

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FORTINET, INC.,
Petitioner,

v.

CROGA INNOVATIONS LTD.,
Patent Owner.

IPR2025-00086
Patent 10,601,780 B2

Before TERRENCE W. McMILLIN, KEVIN C. TROCK, and
RUSSELL E. CASS, *Administrative Patent Judges*.

McMILLIN, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314
Denying Motion for Joinder
35 U.S.C. § 315(c); 37 C.F.R. § 42.122

I. INTRODUCTION

A. *Background and Summary*

Fortinet, Inc. (“Petitioner”)¹ filed a Petition to institute an *inter partes* review of claims 1–20 (the “challenged claims”) of U.S. Patent 10,601,780 B2 (Ex. 1001, the “’780 patent”) pursuant to 35 U.S.C. § 311 *et seq.* Paper 1 (“Petition” or “Pet.”). Petitioner also filed a Motion for Joinder (Paper 3, “Motion” or “Mot.”) requesting that Petitioner be joined to the *inter partes* review in IPR2024-01196 (“the ’1196 IPR”), which was filed by Cisco Systems, Inc. Croga Innovations Ltd. (“Patent Owner”)² filed a Preliminary Response. Paper 8 (“Preliminary Response” or “Prelim. Resp.”).

We have authority to determine whether to institute an *inter partes* review. *See* 35 U.S.C. § 314 (2018); 37 C.F.R. § 42.4(a) (2023). To institute an *inter partes* review, we must determine that the information presented in the Petition shows “a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314(a). For the reasons set forth below, we determine that Petitioner has not demonstrated a reasonable likelihood that it would prevail with respect to at least one challenged claim. Accordingly, we do not institute an *inter partes* review.

B. *Related Proceedings*

The parties identify the following related proceedings: *Croga Innovations Ltd. v. Cisco Systems, Inc.*, 2-24-cv-00065 (E.D. Tex.); *Croga Innovations Ltd. v. International Business Machines Corporation*, 2-23-cv-

¹ Petitioner identifies itself, Fortinet, Inc., as the real party-in-interest. Pet. 85.

² Patent Owner identifies itself, Croga Innovations Ltd., as the real party-in-interest. Paper 4, 2.

00634 (E.D. Tex.); *Croga Innovations Ltd. v. Fortinet, Inc.*, 2-24-cv-00206 (E.D. Tex.); and *Croga Innovations Ltd. v. Amazon Web Services, Inc.*, 1-24-cv-00398 (W.D. Tex.). Pet. 87; Paper 5, 2.

C. The '780 patent

The '780 patent is titled “Internet Isolation for Avoiding Internet Security Threats.” Ex. 1001, code (54). The '780 patent explains that “[s]ecurity systems of various designs have been developed to try to address the problem” of malware that is “downloaded to a computer completely unintentionally and without the knowledge of the individual computer user” over the Internet either by the user “access[ing] a website through an Internet browser” or “via an attachment . . . that is either received or downloaded from a website.” *Id.* at 1:25–32, 1:42–44, 1:59–62, 2:58–60. However, while “it is possible to use two separate computers, one accessing the Internet and the other connected only with a LAN that is completely isolated from the Internet,” this solution “results in a double cost of equipment” and “a problem transferring legitimate data between the machines when necessary and appropriate.” *Id.* at 2:60–66. “Other more software-intensive” solutions “usually expand the demand for bandwidth undesirably, or else do not provide airtight protection against loading of malware.” *Id.* at 2:66–3:2.

The '780 patent suggests that a need exists for “a system for a computer that will allow safe browsing without a risk of such infection,” that will “eliminate the ability of trusted internal host systems on a secure LAN to access the Internet, but to provide access to the Internet through a secure isolated service that can access the Internet, but not the internal trusted LAN

sites,” and “for secure file exchange to transfer data between the Internet and the trusted hosts of the trusted LAN.” *Id.* at 3:6–16.

The ’780 patent is directed to “a networked computer system” with a connection that “communications with the Internet, and a plurality of computer stations” that “are each connected with the local network so as to communicate thereacross.” *Id.* at 3:50–56. “Each computer station operates as a host system” that “communicates over the local network but is restricted against communication with the Internet, except with predetermined Internet sites that have been identified as safe to access.” *Id.* at 3:56–62. “Each computer station also supports operation of a respective virtual computer system thereon” that “communicates via a virtual conduit connection over the local area network with the connection to the Internet, but wherein the virtual computer system is isolated against any other communication over the local area network.” *Id.* at 3:62–4:1. As a result, “[e]ach computer station is isolated against any communication of data to or from the respective virtual computer system operating thereon, except for a limited set of types of permitted data transfers.” *Id.* at 4:1–4.

