (**e.g., the physical computing machine 202 corresponding to the client 144**) is configured to: communicate with the one or more untrusted network destinations (**e.g., the Internet 154**) via a first communication connection (**e.g., through the threat management facility 100**).

5B. communicate with one or more trusted network destinations via a second communication connection; and

Thomas teaches wherein the computer system (**e.g., the physical computing machine 202 corresponding to the client 144**) is configured to: communicate with one or more trusted network destinations (**e.g., other client facilities within the enterprise facility 102**) via a second communication connection (**e.g., through wired network facilities 148 or wireless network facilities 150 within the enterprise facility 102**).

For example, Thomas teaches, "Client facilities 144 within the enterprise facility 102 may be connected to the enterprise facility 102 network by way of wired network facilities 148 or wireless network facilities 150. Client facilities 144 connected to the enterprise facility 102 network via a wired facility 148 or wireless facility 150 may receive similar protection, as both connection types are ultimately connected to the same enterprise facility 102 network, with the same end-point computer security facility 152, and the same threat protected enterprise facility 102 environment." *Id.*, ¶ [0058].

In view of the foregoing, Thomas renders obvious wherein the computer system (**e.g., the physical computing machine 202 corresponding to the client 144**) is configured to: communicate with one or more trusted network destinations (**e.g., other client facilities within the enterprise facility 102**) via a second communication connection (**e.g., through wired network facilities 148 or wireless network facilities 150 within the enterprise facility 102**).

5C. enforce separation of the first communication connection from the second communication connection.

Thomas teaches wherein the computer system (**e.g., the physical computing machine 202 corresponding to the client 144**) is configured to: enforce separation of the first communication connection (**e.g., through the threat management facility 100**) from the second communication connection (**e.g., through wired network facilities 148 or wireless network facilities 150 within the enterprise facility 102**).

For example, Thomas teaches that "if the client facility's 144 end-point computer security facility 152 is unable to establish a secured connection to the threat management facility 100, the end-point computer security facility 152 may inform the user of such, and recommend that the connection not be made." *Id.*, ¶ [0060].

In view of the foregoing, Thomas renders obvious wherein the computer system (**e.g., the physical computing machine 202 corresponding to the client 144**) is configured to enforce separation of the first communication connection (**e.g., through the threat management facility 100**) from the second communication connection (**e.g., through wired network facilities 148 or wireless network facilities 150 within the enterprise facility 102**).

6. Claim 6

6. The networked computer system of claim 1, wherein the host-based firewall is configured to prevent lateral communication and movement of malware between the computer system and other devices on the networked computer system.

Thomas teaches wherein the host-based firewall (**e.g., an end-point computer security facility 152**) is configured to prevent lateral communication and movement of malware between the computer system (**e.g., the physical computing machine 202 corresponding to the client 144**) and other devices (**e.g., other clients 144 or the server 142**) on the networked computer system (**e.g., the enterprise facility 102 and the threat management facility 100**).

For example, Thomas states that "the end-point computer security facility 152, located on a computer's desktop" may "provide threat protection to a user." *Id.*, ¶ [0050]. Thomas further teaches, "The end-point computer security facility 152 may be an application loaded onto the computer platform or computer support component, where the application may accommodate the plurality of computer platforms and/or functional requirements of the component. For instance, a client facility 144 computer may be one of a plurality of computer platforms, such as Windows, Macintosh, Linux, and the like, where the end-point computer security facility 152 may be adapted to the specific platform, while maintaining a uniform product and product services across platforms." *Id.*, ¶ [0050]. Thomas also teaches, "In embodiments, the threat management facility 100, and associated end-point computer security facility 152, may provide seamless threat protection to the plurality of clients 144, and client facility 144 types, across the enterprise facility 102." *Id.*, ¶ [0051]. Thomas further teaches, "In embodiments, the most effective location for threat detection may be at the user's computer desktop end-point computer security facility 152." *Id.*, ¶ [0056].

Moreover, the end-point computer security facility can be configured with network access rules that limit network connections creating network isolation. Thomas teaches, "In embodiments, the computer security facility 152 may be associated with network access control. The network

access control may be related to securing the [host] 204A and the virtual computing machine 204B prior to a network connection." *Id.*, ¶ [0080].

In view of the foregoing, Thomas renders obvious wherein the host-based firewall (**e.g., an end-point computer security facility 152**) is configured to prevent lateral communication and movement of malware between the computer system (**e.g., the physical computing machine 202 corresponding to the client 144**) and other devices (**e.g., other clients 144 or the server 142**) on the networked computer system (**e.g., the enterprise facility 102 and the threat management facility 100**).

7. Claim 7

7. The networked computer system of claim 1, wherein the device is configured to prevent unauthorized communication between the computer system and the one or more untrusted network destinations.

Thomas teaches wherein the device (**e.g., the firewall 138**) is configured to prevent unauthorized communication (**e.g., permit, deny, or proxy data**) between the computer system (**e.g., the physical computing machine 202 corresponding to the client 144**) and the one or more untrusted network destinations (**e.g., the Internet 154**).

For example, Thomas teaches that the network firewall facility 138 "may be a hardware or software device that may be configured to permit, deny, or proxy data through a computer network that has different levels of trust in its source of data." *Id.*, ¶ [0056].

Thomas also explains that "an internal enterprise facility 102 network may have a high level of trust, because the source of all data has been sourced from within the enterprise facility 102. An example of a low level of trust is the Internet 154, because the source of data may be unknown. A zone with an intermediate trust level, situated between the Internet 154 and a trusted internal network, may be referred to as a 'perimeter network'. *Id.*, ¶ [0056].

In view of the foregoing, Thomas renders obvious wherein the device (**e.g., the firewall 138**) is configured to prevent unauthorized communication (**e.g., permit, deny, or proxy data**) between the computer system (**e.g., the physical computing machine 202 corresponding to the client 144**) and the one or more untrusted network destinations (**e.g., the Internet 154**).

8. Claim 8

8A. The networked computer system of claim 1, wherein the host-based firewall is configured to implement a first policy when the computer system is connected to the network and a second policy when the computer system is connected to another network,

Thomas teaches wherein the host-based firewall (**e.g., security facility 152**) is configured to implement a first policy when the computer system is connected to the network (**e.g., enterprise facility 102**) and a second policy when the computer system is connected to another network (**e.g., unprotected secondary location 108**).

Thomas explains that the computer system (e.g., the physical computing machine 202 corresponding to the client 144) "may be connected to a network either through a wired or a wireless connection." *Id.*, ¶ [0067]. Thomas further explains that a client 144 may connect to the enterprise facility 102 or to "an unprotected connection point, such as at a secondary location 108 that is not a part of the enterprise facility 102." *Id.*, ¶ [0060]. This teaches the client 144 can be connected to multiple different types of networks 102 and 108.

Thomas further explains that the host virtual machine 204A on the physical computing machine 202 includes a "host computer security facility 152A." *Id.*, ¶ [0068]. Likewise, the guest virtual computing machine 204B on the physical computing machine 202 includes "a guest computer security facility 152B." *Id.*, ¶ [0069]. The host computer security facility 152A and the guest computer security facility are each "associated with network access control" and "network access control may be related to securing the virtual computing machine 204A and the virtual computing machine 204B prior to a network connection." *Id.*, ¶ [0080].

Importantly, Thomas teaches that the host-based firewall (e.g., end-point computer security facility 152) may implement different policies depending on the network connection:

> In embodiments, the client facility's 144 end-point computer security facility 152 may manage actions in unprotected network environments such as when the client facility 144 is in a secondary location 108 or connecting wirelessly 150 to a non-enterprise facility 102 wireless internet 154 connection, where the end-point computer security facility 152 may dictate what actions are allowed, blocked, modified, or the like. For instance, if the client facility's 144 end-point computer security facility 152 is unable to establish a secured connection to the threat management facility 100, the end-point computer security facility 152 may inform the user of such, and recommend that the connection not be made. In the instance when the user chooses to connect despite the recommendation, the

> end-point computer security facility 152 may perform specific actions during or after the unprotected connection is made, including … restricting access to network and local resources, or the like. In embodiments, the end-point computer security facility 152 may perform specific actions to remediate possible threat incursions or policy violations during or after the unprotected connection.

Id., ¶ 0060.

Furthermore, Thomas also teaches:

> In an embodiment, the end-point computer security facility 152 may provide for a way to control access to the enterprise facility 102 networks. For instance, the enterprise facility 102 may want to restrict access to certain applications, networks, files, printers, servers, databases, or the like. In addition, the enterprise facility 102 may want to restrict user access under certain conditions, such as the user's location, usage history, need to know, job position, connection type, time of day, method of authentication, client-system configuration, or the like.

Id., ¶ [0043]. Thomas further teaches that the "network access rules and control may be responsible for determining if a client facility 144 application should be granted access to a requested network location" that may be on the same network as the facility or may be on another network. *Id.* In addition, "the network access control may verify access rights for client facilities 144 from within the network or may verify access rights of computer facilities from external networks." *Id.* Thomas thus teaches the end-point computer security facility 152 implements different threat protection policies, i.e., sets different access policies, based on the network infrastructure location. Ex. 1008, ¶ 168. Connecting to the enterprise facility 102 network versus the unprotected secondary location 108 network causes the end-point computer security facility 152 (e.g., the host-based firewall) to implement different protection policies, and access rights may be different based on whether the requested network location is on the same network as the facility or on another network. *Id.*

In view of the foregoing, Thomas renders obvious wherein the host-based firewall (**e.g., security facility 152**) is configured to implement a first policy (**e.g., access control**) when the computer system is connected to the network (**e.g., enterprise facility 102**) and a second policy (**e.g., access control**) when the computer system is connected to another network (**e.g., unprotected secondary location 108**).

8B. wherein the first policy permits one or more communications between the host system of the computer system and one or more resources on the network and

Thomas renders obvious wherein the first policy (**e.g., implemented by the end-point computer security facility 152**) permits one or more communications (**e.g., allowing access to network and local resources**) between the host system (**e.g., the host operating system 210A operating on virtual computing machine 204A**) of the computer system and one or more resources on the network (**e.g., requested network location**).

As discussed above, Thomas teaches "the end-point computer security facility 152 may provide for a way to control access to the enterprise facility 102 networks." Ex. 1006, ¶ [0043]. This may include, for example, allowing and/or restricting access to certain applications, networks, files, printers, servers, databases, etc. on the enterprise facility 102 based, for example, on the user's location or connection type. *See id.* That is, when the user makes a request from within the network, the first policy may allow access to the network resource.

In view of the foregoing, Thomas renders obvious wherein the first policy (**e.g., implemented by the end-point computer security facility 152**) permits one or more communications (**e.g., allowing access to network and local resources**) between the host system (**e.g., the host operating system 210A operating on virtual computing machine 204A**) of the computer system and one or more resources on the network (**e.g., requested network location**).

8C. the second policy blocks communications egressing from the host system of the computer system but allows communications egressing from the virtual system.

Thomas renders obvious wherein the second policy (**e.g., access control implemented by the end-point computer security facility 152**) blocks communications (**e.g., denies access to network and local resources**) egressing from the host system (**e.g., the host operating system 210A operating on virtual computing machine 204A**) of the computer system but allows communications (**e.g., allowing access to non-network resources**) egressing from the virtual system (**e.g., the guest operating system 210B operating on virtual computing machine 204B**).

As previously discussed, Thomas teaches "the end-point computer security facility 152 may provide for a way to control access to the enterprise facility 102 networks." *Id.*, ¶ [0043]. Thomas also teaches that implementing the different protection policies includes "restricting access to network and local resources" when "the client facility 144 is in a secondary location 108" that is unprotected. *Id.*, ¶ [0060]. Denying network access when requested from an unprotected

location but allowing non-network access even when requested from an unprotected location is a "second policy" that blocks communications, e.g., denies the requested access of a network location, from the host operating system 210A but allows communications, e.g., allows the requested access of a non-network location, from the guest operating system 210B.

All that remains then is the particular type of communications (ingress/egress) blocked or allowed by Thomas' network access control implemented by the end-point computer security facility 152: that the blocked communications from the host operating system 210A and the allowed communications from the guest operating system 210B are "egressing" communications. The end-point computer security facility 152 has a finite number of identified, predictable options for controlling egress traffic under the second policy:

1. block the host system + block the virtual system;
2. allow the host system + allow the virtual system;
3. block the host system + allow the virtual system; and
4. allow the host system + block the virtual system.

Given that there are only four possible egress traffic control choices for the second policy, it would have been obvious for a POSITA to try the four options and select the policy that blocks communications egressing from the host system while allowing communications egressing from the virtual system. A POSITA reading Thomas would have been motivated to block communications egressing from the host operating system 210A but allow communications egressing from the guest operating system 210B at least because doing so merely amounts to choosing from a finite number of identified, predictable solutions (i.e., the four possible combinations of allowing or blocking egress traffic from the host and virtual machines), with a reasonable expectation of success (i.e., there being only four predictable choices). Ex. 1008, ¶ 176; *see* MPEP § 2143(I)(E) (citing *KSR*, 550 U.S. at 421, 82 USPQ2d at 1397). Furthermore, a POSITA would have understood that blocking host egress, particularly to the network resources, while allowing virtual machine egress, particularly to the non-network resources, would protect the network from potential compromise while preserving virtual machine functionality by utilizing, for example, the protected environment provided by the virtual computing machine 204B as taught by Thomas. *See, e.g.*, Ex. 1006, ¶ [0093]; Ex. 1008, ¶ 176.

