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]

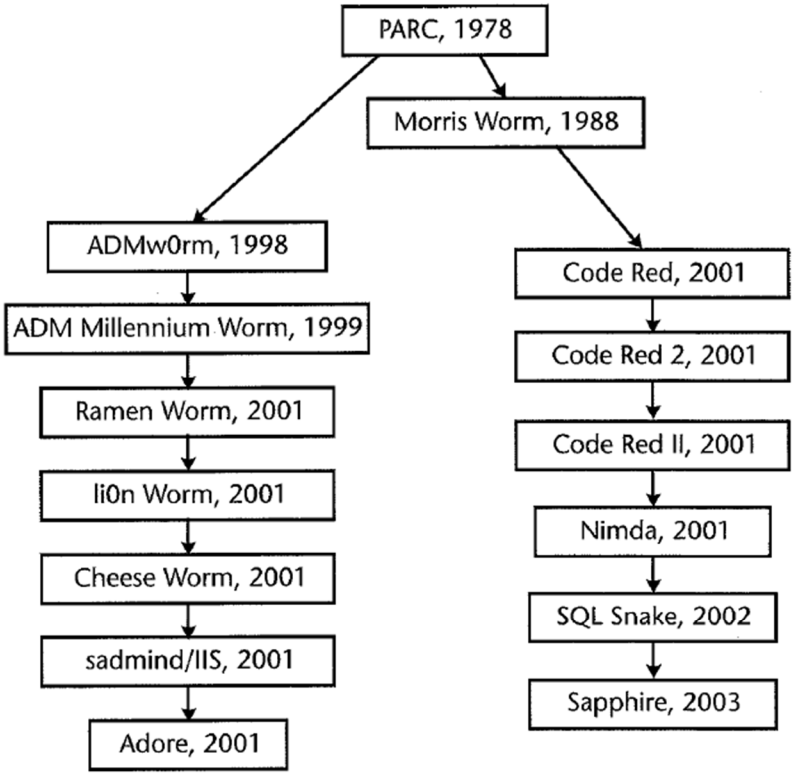


Figure 4.1 A Lineage of Internet Worms. This figure shows the lineage and classification of important Internet worms. From their beginnings with the research at Xerox PARC and then to the Morris worm, recent worms have focused on UNIX hosts (left-hand column) or Windows hosts (right-hand column). The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

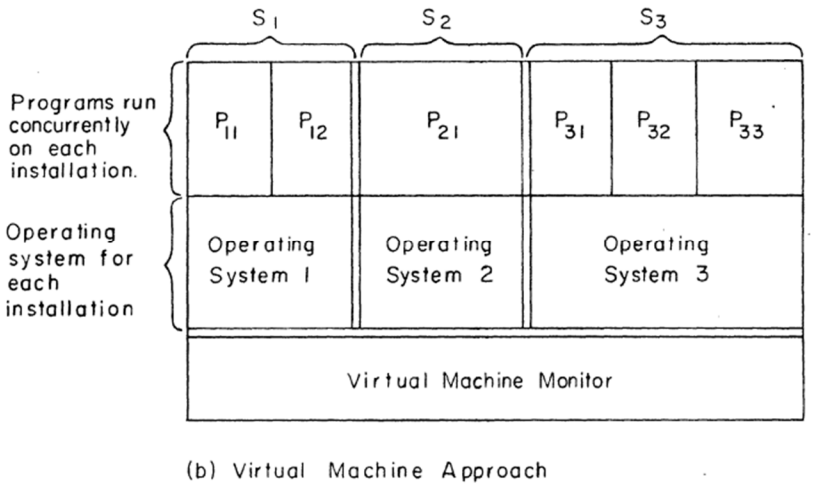
[2] Citations in this Petition are to Exhibit page numbers, not the page numbers of the reference itself, unless otherwise indicated.

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.