Figure 1, reproduced below, illustrates a “system on a local area network using the Internet isolation system” in accordance with the ’780 patent. *Id.* at 6:65–67.

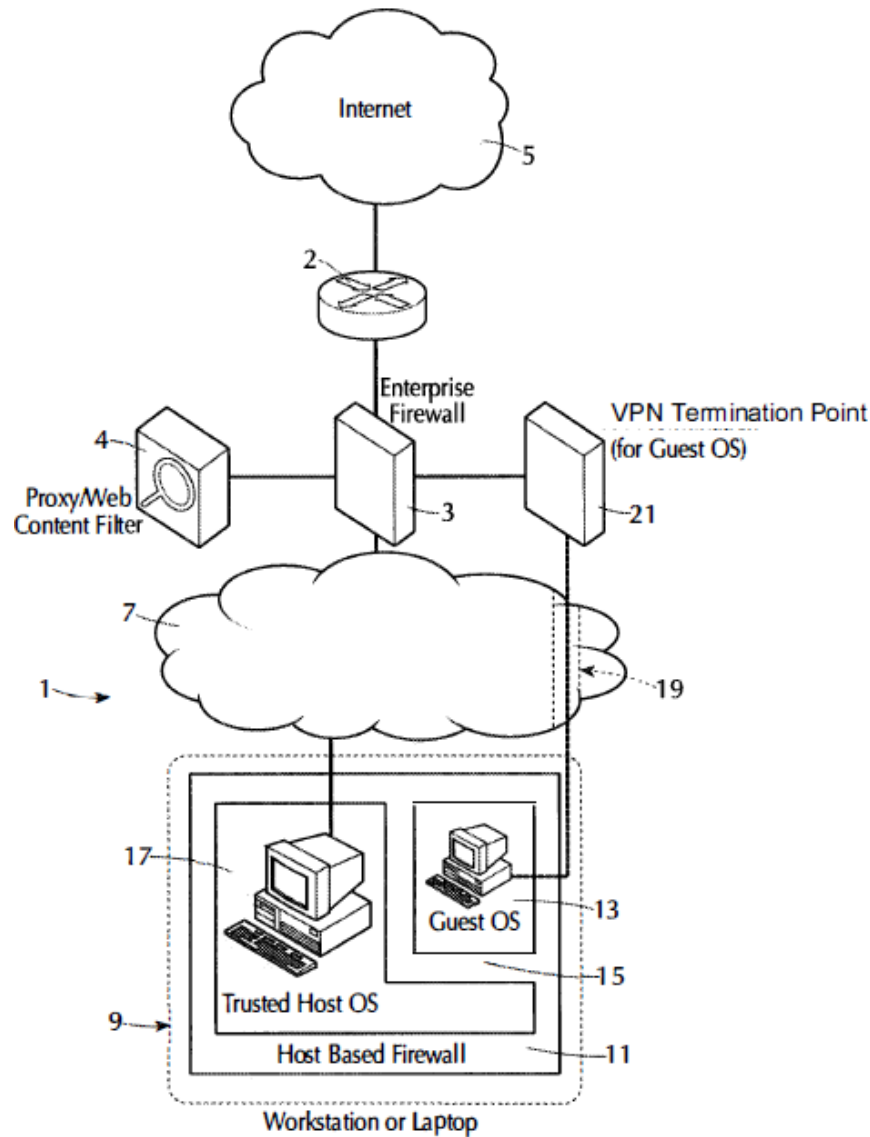


Figure 1 depicts “a networked computer system generally indicated at 1 is linked to the Internet 6 via a firewall 3 and a router 2,” with a “proxy/web-content filter 4 [that] is connected with and cooperates with the firewall hardware 3 to control the type of data permitted to pass from the Internet 5 into the local system 1” that “filter[s] . . . data not intended for the system 1, and also blocks communications from users on the LAN trying to reach disallowed sites,” and with “local system 1 [that] includes a trusted local area network (LAN) 7 that transmits electrical data signals between a

plurality . . . of computer systems each identified by a unique LAN address.” *Id.* at 7:7–22. “Each of the computers on the LAN 7 is configured similarly to the computer system 9 to prevent malware intrusion from the Internet.” *Id.* at 7:22–24.