In view of the foregoing, Thomas renders obvious the second policy (**e.g., access control implemented by the end-point computer security facility 152**) blocks communications (**e.g., denies access to network and local resources**) egressing from the host system (**e.g., the host**

operating system 210A operating on virtual computing machine 204A) but allows communications (**e.g., allowing access to non-network resources**) egressing from the virtual system (**e.g., the guest operating system 210B operating on virtual computing machine 204B**).

9. Claim 9

9. The networked computer system of claim 1, wherein one or more applications or processes are configured to run in the virtual system, and wherein the one or more applications or processes running in the virtual system are configured to communicate with the one or more untrusted network destinations.

Thomas teaches wherein one or more applications or processes (**e.g., for retrieving e-mail**) are configured to run in the virtual system (**e.g., virtual computing machine 204B**), and wherein the one or more applications or processes (**e.g., for retrieving e-mail**) running in the virtual system (**e.g., guest operating system 210B operating on virtual computing machine 204B**) are configured to communicate with the one or more untrusted network destinations (**e.g., mail storage servers on the internet 154**).

For example, Thomas teaches that "the guest operating system 210B may [] store program instruction specific to it in the virtual memory 212B. The virtual memory 212B may store configuration and state information specific to the virtual computing machine 204B. In addition, the virtual memory 212B may be associated with the guest configuration and state facility 214B." Ex. 1006, ¶ [0070].

In addition, Thomas teaches, "In embodiments, the host configuration and state information 214A and guest configuration and state information 214B may be associated with an application software, with a software testing, and the like." *Id.*, ¶ [0090]. Thomas further teaches an example of a computing machine 202 "retrieving e-mail from an internet 154 service provider's mail storage servers 142." *Id.*, ¶ [0051].

In view of the foregoing, Thomas renders obvious wherein one or more applications or processes (**e.g., for retrieving e-mail**) are configured to run in the virtual system (**e.g., guest operating system 210B operating on virtual computing machine 204B**), and wherein the one or more applications or processes (**e.g., for retrieving e-mail**) running in the virtual system (**e.g., guest operating system 210B operating on virtual computing machine 204B**) are configured

to communicate with the one or more untrusted network destinations (**e.g., mail storage servers on the internet 154**).

10. Claim 10

10. The networked computer system of claim 1, wherein one or more applications or processes are configured to run in the host system, and wherein the one or more applications or processes running in the host system are configured to communicate with one or more devices on the network.

Thomas teaches wherein one or more applications or processes (**e.g., for requesting a service**) are configured to run in the host system (**e.g., host operating system 210A operating on virtual computing machine 204A**), and wherein the one or more applications or processes (**e.g., for requesting a service**) running in the host system (**e.g., host operating system 210A operating on virtual computing machine 204A**) are configured to communicate with one or more devices on the network (**e.g., server facility 142**).

For example, Thomas teaches, "The host operating system 210A may be a program loaded on to the computer during boot time and may control other programs, such as, applications, background processes, and the like.... The host operating system 210A may be associated with the virtual memory 212A. The virtual memory 212A may hold instructions related to host operating system 210A. The virtual memory 212A may also hold information related to host configuration and state information 214A. The host configuration and state information 214A may store the information related to configuration such as operating system configuration information, firewall configuration, information application, configuration information, and the like." *Id.*, ¶ [0068].

In addition, Thomas teaches, "In embodiments, the host configuration and state information 214A and guest configuration and state information 214B may be associated with an application software, with a software testing, and the like." *Id.*, ¶ [0090]. Thomas further teaches an example of a computing machine 202 "connecting to an enterprise facility 102 application server facility 142." *Id.*, ¶ [0051]. As described in Thomas, "A server facility 142, which may also be referred to as a server facility 142 application, server facility 142 operating system, server facility 142 computer, or the like, may be an application program or operating system that accepts client facility 144 connections in order to service requests from clients 144. The server facility 142 application may run on the same computer as the client facility 144 using it, or the server facility

142 and the client facility 144 may be running on different computers and communicating across the network." *Id.*, ¶ [0052].

In view of the foregoing, Thomas renders obvious wherein one or more applications or processes **(e.g., for requesting a service)** are configured to run in the host system **(e.g., host operating system 210A operating on virtual computing machine 204A)**, and wherein the one or more applications or processes **(e.g., for requesting a service)** running in the host system **(e.g., host operating system 210A operating on virtual computing machine 204A)** are configured to communicate with one or more devices on the network **(e.g., server facility 142)**.

11. Claim 11

11pre. A method of network isolation in a networked computer system, the method comprising:

To the extent the preamble is limiting, for the reasons previously discussed for element [1pre], Thomas teaches a networked computer system. Furthermore, for the reasons previously discussed for element [1F], Thomas teaches network isolation between a network and a computer system.

In view of the forgoing, Thomas renders obvious a method of network isolation in a networked computer system.

11A. providing a network and at least one computer system that is configured to connect to the network,

This claim element is substantively identical to elements [1A] and [1B]. Thus, it is rendered obvious by Thomas for the reasons previously discussed for elements [1A] and [1B].

11B. the computer system comprising a host system and a virtual system,

This claim element is substantively identical to element [1C]. Thus, it is rendered obvious by Thomas for the reasons previously discussed for element [1C].

11C. wherein the virtual system is a separate operating system or a software module operating on the computer system;

This claim element is substantively identical to element [1D]. Thus, it is rendered obvious by Thomas for the reasons previously discussed for element [1D].

11D. separating the host system from the virtual system using an internal firewall executed on the computer system;

For the reasons previously discussed for element [1E], Thomas teaches an internal firewall configured to separate the host system from the virtual system. Furthermore, the internal firewall is "executed on" the computer system: Thomas discloses the end-point computer security facility 152 may be an application loaded on a computer's desktop. *Id.*, ¶ [0050].

In view of the forgoing, Thomas renders obvious separating the host system from the virtual system using an internal firewall executed on the computer system.

11E. implementing network isolation between the computer system and the network using a host-based firewall executed on the computer system;

This claim element is substantively identical to element [1F]. Thus, it is rendered obvious by Thomas (optionally in view of Garg) for the reasons previously discussed for element [1F].

11F. providing at least one device configured to implement a network firewall or a web proxy; and

This claim element is substantively identical to element [1G]. Thus, it is rendered obvious by Thomas for the reasons previously discussed for element [1G].

11G. implementing network isolation, between one or more untrusted network destinations and the networked computer system, via the at least one device.

This claim element is substantively identical to element [1H]. Thus, it is rendered obvious by Thomas for the reasons previously discussed for element [1H].

12. Claim 12

12. The method of claim 11, wherein the internal firewall is configured to prevent data from being communicated between the virtual system and the host system without an explicit user input.

This claim is substantively identical to claim 2. Thus, it is rendered obvious by Thomas for the reasons previously discussed for claim 2.

13. Claim 13

13. The method of claim 11, further comprising:

the host system storing data in a host data storage; and

the virtual system storing data in a virtual data storage.

This claim recites "data storage" instead of "memory space" but otherwise is substantively identical to claim 3. Memory space is a type of data storage. Thus, this claim is rendered obvious by Thomas for the reasons previously discussed for claim 3.

14. Claim 14

14. The method of claim 11, further comprising preventing malware introduced to the computer system from moving to another computer system of the networked computer system.

This claim is substantively identical to claim 4. Thus, it is rendered obvious by Thomas for the reasons previously discussed for claim 4.

15. Claim 15

15. The method of claim 11, further comprising:

communicating with the one or more untrusted network destinations via a first communication connection;

communicating with one or more trusted network destinations via a second communication connection; and

enforcing separation of the first communication connection from the second communication connection.

This claim is substantively identical to claim 5. Thus, it is rendered obvious by Thomas for the reasons previously discussed for claim 5.

16. Claim 16

16. The method of claim 11, further comprising preventing, via the host-based firewall, lateral communication and movement of malware between the computer system and other devices on the networked computer system.

This claim is substantively identical to claim 6. Thus, it is rendered obvious by Thomas for the reasons previously discussed for claim 6.

17. Claim 17

17. The method of claim 11, further comprising the at least one device preventing unauthorized communication between the computer system and the one or more untrusted network destinations.

This claim is substantively identical to claim 7. Thus, it is rendered obvious by Thomas for the reasons previously discussed for claim 7.

18. Claim 18

18. The method of claim 11, further comprising:

implementing a first policy for the host-based firewall when the computer system is connected to the network, the first policy for the host-based firewall permitting one or more communications between the host system of the computer system and one or more resources on the network; and

implementing a second policy for the host-based firewall when the computer system is connected to another network, the second policy for the host-based firewall blocking communications egressing from the host system of the computer system but allowing communications egressing from the virtual system.

This claim is substantively identical to claim 8. Thus, it is rendered obvious by Thomas for the reasons previously discussed for claim 8.

19. Claim 19

19. The method of claim 11, further comprising running one or more applications or processes in the virtual system that are configured to communicate with the one or more untrusted network destinations.

This claim is substantively identical to claim 9. Thus, it is rendered obvious by Thomas for the reasons previously discussed for claim 9.

20. Claim 20

20. The method of claim 11, further comprising running one or more applications or processes in the host system that are configured to communicate with one or more devices on the network.

This claim is substantively identical to claim 10. Thus, it is rendered obvious by Thomas for the reasons previously discussed for claim 10.

III. SECONDARY CONSIDERATIONS

This Request demonstrates that the Challenged Claims of the '780 Patent are unpatentable as obvious in view of the prior art references. The Applicant did not identify any evidence of secondary considerations during prosecution. Further, the clear teachings in the prior art outweigh any supposed "secondary considerations." *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 36 (1966).

IV. DISCLOSURE OF CONCURRENT LITIGATION, REEXAMINATION, AND RELATED PROCEEDINGS

Based on information available to Requester, the '780 Patent is the subject of four co-pending District Court litigations as well as one *Petition for Inter Partes Review* before the Patent Trial and Appeal Board, as listed below. Requester is unaware of any prior reexaminations or other post-grant proceedings in which the '780 Patent is or has been involved.

- *Croga Innovations Ltd. v. International Business Machines Corporation*, 2:23-cv-00634 (E.D. Tex);
- *Croga Innovations Ltd. v. Cisco Systems, Inc.*, 2:24-cv-00065 (E.D. Tex);
- *Croga Innovations Ltd. v. Fortinet, Inc.*, 2:24-cv-00206 (E.D. Tex)
- *Croga Innovations Ltd. v. Amazon Web Services, Inc.*, 1:24-cv-00398 (W.D. Tex); and

- *Cisco Systems, Inc. v. Croga Innovations Ltd.*, IPR2024-01196 (PTAB).

A. This Request Should Not Be Denied Under 35 U.S.C. § 325(d)

As discussed in Section I.D, none of the prior art presented herein was cited or otherwise considered during prosecution. Thus, this Request should be granted for presenting substantial new questions of patentability. Furthermore, for the reasons discussed below, the substantial new questions of patentability presented by this Request do not fall under the exclusionary provisions of 35 U.S.C. § 325(d).

As noted above, IPR2024-01196 has been filed against the '780 Patent. However, IPR2024-01196 challenges claims 1-20 as being obvious in view of U.S. Patent 8,166,474 ("Delco"), U.S. Publication 2010/0077476 ("Adams"), and U.S. Patent 7,886,351 ("Dadhia"), and an institution decision has not been made. Although Thomas is briefly mentioned in IPR2024-01196, it serves merely as a background reference, being cited only twice. And furthermore, IPR2024-01196 relies upon Delco as the primary reference in its grounds of challenge. In this Request, however, Thomas is used as the primary reference and is combined with entirely different prior art (i.e., Garg) not relied upon in IPR2024-01196. Thus, the prior art presented herein was not previously presented to the Office, either during prosecution or as the basis of a challenge. Furthermore, the teachings found in the combination of this prior art and the arguments related to this prior art have also never been presented to the Office.

Requester also notes that the Office has previously rejected a 35 U.S.C. § 325(d) challenge and granted a reexamination request when different grounds than an IPR petition were used to challenge the same patent. *See in re: Sound View Innovations*, LLC, No. 2022-161, slip op. at 2-3 (Fed. Cir. Nov. 2, 2022) (nonprecedential) (*available at* https://cafc.uscourts.gov/opinions-orders/22-161.ORDER.11-22-2022_2037240.pdf). Similarly, because this Request presents different grounds than IPR2024-01196, the facts here weigh against discretionary denial.

Thus, this Request should not be rejected because the prior art and arguments presented in this Request are not "the same or substantially the same prior art or arguments" previously presented to the Office, and more specifically, because this Request applies a different combination of art in a distinct manner from those previously presented. *See* 35 U.S.C. § 325(d) ("In determining whether to institute or order a proceeding under this chapter, chapter 30, or chapter 31, the Director may take into account whether, and reject the petition or request because, the same or substantially the same prior art or arguments previously were presented to the Office."). This

Request does not rely on "the same or substantially the same prior art or arguments" as IPR2024-01196 because it presents new prior art and in a different combination than that presented in IPR2024-01196. Accordingly, this Request should be granted.

