

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,
Petitioner

IPR2024-01196
U.S. Patent No. 10,601,780

**PETITION FOR *INTER PARTES* REVIEW
UNDER 35 U.S.C. § 312 AND 37 C.F.R. § 42.104**

TABLE OF CONTENTS

PETITIONER’S EXHIBIT LIST	5
I. INTRODUCTION	6
II. GROUNDS FOR STANDING.....	7
III. NOTE.....	7
IV. TECHNOLOGY BACKGROUND.....	7
V. SUMMARY OF THE ’780 PATENT	7
A. Overview of the ’780 Patent.....	7
B. Prosecution History of the ’780 Patent.	10
VI. LEVEL OF ORDINARY SKILL IN THE ART.....	11
VII. CLAIM CONSTRUCTION	12
VIII. RELIEF REQUESTED AND REASONS FOR THE REQUESTED RELIEF	12
IX. DISCRETIONARY DENIAL WOULD BE INAPPROPRIATE.....	12
A. Discretionary denial under the <i>Fintiv</i> factors is not appropriate.....	12
1. No evidence regarding a stay	13
2. Parallel proceeding trial date	13
3. Investment in the parallel proceeding.....	14
4. Overlapping issues with the parallel proceeding	15
5. Identity of parties	15
6. Other circumstances.....	15

B.	Discretionary denial under 35 U.S.C. § 325(d) is not appropriate. ...	16
X.	IDENTIFICATION OF HOW THE CLAIMS ARE UNPATENTABLE....	17
A.	Challenged Claims and Statutory Grounds for Challenge	17
B.	Ground 1: Claims 1-7, 9-17, and 19-20 are obvious in view of Delco and Adams.	18
1.	Summary of Delco.	18
2.	Summary of Adams	21
3.	Reasons to Combine Delco and Adams.....	22
4.	Claim 1	25
5.	Claim 2.....	50
6.	Claim 3	52
7.	Claim 4.....	54
8.	Claim 5	55
9.	Claim 6.....	61
10.	Claim 7	62
11.	Claim 9	63
12.	Claim 10	65
13.	Claim 11	67
14.	Claim 12	69
15.	Claim 13	69
16.	Claim 14	70

17.	Claim 15	70
18.	Claim 16	71
19.	Claim 17	71
20.	Claim 19	71
21.	Claim 20	71
C.	Ground 2: Claims 8 and 18 are obvious in view of Delco, Adams, and Dadhia.....	71
1.	Summary of Dadhia.	72
2.	Reasons to Combine Dadhia with Delco and Adams	73
3.	Claim 8	77
4.	Claim 18	83
XI.	CONCLUSION.....	84
XII.	MANDATORY NOTICES	85
A.	Real Party-in-Interest	85
B.	Related Matters.....	85
C.	Lead and Back-up Counsel and Service Information	85
	CERTIFICATE OF WORD COUNT	87
	CERTIFICATE OF SERVICE	88

PETITIONER’S EXHIBIT LIST

Ex.1001	U.S. Patent No. 10,601,780 to Hoy et al.
Ex.1002	Prosecution History of U.S. Patent No. 10,601,780.
Ex.1003	Declaration of Dr. Prashant Shenoy under 37 C.F.R. § 1.68.
Ex.1004	<i>Curriculum Vitae</i> of Dr. Shenoy.
Ex.1005	U.S. Patent No. 8,166,474 to Delco (“Delco”).
Ex.1006	U.S. Patent Publication No. 2010/0077476 to Adams et al. (“Adams”).
Ex.1007	U.S. Patent No. 7,886,351 to Dadhia (“Dadhia”).
Ex.1008	U.S. Patent Publication No. 2006/0262916 to Marascio et al. (“Marascio”).
Ex.1009	U.S. Patent No. 8,468,256 to McArdle (“McArdle”).
Ex.1010	U.S. Patent Publication No. 2008/0267387A1 to Strathmeyer (“Strathmeyer”).
Ex.1011	Complaint - <i>Croga Innovations Ltd. v. Cisco Systems, Inc.</i> EDTX-2-24-cv-00065.
Ex.1012	Docket Control Order - <i>Croga Innovations Ltd. v. Cisco Systems, Inc.</i> , No. 2-24-cv-00065, Dkt. 42 (E.D. Tex. June 21, 2024).
Ex.1013	Federal Court Trial Statistics – Dec. 31, 2023.
Ex.1014	U.S Patent Publication No. 2009/0241192 to Thomas et al. (“Thomas”).
Ex.1015	RFC 2131
Ex.1016	List of patent trials scheduled before Judge Gilstrap (E.D. Tex.) on October 20, 2025.

I. INTRODUCTION

Pursuant to 35 U.S.C. §§ 311, 314(a), and 37 C.F.R. § 42.100, Cisco Systems, Inc. (“Petitioner”) respectfully requests that the Board review and cancel as unpatentable under (pre-AIA) 35 U.S.C. §103(a) claims 1-20 (the “Challenged Claims”) of U.S. Patent No. 10,601,780 (“’780 patent,” Ex.1001).

The ’780 patent describes and claims nothing more than well-known techniques to provide network security to a “host computer [that] supports a virtual guest system running thereon.” Ex.1001, abstract. The purported novelty of the ’780 patent—as described in the prosecution history—is “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.” Ex.1002, 151.

However, the claimed arrangement of three distinct methods of isolation was already known. For example, Delco describes a host system that supports a number of virtual machines. Ex.1005, 5:18-22. Delco’s system includes (1) packet filters 74 (“*internal firewall*”) that isolate the virtual machine from the host system, (2) a packet filter 32 (“*host-based firewall*”) that protects the host, and an external firewall system 30 (“*network firewall*”) that provides additional protection. *See* Ex.1005, 7:4-18, 4:62-5:17.

Delco, along with the other references presented in this Petition, thus render obvious the Challenged Claims, which should be canceled for unpatentability.

II. GROUNDS FOR STANDING

Petitioner certifies that the '780 Patent is eligible for IPR and that Petitioner is not barred or estopped from requesting IPR challenging the patent claims. 37 C.F.R. § 42.104(a).

III. NOTE

Petitioner cites to exhibits' original page numbers. Emphasis in quoted material has been added.

IV. TECHNOLOGY BACKGROUND

The '780 patent relates to virtual machines and firewalls. Virtualization provides the “ability to concurrently support multiple operating system environments on a single physical computer system hardware platform.” Ex.1005, 1:17-20. A “firewall system 30 is conventionally a network appliance implementing any or all of a variety of packet inspection and control functions.” Ex.1005, 4:65-67. A more detailed summary of virtual machines and firewalls can be found in Dr. Shenoy's declaration. Ex.1003, ¶30-32.

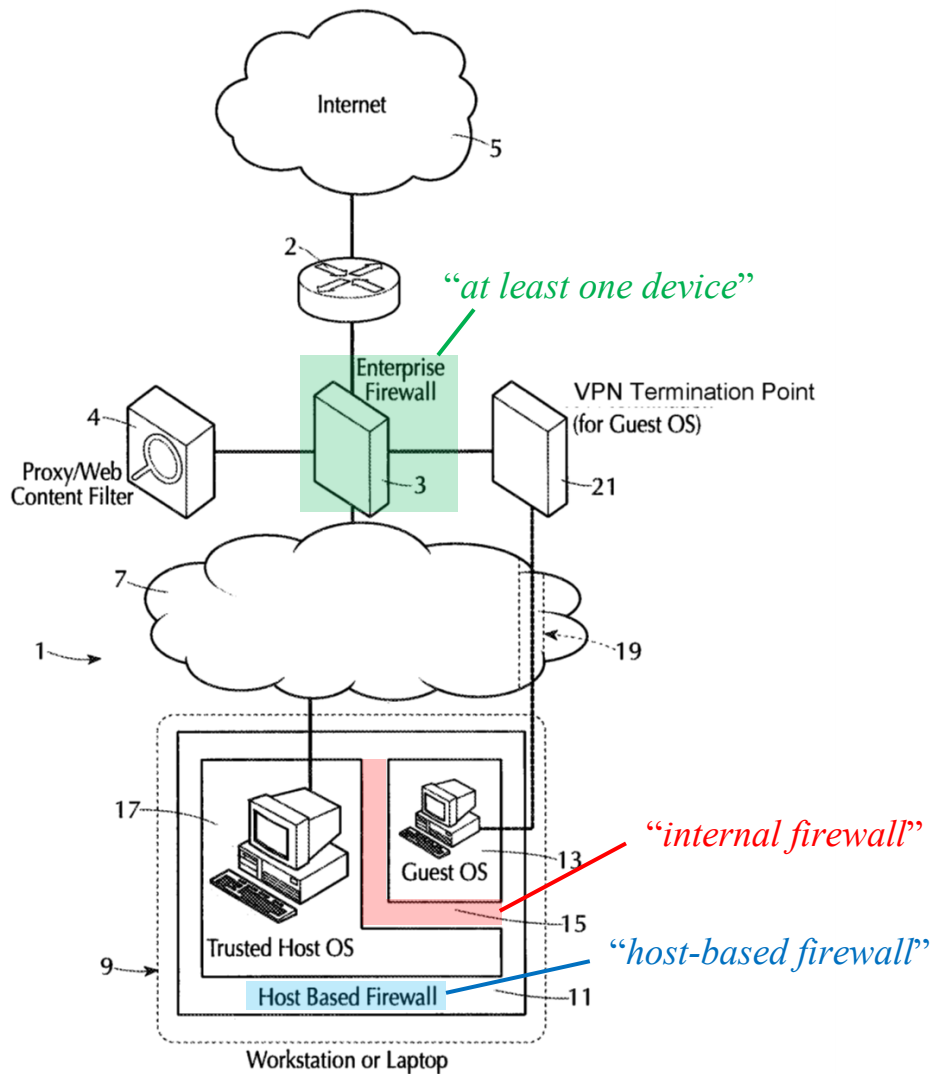
V. SUMMARY OF THE '780 PATENT

A. Overview of the '780 Patent

The '780 patent describes and claims nothing more than well-known techniques to provide network security. The '780 patent relates to “the protection of computer systems from injurious software that can be encountered while

browsing or accessing the Internet.” Ex.1001, 1:17-29. To provide such protection, the ’780 patent describes an environment that includes a “host computer [that] supports a virtual guest system running thereon.” Ex.1001, abstract.