The ’780 patent discloses that the host system 9 has “a host-based firewall 11 that provides restrictive egress from the computer 9.” *Id.* at 7:42–44. “This host based firewall 11 blocks all communications from the computer 9 except that it permits passage through it only of communications to the IP addresses of other computers on the trusted network 7,” and “specifically does not permit the computer 9 to access ports . . . that may or may become vulnerable to malware or security threats at some point in the future” while “allow[ing] the computer 9 only some limited use of these ports if the communication is purely with pre-determined trusted Internet sites.” *Id.* at 7:49–60. The firewall 11 in the ’780 patent “is therefore a preventative barrier to any access of the Internet from host system 9 through its ports or directly to the firewall 3 via the LAN.” *Id.* at 7:60–62.

The ’780 patent discloses that the host system 9 also “creates a hypervisor on the computer system 9,” and that “the hypervisor effectively creates a virtual machine,” such as “virtual guest system or guest OS 13,” “operating on the host computer that has a virtual configuration different from the real hardware and software configuration of the computer 9.” *Id.* at 7:63–8:12. The “hypervisor also provides an additional internal host-supported firewall indicated at 15 that separates and restricts interaction between virtual guest system 13 and the trusted-host operating system 17,

which is the standard operating system running the host computer 9.” *Id.* at 8:13–18.

D. Challenged Claims

Petitioner challenges claims 1–20 (all) of the ’780 patent. Pet. 17. Claim 1 is an independent system claim and claim 11 is an independent method claim. Ex. 1001, 12:63–13:13, 13:65–14:17. Claims 2–10 depend directly from claim 1, and claims 12–20 depend directly from claim 11. *Id.* at 13:14–64, 14:18–65. Although claims 1–10 are system claims and claims 11–20 are method claims, the language of the system and method claims is substantially similar. *Compare id.* at 12:63–13:64 *with id.* at 13:65–14:65. Claim 1 is illustrative and recites:

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.

Id. at 12:63–13:13 (emphasis added). We refer to the highlighted text in system claim 1 and the recitation in method claim 11 of “***separating the host system from the virtual system using an internal firewall executed on the***

computer system” (*id.* at 14:7–8 (emphasis added)) as the “internal firewall limitations.” By virtue of their dependency on the challenged independent claims, the remaining challenged claims are construed as incorporating the internal firewall limitations. *See* 35 U.S.C. § 112(d).

E. The Asserted Grounds

Petitioner challenges claims 1–20 of the ’780 patent based on the grounds set forth in the table below.

Claims Challenged	35 U.S.C. §	References
1–7, 9–17, 19, 20	103	Delco ³ , Adams ⁴
8, 18	103	Delco, Adams, Dadhia ⁵

Pet. 17. In support of their respective arguments, Petitioner submits the Declaration of Prashant Shenoy, Ph.D. (Ex. 1003) and Patent Owner submits the Declaration of Eric Cole, Ph.D. (Ex. 2001).

II. OBVIOUSNESS ANALYSIS

A. Principles of Law

Under 35 U.S.C. § 103(a),⁶ a patent claim is unpatentable if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. *See KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007) (similar language). The question of obviousness

³ US 8,166,474 B1, issued Apr. 24, 2012 (Ex. 1005).

⁴ US 2010/0077476 A1, published Mar. 25, 2010 (Ex. 1006).

⁵ US 7,886,351 B2, issued Feb. 8, 2011 (Ex. 1007).

⁶ Because the ’780 patent is based on a provisional application filed before March 16, 2013 (the effective date of the Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 287–88 (2011)), the pre-AIA version of § 103 applies.

involves resolving underlying factual determinations including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and when presented (4) objective evidence of non-obviousness (not presented here). *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). Further, “there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.” *See KSR*, 550 U.S. at 418.

“In an [*inter partes* review], the petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable.” *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3) (requiring *inter partes* review petitions to identify “with particularity . . . the evidence that supports the grounds for the challenge to each claim”)). Petitioner cannot satisfy its burden of proving obviousness by employing “mere conclusory statements.” *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016).

B. Level of Ordinary Skill in the Art

With regard to the level of ordinary skill in the art, Petitioner contends a person of ordinary skill in the art “would have a bachelor’s degree in electrical engineering, computer science, or equivalent training, and approximately two years of experience working in the field of virtual computing systems.” Pet. 11–12 (citing Ex. 1003 ¶¶ 23–25). Patent Owner does not address the level of ordinary skill in the art. *See generally* Prelim. Resp.