Finally, to the extent the Office is inclined to discretionarily deny this Request under 35 U.S.C. § 325(d), Requestor requests, in the alternative, that this Request be granted but the proceeding stayed pending the outcome of IPR2024-01196. In this way, the Office's resources may be conserved while still acknowledging the substantial new questions of patentability raised by this Request. *See* 35 U.S.C. § 304 ("If…a substantial new question of patentability…is raised, the determination will include an order for reexamination of the patent").

V. CONCLUSION

The Commissioner is hereby authorized to charge Deposit Account DA506990, under Docket No. UP-EPR-10601780, the *Ex Parte* Reexamination fee of $12,600 under 37 C.F.R. § 1.20(c)(2). Requester believes no other fee is due with this submission, however the Commissioner is hereby authorized to charge any fee deficiency or credit any over-payment to Deposit Account DA506990.

Please direct all correspondence in this matter to the undersigned.

Dated: August 28, 2024

Respectfully submitted,

By: */Stephen A. Cortiaus/*

Stephen A. Cortiaus
Reg. No. 74750
scortiaus@slatermatsil.com
T: 972-707-9018

SLATER MATSIL, LLP
17304 Preston Rd., Ste. 900
Dallas, Texas 75252

Counsel for Requester
Unified Patents, LLC

EXHIBIT C

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

AMAZON WEB SERVICES, INC.,

Petitioner,

v.

CROGA INNOVATIONS, LTD.,

Patent Owner.

Case: IPR2025-00884

U.S. Patent No. 10,601,780

PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 10,601,780

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(Continued)

Page

TABLE OF CONTENTS
(Continued)

Page

TABLE OF CONTENTS
(Continued)

Page

TABLE OF AUTHORITIES

Page(s)

CASES

TABLE OF AUTHORITIES
(Continued)

Page(s)

STATUTES AND RULES

OTHER AUTHORITIES

EXHIBIT LIST (37 C.F.R. § 42.63(E))

Exhibit	Description
1001	U.S. Patent No. 10,601,780
1002	Declaration of Nicholas Bambos, Ph.D.
1003	Curriculum vitae of Nicholas Bambos
1004	File History of U.S. Patent No. 10,601,780
1005	Jose Nazario, DEFENSE AND DETECTION STRATEGIES AGAINST INTERNET WORMS (Artech House, 2004) ("Nazario")
1006	U.S. Patent Publication No. 2010/0122343 to Ghosh et al., filed on September 14, 2009 and titled "Distributed Sensor for Detecting Malicious Software" ("Ghosh")
1007	William R. Cheswick et al., FIREWALLS AND INTERNET SECURITY, REPELLING THE WILY HACKER (Brian W. Kernighan et al., 2nd ed. 2003) ("Cheswick")
1008	Michael Rash, LINUX FIREWALLS: ATTACK DETECTION AND RESPONSE WITH IPTALBES, PSAD, AND FWSNORT (Christina Samuell & William Pollock eds., 2007) ("Rash")
1009	Steven E. Madnick & John J. Donovan, *An Approach to Information System Isolation and Security in a Shared Facility* (1973) ("Madnick")
1010	Robert P. Goldberg, *Survey of Virtual Machine Research*, 7(6) COMPUTER 34 (1974) ("Goldberg")
1011	Average Time to Trial for Patent Cases – Western District of Texas
1012	Average Time to Trial for Patent Cases – J. Albright
1013	Patent Assignment at Reel 065999, Frame 0444 (CROGA-AWS-00003324-28)
1014	Declaration of Rachel J. Watters

U.S. Patent No. 10,601,780 (EX1001, the "780 patent") relates to conventional technology for providing network security to a computer system connected to the Internet.[1] The claims require using firewalls and virtual machines—functionalities that were both already well known in the art—as security measures. For decades before the January 27, 2011 priority date of the 780 patent, it was already a well-known network security technique to combine firewalls with virtual machines, and the patent does not claim any novel way to make this combination. This Petition demonstrates that claims 1, 3, 7, 10, 11, 13, 17, and 20 of the 780 patent are unpatentable.

I. BACKGROUND

The 780 patent purports to address the issue of harmful data, such as "malicious software or malware," which can be downloaded onto a computer from the Internet "completely unintentionally and without the knowledge of the individual computer user." EX1001, 1:25-33. Malicious software, such as Internet worms,

[1] For the purposes of this proceeding only, Petitioner does not challenge the asserted priority date—January 27, 2011—of the 780 patent. EX1001, Cover.

have been a prevalent security risk "since the early days of the publicly available Internet." EX1005, pp. 67-68, FIG. 4.1 (reproduced below).[2]

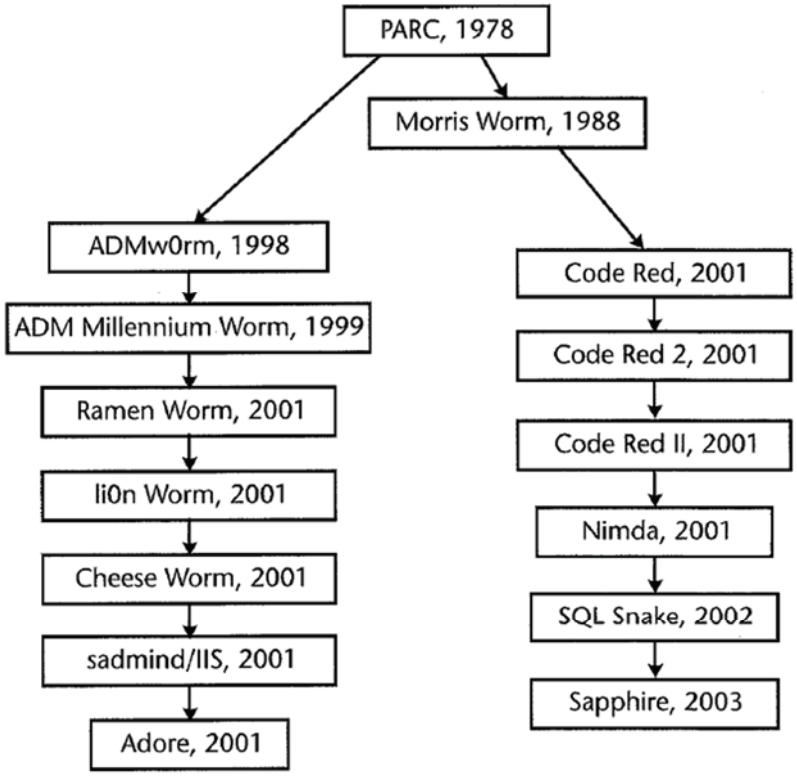


Figure 4.1 A Lineage of Internet Worms. This figure shows the lineage and classification of important Internet worms. From their beginnings with the research at Xerox PARC and then to the Morris worm, recent worms have focused on UNIX hosts (left-hand column) or Windows hosts (right-hand column). The arrows represent intellectual relationships, sometimes exemplified in code reuse between worms.

See also EX1002, ¶¶ 53-54. Malware "may be automatically downloaded to a user's computer through a webpage" or "via an attachment (typically a PDF) that is either received or downloaded from a website." EX1001, 1:42-62. Once downloaded,

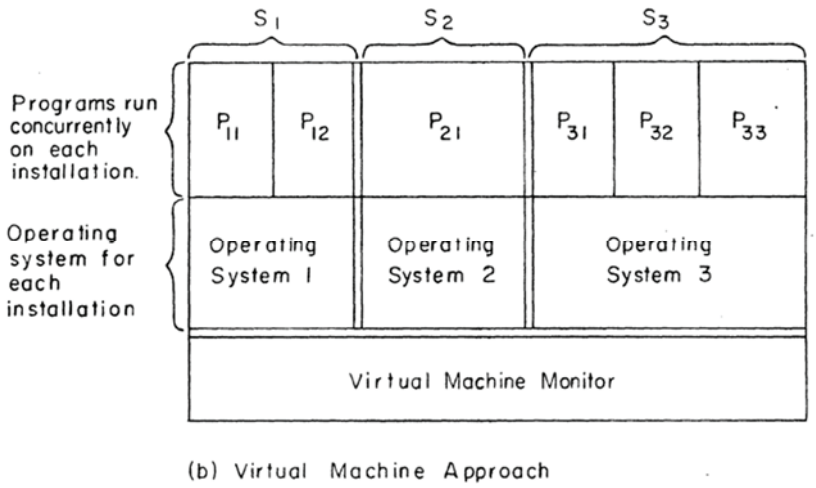
[2] Citations in this Petition are to Exhibit page numbers, not the page numbers of the reference itself, unless otherwise indicated.

malware can cause "malfunctions or inefficiency," including the possible loss of all data accessible to the computer system, and/or installation of various software that allows for remote control of the computer. *Id.*, 1:34-41. The 780 patent discusses protecting computer systems from the malicious attacks of Internet worms using virtual systems and firewalls—concepts that were well-known in the art before the January 27, 2011 priority date of the 780 patent.

1. Virtual Systems

From as far back as the early 1970s, virtualization techniques and virtual machines have been well known. EX1002, ¶ 53, ¶ 55. Virtualization allows several different operating systems, each in their own virtual machines, to run concurrently on a host operating system. EX1010, p. 3. Systems running virtual machines may include a hypervisor, which is sometimes referred to as a "virtual machine monitor," that creates and manages virtual machines on a host operating system. *Id.*; *see also* EX1001, 5:16-18; EX1006, [0032]; EX1002, ¶ 56. The hypervisor isolates each virtual machine under its control such that errors in the operation of one virtual machine will not affect other virtual machines or the underlying host operating system. EX1010, p. 10; EX1006, [0032]; EX1002, ¶¶ 56-57. With virtualization, multiple virtual machines can be run simultaneously on the same host computer, each with individual operating systems and different programs running on the

individual virtual machine. EX1009, Title, Abstract, FIG. 3 (reproduced, in part, below).



(b) Virtual Machine Approach

Accordingly, virtualization techniques and virtual systems can prevent malware infecting one application running on a computer from infecting the entire computer. EX1002, ¶¶ 56-57. This benefit was well known in the art long before the purported invention date of the 780 patent. EX1002, ¶¶ 55-58.

2. Multiple Layers of Firewalls

The 780 patent purports to mitigate the security risks of connecting a computer to the Internet by using virtualization in a networked computer system connected to the Internet in combination with firewalls at various levels within the system. EX1001, Abstract, 1:17-21. This approach is well documented in the prior art. *See, e.g.*, EX1002, ¶¶ 55-82. Network defenses are often placed at "various levels," so that "where an attack compromises one security device, another device may succeed in limiting additional damage." EX1008, p. 26. Combining different levels and

types of network security defenses increases the "the hurdles required to penetrate a system and cause damage." EX1005, p. 245; *see also infra* § II.A.1. And the concept of multiple layers "has been a vital component of security for thousands of years." EX1007, p. 24. Therefore, a person of ordinary skill in the art ("POSITA") would have known to secure a computer connected to Internet using multiple security layers. EX1002, ¶¶ 59-63.

Network firewalls and web-proxies were well known in the field as "readily deployable security tool[s]" for protecting multiple computers connected to the network. EX1005, p. 274. For example, Nazario (EX1005) is a computer security book published in 2004 that focuses on the history of internet worms and the tools developed to defend against them. A POSITA interested in network security could have considered this reference for its disclosures related to security mechanisms for computers and network systems. EX1002, ¶101; *see also infra* § III.B.1. Nazario describes network firewalls and web proxies among other examples of tools that prevent malware from entering or leaving a network by managing both the destinations and sources of network communications. EX1005, pp. 265-66; *see also* EX1002, ¶¶ 86-87. However, network firewalls and web proxies are not without weaknesses. For example, a network firewall may fail if the security policies enforced for individual computers connected to the network differ, or if traffic for the entire network exceeds the firewall's resource constraints. EX1005, pp. 245,

274. Because a network firewall handles traffic for several computers, it could become stressed due to a high number of active connections and fail due to resource constraints. *Id.*, p. 274.

Given the weaknesses of network firewalls, they are commonly combined with host-based firewalls, which protect individual computers on a network if malware penetrates or bypasses a network firewall. *Id.*, p. 245. Nazario teaches that the "biggest strength" of host-based firewalls is that "the security can be tailored for individual hosts" and "a security policy that is applicable for one host and not for another can be applied to satisfy the requirements of the other host." *Id.*, p. 261.

Furthermore, "host-based firewalls may be an appropriate solution to defending a set of [computers]," for example, in "situations where the default network security policy is absent but the security requirements for the host are more demanding." *Id.*, p. 245. But host-based firewalls also have weaknesses. While host-based firewalls protect individual computers, some malware—like Internet worms—affect the connection and bandwidth of the entire network. *Id.*, pp. 261-62. Therefore, network firewalls are often implemented in combination with host-based firewalls to protect against both large-scale attacks on the entire network and focused attacks on individual computers in the network.