The purported novelty of the ’780 patent—as described in the prosecution history—is “**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.” Ex.1002, 151. The independent claims recite (1) “**an internal firewall** *is configured to separate the host system from the virtual system in the computer system,*” (2) “**a host-based firewall** *executed on the computer system is configured to implement network isolation between the computer system and the network,*” and (3) “**at least one device** *configured to implement at least one of a network firewall or a web proxy.*” Ex.1001, Claim 1. These three distinct methods of isolation are illustrated in Fig. 1 below.



Ex.1001, Fig. 1 (annotated).

First, the host system is protected from any potential malware on the virtual machine through the “internal firewall.” Ex.1001, 3:42-45. “[T]he 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.” Ex.1001, 8:13-17. Second, “[t]he host system 9 also has stored data in the form of software instructions that cause the host system to have **a**

host-based firewall 11 that provides restrictive egress from the computer 9.”

Ex.1001, 7:42-45. Third, “[a] proxy/web-content filter 4 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, filtering e.g., pornographic material or data not intended for the system 1.” Ex.1001, 7:10-14.

However, as will be explained in detail below, the arrangement in which three methods of isolation are used to protect a computing system was already known at the time the ’780 patent was filed. Ex.1003, ¶¶33-37.

B. Prosecution History of the ’780 Patent.

The ’780 patent was filed March 2, 2018 and ultimately claims priority to a provisional application filed January 27, 2011. The Office issued a first office action on June 5, 2018. The Office rejected the claims as being unpatentable over U.S. Patent Publication No. 2007/0260873 to Hatfalvi (“Hatfalvi”) in view of a piece of non-patent literature entitled “A Survey on Virtual Machine Security” to Reuben (“Reuben”). Ex.1002, 91-103.

In response, the Applicant argued that “there is absolutely no mention in Hatfalvi about use of a host-based firewall on the protected computer systems.” Ex.1002, 120. The Examiner nevertheless maintained the rejection in a Final Office Action dated March 19, 2019. Ex.1002, 124-38. The Applicant then argued without amendment that “none of the asserted references, either alone or in

combination, 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.” Ex.1002, 151.

After the case was assigned to a new Examiner, the Office then issued a new non-final Office Action that withdrew the obviousness rejection and included only a double patenting rejection. Ex.1002, 188-193. After the Applicant filed a terminal disclaimer, the Office issued a Notice of Allowance. Ex.1002, 351-53. The ’780 patent then issued on March 24, 2020.

However, as evidenced by Delco and as outlined below, it was already known to use “three distinct methods of isolation” using an “internal firewall, a host-based firewall, and a network firewall” as described and claimed in the ’780 patent. Ex.1003, ¶¶38-39.

VI. LEVEL OF ORDINARY SKILL IN THE ART

A Person of Ordinary Skill in The Art (“POSITA”) in January of 2011 would have been someone knowledgeable and familiar with computers, computer networks, network security, and virtualization technologies. A POSITA would have been familiar with virtual machines, guest operating systems, and firewall technologies that existed as of that time. That person 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. Lack of work experience can be remedied by additional education, and vice versa. Ex.1003, ¶¶23-25.

VII. CLAIM CONSTRUCTION

Claim terms in IPR are construed according to their “ordinary and customary meaning” to those of skill in the art. 37 C.F.R. § 42.100(b). *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) (en banc). Petitioner submits that, for the purposes of this proceeding and the grounds presented herein, no claim term requires express construction. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017). Ex.1003, ¶40.

VIII. RELIEF REQUESTED AND REASONS FOR THE REQUESTED RELIEF

Petitioner asks that the Board institute a trial for *inter partes* review and cancel the Challenged Claims in view of the analysis below.

IX. DISCRETIONARY DENIAL WOULD BE INAPPROPRIATE

A. Discretionary denial under the *Fintiv* factors is not appropriate.

The six factors considered for § 314 discretionary denial strongly favor institution given Petitioner’s prompt filing and the compelling merits of this case. *See Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020) (precedential).

1. No evidence regarding a stay

No motion to stay has been filed, so the Board should not infer the outcome of such a motion. *Sand Revolution II LLC v. Continental Intermodal Group – Trucking LLC*, IPR2019-01393, Paper 24 at 7 (PTAB June 16, 2020) (informative); *see also Dish Network L.L.C. v. Broadband iTV, Inc.*, IPR2020-01359, Paper 15 (Feb. 12, 2021) (“It would be improper to speculate, at this stage, what the Texas court might do regarding a motion to stay...”). Thus, this factor is neutral on discretionary denial.

2. Parallel proceeding trial date

The co-pending district court case was filed in the Eastern District of Texas on February 1, 2024. The most recent statistics currently available for the Eastern District of Texas show a median time-to-trial of 21.4 months. Ex.1013, 35. Thus, the estimated trial date is December 2025.¹ The Board’s final written decision is

¹ The docket control order sets the case for trial on October 20, 2025. Ex.1012, 1. Regardless, “a court’s general ability to set a fast-paced schedule is not particularly relevant...where, like here, the forum itself has not historically resolved cases so quickly.” *In re Apple Inc.*, 979 F.3d 1332, 1344 (Fed. Cir. 2020). Notably, the court already has five other patent trials—plus four other trials—scheduled to begin October 20, 2025. *See* Ex.1016.

expected shortly after that date—in January or February of 2026. Given the proximity of the Board’s expected Final Written Decision and the estimated trial date, this factor is at least neutral. *See e.g., Cisco Systems Inc., v. Video Solutions PTE. Ltd.*, IPR2024-00194, Paper 7 (PTAB March 28, 2024) (granting institution and finding factor two neutral where “trial is likely to begin within approximately one month of [the Board’s] final written decision”).

3. Investment in the parallel proceeding

The co-pending litigation is in its early stages, with major activities including a *Markman* hearing and the close of discovery scheduled for after the Board’s expected decision on institution. *See* Ex.1012, 4 (Claim Construction hearing on April 30, 2025; close of fact discovery on May 23, 2025; close of expert discovery on July 8, 2025). Moreover, Petitioner has acted with diligence to prepare this Petition within six months after Petitioner was served with a complaint. Under *Fintiv*, Petitioner’s prompt filing “weigh[s] against exercising the authority to deny institution.” *Fintiv*, Paper 11 at 11 (“If the evidence shows that the petitioner filed the petition expeditiously, such as promptly after becoming aware of the claims being asserted, this fact has weighed against exercising the authority to deny institution under NHK”).

4. Overlapping issues with the parallel proceeding

There is no present overlap of prior art issues in the district court litigation. Moreover, Petitioner offers the following stipulation: Petitioner stipulates that if trial is instituted, it will not pursue the same grounds in the district court litigation. *See Sand Revolution II, LLC v. Cont'l Intermodal Group-Trucking LLC*, IPR2019-01393, Paper 24 at 12 (PTAB June 16, 2020). Consequently, this factor favors institution.

5. Identity of parties

Petitioner is a defendant in the litigation. That is true of most Petitioners in IPR proceedings. Accordingly, this factor should not be a basis for denying institution.

6. Other circumstances

The prior art presented in this Petition presents a compelling case on the merits. The claims of the '780 patent were allowed after the Applicant argued that “none of the asserted references, either alone or in combination, 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.” Ex.1002, 151. As will be explained in detail below, Delco teaches three distinct methods of isolation: a packet filter 74 (“*internal firewall*”), a packet filter application 32

(“*host-based firewall*”), and an external firewall system 30 (“*web proxy*”). *See* Ex.1005, Figs. 1-3.

The Board’s current policy is to “not deny institution of an IPR or PGR under *Fintiv* (i) when a petition presents compelling evidence of unpatentability.” Memorandum dated June 21, 2022 (“Memo”), 9. “Compelling, meritorious challenges are those in which the evidence, if unrebutted in trial, would plainly lead to a conclusion that one or more claims are unpatentable by a preponderance of the evidence.” Memo, 4. Here, the Petition plainly shows that the concept of using three different mechanisms of isolation for a host system was taught by Delco. Notably, the prosecution examiner allowed the claims without evaluating their unpatentability in view of Delco’s disclosure.

The evidence of unpatentability is compelling here, and the PTAB should not deny institution under *Fintiv*.