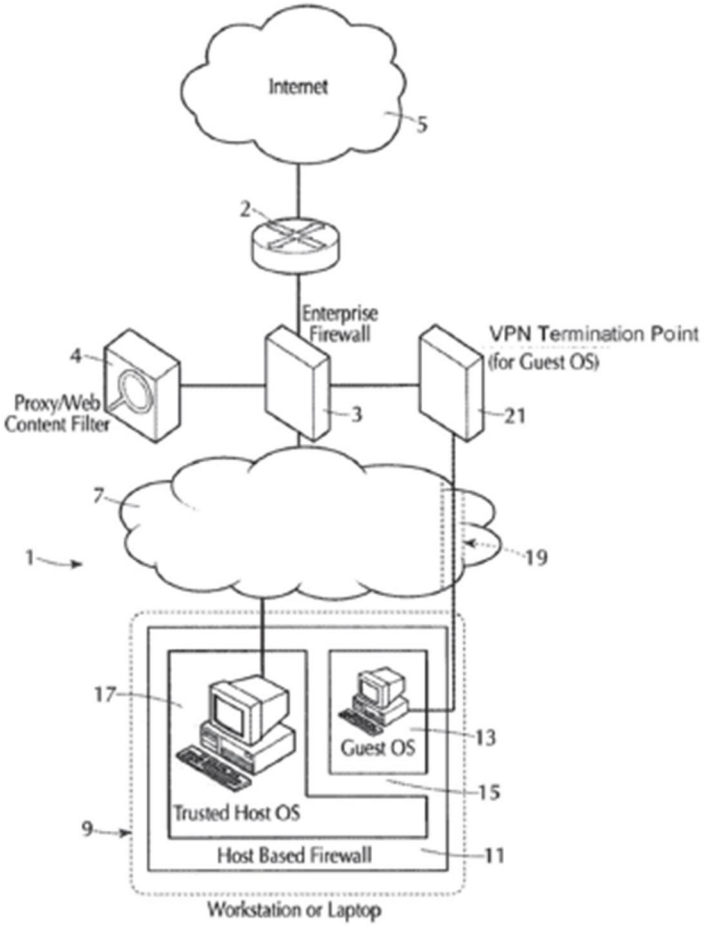


FIG. 1

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.

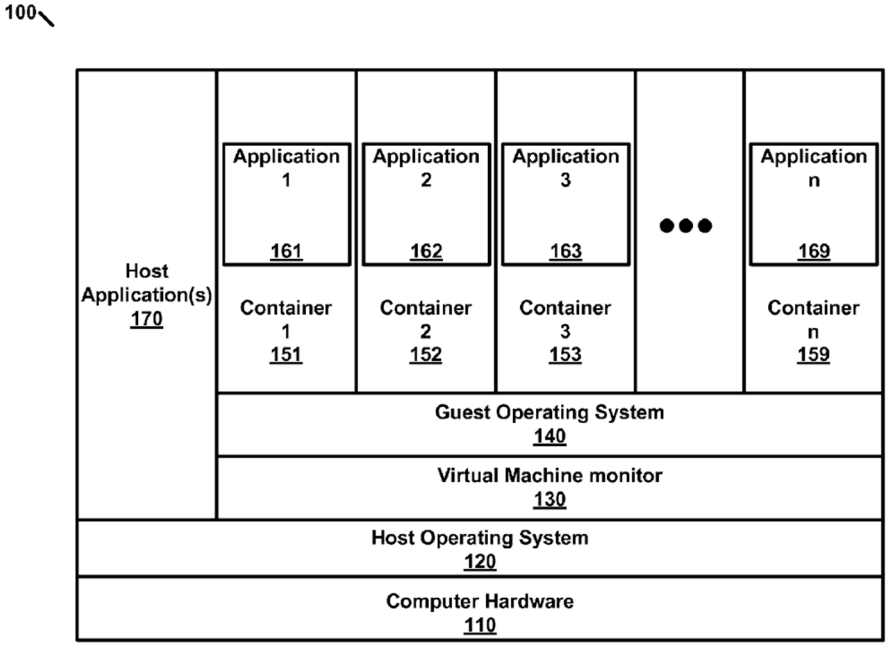


FIG. 1

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.