For purposes of this Decision, we adopt Petitioner’s definition of the level of ordinary skill in the art because it is consistent with the ’780 patent and the asserted prior art.

C. Claim Construction

In an *inter partes* review, “[claims] of a patent . . . shall be construed using the same claim construction standard that would be used to construe the [claims] in a civil action under 35 U.S.C. § 282(b), including construing the [claims] in accordance with the ordinary and customary meaning of such claims 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) (2018); *see also Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–1314 (Fed. Cir. 2005).

Petitioner submits that, “for the purposes of this proceeding and the grounds presented herein, no claim term requires express construction.” Pet. 12. Patent Owner argues that, with regard to the internal firewall limitations, “Petitioner’s mappings of the asserted art to the limitations . . . rely on implicit constructions of those terms without any support in the ’780 specification.” Prelim. Resp. 2. However, Patent Owner does not propose any express claim construction. *Id.*

No need exists to expressly construe any claim terms to resolve the parties’ dispute. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (“[W]e need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy.’” (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

D. Petitioner Fails to Show the Cited Art Teaches the Internal Firewall Limitations

Petitioner challenges independent claims 1 and 11 as obvious over Delco and Adams. *See* Pet. 17, 27–52 (claim 1), 69–71 (claim 11). For the internal firewall limitations, Petitioner cites only Delco. *See id.* at 40–43

(claim 1), 70 (claim 11).⁷ Patent Owner disputes the showing in the Petition as to the internal firewall limitations in claims 1 and 11. Prelim. Resp. 4–10. We start with a description of the disclosure of Delco and then consider the arguments and evidence presented by the parties with regard to the internal firewall limitations.

1. Delco (Ex. 1005)

Delco is titled “System and Methods for Implementing Network Traffic Management for Virtual and Physical Machines.” Ex. 1005, code (54). Specifically, Delco discloses a “virtualization framework that supports secure network communications among the virtual machines, host operating system . . . and a physical network coupled to the underlying physical computer platform” and that “includes a network interface controller driver that provides an interface to the platform network interface controller and supports execution of a plurality of virtual machines.” *Id.* at 3:25–33. Delco discloses “the distributed implementation of packet filters in the individual virtual machines,” which “enables each virtual machine to discretely manage

⁷ Petitioner relies heavily on its showing for independent system claim 1 for its showing for independent method claim 11. For example, the entire presentation in the Petition as to the internal firewall limitation of claim 11 is:

As explained above [with regard to the internal firewall limitation [1.5] of claim 1], Delco teaches “*wherein an internal firewall is configured to separate the host system from the virtual system in the computer system.*” For similar reasons, Delco teaches “*separating the host system from the virtual system using an internal firewall executed on the computer system*” as claimed. Ex.1003, ¶168.

Pet. 70. Cited paragraph 168 of the Shenoy Declaration (Ex. 1003) is a verbatim copy of the quoted paragraph from page 70 of the Petition with no additional analysis or discussion.

network communications with respect to all external entities, including the host operating system and other virtual machines” and “supports the coordinated management of the different packet filter configurations to ensure that security is maintained even where security concerns are changed.” *Id.* at 3:46–49. Delco also discloses “that the virtual machine network traffic packet filters are implemented in a fundamentally secure location relative to the potential execution of insecure or compromised applications anywhere within the host computer system platform,” and that “[l]ocating the packet filters within the reserved space of a virtual machine limits inappropriate access by host-based applications and those executed in other virtual machines” and “the effective positioning of the filters outside of the nominal application execution space of the guest operating systems precludes . . . improper access by programs executed on the local guest operating system.” *Id.* at 3:50–61.

2. *Analysis of Arguments and Evidence Related to the Internal Firewall Limitations*