B. Discretionary denial under 35 U.S.C. § 325(d) is not appropriate.

Denial under § 325(d) is not warranted because the challenges presented in this petition are neither cumulative nor redundant to the prosecution of the ’780 patent. The Examiner did not consider any of the references relied upon in this petition. Moreover, the challenges in this petition are non-cumulative because the prior art presented here describes the claim limitations that were distinguished by the Applicant to gain allowance. *See* Ex.1002, 370; Ex.1005, Figs. 1-3.

Accordingly, the Board should not exercise its discretion to deny this petition under § 325(d).

X. IDENTIFICATION OF HOW THE CLAIMS ARE UNPATENTABLE

A. Challenged Claims and Statutory Grounds for Challenge

Grounds	Claims	Basis
#1	1-7, 9-17, and 19-20	35 U.S.C. § 103 (Pre-AIA) over Delco and Adams
#2	8 and 18	35 U.S.C. § 103 (Pre-AIA) over Delco, Adams, and Dadhia

U.S. Patent No. 8,166,474 to Delco et al. (“Delco”) was filed on September 19, 2005. Delco issued on April 24, 2012 and is thus prior art to the ’780 patent under (pre-AIA) 35 U.S.C. 102(e).

U.S. Patent Publication No. 2010/0077476 to Adams (“Adams”) was filed on September 23, 2008 and published on March 25, 2010. Adams is thus prior art to the ’780 patent under (pre-AIA) 35 U.S.C. 102(a) and (e).

U.S. Patent No. 7,886,351 to Dadhia et al. (“Dadhia”) was filed on June 19, 2006. Dadhia issued on February 8, 2011 and is thus prior art to the ’780 patent under (pre-AIA) 35 U.S.C. 102(e).²

² If Patent Owner argues that the ’780 patent is an AIA patent, Delco, Adams, and Dadhia would still qualify as prior art under post-AIA 35 U.S.C. §102(a).

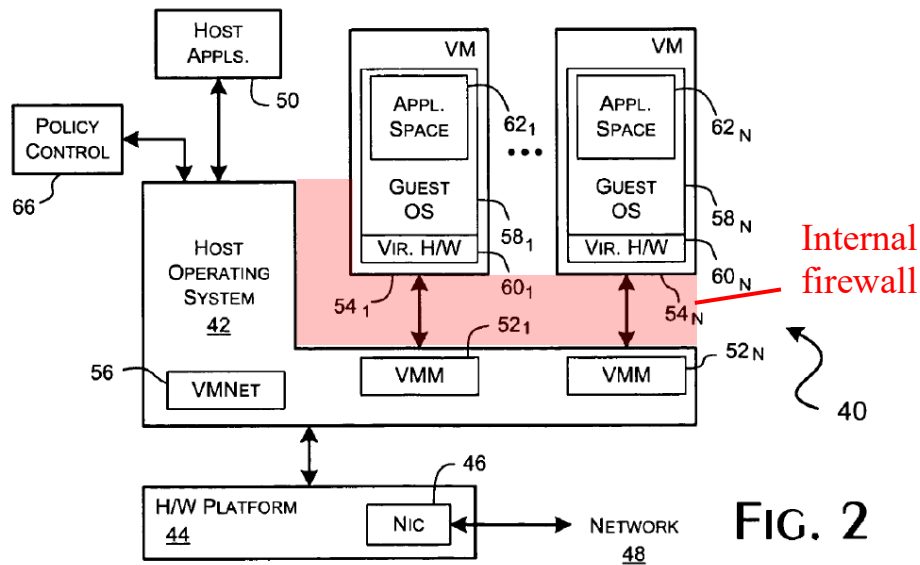
B. Ground 1: Claims 1-7, 9-17, and 19-20 are obvious in view of Delco and Adams.

1. Summary of Delco.

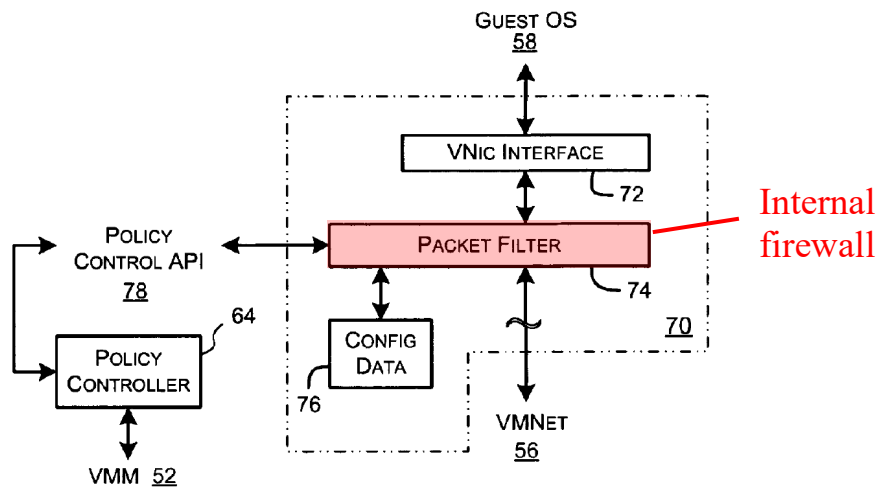
Delco, like the '780 patent, describes an environment in which a host system supports a number of virtual machines. “A host system platform 12 includes a local processor 14 and memory 16 providing a program execution space.” Ex.1005, 4:55-58. “[T]he host system platform 12 further supports the execution of guest operating systems, here represented as virtual machines 26, 28, the individual guest operating system environments.” Ex.1005, 5:18-21.

Also, like the '780 patent, Delco's system uses three distinct mechanisms for providing isolation. Delco describes (1) an internal firewall that separates the virtual machine from the host system, (2) a host-based packet filter application 32, and (3) an external firewall system 30.

The internal firewall that separates the virtual machines and guest operating systems from the host system is illustrated in Figs. 2 and 3 below.



Ex.1005, Fig. 2 (annotated); Ex.1003, ¶46.

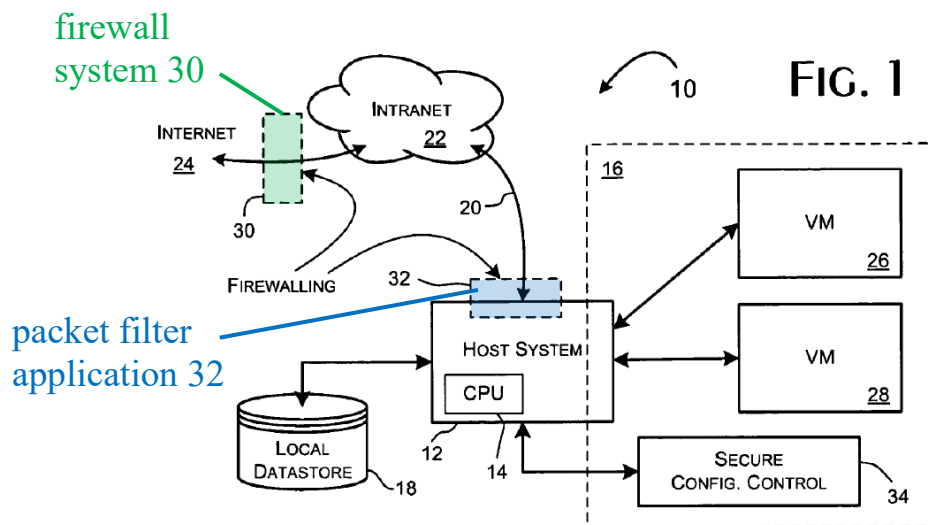


Ex.1005, Fig. 3 (annotated); Ex.1003, ¶46.

Delco describes separation between the guest operating systems and the host operating systems. For example, Delco describes a packet filter 74: “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_{1-N}.” Ex.1005, 10:28-31.

The external firewall 30 and host-based packet filter application 32 are illustrated in Fig. 1 below.



Ex.1005, Fig. 1 (annotated); Ex.1003, ¶48.

Delco’s host system is connected to a network (intranet 22) that is protected by an external firewall 30. “[A]n independent firewall system 30 can be installed generally as shown to provide network protection to the intranet 22 including the host system platform 12. The firewall system 30 is conventionally a network appliance implementing any or all of a variety of packet inspection and control functions.” Ex.1005, 4:62-65. Delco’s host system also includes its own firewall. “Alternately, though more typically in conjunction, a packet filter application 32 is

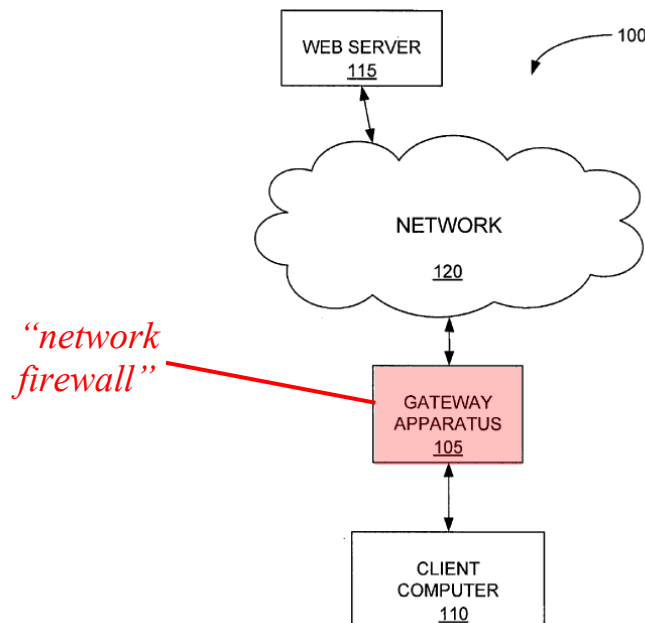
conventionally implemented and executed within the program execution space of the host system platform 12.” Ex.1005, 5:8-10.