Even the combination of network firewalls and host-based firewalls may still not provide complete protection for a networked computer system. Malicious actors

are constantly developing new malware capable of bypassing known security measures—such as network firewalls and host-based firewalls—so computer systems must also implement internal defenses to contain damage to specific parts of the computer. EX1007, p. 185. For example, in a security measure called "jailing," infected applications or programs are confined from transmitting or receiving data so that the infected application does not compromise the rest of the computer. *Id.* Nazario explains that security mechanisms internal to a computer isolate the services and processes running in an infected portion so that, in the event of compromise by malicious software, "it cannot take full control of the host and therefore cannot cause further damage." EX1005, p. 251. When employing these security mechanisms that are internal to a computer, if a service is executed in a virtual machine, an "attacker can probe and attack the service, but any compromise is contained to the virtual machine running on the host." *Id.*, p. 194.

That said, these internal security mechanisms also have their weaknesses. If malware breaks through them, it can infect the entire computer—including the host operating system—and even spread to other computer systems within the network. *Id.*, p. 252. Therefore, network firewalls and host-based firewalls are often implemented in combination with these internal defenses to prevent the spread of malware from an infected portion of a computer—such as a virtual machine—outward through the rest of the computer and/or network. *Id.*, p. 257.

Accordingly, a combination of internal defenses, host-based firewalls, and network firewalls can protect a computer system by (1) filtering incoming attacks from untrusted sources at both the network and host-level, (2) isolating malicious software from untrusted sources within the computer system, and (3) preventing the spread of malicious software from a compromised portion of a computer system through the rest of the computer system and network. A POSITA would have understood each of these layers of defense well before the time of the invention, and would have understood that defenses like these are employed in combination to protect computers connected to the Internet. EX1002, ¶¶ 64-82.

II. OVERVIEW OF THE 780 PATENT

A. Alleged Invention

The "Field of Invention" section of the 780 patent discusses the "protection of computer systems from injurious software that can be encountered while browsing or accessing the Internet" and "the protection of local Internet networks (LANS) that have access to the Inter[net]." EX1001, 1:17-21. The 780 patent purports to address this problem using a combination of existing solutions including virtual machines and the various security mechanisms discussed above. *Id.*; *see also* EX1002, ¶¶ 37-40.

1. Virtual Machines

The 780 patent describes a computer system running a "virtual guest system" (or virtual machine) in combination with other generic security mechanisms.

EX1001, 4:29-62. In addition to the virtual guest system, the computer system runs a "host operating system" and a "hypervisor" application. The host operating system is the "standard operating system" that allows the computer system to function "as is well known in the art," and stores information corresponding to all the software needed to operate the computer system. *Id.*, 7:31-41. The host operating system supports or cooperates with the hypervisor, which creates one or more virtual machines (the virtual guest systems). *Id.*, 8:2-20; EX1002, ¶ 39.

Virtual machines operate on a physical computer, for example a laptop or desktop, that supports one or more virtual machines as guest systems. EX1001, 3:25-28; EX1002, ¶39. Each virtual machine is a simulated computer that operates independently from the host system on the physical computer with a "virtual configuration different from the real hardware and software configuration of the computer 9." EX1001, 8:2-12. In FIG. 1, reproduced below, the host operating system ("Trusted Host OS 17") and the guest operating system ("Guest OS 13") are independent and separate components within the "workstation or laptop." The virtual guest system runs a browser which contacts the Internet freely via an Internet access connection that is "completely separate" from the host computer connection. *Id.*, 3:34-42; *see also id.*, 8:36-49.

However, as explained in this Petition, running a virtual machine on a computer system was already known when the 780 patent was filed. *See also* EX1002, ¶¶ 53-58; *supra* § I.1.

2. Firewalls

To protect the computer system against malware downloaded from the Internet, the 780 patent purports to isolate the host system and the virtual guest system from each other and the Internet using a combination of three generic "firewalls" located at different levels. EX1002, ¶¶ 37-39.

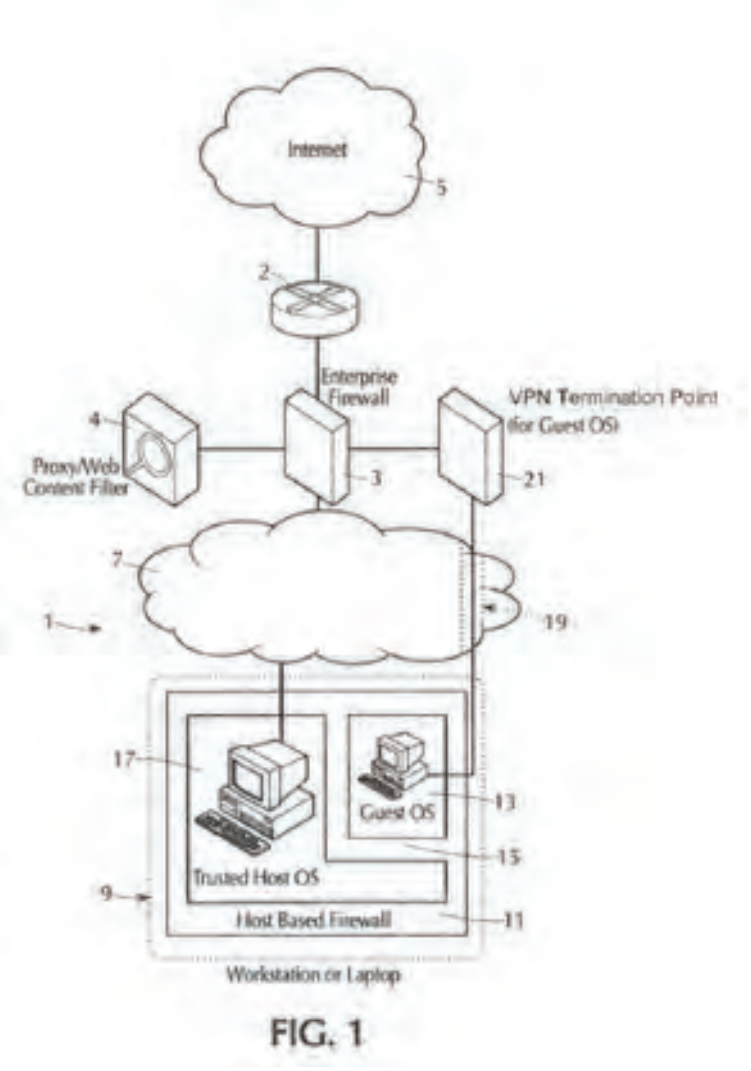


FIG. 1

FIG. 1 illustrates a "networked computer system" as claimed, which comprises a local area network ("LAN") [7] and a computer system [9]. EX1001, cls. 1, 11. A first firewall is implemented outside of the computer system as a network firewall [3] or web proxy [4] to limit access between the computer system [9] and the Internet [5]. *Id.*, 7:7-24, cls. 1, 11.

Two other firewalls are located within the computer system [9], which comprises a "host system" [17] and a "virtual system" [13]. EX1001, 7:49-52. The two firewalls within the computer system are an "internal firewall [15]" that limits access between the "host system" and the "virtual system," and a "host-based firewall [11]" that limits access between the "computer system [9]" and the LAN [7]. *Id.*; *see also id.*, 11:44-48 (an "internal firewall" that is "defined by the hypervisor that restricts the interaction between the host and guest.").

As explained in this Petition, providing network security by arranging these three firewalls—and the use of virtualization technology—in a networked computer system was already known well before the effective filing date of the 780. EX1002, ¶¶ 53-83; *supra* § I.2.

B. Prosecution History

The 780 patent was filed on March 2, 2018. EX1001, Cover. The United States Patent and Trademark Office ("USPTO") issued a first Office Action on June 5, 2018, rejecting the claims as unpatentable over U.S. Patent Publication No. 2007/0260873 to Hatfalvi ("Hatfalvi") in view of non-patent literature entitled "A Survey on Virtual Machine Security" ("Reuben"). EX1004, pp. 88-101. In response, the Applicant did not amend the claims but argued that Reuben does not "teach or suggest a host-based firewall executed on the computer system is configured to implement network isolation between the computer system and the

network..." *Id.*, p. 112 (emphasis omitted.). The USPTO maintained its rejection over Hatfalvi and Reuben, issuing a Final Office Action on March 19, 2019. *Id.*, pp. 126-40.

The Applicant then argued that these references do not "teach or suggest three distinct methods of isolation through a combination of an internal firewall, a host-based firewall, and a network firewall or web proxy as claimed." EX1004, p. 156. The USPTO issued a new non-final Office Action on July 25, 2019 that included only a double patenting rejection over claims of U.S. Patent No. 9,942,198. *Id.*, pp. 161-65. The Applicant filed a terminal disclaimer to obviate the double patenting rejection. The USPTO issued a Notice of Allowance on November 8, 2019. *Id.*, pp. 344-50. The 780 patent issued on March 24, 2020. EX1001, Cover.

C. Priority Date

The 780 patent purports to be a continuation of U.S. Patent No. 9,942,198, which claims priority to U.S. Provisional Application No. 61/436,932, filed on January 27, 2011 (the "effective filing date"). EX1001, Cover. For the purposes of this proceeding only, Petitioner does not dispute that the priority date is January 27, 2011.[3]

[3] Petitioner reserves the right to challenge the 780 patent's effective filing date.

This Petition shows the challenged claims were invalid as of the effective filing date.

III. IDENTIFICATION OF CHALLENGE

A. Statutory Grounds

Petitioner requests *inter partes* review and cancellation of the challenged claims on the following grounds:

Ground	Claims	Statutory Basis	Prior Art
1	1, 3, 7, 10, 11, 13, 17, 20	35 U.S.C. §103	Nazario and Ghosh

Ground 1 demonstrates that any differences between the claimed subject matter and the prior art are such that the subject matter as a whole would have been obvious to a POSITA at the time of the effective filing date of the 780 patent. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007).

B. Prior Art

1. Nazario (EX1005)

Nazario is titled "Defense and Detection Strategies Against Internet Worms," and is prior art under 35 U.S.C. § 102(a) and (b) (pre-AIA) because it was published in 2004, more than one year before the effective filing date of the 780 patent.[4]

[4] If Patent Owner argues the 780 patent is an AIA patent, Nazario would still qualify as prior art under post-AIA 35 U.S.C. § 102(a).

EX1005. Nazario has been publicly available since at least mid-January 2004. EX1014; *see also Cisco Sys., Inc. v. Centripetal Networks, Inc.*, IPR2018-01454, 2020 WL 1080533, at *17 (P.T.A.B. Mar. 5, 2020) (finding a textbook was authentic under Fed. R. Evid. 901(b) as an ancient document because it appeared to be over twenty years old "according to its copyright page" and the Board found "no suspicion about the authenticity of th[e] photocopy."). Nazario was not considered during the prosecution of the 780 patent. EX1004, FIG 4.1.

Nazario recognizes a need for "improved detection and defense measures" given the large number of network worms that existed, for example the Morris worm in 1988, Ramen in 2000, Code Red in 2001, Nimda in 2001, and the risk of more powerful worms in the future. EX1005, p. 164. To protect computers and networks against worms downloaded from the Internet, Nazario teaches various defenses including "host-based defenses" and "network defenses." *Id.*, Title, pp. 243, 261, 265, and 267.

Nazario's so-called "host-based defenses" execute on a host or provide protections tailored for an individual host. *Id.*, pp. 251-52. These defenses include "host-based firewalls" that protect the host against malicious attacks from the Internet. *Id.* If a computer is compromised by malicious software, Nazario describes "virtual hosts" that confine the damage to a small portion of the computer. *Id.*

Nazario's "network defenses" execute on a device that is part of a network. Nazario describes several examples of network defenses, including a "firewall device" to enforce a "network security policy" across multiple hosts connected via a network, "network firewalls" (also referred to as "perimeter firewalls") to isolate a "trusted" internal network from "untrusted" external networks, and "proxy-based defenses" (also referred to as "web-based proxies") to serve as intermediaries for data traveling over the network. EX1005, Title, pp. 243-44, 261, 265, 267-68, 283; *see also* EX1002, ¶¶ 86-87.

Nazario recognizes that a single defense mechanism cannot adequately meet the security requirements for an entire network, or even a single computer system connected to a network or the Internet, and explicitly teaches combining the defenses described above to improve overall computer and network security. EX1005, p. 271. This is because each defense "can fail in a number of ways, including misconfiguration, a weakness in the security application itself, or by using a channel different than the bypassed security guard was designed to defend." EX1005, p. 245. But, as Nazario explains, "[w]ith multiple defenses, the hurdles required to penetrate a system and cause damage increase." *Id.* Nazario describes the strengths and weaknesses of each type of defense and illustrates how multiple defenses may operate collectively to strengthen the total protection of a networked computer system.

As an example, Nazario teaches that a network-based firewall can be deployed across an entire network and provide security to multiple hosts connected to the network, but it can be unduly stressed or even fail since it processes traffic for entire network. *Id.*, p. 274. "Host-based firewalls" are "a complement to a network-based firewall" because they can act as "as a failover protection for the network-based firewall should any attack bypass that mechanism." *Id.*, p. 245. The strength of host-based firewalls is that they provide the ability to tailor security policies "for individual hosts" so that "a security policy that is applicable for one host and not for another can be applied." *Id.*, p. 261. But host-based firewalls do not scale well to large or decentralized networks and applying them on all hosts in a network can be a time and resource-consuming process. *Id.*, pp. 261-62.