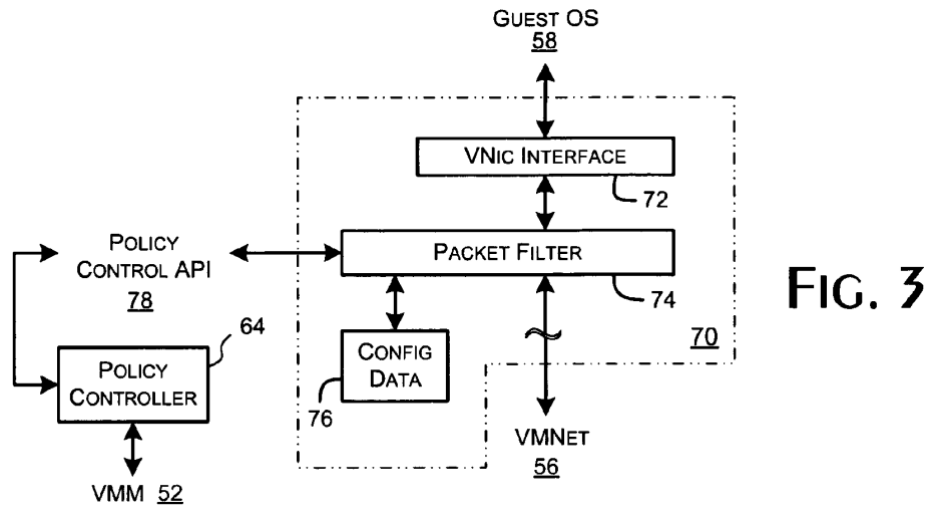
As noted above, the internal firewall limitation of independent system claim 1 is “***wherein an internal firewall is configured to separate the host system from the virtual system in the computer system***” (Ex. 1001, 13:2–4) (emphasis added) and the internal firewall limitation of independent method claim 11 is “***separating the host system from the virtual system using an internal firewall executed on the computer system***” (*id.* at 14:7–8) (emphasis added). Petitioner relies on Delco for allegedly teaching these internal firewall limitations. Pet. 40–43 (citing Ex. 1003 ¶¶ 90–96,⁸

⁸ Patent Owner criticizes the Shenoy Declaration as related to the internal firewall limitations and argues that this testimony should be given little weight:

Ex. 1005, 1:65–2:5, 3:40–46, 7:4–18, 7:29, 8:36, 8:43–45, Figs. 2, 3), 70.

We have considered Delco and all its teachings and suggestions and determine that Petitioner has not sufficiently shown that Delco teaches or suggests the internal firewall limitations.

Petitioner contends that “each of Delco’s virtual machines includes a packet filter 74 (*‘internal firewall’*) that filters packets passing between the virtual system and the host system” and “[b]y filtering packets between the virtual machine and the host system, the packet filter is *‘configured to separate the host system from the virtual system in the computer system.’*” Pet. 40 (citing Ex. 1005, 7:4–18, Fig. 3). The cited Figure 3 of Delco is reproduced below.



The testimony of Petitioner’s expert as to the “internal firewall” limitation should be given little weight as, apart from a single extended quotation in ¶91, it merely repeats verbatim the assertion in the Petition it purportedly supports. *Compare* Pet. at 39–42 *with* EX1003 at ¶¶ 90–96; *see Xerox Corp. v. Bytemark, Inc.*, IPR2022-00624, Paper No. 9 at 15 (PTAB Aug. 24, 2022) (precedential).

Prelim. Resp. 4 n.1. We agree with Patent Owner. The testimony of Dr. Shenoy is not supported by Delco for the same reasons that the largely verbatim argument in the Petition is not supported by Delco.

Figure 3 depicts “preferred component architecture of a virtual network interface controller [70] and packet filter [74].” Ex. 1005, 4:36–38. The cited passage in Delco provides:

A virtual network interface controller (VNic) is preferably implemented and executed as a component within the virtual hardware component layer 60_{1-N}. As shown in FIG. 3, in accordance with a preferred embodiment of the present invention, a virtual network interface controller component 70 includes, representationally, a virtual network interface layer 72 combined with a **packet filter layer 74**. The network interface layer 72 preferably implements an interface emulation of a conventional network interface controller, enabling a conventional vendor supplied network interface controller driver to be loaded and used by the guest operating system 58_{1-N}. In effect, data link level network packet traffic is transferred by the network interface layer 72 between a guest operating system 58_{1-N} and the virtual network controller 56 through the **packet filter layer 74**.