Accordingly, Delco provides evidence that using three distinct mechanisms of isolation as described and claimed in the ’780 patent was already known.

Ex.1003, ¶44-50.

2. Summary of Adams

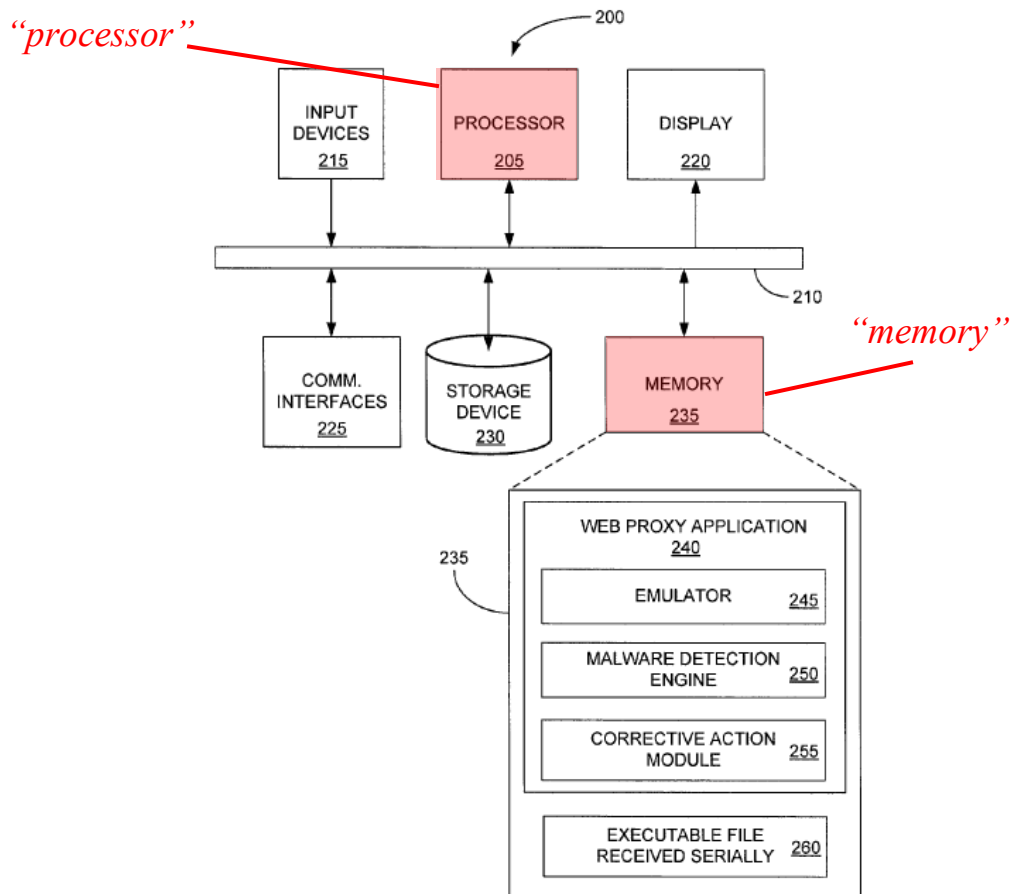
Adams, like Delco and the ’780 patent, relates to network security. Adams describes a “gateway apparatus 105” in Fig. 1, reproduced below.



Ex.1006, Fig. 1 (annotated); Ex.1003, ¶51.

Adams’ “gateway apparatus 105” may be any of “a Web proxy server, a router, and a firewall appliance.” Ex.1006, [0021]. Adams provides more details

about the structure of the external firewall. For example, the gateway apparatus can include a “processor 205” and a “memory 235” as show in Fig. 2 below.



Ex.1006, Fig. 2 (annotated); Ex.1003, ¶53.

Adams explains that its gateway apparatus includes a web proxy application stored in memory. That application isolates the client computer 110 from the network 120. Ex.1003, ¶¶51-54.

3. Reasons to Combine Delco and Adams

While a POSITA would have recognized that Delco’s network appliance

would have inherently included a processor and memory, a POSITA would have also found it obvious for Delco's external firewall system 30 to include a processor and a memory as taught by Adams. Ex.1003, ¶54.

Delco describes "an independent firewall system 30... to provide network protection to the intranet 22 including the host system platform 12. The firewall system 30 is conventionally a network appliance implementing any or all of a variety of packet inspection and control functions." Ex.1005, 4:62-65. While Delco does not describe the structural details of the firewall system 30, a POSITA would have found it obvious for such a "network appliance" to include a processor and memory. Ex.1003, ¶56. This is evidenced by Adams, which provides additional details about such network appliances.

Adams describes a gateway apparatus 105, which like Delco's firewall system 30, is a "firewall appliance." Ex.1006, [0021]. Adams provides additional structural details about the firewall appliance. Adams describes "a functional block diagram of one type of gateway apparatus" such as the gateway apparatus 105 of Fig. 1. The gateway apparatus can include a "processor 205" and a "memory 235" as shown in Fig. 2. Thus, Adams provides evidence that it would be obvious for a firewall network appliance such as Delco's to include a processor and a memory to perform its intended functions. Ex.1003, ¶57.

A POSITA would have had a reasonable expectation of success in

combining the teachings of Delco and Adams because Adams' gateway apparatus provides firewall functionality like that provided by Delco's firewall system 30.

Ex.1003, ¶58. Adams explains that “[i]n the computer industry, a firewall commonly refers to a device, set of devices, and/or software/firmware configured to permit or deny, encrypt, decrypt, or proxy all network traffic between different security domains in accordance with a set of rules or other criteria.” Ex.1006, [0036]. Delco similarly explains that its firewall acts as a packet filter “such as exemplified by the conventional IPTables and IPChains packages, content filters, such as the well-known SpamAssassin and Clam AntiVirus (ClamAV) packages, deep packet analysis and scrubbing packages, and other packages implementing network packet security functions.” Ex.1005, 5:2-7; Ex.1003, ¶58. A POSITA would have recognized these “packages” as software that were commonly stored in computer memory and executed by a computer processor. Ex.1003, ¶58; Ex.1005, 2:5-6.

Accordingly, the combination of Delco and Adams achieves the predictable result of using a processor and memory to perform the described firewall functions. Adams explains that “Web proxy application 240 and its functional modules shown in FIG. 2 are implemented as software that is executed by processor 205. Such software may be stored, prior to its being loaded into RAM for execution by processor 205, on any suitable computer-readable storage medium such as a hard

disk drive, an optical disk, or a flash memory (see storage device 230).” Ex.1006, [0028]. Ex.1003, ¶59.

Accordingly, the combination of Delco and Adams merely represents applying a known technique (implementing a network appliance with a processor and memory as taught by Adams) to a known device (Delco’s firewall appliance) ready for improvement to yield predictable results. The combination of Delco and Adams is also merely the combination of prior art elements (a processor and memory with a firewall appliance) according to known methods to yield predictable results (executing code from memory on the processor to perform firewall functions). Ex.1003, ¶60.

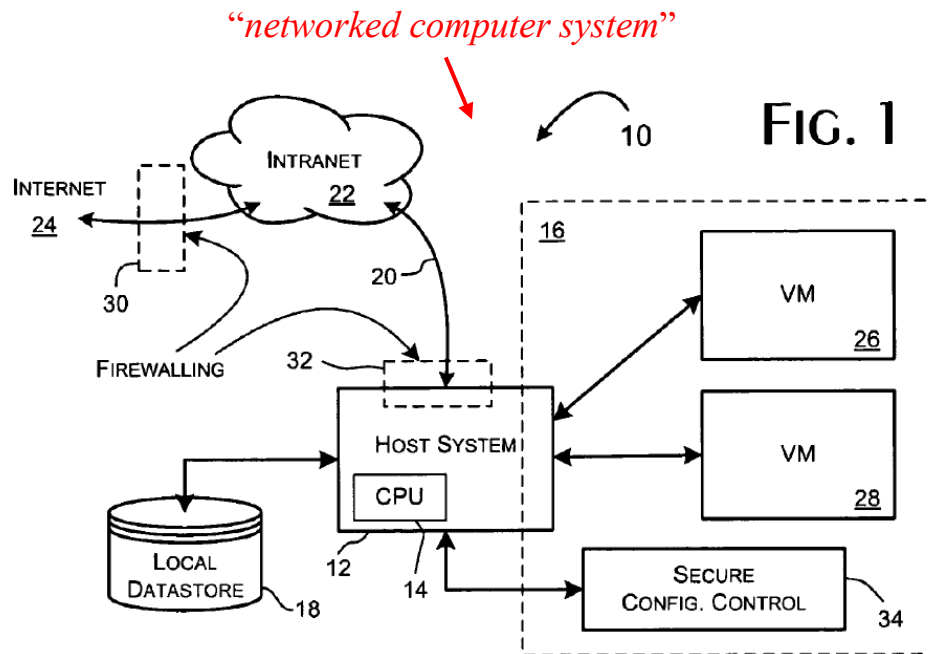
4. Claim 1

[1.0] *A networked computer system comprising:*

To the extent the preamble is limiting, it is rendered obvious by Delco.