To address this, Nazario suggests operating multiple defenses collectively to strengthen the overall protection of a networked computer system. For example, using a host-based firewall as a "complement" to a network-based firewall—the host-based firewall will act as "failover protection" should an attack from an untrusted source successfully bypass "the network-based firewall." *Id.*, p. 245. If an attack bypasses both a network firewall and a host-based firewall, Nazario suggests implementing other defenses on the computer to provide greater protection. For example, using virtualization technology to run a "virtual host" on the

computer—the virtual host will contain the damage so that the malicious software cannot take full control of the computer and cause further damage. *Id.*, p. 251.

Thus, Nazario explains how a network-based firewall, a host-based firewall, a virtual host, and other defenses can complement each other and suggests combining these defenses to improve overall network security. EX1002, ¶¶ 83-93.

2. Ghosh (EX1006)

Ghosh is a published patent application, U.S. Patent Publication No. 2010/0122343, and is prior art under § 102(a) and (e) (pre-AIA) because it was "known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention by the applicant for the 780 patent." 35 U.S.C. § 102(a). Ghosh was filed on September 14, 2009, and published May 13, 2010.[5] EX1006, Cover. Ghosh was not cited during the prosecution of the 780 patent. EX1004.

Ghosh describes techniques for using "virtualization technologies" to provide a "clean and isolated environment for instances of network applications" exposed to the Internet and susceptible to attacks from malicious actors, such as a web browser visiting a website hosting malicious software. *Id.*, [0004], [0007]-

[5] If Patent Owner argues the 780 patent is an AIA patent, Ghosh would still qualify as prior art under post-AIA 35 U.S.C. § 102(a).

[0009], [0022]; *see also* EX1002, ¶¶ 94-97. Ghosh describes how virtualization techniques separate a "guest OS" running inside a virtual machine from the "host OS" to prevent malware infecting a virtual machine from infecting the host OS. *Id.*, [0032]. Because of this separation, if the virtual machine becomes infected with malware, the malware must *also* penetrate the virtual machine monitor or the hypervisor before infecting the host OS. *Id.* Ghosh provides examples of systems that use virtual machines and hypervisors to support virtualization including VMware Workstation or Xen. *Id.*

Ghosh also describes running network applications within "containers" running on the guest operating system thereby "provid[ing] strong isolation between" applications, for example, "network applications" and "the host OS." *Id.*, [0038], FIG. 1 (reproduced below); *see also* EX1002, ¶ 98.

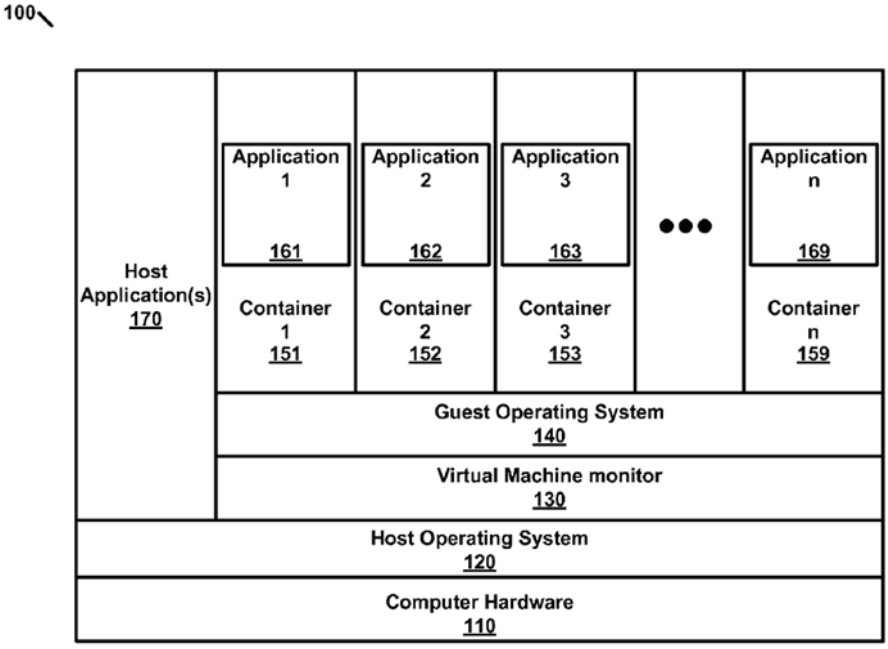


FIG. 1

IV. LEVEL OF ORDINARY SKILL IN THE ART

A person of ordinary skill in the art (POSITA) for the 780 patent would have had a bachelor's degree in electrical engineering, computer engineering, computer science, or the equivalent, and either (a) a master's degree in electrical engineering, computer engineering, computer science, or the equivalent, or (b) two years of work/research experience in computer systems and networks. EX1002, ¶ 48. Additional work/research experience may substitute for education and vice versa. *Id.*

V. CLAIM CONSTRUCTION

Claims subject to *inter partes* review are "construed using the same claim construction standard that would be used to construe the claim in a civil action under 3c5 U.S.C. § 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent." 37 C.F.R. § 42.100(b). Further, "[a]ny prior claim construction determination concerning a term of the claim in a civil action…that is timely made of record in the *inter partes* review proceeding will be considered." *Id.*

Petitioner applies the plain-and-ordinary meaning to all claim terms. 37 C.F.R. § 42.100(b); *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005)

(en banc).[6] For the purposes of this proceeding and the grounds presented, no claim term requires express construction.[7]

VI. GROUND 1: NAZARIO AND GHOSH

A. Motivation to Combine Nazario and Ghosh

A POSITA would have found it obvious to combine Nazario and Ghosh. EX1002, ¶¶ 101-105. Both references relate to protecting computers from malicious attacks over the Internet. EX1002, ¶ 102. Nazario explains that "malicious software [can] quickly lead to large scale problems" in "a network-centric computing model" where computing systems are connected to the Internet. EX1005, p. 31. Nazario discloses different types of security measures for defending against attacks from the

---

[6] In the related district court litigation, the parties agreed that the plain and ordinary meaning for the term "network isolation" is "restrict network communications." *Croga Innovations, Ltd. v. Amazon Web Services, Inc.*, Dkt. 34 at 4 (W.D. Tex. Apr 16, 2023). The parties also agreed in part that the plain and ordinary meaning for the terms "an internal firewall is configured to separate the host system from the virtual system" / "separating the host system from the virtual system using an internal firewall" is "a firewall that separates and restricts interactions between the virtual and host systems." *Id.*, Dkt. 34 at 9; Dkt. 37 at 9.

[7] Petitioner reserves the right to offer different claim constructions in other forums.

Internet. *See, e.g.*, EX1005, pp. 243, 245-46, 261, 265-69, 277-80, 283-85; EX1002, ¶¶ 85-87. Nazario also discloses that collectively implementing multiple security measures improves security by making it harder for the malicious software "to penetrate a system and cause damage." *See, e.g.*, EX1005, p. 245; EX1002, ¶¶ 88- 93. As one of those security measures, Nazario discloses using "virtual hosts"—virtual machines running on a computer connected to the Internet—such that if a service executing within a virtual machine is attacked, "any compromise is contained to the virtual machine" running on the computer. EX1005, p. 194; EX1002, ¶ 103. This contains the damage to the compromised portion of the computer and prevents malicious software from spreading and taking over the rest of the computer. EX1005, pp. 193-94, 302-03; EX1002, ¶ 103.

Similarly, Ghosh acknowledges that an end user's computer can be compromised due to malicious software hosted on the Internet. EX1006, [0004]; EX1002, ¶ 103. Like Nazario, Ghosh discloses protecting an end user's computer from "Internet-borne attacks" using "virtualization technologies" to confine damage to portion of the computer that has been compromised so that malicious software does not infect the rest of the computer. EX1006, [0007]-[0009], [0022]. [0032], [0038]; EX1002, ¶ 103. Ghosh discloses virtualization techniques which provide "strong isolation" by separating "a guest OS" that runs "inside the virtual machine" from the "host OS." EX1006, [0032], [0038]; EX1002, ¶ 103. This "strong

isolation" prevents malware from infecting the host OS if a virtual machine is attacked by malware since "the malware will still need to penetrate the virtual machine monitor to infect the host OS." EX1006, [0032]; EX1002, ¶ 103.

A POSITA would have found it obvious to combine the "virtualization technologies" of Ghosh with the "virtual hosts" of Nazario to enhance security of a computer connected to the Internet. EX1002, ¶¶ 101-104. The combination would include an isolated environment within a computer where an Internet-facing application would execute, with the intention of containing any damage if the application is compromised. *Id.* A POSITA would have known that the "strong isolation" of Ghosh would isolate damage caused by malicious software to just the "virtual host" running the Internet-facing application in Nazario, thereby preventing the malicious software from spreading and taking over the rest of the computer. *Id.* Accordingly, Ghosh's "strong isolation" techniques would be one of Nazario's multiple security measures applied collectively to a computer to protect it from being fully compromised by malicious software. *Id.* Additional motivations to combine the references are provided below.

A POSITA would have had a reasonable expectation of success in making this combination because it is a simple combination of prior art elements disclosed in Nazario and Ghosh, combined according to known methods to yield predictable results. EX1002, ¶ 105. A POSITA would have been able to make the combination

by simply implementing the virtual hosts disclosed in Nazario using the virtualization technologies disclosed in Ghosh. *Id.* The primary change to a system implementing the multiple defenses as taught by Nazario would be to implement the virtual hosts disclosed in Nazario using "virtualization technologies" taught in Ghosh. EX1005, pp. 162-63, 230; EX1006, [0032]. Virtual hosts as disclosed in Nazario run "the same or alternative operating systems" on a "host operating system" of a computer. EX1005, p. 252. Similarly, "virtual machine[s]" created by a hypervisor as disclosed in Ghosh run a "guest OS" on a "host OS." EX1006, [0032]; EX1002 ¶ 105. A POSITA would have known that the virtual host disclosed in Nazario can be created as a virtual machine using a hypervisor as disclosed in Ghosh. EX1002 ¶ 105. A POSITA would have predicted the result and would have had reasonable expectation of success because both Nazario and Ghosh describe the same technology—virtualization technology for creating a guest operating system over a host operating system—that can be used interchangeably. EX1002, ¶ 105.

B. Claim 1

For reasons explained below, Nazario in combination with Ghosh discloses or renders obvious claim 1.

[1.pre] "A networked computer system comprising:"

To the extent the preamble of claim 1 is limiting, Nazario discloses a networked computer system. EX1002, ¶¶ 107-109. Nazario discloses strategies to

defend a computing device connected to the Internet against malicious software such as "network-based worms coming from the Internet." EX1005, Title, pp. 115-42, 243-62; EX1002, ¶ 108. Nazario explains that these computing devices include "servers," "workstations," "desktops," "laptop[s]," "embedded devices," among others. EX1005, pp. 135-40, 304; EX1002, ¶ 108. Additionally, the computing devices may be part of an "Intranet system[]" that is connected by a network such as a "local area network" or the "Internet." EX1005, pp. 137-39; EX1002, ¶ 108. A POSITA would have understood Nazario's computing device connected to a network such as a "local area network" or the "Internet" to be a networked computer system. EX1002, ¶ 109.

[1.a] "a network"

Nazario discloses a network. EX1002, ¶¶ 110-112. Nazario discloses computing devices that are connected by a network such as a "local area network" or the "Internet." EX1005, pp. 135-37; EX1002, ¶ 111. A POSITA would have understood that a "local area network" and the "Internet" are each an example of a network. EX1002, ¶ 112.

[1.b] "at least one computer system configured to connect to the network, the computer system comprising a host system and a virtual system wherein the virtual system is a separate operating system or a software module operating on the computer system;"

Nazario discloses this limitation or renders it obvious. EX1002, ¶ 113-116. In the 780 patent, a computer connected to a network runs a host operating system

("Host OS") and a guest operating system ("Guest OS"). EX1001, FIGs. 1, 2; EX1002, ¶¶ 39-40. The 780 patent defines the claimed "host system" as "an operating system and one or more program applications." EX1001, 3:56-58 ("Each computer station operates as *a host system* according to stored data *corresponding to an operating system and one or more program applications*.") (emphases added). One such program application is a "hypervisor" that "creates a virtual machine environment" for guest systems. *Id.*, 5:16-18 ("Also operating on the host computer is a *hypervisor* system that *creates a virtual machine environment that is separate from the host* computer's operating system.") (emphases added). Thus, in the 780 patent, the Host OS, including a hypervisor and any additional software applications running on the Host OS, constitutes the "host system" and the Guest OS constitutes the "virtual system." EX1001, 7:25-8:12, 11:39-44, FIGs. 1, 2; EX1002, ¶ 39.

Nazario discloses a computer connected to a "local area network" or the "Internet." EX1005, pp. 135-37; EX1002, ¶ 114. Nazario explains that the computer accesses the Internet using "network client applications" such as the "Web browser Internet Explorer" or a "Messenger client." EX1005, p. 139; EX1002, ¶ 114. A POSITA would have understood that Nazario's computer accessing the Internet using a network client application is "at least one computer system configured to connect to the network." EX1002, ¶ 114.