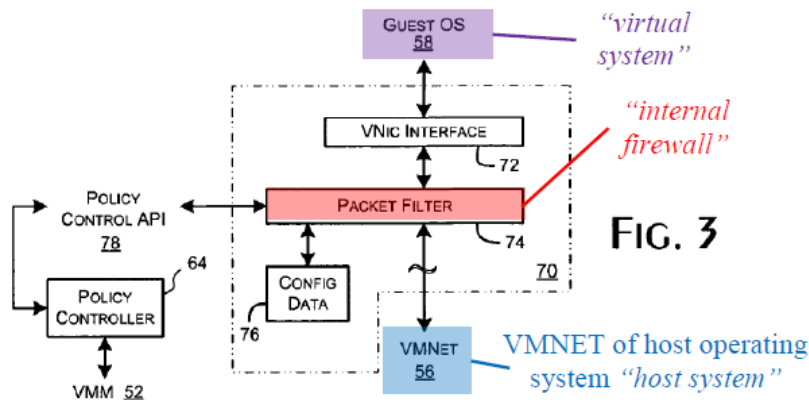
Ex. 1005, 7:4–18 (emphasis added). To the extent that the quoted paragraph addresses functioning of packet filter layer 74, it does so in only the last sentence of this paragraph. This sentence provides that network packet traffic is transferred between Guest OS 58 and VMNet 56 through packet filter layer 74. There is no explanation as to how or why this sentence (or this paragraph or figure) teaches or suggests separating the host system from the virtual system as recited in the internal firewall limitations.

Petitioner contends that “Delco’s packet filter layer 74 is an “*internal firewall*” because it performs the function of a firewall—filtering packets—between the internal virtual machine and destinations that are external to the virtual machine (e.g., the host system 42 or over the Internet).” Pet. 41 (footnote omitted). Petitioner supports this assertion with a footnote that quotes a passage from the “Background of the Invention” in Delco that

provides “**Firewall** system architectures are conventionally well-known as implementing various stateful and stateless **network packet processing functions** to selectively control the network traffic passed through the firewall system. The packet processing functions typically include **discrete packet filtering.**” *Id.* at 41 n.4 (bolding by Petitioner). However, the immediately preceding sentence in Delco states that this passage relates to a background “typical use scenario” of an “external firewall system” and is not a disclosure of how the proposed invention’s alleged internal firewall (Delco’s packet filter 74), upon which Petitioner relies, actually functions. Ex. 1005, 1:62–67. More specifically, this sentence states, “In a typical use scenario, a physical computer system may rely on an **external firewall system**, as typically implemented in a corporate or hosted provider network environment, **to selectively filter network traffic to and from the physical computer system.**” *Id.* (emphasis added). This passage in Delco specifically relates to prior art external firewall systems that filter network traffic. Here again, there is no explanation as to how or why this passage from Delco relates to Delco’s packet filter 74 or teaches or suggests separating the host system from the virtual system as recited in the internal firewall limitations.

Petitioner argues:

Delco’s packet filter 74 is placed between the host operating system 42 and the guest operating systems 58 and is thus “*configured to separate the host system from the virtual system in the computer system.*” Specifically, the virtual network interface component 70 is placed between the Guest OS 58 (“*virtual system*”) and the VMNet 56 of the host operating system (“*host system*”) as shown below.



Ex.1005, Fig. 3 (annotated); Ex.1003, ¶94.

Pet. 42 (footnote omitted⁹). Packet filter 74 is positioned to protect Guest OS 58 from external network packets not from the host system or packets originating from the host system. Delco states that “virtual network controller (VMNet) 56 . . . provides coordinated routing of network traffic between the virtual machines 54 and the various conventional interface points of a conventional network protocol stack.” Ex. 1005, 6:25–28. Delco provides that packet filter layer 74 restricts and controls packets coming from the external network via VMNet 56 to Guest OS 58. *Id.* at 7:15–18 (“[D]ata link level network packet traffic is transferred by the network

⁹ The omitted footnote states “Fig. 2 illustrates the VMNet 56 as part of the host operating system 42.” Pet. 40 n.5. Figure 2 is “a block diagram of a preferred software architecture.” Ex. 1005, 4:32–33. We interpret Figure 2 as illustrating that the disclosed software includes software that when executed provides virtual network controller (VMNet) 56 in the same manner that execution of the VMM software also shown as part of the host operating system in Figure 2 provides a set of virtual machines. *See id.* at 6:20–30. Stated differently, Figure 2 depicts where the software that creates the virtual machines and virtual network controller resides prior to execution. Petitioner does not provide an adequate explanation as to how or why Figure 2 supports its argument that packet filter 74 is an internal firewall between the host system and the virtual system.

interface layer 72 between a guest operating system 58_{1-N} and the virtual network controller 56 through the packet filter layer 74.”), 10:28–32 (“Network access, though only subject to the specific restrictions and controls established by the corresponding packet filter 74, is then available 108 to the guest operating system 58.”). Thus, Petitioner’s argument, that the position of packet filter 74 in Figure 3 supports its contention that packet filter 74 is an internal firewall separating the host system from the virtual system, is contradicted by Delco.