Delco’s Fig. 1 illustrates what it refers to as a “preferred environment” of its invention, which includes a computer system 10 (“*networked computer system*”):

“**A computer system 10**, demonstrating **a preferred environment for implementation of the present invention**, is shown in FIG. 1.” Ex.1005, 4:53-56.



Ex.1005, Fig. 1 (annotated); Ex.1003, ¶62.

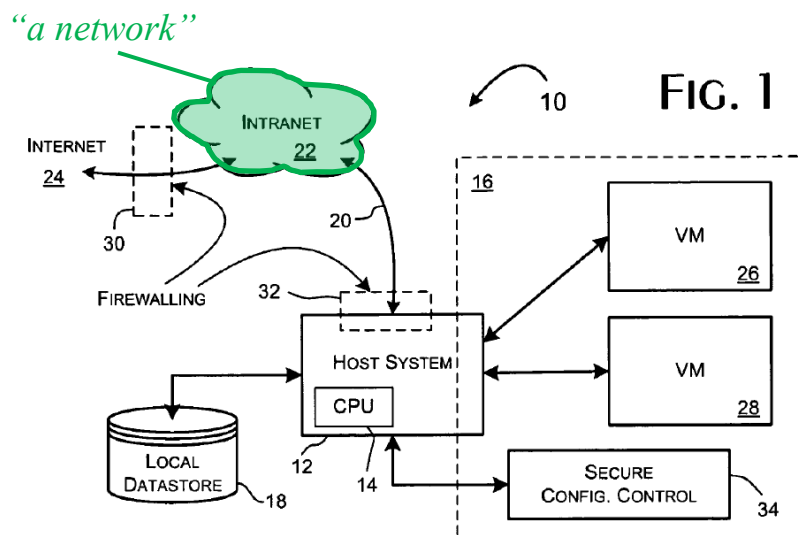
Delco's computer system 10 is a "*networked computer system*" as claimed. As shown in Fig. 1, Delco's computer system 10 includes a "host system platform 12" (Ex.1005, 4:55) connected to a "local intranet 22" and "Internet" 24. (Ex.1005, 4:58-61). Delco's computing system 10 is thus *networked* because it includes a host system 12 that is connected to the local intranet 22 and Internet 24.

Thus, because Delco describes a computer system 10 that includes a host system connected to the local intranet 22 and Internet 24, Delco renders obvious a “*networked computer system*” as claimed. Ex.1003, ¶¶61-64.

[1.1] *a network;*

Delco's computer system 10 includes an intranet 22 ("*network*") that

connects the host system 12 to the Internet 24. “The host system platform 12 preferably supports a local datastore 18 and a network interface 20 permitting connection to **a local intranet 22**, as shown, and further, or directly in alternate scenarios, to a public communications network 24, such as the Internet.” Ex.1005, 4:53-61. The local intranet 22 is illustrated in Delco, Fig. 1, shown below and highlighted in green.



Ex.1005, Fig. 1 (annotated); Ex.1003, ¶¶66.

Thus, because Delco describes a computing system 10 that includes a local intranet 22, Delco renders obvious “a network” as claimed. Ex.1003, ¶¶65-67.

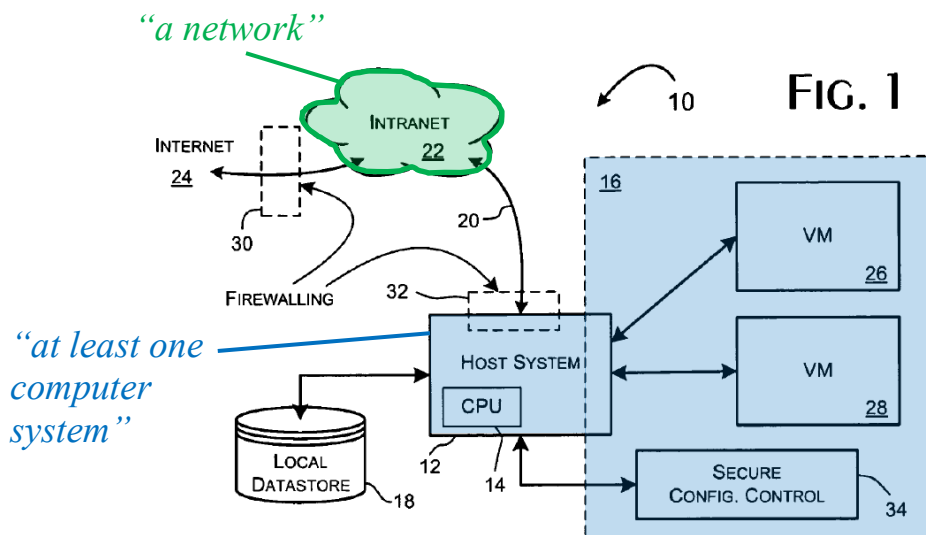
[1.2] at least one computer system configured to connect to the network,

First, Delco’s system 10 includes a host system platform 12 (“at least one computer system”). “A host system platform 12 includes a local processor 14 and

memory 16 providing a program execution space.” Ex.1005, 4:53-61.

Regarding the description accompanying Fig. 1, Delco describes “a host system platform 12” with “a local processor 14 and a memory 16 providing a program execution space.” Ex.1005, 4:55-56. As relevant to limitation [1.3] below, “the host system platform 12 further supports the execution of guest operating systems, here represented as virtual machines 26, 28.” Ex.1005, 5:18-20.

Accordingly, the host processing system and its supported virtual machines together teach “*at least one computer system*” as highlighted in blue in Fig. 1 below.



Ex.1005, Fig. 1 (annotated); Ex.1003, ¶69.

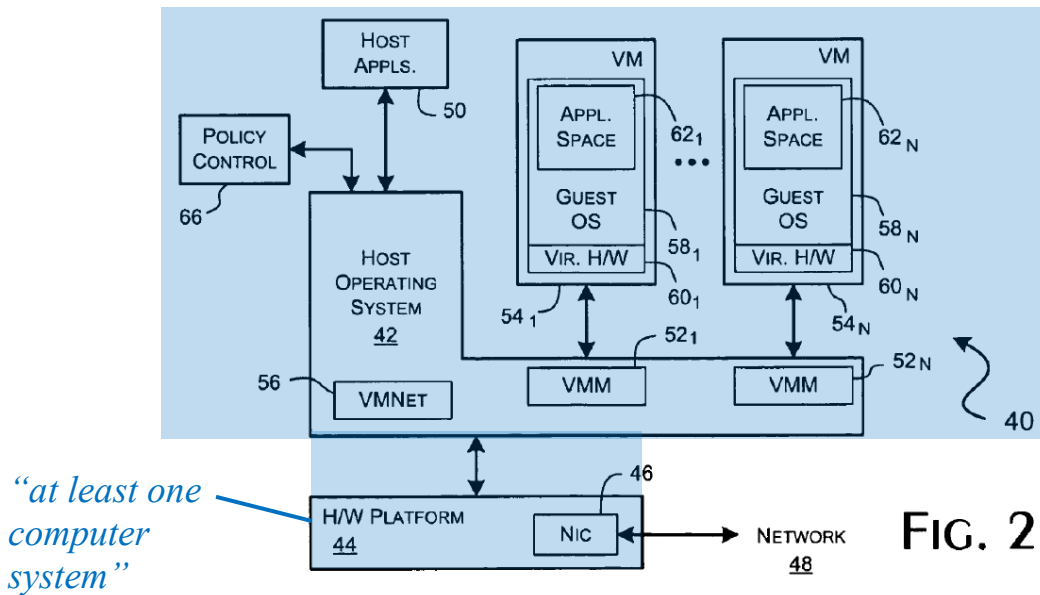
While Fig. 1 illustrates the “preferred environment” for Delco’s host system platform, Fig. 2 illustrates a “preferred embodiment” in which a host operating

system “is executed on a hardware platform 44.” Ex.1005, 4:53-55, 6:13-30. Thus, a POSITA would have naturally read Delco’s disclosures relating to Figures 1 and 2 as overlapping and intended to be integrated and understood together such that the hardware platform 44 in Fig. 2 is an implementation of the host system platform 12 in Fig. 1. Ex.1003, ¶70.

For example, Delco explains that “[t]he hardware platform 44 also preferably includes a central processor 14 and a local datastore 18.” Ex.1005, 6:16-18. The “local datastore 18,” however, is depicted only in Figure 1 and not in Figure 2. This further confirms a POSITA’s understanding that the hardware platform 44 and the systems it supports are an implementation of the host system platform 12 described with respect to Fig. 1. Ex.1003, ¶71. It would have been obvious to a POSITA, therefore, to combine features of Delco’s Fig. 1 and Fig. 2 disclosures.