The computer system in Nazario includes both "a host system and a virtual system." EX1002, ¶¶ 115-116. Nazario discloses a computer running a "host operating system" with virtual system images residing in "memory partitioned from the host operating system." EX1005, p. 252. Nazario explains this separation allows a "single" "host operating system" to support "several guest installations." *Id.* A POSITA would have understood that applications running in the host operating system would support these guest installations, or virtual system images. EX1002, ¶ 115. A POSITA would have thus understood that Nazario's host operating system and the applications running in the host operating system constitute the claimed "host system." *Id.*

Nazario further discloses that these virtual system images, which Nazario calls "virtual hosts," have separate operating systems because they may have "the same or alternate operating systems" as the host system. EX1005, p. 252; EX1002, ¶ 116. These virtual system images function to isolate applications running within them that could be exposed to malicious software from the Internet, thereby protecting the host system from attacks. EX1005, p. 252; EX1002, ¶ 116. A POSITA would have understood that Nazario's virtual system image, which has a guest operating system that is separate from the host system, corresponds to the claimed "virtual system." EX1002, ¶ 116.

Nazario thus discloses or renders obvious "at least one computer system configured to connect to the network, the computer system comprising a host system and a virtual system wherein the virtual system is a separate operating system or a software module operating on the computer system."

[1.c] "wherein an internal firewall is configured to separate the host system from the virtual system in the computer system,"

Nazario alone and/or in combination with Ghosh discloses this limitation or renders it obvious. EX1002, ¶¶ 117-124.

Nazario provides various "defense measures" to protect computer systems from malicious attacks on the Internet. *E.g.*, EX1005, pp194-95, 243-62, 265-69, 277-80, 283-85, 289-91; *see also* EX1002, ¶¶ 85-92. As one defense measure, Nazario discloses mechanisms to "separate the host system from the virtual system in the computer system." EX1001, cl. 1; EX1005, pp. 194-95, 251-53; EX1002, ¶¶ 118-119. This defense measure contains potential damage to a portion of the computer system that has been compromised (i.e., the virtual system) to prevent malicious software from spreading and taking over the rest of the computer system, including the host system, which is separated from the compromised portion. EX1005, pp. 244, 251-52; EX1002, ¶¶ 118-119. Nazario's "virtual hosts"—virtual machines running on a computer connected to the Internet—act as "logical jails": if a service or application executing within a virtual machine is attacked, "any compromise is contained to the virtual machine" and does not spread to the host

system. EX1005, p. 194; EX1002, ¶ 119. A POSITA would have understood that the virtual machines described in Nazario are separate from the host operating system running on the computer system. EX1002, ¶ 119. Furthermore, a POSITA would have known that virtual machines are created by hypervisors—this was well understood in the art since at least the 1970s. EX1002, ¶ 119; *see also supra* § I.1. As the 780 patent describes, "host and guest systems" are separated by an "internal firewall" that is "defined by the hypervisor that restricts the interaction between the host and guest." EX1001, 11:44-48. Thus, a POSITA would have implemented the virtual machine of Nazario using a hypervisor, which would have also acted as an "internal firewall." EX1002, ¶ 119.

Ghosh also provides an explanation of how virtualization can achieve the same goal of preventing the spread of malicious software that has infected a virtual machine to the rest of the computer system. EX1002, ¶¶ 120-121. Ghosh discloses protecting an end user's computer from "Internet-borne attacks" using "virtualization technologies" to confine damage to the portion of the computer that has been compromised; in this way the malicious software cannot infect the rest of the computer. EX1006, [0004], [0007]-[0009], [0022]-[0023], [0032]; EX1002, ¶ 120. As one example of virtualization technology, Ghosh discloses a "virtual machine monitor or hypervisor" which implements virtual machines in a computer system. EX1006, [0032]; EX1002, ¶ 120. Ghosh explains that in a virtual machine

created by the virtual machine monitor, "[t]he OS running inside the virtual machine is called the guest OS, and the original OS is called host OS." EX1006, [0032]; EX1002, ¶ 120. Ghosh further explains that the "virtual machine monitor provides the separation between the guest OS and the host OS." EX1006, [0032]. This separation creates a "strong isolation" between the guest OS and the host OS so that "even if the guest OS kernel is compromised, the malware will still need to penetrate the virtual machine monitor to infect the host OS." *Id.* Accordingly, a POSITA would understand the "virtual machine monitor" of Ghosh separates and restricts interactions between the host OS and guest OS thereby preventing an infection in the guest OS from spreading to the host OS. EX1002, ¶ 120.

In the 780 patent, "host and guest systems 25 and 27 are separated by an internal firewall 29 defined by the hypervisor." EX1001, 11:44-45. The Type 2 "virtual machine monitor or hypervisor" of Ghosh performs this same separation: it acts as "an internal firewall configured to separate the host system from the virtual system in the computer system." EX1001, cl. 1; EX1006, [0032]; EX1002, ¶ 120.

Ghosh also teaches running "virtual environments" called "containers" for securely running an application "inside a container." EX1006, [0038]. If the application running in a container is compromised, the "malicious code or intruders in the containers" are not "granted unfettered access to the host operating system;" which prevents the infection from spreading to the host operating system. EX1006,

[0041]; *see also id.*, [0039]. This "provides strong isolation between network applications" that are exposed to the Internet and "the host OS." *Id.*, [0032], [0038]. A POSITA would have understood or found it obvious that running virtual environments in containers also functions as an "internal firewall" mechanism that separates the applications running in the containers from the host OS of the computer. *Id.*; EX1002, ¶ 121.

As explained in Section VI.A, *supra*, a POSITA would have understood Nazario and Ghosh to disclose compatible defense measures, including measures using virtualization technologies. *See also* EX1002, ¶¶ 101-105, 122-123. With respect to this "internal firewall" limitation, a POSITA would have been motivated to modify the computer system described in Nazario—which includes virtual machines—to incorporate the "virtual machine monitor or hypervisor" and/or containers of Ghosh. EX1002, ¶¶ 122-123. This modification would further allow Nazario to achieve its objective of "minimiz[ing] any damage an attacker will make" and "prevent[ing] attacks that are able to break out of the" confined area of the computer system. EX1005, p. 251; EX1002, ¶¶ 122-123. As modified, the "virtual machine monitor or hypervisor" and/or containers of Ghosh would provide a "strong isolation" between the "host operating system" and the "virtual host" of Nazario such that the malicious software infecting the "virtual host" would not be able to penetrate the "host operating system." EX1005, p. 252; EX1006, [0032]; EX1002,

¶¶ 122-123. This would limit damage to a compromised portion of the computer system, preventing the malicious software from spreading and taking over the rest of the computer as intended by Nazario. EX1002, ¶¶ 122-123.

This modification is a combination of prior art elements disclosed in Nazario and Ghosh according to known methods to yield predictable results. EX1002, ¶ 124. Nazario discloses the use of virtual machines on a computer system connected to the Internet, so-called "virtual hosts," as a security measure to protect the computer against malicious attacks from the Internet. EX1005, pp. 194, 251; EX1002, ¶ 119. Likewise, Ghosh discloses a known method to implement virtual machines on a computer system—using a "virtual machine monitor or hypervisor," which protects against malicious attacks. EX1006, [0032]; EX1002, ¶ 120; *see also supra* §§ I.1, III.B.2. Ghosh further teaches the use of containers to protect against malicious attacks from the Internet. EX1006, [0038]; EX1002, ¶ 121; *see also supra* § III.B.2. The combined system would operate in an expected way to achieve expected results, with the "virtual machine monitor or hypervisor" serving as a barrier between the host operating system and the virtual machine and/or containers serving to contain damage inside themselves to prevent the spread of malware to the host system. EX1002, ¶ 124. A POSITA would have had a reasonable expectation of success making this combination because using a virtual machine monitor or hypervisor and/or containers in this way was conventional. *Id.*

Nazario alone and/or in combination with Ghosh thus discloses or renders obvious "wherein an internal firewall is configured to separate the host system from the virtual system in the computer system."

[1.d] "a host-based firewall executed on the computer system is configured to implement network isolation between the computer system and the network;"

Nazario discloses this limitation. EX1002, ¶¶125-128. As explained above, Nazario discloses using various security measures collectively to protect a computer from malicious attacks over the Internet. *Supra* § III.B.1. These security measures include "host-based" security measures, such as "host-based firewalls," for protecting a computer against "network-based worms." *Id.*; EX1005, pp. 243-46; EX1002, ¶ 125.

The "host-based firewalls" disclosed in Nazario execute on the computer systems they protect. EX1002, ¶¶ 126, 128. And as Nazario explains, a "host-based firewall" may be located on a "workstation" or "desktop" connected to the network. EX1005, pp. 245-47; EX1002, ¶¶ 126. To provide a "deeper entrenchment of the defenses"—and to serve as "a complement to a network-based firewall"—these "host-based firewalls" act "as a failover protection for the network-based firewall should any attack bypass that mechanism." EX1005, p. 245; EX1002, ¶¶ 125. To help protect against a worm that penetrates a network firewall, a POSITA would have known that these "host-based firewalls" would execute on the computer

systems they protect, creating a "secure Internet workstation." EX1005, pp. 245-47; EX1002, ¶¶ 127-128.

Nazario teaches that "host-based firewalls" represent "an appropriate solution" for defending "hosts." EX1005, p. 245; EX1002, ¶ 126. A POSITA would have understood or found it obvious that a host-based firewall of Nazario would be based in the host operating system of the computer "workstation" or "desktop." EX1002, ¶¶ 125-128.

Nazario's host-based firewalls provide isolation between the network and the computer systems they protect. EX1002, ¶¶ 125-128. Nazario teaches the "host-based firewalls" "can help prevent a network worm from entering a system." EX1005, p. 246; EX1002, ¶ 125. A POSITA would have understood that the network worm would attempt to enter the computer system from the network. EX1005, pp. 245-46; EX1002, ¶ 125. Nazario discloses several methods to apply the "host-based firewall" defense measure to the computer system: adding network addresses to the list of blocked addresses; allowing access to only certain network ports and their associated services while blocking others; applying a default deny policy for access by network sources on the network except allowing access by only certain network addresses; and using antivirus software that detects and removes worms from the computer system. EX1005, pp. 245-46; EX1002, ¶ 127. The host-based firewall disclosed in Nazario therefore provides a barrier and prevents a

network worm from entering the computer system. EX1005, p. 245; EX1002, ¶ 127. Accordingly, the host-based firewall disclosed in Nazario provides "network isolation between the computer system and the network." EX1002, ¶128.

Nazario thus discloses "a host-based firewall executed on the computer system is configured to implement network isolation between the computer system and the network."

[1.e] "at least one device configured to implement at least one of a network firewall or a web proxy, wherein the device comprises a processor and a memory configured to implement network isolation between one or more untrusted network destinations and the networked computer system."

Nazario discloses this limitation. EX1002, ¶¶ 129-138. In Nazario, a "network-based firewall" is one of multiple security measures collectively applied to protect a computer from malicious attacks over the Internet. *See* EX1005, pp. 245-46 (explaining applying network firewalls as a first line of defense against network worms and that "[h]ost-based firewalls are a complement to a network-based firewall"), pp. 265-74 (describing network firewalls); EX1002, ¶¶ 85-90.

Nazario discloses two types of network firewalls: firewalls on the perimeter of a network and firewalls built on proxy servers in the network. EX1005, pp. 265-74; EX1002, ¶¶ 130-136. A network firewall placed "on the border of a network," which Nazario calls a "perimeter firewall," was a common defense mechanism used to provide network security by creating a boundary within which internal network policies could be enforced. EX1005, pp. 268-69; EX1002, ¶ 130. And a firewall

built on a proxy server—an intermediate system inside the network that brokers communications between network participants—was a defense mechanism known to provide security by enforcing communications policies. EX1005, pp. 277-78; EX1002, ¶¶ 134-135. Nazario specifically identifies "Web proxies" as a popular type of proxy server "not only for content screening but also for performance reasons." EX1005, p. 283; EX1002, ¶ 136.

Nazario also discloses examples of "firewalling devices" capable of implementing network firewalls and proxies. EX1005, pp. 266-68. Exemplary "firewalling devices" include "Cisco IOS-based routers," "dedicated firewall device[s]" such as "Cisco PIX," "Juniper routers," and "a filtering host" built using an "IP Filter (IPF) tool." EX1005, pp. 267-68; EX1002, ¶ 131. The "[w]eb-based proxies" of Nazario can also be implemented on application gateway devices. EX1005, pp. 277, 283; EX1002, ¶ 134. A POSITA would have understood that each of these exemplary firewalling devices and application gateway devices would comprise a processor and memory configured to implement their respective security functions. EX1002, ¶¶ 131, 136. As a result, Nazario meets those limitations too.

The network firewalls disclosed by Nazario meet the limitation "to implement network isolation between one or more untrusted network destinations and the networked computer system." *See, e.g.*, EX1002, ¶ 137. Nazario teaches that "perimeter firewalls" isolate "a trusted internal network" from "untrusted" "external

networks." EX1005, pp. 268-69; EX1002, ¶131. This isolation can be achieved using a "packet filter," a type of firewalling device that "determin[es] the passage or rejection" of each packet in a communications stream. EX1005, p. 266; EX1002, ¶ 133. Nazario gives examples of filtering statements and rules implemented in the packet filter to "allow" or "block" network traffic between "trusted internal network" and "untrusted" "external networks," respectively. EX1005, pp. 267-68; EX1002, ¶¶ 132-133. A POSITA would have known that this operation of the perimeter firewall in Nazario implements network isolation between "a trusted internal network," like the claimed "networked computer system," and "untrusted" "external networks," like the claimed "one or more untrusted network destinations." EX1001, cl. 1; EX1002, ¶ 133.