Petitioner further argues:

Delco explains that “[a]n advantage of the present invention is that the distributed implementation of packet filters in the individual virtual machines enables each virtual machine to discretely manage network communications with respect to **all external entities, including the host operating system** and other virtual machines.” Ex.1005 3:40-46. By filtering traffic between the virtual system and the host system, the packet filter 74 acts as an internal firewall that implements isolation between the virtual machine(s) and the host operating system.

Pet. 42–43. However, the quoted passage from Delco does not refer to packet filter 74 and managing network communications is not the equivalent of implementing isolation. And, we do not believe in light of the whole of the disclosure of Delco that this sentence adequately supports Petitioner’s contention that Delco’s packet filter 74 is an internal firewall that separates the virtual machine from the host system.

Patent Owner disputes the Petition’s showing as to the internal firewall limitations. Prelim. Resp. 4–10. Patent Owner argues that, “[a]s Petitioner and its expert acknowledge, Delco’s packet filter 74 operates to ‘filter out harmful packets from untrusted destinations such as the Internet.’”

Id. at 4–5 (citing Pet. 59; Ex. 1003 ¶¶ 131–135; Ex. 1005, 2:26–59) (footnote omitted¹⁰). The Petition states:

Delco’s virtual machines also communicate with destinations over the Internet. The virtual machines’ connection to the Internet passes through a virtual network interface. “A virtual network interface controller (VNic) is preferably implemented and executed as a component within the virtual hardware component layer 60_{1-N}.” Ex.1005, 7:4-18. The “virtual network interface controller component 70 includes, representationally, a virtual network interface layer 72 combined with a packet filter layer 74.” Ex.1005, 7:8-10. Delco’s packet filter is intended to filter out harmful packets from untrusted destinations such as the Internet. *See* Ex.1005, 2:26-59; Ex.1008, [0006].

Pet. 58–59. We determine that this passage in the Petition more accurately describes the function of the packet filter 74 as disclosed in Delco than the presentation in the Petition related to the internal firewall limitations (*see id.* at 40–43, 70).

Patent Owner also argues that “[n]etwork isolation via packet filtering (e.g., Delco’s packet filter 74) does not separate the host system from the virtual system because it does not restrict access to host operating system resources” and “a firewall configured for network isolation is not the same as a firewall configured to separate a host system from a virtual system.” Prelim. Resp. 6 (citing Ex. 2001¹¹ ¶¶ 46–49, 53–56). This argument has merit. Filtering packets from an external network from being transferred to the virtual system as disclosed by Delco (*see* Ex. 1005, code (57), 7:15–18,

¹⁰ The omitted footnote is discussed in footnote 7 *supra*.

¹¹ Patent Owner cites Ex. 2006, but since that exhibit does not exist, we presume the intention was to cite to the expert declaration in Ex. 2001.

10:28–32) does not separate the host system from the virtual system as recited in the internal firewall limitations.

In addition, we note that the Abstract of Delco addresses the functioning of the packet filter. *See* Ex. 1005, code (57). The Abstract states that “[e]ach virtual network interface controller further contains a programmable network packet filter that controls the selective transfer of network packets with respect to a corresponding virtual machine.” *Id.* The Abstract contradicts Petitioner’s argument that the packet filter 74 functions as an internal firewall to separate the host system from the virtual system.

And, we also note that Delco discloses isolating the virtual machines from the host machine in a manner unrelated to packet filter 74, the alleged internal firewall. *See* Ex. 1005, 6:36–60. Delco provides:

The virtual machines 54_{1-N} functionally encapsulate guest operating systems 58. **Each of the virtual machines 54_{1-N}, when executing, are effectively isolated from one another and from the host operating system 42 as a function of the applied virtual machine world context switch.** The hardware platform 44, as programmed in conjunction with the world context switch, establishes conventional memory space controls that restrict the accessible memory space to that defined for the executing virtual machine 54_{1-N}. . . .

As is typical of conventional operating systems, the guest operating systems 58_{1-N} define and constrain the execution of programs within the program execution spaces 62_{1-N} to preclude, at a minimum, memory accesses beyond the boundaries of the program execution spaces 62_{1-N}.

Id. (emphasis added). In the Petition, there is no argument that this passage teaches or suggests an internal firewall and this passage from Delco is not discussed or cited in relation to the internal firewall limitations. *See* Pet. 40–43, 70.

We further note that Figure 1 of Delco, reproduced below, depicts two firewalls and neither of these two firewalls are between host system platform 12 and virtual machines 26 and 28.