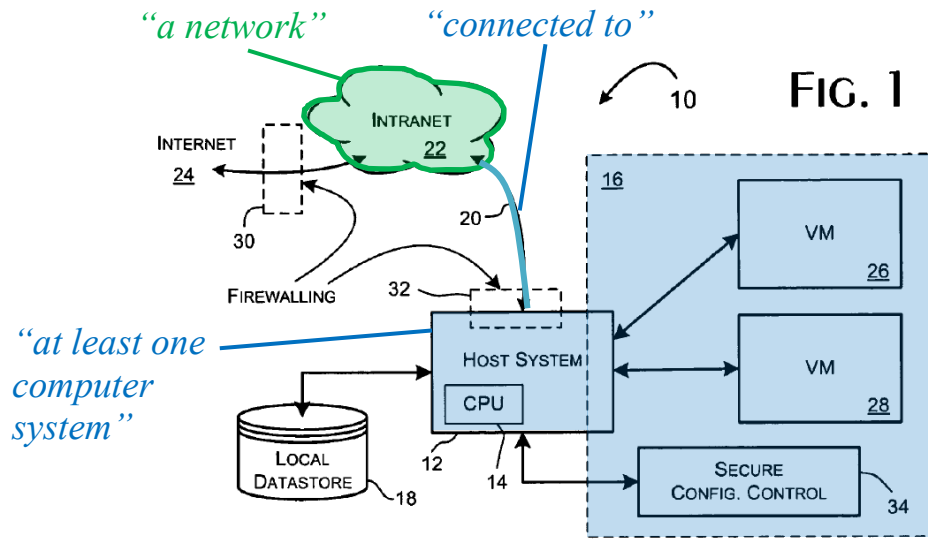
Delco illustrates in Fig. 2 that the hardware platform 44 supports a host operating system 42 and virtual machines 54_{1-N}. “[H]ost operating system 42” (Ex.1005, 6:15) runs “instances of a virtual machine monitor (VMM) 52_{1-N} provided to support a set of one or more virtual machines (VM) 54_{1-N}” (Ex.1005, 6:23-25). Delco’s Fig. 1 illustrates the host system platform 12 which supports virtual machines 26 and 28. The hardware platform 44 similarly supports a host operating system 42 and virtual machines 54_{1-N}. Accordingly, Delco’s host system

platform 12, which may be implemented as hardware platform 44 to support host operating system 42 and virtual machines 54_{1-N} as shown in Fig. 2, teaches “*at least one computer system*” as claimed.



Ex.1005, Fig. 2 (annotated); Ex.1003, ¶72.

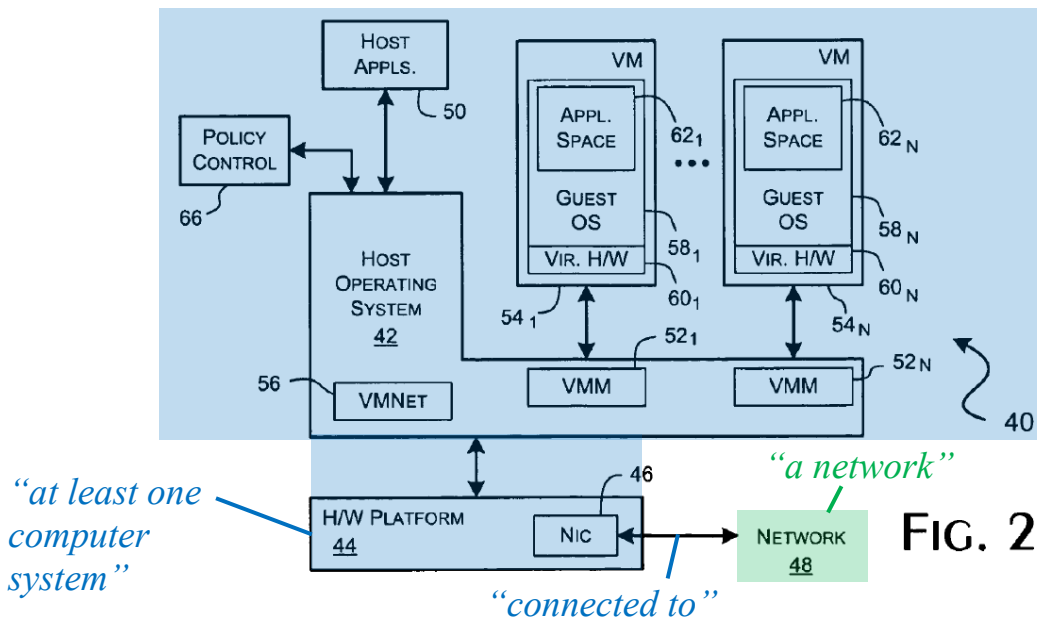
Second, Delco explains that the host system platform 12 is connected to the intranet 22 and is thus “*connected to the network.*” As explained above at [1.1], Delco’s computer system 10 includes an intranet 22 (“*network*”) that connects the host system 12 to the Internet 24. *See* Ex.1005, 4:53-61.



Ex.1005, Fig. 1 (annotated); Ex.1003, ¶73.

Delco also explains that “configuration files” may be received by the host system 12 and stored “through a secure network connection with a remote configuration server accessible through the network 20.” Ex.1005, 6:4-7. Because network 20 connects to Intranet 22, which a POSITA would have understood is in turn connected to a remote configuration server, Delco renders obvious that the host system is “*configured to connect to the network.*” Ex.1003, ¶74.

Delco further teaches that in the example embodiment of Fig. 2, the hardware platform 44—which is an implementation of host system platform 12—is connected to a network. Fig. 2 illustrates hardware platform 44 connected to “external communications network 48.” Ex.1005, 6:19–20.



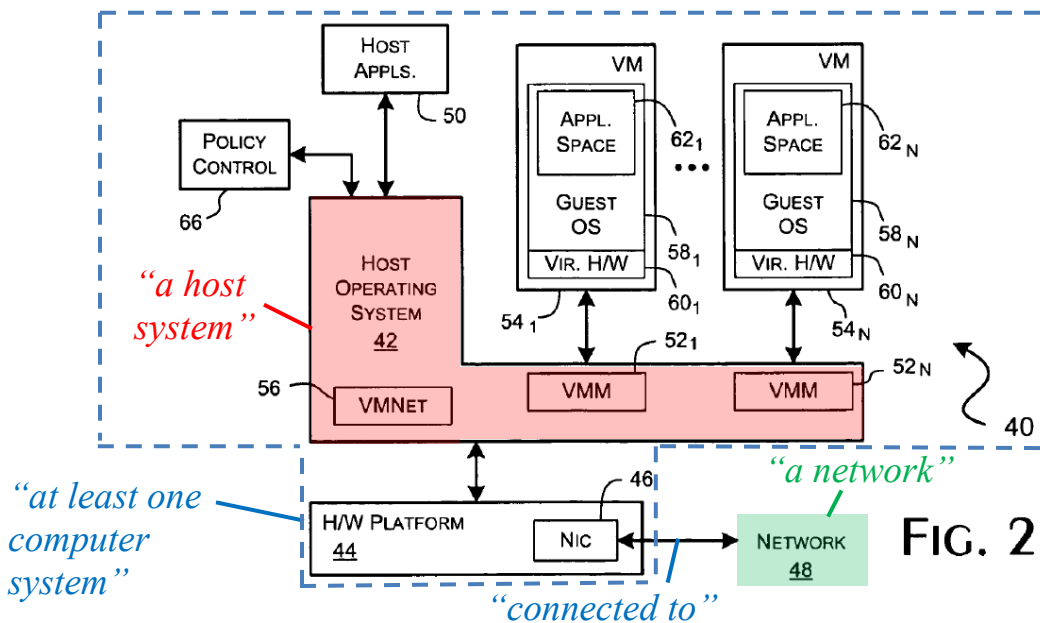
Ex.1005, Fig. 1 (annotated); Ex.1003, ¶75.

It would have been obvious that the network 48 may be or include features or characteristics of a local intranet, such as intranet 22. Ex.1003, ¶76. For example, Delco describes defining a “network zone” based on “characteristics of the network 48.” Ex.1005, 9:7-17; *see also* 10:51. Delco’s Fig. 1 and accompanying text describe at least one computer system (the host system platform 12 in conjunction with virtual machines 26 and 28) configured to connect to the network (connected to intranet 22). Delco’s Fig. 2 describes an implementation of the host system platform 12 as hardware platform 44 that supports the host operating system 42 in conjunction with virtual machines 54 and is configured to connect to the network 48. Accordingly, the intranet 22 shown in Delco, Fig. 1 and/or the network 48 shown in Delco, Fig. 2 correspond to a network, as claimed.

Thus, because Delco describes a network-connected host system platform 12 that is implemented as hardware platform 44 supporting a host operating system and virtual machines, Delco renders obvious “*at least one computer system configured to connect to the network*” as claimed. Ex.1003, ¶¶68-78.

[1.3] the computer system comprising a host system and a virtual system,

First, Delco explains that a “host operating system 42 is executed on a hardware platform 44.” Ex.1005, 6:13-30. Delco’s host operating system teaches a “*host system*” as claimed.