The "proxy server" disclosed in Nazario also "implement[s] network isolation between one or more untrusted network destinations and the networked computer system." EX1002, ¶¶ 135, 137. The proxy server is an "intermediate system for a network connection" that "receives a request for a network action" from a client and interacts with the destination such that "[a]t no time do the client and final destination make direct contact." EX1005, p. 277; EX1002, ¶135. Accordingly, a "proxy server" provides isolation between clients sending requests and servers processing the requests. EX1002, ¶135. A POSITA reading Nazario would also understand that the client sending an outgoing request would be the "networked

computer system" and the target of an outgoing request would be the "untrusted network destination." EX1002, ¶135. Accordingly, Nazario discloses a device configured to implement a web proxy that provides "network isolation between one or more untrusted network destinations and the networked computer system." EX1002, ¶137.

Nazario thus discloses "at least one device configured to implement at least one of a network firewall or a web proxy, wherein the device comprises a processor and a memory configured to implement network isolation between one or more untrusted network destinations and the networked computer system."

C. Claim 3: "The networked computer system of claim 1, wherein the host system is configured to store data in a host memory space and the virtual system is configured to store data in a virtual memory space that is segregated from the host memory space."

Nazario in combination with Ghosh discloses or renders obvious claim 1, from which claim 3 depends. *Supra* § VI.B. Nazario discloses or renders obvious claim 3. EX1002, ¶¶ 139-143.

As discussed in relation to 1.b, Nazario discloses a computer system that includes a host system and a virtual system, wherein the virtual system is a separate operating system or a software module. *See supra* § VI.B.[1.b]; EX1002, ¶¶ 114-116. Nazario also explains that the computer system runs a host operating system, which is part of the host system. EX1005, p. 252.

Nazario describes segregated memory spaces used by the host system and virtual systems. EX1002, ¶¶ 140-141. The virtual systems are "full system images that reside in memory *partitioned from* the host operating system." EX1005, p. 252 (emphasis added); EX1002, ¶ 140. A POSITA would understand "partitioned" memory to be segregated memory, such that the virtual system is not configured to store data in the same memory space as the host system. EX1002, ¶¶ 140-141. Furthermore, a POSITA would have found it obvious to provide segregated memory space for the virtual and host systems. EX1002, ¶141. This is because, as explained in Nazario, a shared memory space increases the risk of an infectious attack. EX1005, p. 252 ("For example, if two processes share a common library with shared memory segments, an attacker may abuse this overlapping access to begin control of the process that has been initiated outside of the restricted area."); EX1002, ¶ 140.

Accordingly, a POSITA would have found it obvious based on the disclosure of Nazario that a host system is configured to store data in a host memory space and the virtual system is configured to store data in a virtual memory space that is segregated from the host memory space. EX1002, ¶ 142. Thus, Nazario discloses or renders obvious claim 3.

D. Claim 7: "The networked computer system of claim 1, wherein the device is configured to prevent unauthorized communication between the computer system and the one or more untrusted network destinations."

Nazario in combination with Ghosh discloses or renders obvious claim 1, from which claim 7 depends. *Supra* § VI.B. Nazario discloses or renders obvious claim 7. EX1002, ¶¶ 144-148.

As discussed in 1.e, the network firewall of Nazario acts as the claimed "device." *See supra* § VI.B.[1.e]. The network firewall allows or blocks network traffic between "trusted internal network" and "untrusted" "external networks." *Id.*; EX1005, pp. 267-69; EX1002, ¶ 145. Additionally, the network firewall "enforce[s] a network security policy" that represents "authorization to establish communications between two endpoints." EX1005, p. 265; EX1002, ¶ 145. Accordingly, a POSITA would have found it obvious that one of the endpoints would be a computer on the trusted internal network and the other endpoint would be a computer on the untrusted external network. EX1002, ¶ 145. A POSITA would have also known that the computer on the trusted internal network would be the claimed "computer system" of the "networked computer system" and a computer on the untrusted external network would be the claimed "untrusted network destination." *Id.*

Nazario also discloses that the network firewall implements both "[i]nbound and outbound rules." EX1005, p. 270; EX1002, ¶ 146. An "outbound firewall

enforces policies on traffic as it leaves the network." EX1005, p. 270; EX1002, ¶ 146. Thus, a POSITA would have known that outbound security policies are applied to traffic that leave from the endpoint on the trusted internal network to go to the endpoint on the untrusted external network. EX1002, ¶ 146. Accordingly, a POSITA would have known that the outbound security policies are applied to the traffic that leave from the claimed "computer system" to go to the claimed "untrusted network destination." *Id.*

Furthermore, Nazario explains that the network firewall "protect[s] services from being viewed by unauthorized parties." EX1005, p. 266; EX1002, ¶ 145. A POSITA would find it obvious that unauthorized parties would be the computers on the external untrusted network, i.e., the claimed "one or more untrusted network destinations." EX1002, ¶ 145. A POSITA would have also known that communications from unauthorized parties would be the claimed "unauthorized communications" and a device that protects services from being viewed by unauthorized parties would "prevent unauthorized communications."[8] EX1002,

[8] Nazario provides examples of network firewall devices that implement network policies such as "Cisco IOS-based router[]" that "*uses access-list* (ACL) statements, *access-group* statements and rules to manage traffic decisions or a "Cisco PIX product" that "features a filtering statement in addition to the *access-list* and *access-*

¶¶ 145, 147. A POSITA would thus have found it obvious that the network firewall of Nazario would prevent unauthorized communication from the unauthorized parties on the external untrusted network to the computer on the trusted internal network. EX1002, ¶¶146-147. Accordingly, a POSITA would have known that the network firewall of Nazario would prevent unauthorized communication from the claimed "one or more untrusted network destinations" to the claimed "computer system." EX1002, ¶¶ 145-147.

Because Nazario implements perimeter firewall security policies in both directions, a POSITA would have also understood that the network firewall of Nazario prevents unauthorized communication *between* the "one or more untrusted network destinations" and the "computer system." EX1002, ¶ 146. Thus, Nazario discloses or renders obvious claim 7.

---

group statements" that "would block any TCP traffic" from a specific source network address to a target network address. EX1005, p. 267 (emphases in original). A POSITA would have understood that a device configured to implement access-list statements to manage traffic decisions or block network traffic from specific network addresses would be configured to prevent unauthorized communications from unauthorized parties. EX1002, ¶ 147.

E. Claim 10: "The networked computer system of claim 1, wherein one or more applications or processes are configured to run in the host system, and wherein the one or more applications or processes running in the host system are configured to communicate with one or more devices on the network."

Nazario in combination with Ghosh discloses or renders obvious claim 1, from which claim 10 depends. *Supra* § VI.B.. Nazario and Ghosh each individually disclose or render obvious the limitations of claim 10. EX1002, ¶¶ 149-152.

Nazario discloses processes and applications running on computers connected with a network which interact with devices on the network. These processes and applications include "web server," "mail server," "file server," and "name servers," among others. EX1005, pp. 248-50. A POSITA would have understood that these processes and applications could be run on the host system and communicate with devices on the network. EX1002, ¶ 150. For example, web servers receive "requests from a multitude of clients," mail servers receive "mail messages," and so on. EX1005, pp. 83, 227. Thus, Nazario discloses or renders obvious claim 10.

Alternatively, Ghosh discloses processes and applications running on computers connected with a network which interact with devices on the network. EX1002, ¶ 151. For example, Ghosh describes "a network communications module" running on the computer system that is "configured to transmit activity reports" "over [the] network." EX1006, [0072], [0085]. These reports are "sent through the network 901 to a central collection network appliance." *Id.*, [0070], FIG. 8.

Accordingly, Ghosh also discloses this limitation. EX1002, ¶ 151. Thus, Ghosh discloses or renders obvious claim 10.

F. Claim 11

For reasons explained below, Nazario in combination with Ghosh discloses or renders obvious claim 11.

[11.pre] "A method of network isolation in a networked computer system, the method comprising:"

To the extent the preamble of claim 11 is limiting, Nazario discloses it. EX1002, ¶ 154. As described above in relation to 1.pre, Nazario discloses a networked computer system. *Supra* § VI.B.[1.pre]. As explained in relation to 1.d and 1.e, Nazario explains providing network isolation in a networked computer system. *Supra* §§ VI.B.[1.d], VI.B.[1.e]. A POSITA would thus have understood that the networked computer system of claim 1.pre would execute a method of network isolation. EX1002, ¶ 154.

[11.a] "providing a network and at least one computer system that is configured to connect to the network, the computer system comprising a host system and a virtual system, wherein the virtual system is a separate operating system or a software module operating on the computer system;"

Limitation 11.a is substantively the same as limitations 1.a and 1.b. EX1002, ¶ 155. Thus, for the reasons described above in relation to 1.a and 1.b, Nazario discloses limitation 11.a. *Supra* §§ VI.B.[1.a], VI.B.[1.b].

[11.b] "separating the host system from the virtual system using an internal firewall executed on the computer system;"

Limitation 11.b is substantively the same as limitation 1.c. EX1002, ¶ 156. Thus, for the reasons described above in related to 1.c, Nazario and Ghosh disclose limitation 11.b. *Supra* § VI.B.[1.c].

[11.c] "implementing network isolation between the computer system and the network using a host-based firewall executed on the computer system;"

Limitation 11.c is substantively the same as limitation 1.d. EX1002, ¶ 157. Thus, for the reasons described above in relation to 1.d, Nazario discloses limitation 11.c. *Supra* § VI.B.[1.d].

[11.d] "providing at least one device configured to implement a network firewall or a web proxy; and implementing network isolation, between one or more untrusted network destinations and the networked computer system, via the at least one device."

Limitation 11.d is substantively the same as limitation 1.e. EX1002, ¶ 158. Thus, for the reasons described above in relation to 1.e, Nazario discloses limitation 11.d. *Supra* § VI.B.[1.e].

G. Claim 13: "The method of claim 11, further comprising: the host system storing data in a host data storage; and the virtual system storing data in a virtual data storage."

Claim 13 is substantively the same as claim 3. EX1002, ¶ 161. Thus, for the reasons described above in relation to claim 3, Nazario discloses claim 13. *Supra* § VI.C.

H. Claim 17: "The method of claim 11, further comprising the at least one device preventing unauthorized communication between the computer system and the one or more untrusted network destinations."

Claim 17 is substantively the same as claim 7. EX1002, ¶ 163. Thus, for the reasons described above in relation to claim 7, Nazario discloses claim 17. *Supra* § VI.D.

I. Claim 20: "The method of claim 11, further comprising running one or more applications or processes in the host system that are configured to communicate with one or more devices on the network."

Claim 20 is substantively the same as claim 10. EX1002, ¶ 165. Thus, for the reasons described above in relation to claim 10, Nazario discloses claim 20. *Supra* § VI.E.

VII. CONCLUSION

For these reasons, Petitioner requests the Board institute a trial *inter partes* review and cancel the challenged claims.

VIII. DISCRETIONARY ANALYSIS

A. *Fintiv*

Analysis of the *Fintiv* factors does not warrant discretionary denial. Each factor either favors institution or is neutral. Thus, the Board should not deny institution on discretionary grounds.

The first *Fintiv* factor considers whether a stay has been granted, or if there is evidence one may be granted if review is instituted. *Apple Inc. v. Fintiv, Inc.,*

IPR2020-00019, Paper 11 at 6 (Mar. 20, 2020) (precedential). Because there has been no motion to stay in the parallel litigation, this factor is neutral. *Sand Revolution II, LLC v. Continental Intermodal Grp. – Trucking LLC*, IPR2019-01393, Paper 24 at 7 (PTAB June 16, 2020) (informative) ("In the absence of specific evidence" regarding a stay "we do not find that this factor weighs in favor of either exercising or not exercising discretion to deny institution.").

The second *Fintiv* factor looks at the "proximity of the court's trial date to the Board's projected statutory deadline." *Apple Inc.,* IPR2020-00019, at 6. Here, uncertainty in the schedule of the parallel litigation makes the second factor favor institution, or at least makes it neutral. This uncertainty is due in part to the fact that the parallel litigation's trial judge has changed twice in a short period of time—once on February 3, 2025, and again on March 25, 2025. *Croga Innovations, Ltd. v. Amazon Web Services, Inc.*, 1:24-CV-00398-ADA, Dkt Nos. 33, 38 (W.D. Tex. Apr. 16, 2023). The current date for trial is June 15, 2026, before the statutory deadline of October 17, 2026, but there is little certainty that trial will proceed on that date given the recent reassignments of the matter to different judges. Thus, based on this scheduling uncertainty, the second factor favors institution or is at least neutral. *See Dolby Laboratories, Inc. v. Intertrust Techs. Corp.*, IPR2020-01106, Paper 12 at 10 (PTAB January 5, 2021) (finding that an uncertain trial date weighed against discretionary denial); *see also In re Apple Inc.*, 979 F.3d 1332, 1344 (Fed. Cir. 2020)

(finding that a fast-paced schedule is not relevant where "the forum itself has not historically resolved cases so quickly"). Furthermore, as shown in EX1011, the average time to trial for patent case in the Western District of Texas over the past five years is 29 months. This is also the average time to trial for patent cases in front of Judge Albright in the same time period. EX1012. If the parallel proceeding follows the average time to trial, trial would occur shortly before the statutory deadline. However, given the uncertainties in the current schedule and multiple re-assignments, it is unlikely this case will progress according to the average timeline.