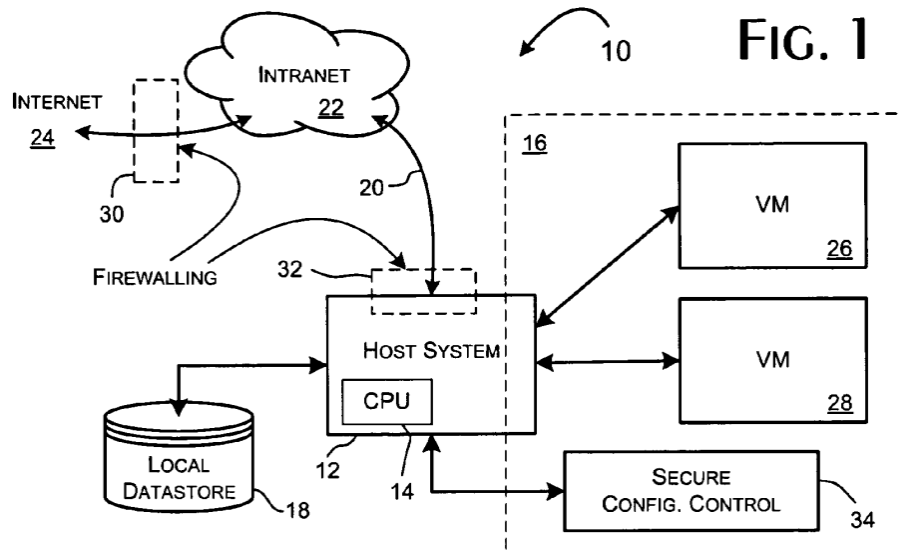


Figure 1 depicts “a computer system platform suitable for implementation of the present invention” and “[a] computer system 10, demonstrating a preferred environment for implementation of the present invention.”

Ex. 1005, 4:30–31, 4:53–54. In Figure 1, the depicted “Firewalling” is: (1) “independent firewall system 30 . . . to provide network protection to the intranet 22 including the host system platform 12” (*id.* at 4:62–65) between internet 24 and intranet 22; and (2) “host-based packet filters 32” (*id.* at 5:24) between intranet 22 and host system platform 12. As further supported by Figure 1, there is no firewall depicted or described in Delco that separates the host system from virtual system.

3. Summary as to the Internal Firewall Limitations

We determine that Petitioner has failed to show that Delco teaches or suggests the internal firewall limitations of the challenged claims. Delco does not teach or suggest an internal firewall that is configured to separate

the host system from the virtual system as recited in independent claim 1 and does not teach or suggest separating the host system from the virtual system using an internal firewall as recited in independent claim 11. The packet filter 74 of Delco is not an internal firewall separating the host system from the virtual system as argued in the Petition (*see* Pet. 40). The packet filter 74 of Delco restricts and controls network traffic from accessing a virtual machine and does not separate the virtual machine from the host machine. Ex. 1005, code (57), 7:15–18, 10:28–32.

III. JOINDER

In this proceeding, Petitioner seeks to join IPR2024-01196. However, the Board did not institute an *inter partes* review in that proceeding, relying on substantially identical reasoning as here. Thus, there is no pending proceeding in the '1196 IPR to join. As a result, Petitioner's request to join the '1196 IPR is denied.

IV. CONCLUSION

Petitioner has not shown that the cited art teaches or suggests the internal firewall limitations of the claims of the '780 patent. Thus, Petitioner has failed to establish that the cited art teaches or suggests all the limitations of any challenged claim. Considering the entire record as a whole and weighing the evidence presented, we determine that Petitioner has not demonstrated a reasonable likelihood of showing at least one of the claims challenged in the Petition would have been obvious.

V. ORDER

In consideration of the foregoing, it is hereby
ORDERED that the Motion for Joinder is denied; and

FURTHER ORDERED that the Petition is denied as to all challenged claims of the '780 patent, and no *inter partes* review is instituted.

IPR2025-00086
Patent 10,601,780 B2

FOR PETITIONER:

Patrick D. McPherson
David C. Dotson
Daniel D. Mitchell
DUANE MORRIS LLP
pdmcpherson@duanemorris.com
dcdotson@duanemorris.com
dmitchell@duanemorris.com

FOR PATENT OWNER:

Brett Cooper
Seth Lindner
BC LAW GROUP, P.C.
bcooper@bc-lawgroup.com
slindner@bc-lawgroup.com

Robert A. Auchter
AUCHTER PLLC
robert@auchterlaw.com