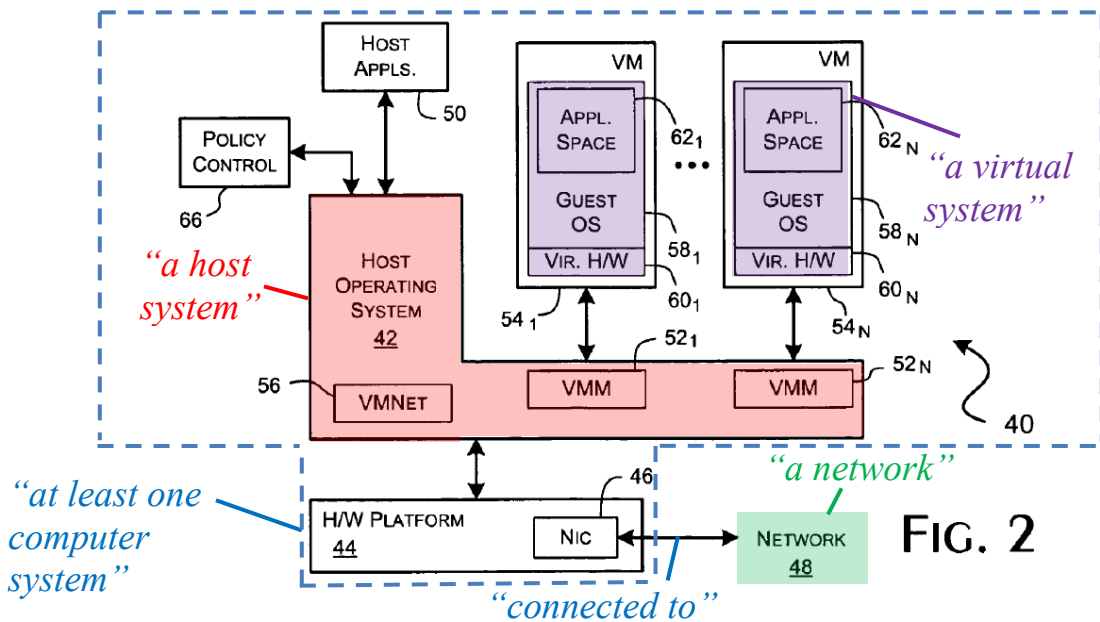


Ex.1005, Fig. 1 (annotated); Ex.1003, ¶79.

Second, Delco’s host operating system 42 supports virtual machines 54_{1-N}, that execute guest operating systems, any of which is “*a virtual system*” as claimed. “The host operating system 42 supports the execution of any number of

conventional applications 50 and the components of the virtualization framework, which include instances of a virtual machine monitor (VMM) 52_{1-N} provided to support a set of one or more virtual machines (VM) 54_{1-N}.” Ex.1005, 6:13-30. “The virtual machines 54_{1-N} functionally encapsulate **guest operating systems 58_{1-N}**.” Ex.1005, 6:31-60. The guest operating systems make use of “guest operating system execution space above a virtual hardware component layer 60_{1-N}.” Ex.1005, 6:31-60. Delco further explains that “[a]s 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}.” Ex.1005, 6:31-60.

Accordingly, Delco’s virtual machines support guest operating systems 58_{1-N}. Any of the guest operating systems 58_{1-N}, which execute on the virtual machines 54_{1-N}, teach a “*virtual system*” as claimed.



Ex.1005, Fig. 1 (annotated); Ex.1003, ¶80.

Thus, Delco teaches a host system platform 12 implemented as a hardware platform 44 that executes a host operating system 42 supporting a number of virtual machines with guest operating systems, which renders obvious “*the computer system comprising a host system and a virtual system*” as claimed. Ex.1003, ¶¶79-82.

[1.4] wherein the virtual system is a separate operating system or a software module operating on the computer system³,

First, Delco’s virtual machines 54_{1-N} support guest operating systems

³ A POSITA would have understood that “the computer system” refers to “the at least one computer system.” Ex.1003, ¶83.

(“virtual system[s]”) which are “*separate operating system[s]*” consistent with a POSITA’s understanding of virtual machines. Ex.1003, ¶83. Delco describes virtual machines as “**separate** virtual machine execution processes” which are “effectively **isolated** from one another and from the host operating system.” Ex.1005, 6:31-60. Delco explains that “the virtual machines 54_{1-N} are preferably executed as individual instances of a virtual machine application loaded and managed through **separate** virtual machine execution processes.” Ex.1005, 6:31-60. “The virtual machines 54_{1-N} functionally **encapsulate guest operating systems** 58_{1-N}. 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.” Ex.1005, 6:31-60.

Delco also explains that guest operating systems are “*separate operating system[s]*” because the virtual machines “logically encapsulate[] a separate instance of an operating system.” Ex.1005, 1:21-23. Delco further explains that this “virtualization architecture...enforce[s] **isolation** between the multiple virtual machines.” Ex.1005, 1:37-39. “This isolation enables the virtual machines to encapsulate and **execute a different operating system**[], whether based on type, such as Windows7 and Linux7, specific OS variant, such as WindowsXPJ or RedHat7 Linux, or OS version.” Ex.1005, 1:43-47. This isolation is accomplished by “restrict[ing] the accessible memory space to that defined for the executing

virtual machine 54_{1-N}.” Ex.1005, 6:43-45.

Delco also teaches the alternatively claimed limitation in which the virtual machines are “*software module[s]*.” Delco explains that “[t]he virtual hardware component layer 60_{1-N} of the virtual machines 54_{1-N} is preferably implemented **as a coordinated set of software components**.” Ex.1005, 6:61-63. Thus, while Delco’s description of virtual machines 26, 28, and/or 54 as operating systems is adequate to render the claim language obvious, Delco also renders the alternatively claimed limitation obvious.

Second, Delco’s guest operating systems 58_{1-N} “*operat[e] on*” the hardware platform 44 (“*the computing system*”), which in Fig. 1 is represented as the host system 12. Delco explains that its systems “allow direct execution of the in-context virtual machine 26, 28 **on the host system 12**.” Ex.1005, 5:51-52. In addition, “the host system platform 12...supports the execution of guest operating systems, here represented as virtual machines 26, 28.” Ex.1005, 5:18-20.

Like the virtual machines 26, 28 described with respect to Fig. 1, the virtual machines 54_{1-N} and their guest operating systems 58_{1-N} are executed on the hardware platform (“*the computing system*”). “In the preferred embodiments, the virtual machines 54_{1-N} are preferably executed as individual instances of a virtual machine application loaded and managed through separate virtual machine execution processes (designated as VMX processes) instantiated within the

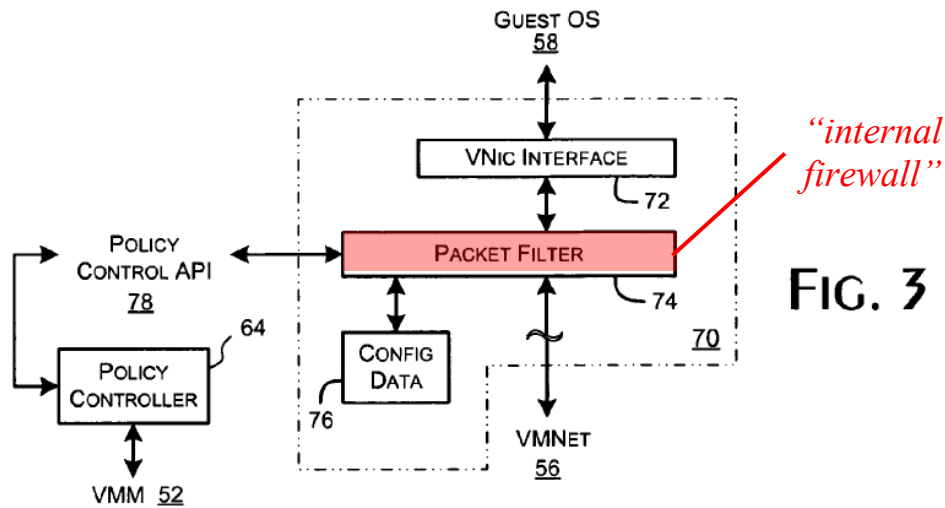
program execution space of the host operating system 42.” Ex.1005, 6:31-36. In addition, “the virtual machines 54_{1-N}” operate “with support from the virtual machine monitor 52_{1-N}, host operating system 42 resident drivers, and the underlying hardware platform 44.” Ex.1005, 6:65-67.

Thus, because Delco’s guest operating systems running on the virtual machines are separate operating systems running on the host system platform, Delco renders obvious “*wherein the virtual system is a separate operating system or a software module operating on the computer system*” as claimed. Ex.1003, ¶¶83-89.

[1.5] *wherein an internal firewall is configured to separate the host system from the virtual system in the computer system, and*

First, 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. Ex.1005, 7:4-18. By 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.*”

Delco’s packet filter is implemented by a “virtual network interface component 70.” Ex.1005, 7:4-18. The virtual network interface component 70 is shown in Fig. 3, below.



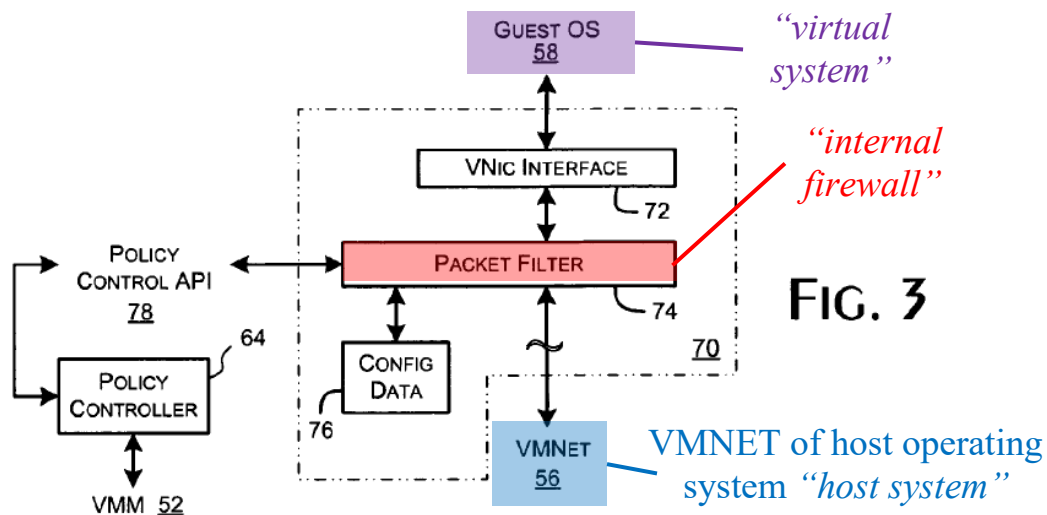
Ex.1005, Fig. 3 (annotated); Ex.1003, ¶92.