The third *Fintiv* factor favors denial when "the district court has issued substantive orders related to the patent at issue in the petition." *Apple Inc*, IPR2020-00019, at 9-10 (precedential). Because the district court has issued no such orders, this factor favors institution. In fact, the court explicitly "defer[red] the question of patent eligibility" in its denial of Defendant's Motion to Dismiss. *Croga Innovations, Ltd. v. Amazon Web Services, Inc.*, 1:24-CV-00398-ADA, Dkt No. 35 (W.D. Tex. Apr. 16, 2023). Additionally, the parties only just completed briefing claim construction less than a week ago, with the *Markman* hearing currently scheduled for June 11, 2025. Thus, to date the court has not issued any substantive orders on the 780 patent. The limited investment by the court and parties in the parallel proceeding—and significant remaining effort—weighs against exercising discretion to deny institution of this Petition. *Samsung Bioepis Co., Ltd. v.*

Regeneron Pharmaceuticals, Inc., IPR2023-00422 at 23 (PTAB Nov. 17, 2023); *Home Depot U.S.A., Inc. v. RavenWhite Security, Inc.*, IPR2024-00890, Paper 12 (PTAB Mar. 24, 2025).

Fintiv factors four and five look at the overlap between the issues in the parallel litigation and if the parties are the same. *Apple Inc*., IPR2019-00019, at 2. Although the parallel litigation involves the same parties and same issues, this is true for most Petitioners in IPRs and is not a basis for denial of institution. *See Philip Morris Products, S.A. v. RAI Strategic Holdings, Inc.*, IPR2020-00921, Paper 13 at 7-9 (PTAB Aug. 5, 2021). If anything, factors four and five are neutral. *Id.*

Finally, the sixth *Fintiv* factor asks the Board to consider "other circumstances that impact the Board's exercise of discretion, including the merits" of the petition. *Apple Inc*., IPR2020-00019, at 6. This factor favors institution because, as explained above, the cited prior art raises substantial questions of validity for each limitation. Additionally, no venue has considered the prior art grounds raised in the Petition. In fact, the Board recently denied a petition on the same patent because the prior art cited lacked a clear disclosure of an "internal firewall" separating the host system from the virtual system. *Fortinet v. Croga Innovations Ltd.*, IPR2025-00086 Paper 9 (PTAB March 27, 2025). This is not the case here: as explained above, the combination of Nazario and Ghosh discloses hypervisors or "virtual machine monitor[s]" that separate and restrict interactions between the host system and the

virtual system thereby preventing a malware in the virtual system from spreading to the host system. EX1006, [0032]. *See also supra* § VI.B.[1.c].

Proceeding on the grounds in this Petition—which may not be fully resolved in the parallel litigation—"serve[s] the interest of overall system efficiency and integrity." *Apple Inc.*, IPR2020-00019, at 15 (precedential). Thus, the merits of this Petition heavily weigh in favor of institution. *Samsung Bioepis.*, IPR2023-00442, at 32.

B. *Advanced Bionics*

The challenges presented in this petition are neither cumulative nor redundant to the prosecution of the 780 patent. Therefore, denial under 35 U.S.C. § 325(d) is not warranted. A*dvanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6 (Feb. 13, 2020) (precedential). Indeed, the examiner neither cited to nor relied on either reference—Nazario or Ghosh—during prosecution. EX1002, ¶¶ 84, 95. Consequently, institution should not be denied under § 325(d) because the same or substantially the same prior art or arguments were not presented to the Office.

C. Additional Considerations Identified by the Director Also Favor Institution

Recent guidance from the Director for managing the workload of the Patent Trial and Appeal Board (PTAB) provides additional factors to be considered before discretionary denial. Memorandum from Coke Morgan Stewart, Acting Under

Sec'y of Com. for Intellectual Prop. & Acting Dir. of the U.S. Patent & Trademark Off., to All PTAB Judges (Mar. 26, 2025) (on file with the U.S. Patent & Trademark Off.). Analysis of these factors also favors granting institution.

The first factor—which considers whether the PTAB or another forum has already adjudicated the validity or patentability of the challenged claims—favors institution. Indeed, although multiple actions are proceeding (*see infra* § X.B), neither the PTAB nor any other forum has adjudicated the validity or patentability of the challenged patent claims. Thus, this factor favors institution as it allows the PTAB to provide a definitive ruling on the patentability of the claims under the theories presented in this Petition.

The second factor—changes in law or new judicial precedent that may affect patentability—is at most neutral and should not weigh against institution. The claims of the 780 patent issued March 24, 2020, there have been no changes in the law or new judicial precedents issued since the issuance of the claims that may affect their patentability. Consistent with current PTAB precedent, this factor does not weigh against institution.

The third factor considers the strength of the unpatentability challenge, which—as detailed above—is compelling. No venue has considered the cited prior art and it raises substantial questions of validity. EX1002, ¶¶ 84, 95, 100. Furthermore, this Petition addresses the issues the Board found in denying institution

of a separate petition against the 780 patent. Compare *Fortinet*, IPR2025-00086 Paper 9 (denying institution because the "internal firewall" limitation was missing in the prior art) with *supra* § VI.B.[1.c]; EX1002, ¶¶ 117-124. Therefore, this factor strongly favors institution as it indicates a high likelihood that the petitioner will prevail in demonstrating the unpatentability of the challenged claims. The fourth factor—reliance on expert testimony—also relates to the merits of the Petition, and similarly favors institution. The reliance on expert testimony (EX1002) in this petition is appropriate given the level of skill and knowledge of a POSITA, and the explanations provided by the expert enhances the strength of the unpatentability challenge. This factor, therefore, favors institution as it indicates a well-supported and thoroughly argued petition.

The fifth factor looks at the settled expectations of the parties, and also favors institution or is at least neutral. The claims of the 780 patent issued in March 2020, but Patent Owner did not acquire the patent until September 2023. *See* EX1013. Until the Patent Owner acquired the 780 patent, the claims had never been asserted. Additionally, the Patent Owner did not attempt to notify Petitioner of the 780 patent before filing the parallel litigation in April 2024. Given the Petitioner's lack of prior knowledge of the patent and the Patent Owner's brief ownership period, the parties have limited settled expectations. Plus, the Patent Owner—Croga Innovations Ltd.—is a patent monetization firm that acquired this patent solely to assert against

various entities' well-established inventions.[9] The lack of use of these claims to protect a product or service diminishes any settled expectations that might weigh against institution.

The sixth factor asks if there are compelling economic, public health, or national security interests at stake. Here, compelling economic interests favor institution. The Patent Owner broadly accuses products and services related to Petitioner's cloud computing business, which provides resources to a myriad of individuals and companies. The assertion of invalid claims here can impede innovation and impose undue economic burdens on companies that are contributing to the economy through their productive activities. Furthermore, the Patent Owner is a non-practicing entity—providing no products or services let alone anything that competes with the allegedly infringing products—which exacerbates the potential economic harm. Granting institution would serve the public interest by addressing potential abuses of the patent system and ensuring enforcement of only valid patents. Thus, this factor strongly favors institution.

---

[9] *See, e.g.*, *Croga Innovations Ltd. v. Int'l Bus. Machines Corp.*, Case No. 2-23-cv-00634; *Croga Innovations Ltd. v. Cisco Sys., Inc.*, Case No. 2-24-cv-00065; *Croga Innovations Ltd. v. Fortinet, Inc.*, Case No. 2-24-cv-00206.

The last factor asks if there are any other considerations bearing on the Director's discretion, such as the need to maintain the integrity of the patent system and to prevent the misuse of patents by entities that do not contribute to technological advancement. As explained above, Patent Owner does not contribute to technological advancement. Instead, they stifle advancement by procuring and immediately asserting patents against entities that are engaged in technological innovation. Thus, this factor favors institution. The PTAB plays a crucial role in ensuring that only valid patents are enforced which is essential in maintaining a balanced and fair patent system. This overarching consideration supports the institution of the *inter partes review* to address the validity of the challenged claims, and none of the factors identified in the recent guidance from the Director change this analysis.

IX. STANDING

Petitioner certifies pursuant to Rule 42.104(a) that Petitioner is not barred or estopped from requesting this *inter partes* review and the 780 patent is IPR eligible.

X. MANDATORY NOTICES

A. Real Party-in-Interest

Petitioner is the real party in interest. No other party directed, controlled, or funded this IPR proceeding.

B. Related Matters

Patent Owner asserts the 780 patent against Petitioner in *Croga Innovations, Ltd. v. Amazon Web Services, Inc.*, 1:24-CV-00398-ADA (W.D. Tex. April 16, 2023) (the "parallel litigation").

Petitioner is aware of the following additional related matters involving the 780 patent and/or related patents:

Case Caption	Forum	Patents
Croga Innovations Ltd. v. Int'l Bus. Machines Corp., Case No. 2-23-cv-00634	EDTX	10,601,780 11,178,104
Croga Innovations Ltd. v. Cisco Sys., Inc., Case No. 2-24-cv-00065	EDTX	10,601,780 11,223,601 7,738,368
Croga Innovations Ltd. v. Fortinet, Inc., Case No. 2-24-cv-00206	EDTX	10,601,780
Cisco Sys., Inc. v. Croga Innovations Ltd., Case No. IPR2024-01196	PTAB	10,601,780
Fortinet, Inc. v. Croga Innovations Ltd., Case No. IPR2025-00086	PTAB	10,601,780
Int'l Bus. Machines Corp. v. Croga Innovations Ltd., Case No. IPR2025-00380	PTAB	10,601,780
Croga Innovations Ltd. v. Palo Alto Networks, Inc., Case No. 2-24-cv-00208	EDTX	11,223,601
Int'l Bus. Machines Corp. v. Croga Innovations Ltd., Case No. IPR2025-00379	PTAB	11,178,104
Palo Alto Networks, Inc. v. Croga Innovations Ltd., Case No. IPR2024-01421	PTAB	11,223,601
Cisco Sys., Inc. v. Croga Innovations Ltd., Case No. IPR2024-01282	PTAB	7,738,368
Cisco Sys., Inc. v. Croga Innovations Ltd., Case No. IPR2024-01283	PTAB	11,223,601

Case Caption	Forum	Patents
U.S. Patent and Trademark Office. Ex Parte Reexamination (Patent No. 10,601,780)	USPTO	10,601,780

C. Lead and Backup Counsel

Pursuant to 37 C.F.R. § 42.8(b)(3) and 42.10(a), Petitioner designates J. David Hadden (Reg. No. 40,629) as lead counsel and Allen Wang (Reg. No. 68,456), Rajendra Panwar (Reg. No. 63,165), and Ruchika Verma (Reg. No. 75,879) as backup counsel, each of Fenwick & West LLP.

D. Service Information

Petitioner consents to service by electronic mail at:

Amazon-Croga-IPR@fenwick.com

Petitioner's counsel may also be served by mail or hand delivery at Fenwick & West LLP, 801 California Street, Mountain View, CA 94041. Petitioner's counsel may be reached by telephone at (650) 988-8500.

E. Fees

The Office is authorized to charge fees for this Petition to Deposit Account 19-2555.

Dated: April 17, 2025

Respectfully submitted,

FENWICK & WEST LLP

/J. David Hadden/
J. David Hadden
Reg. No. 40,629

Attorneys for Petitioner
Amazon Web Services, Inc.

CERTIFICATE OF WORD COUNT

The undersigned certifies pursuant to 37 C.F.R. § 42.24 that the foregoing Petition for *Inter Partes* Review, excluding any table of contents, mandatory notices under 37 C.F.R. § 42.8, certificates of service or word count, or appendix of exhibits, contains 11,421 words according to the word-processing program used to prepare this document (Microsoft Word).

Dated: April 17, 2025

FENWICK & WEST LLP

/J. David Hadden/
J. David Hadden
Reg. No. 40,629

Attorneys for Petitioner
Amazon Web Services, Inc.

CERTIFICATE OF SERVICE ON PATENT OWNER UNDER 37 C.F.R. § 42.105

I hereby certify, pursuant to 37 C.F.R. Sections 42.6 and 42.105, that a complete copy of the attached **PETITION FOR INTER PARTES REVIEW OF U.S. PATENT NO. 10,601,780,** including all exhibits (**Nos. 1001-1014**), is being served via Federal Express on April 17, 2025. upon Patent Owner by serving the correspondence address of record with the USPTO as follows:

Lombard Geliebter LLP
1325 Avenue of the Americas, 28th Floor
New York, NY 10019

The foregoing was also served via Federal Express upon counsel of record for Patent Owner in the litigation pending before the U.S. District Court for the Western District of Texas entitled *Croga Innovations, Ltd. v. Amazon Web Services, Inc.*, No. 1:24-cv-00398-DII (W.D. Tex.) as follows:

Brett E. Cooper
BC Law Group, P.C.
200 Madison Avenue, 24th Floor
New York, NY 10016

Dated: April 17, 2025

FENWICK & WEST LLP

/J. David Hadden/
J. David Hadden
Reg. No. 40,629

Attorneys for Petitioner
Amazon Web Services, Inc.