Delco’s packet filter layer 74 is an “*internal firewall*” because it performs the function of a firewall—filtering packets⁴—between the internal virtual machine and destinations that are external to the virtual machine (e.g., the host system 42 or over the Internet). Delco explains that the packet filter layer 74 may be configured according to “a set of policy rules.” Ex.1005, 7:29. Delco describes a wide range of different customized policy rules such as “per-packet” filtering (Ex.1005, 8:36) or

⁴ See e.g., Ex.1005, 1:65-2:5 (“**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**.”).

which ports the virtual machine can access (*see* Ex.1005, 8:43-45).

Second, 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 system⁵ (“*host system*”) as shown below.



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

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

⁵ Fig. 2 illustrates the VMNet 56 as part of the host operating system 42.

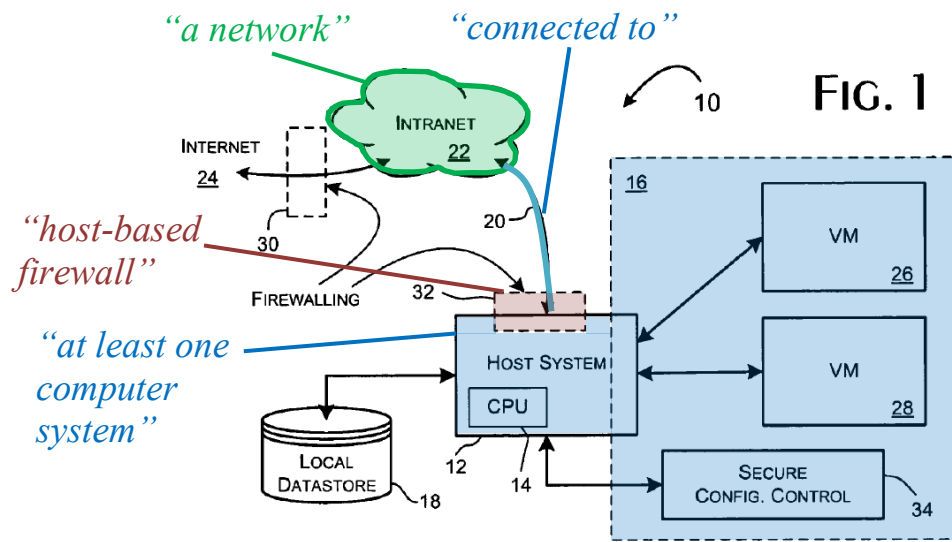
respect to **all external entities, including the host operating system** and other virtual machines.” Ex.1005 3:40-46. By filtering traffic between the virtual system and the host system, the packet filter 74 acts as an internal firewall that implements isolation between the virtual machine(s) and the host operating system.

Thus, because Delco’s packet filter acts as a firewall that separates the virtual machine from the host system and the network, Delco renders obvious “*wherein an internal firewall is configured to separate the host system from the virtual system in the computer system*” as claimed. Ex.1003, ¶¶90-96.

[1.6] *a host-based firewall executed on the computer system is configured to implement network isolation between the computer system and the network; and*

Delco describes a packet filter application 32 (“*host-based firewall*”) that is executed on the host system platform 12 (“*executed on the computer system*”).

“[A] packet filter application 32 is conventionally implemented and executed within the program execution space of the host system platform 12.” Ex.1005, 5:8-17.



Ex.1005, Fig. 1 (annotated); Ex.1003, ¶97.

The packet filter 32 is a “firewall” because it performs the function of a firewall—filtering packets. *See e.g.*, Ex.1005, 1:65-2:5. Indeed, Delco’s Fig. 1 labels the packet filter application 32 as “FIREWALLING.” Ex.1005, 4:65, 5:8-9. Because the packet filter application 32 is positioned between the host system platform 12 and the intranet 22, it performs network isolation between the host system platform 12 (“the computer system”) and the intranet 22 (“the network”).

As shown in Fig. 1, the packet filter application 32 is positioned between the host system 12 and the intranet 22. Therefore, a POSITA would have understood that the packet filter application 32 isolates the host system 12 from the intranet 22. Delco explains that the firewall 32 is designed to protect the host system 12, and the virtual machines 26, 28, from vulnerabilities. *See* Ex.1005, 5:22-24. A POSITA

would have recognized that the filter 32 would selectively isolate the host system 12 from the intranet 22 to prevent malicious files from being transferred to the host system 12 and vice versa. Ex.1003, ¶199.

The '780 patent itself further confirms a POSITA's understanding that Delco's packet filter application 32, which performs firewall functions, teaches a firewall. Ex.1003, ¶100. The '780 patent explains that its architecture "is preferably implemented by commercial-off-the-shelf (COTS) hardware, all of which is readily available. The computers described herein and the networks, both local area and the internet, rely on the standard well known network hardware now in common use." Ex.1001, 4:50-55. The '780 patent then specifically admits that there is nothing novel about the host-based firewall specifically, explaining that it "may be implemented using software such as, for example, that sold under the names Symantec Endpoint Protection or MacAfee Host-Based Security Systems." Ex.1001, 7:45-48. Delco similarly explains that "Various network security and content filter applications for client system platform configurations are available from Symantec Corporation, Cupertino, Calif." Ex.1005, 5:12-14.

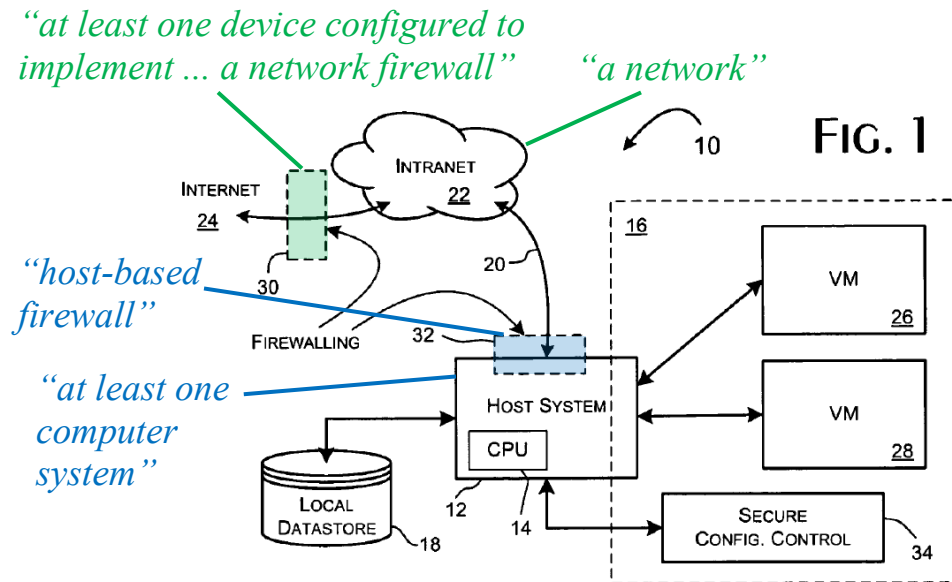
Thus, because Delco discloses the conventional host-based firewall (packet filter application 32) executed on the computer system (host system 12), which is configured to implement network isolation between the computer system and the network (to prevent malicious files from begin transferred to the host system 12),

Delco renders obvious “a host-based firewall executed on the computer system is configured to implement network isolation between the computer system and the network” as claimed. Ex.1003, ¶¶97-101.

[1.7] at least one device configured to implement at least one of a network firewall or a web proxy,

Delco further describes an independent firewall system 30 (“network firewall”) that is external to the host system platform. Delco explains that conventionally, “an independent firewall system 30 can be installed generally as shown to provide network protection to the intranet 22 including the host system platform 12. The firewall system 30 is conventionally a network appliance implementing any or all of a variety of packet inspection and control functions.” Ex.1005, 4:62-5:7.

The firewall system 30 in Fig. 1 is positioned between the intranet 22 and the internet 24. Delco explains that this **firewall 30** “selectively filter[s] network traffic to and from the physical computer system.” Ex.1005, 1:63–67.



Ex.1005, Fig. 1 (annotated); Ex.1003, ¶103.

Delco’s firewall system 30 is analogous to the “*network firewall*” described and claimed in the ’780 patent. The ’780 patent explains that the network firewall is a conventional product. It first describes “a firewall 3 and a router 2 of conventional configuration that is well-known in the art.” Ex.1001, 7:9-10. Delco’s firewall system is an example of the “firewall” that the ’780 patent acknowledges is well-known in the art.

Thus, because Delco describes an external device that functions as a firewall system, Delco renders obvious “*at least one device configured to implement at least one of a network firewall*” as claimed. Ex.1003, ¶¶102-05.

Alternatively, as discussed further for limitation [1.8] below, Adams describes a “gateway apparatus 105” that operates as a “Web proxy... and a

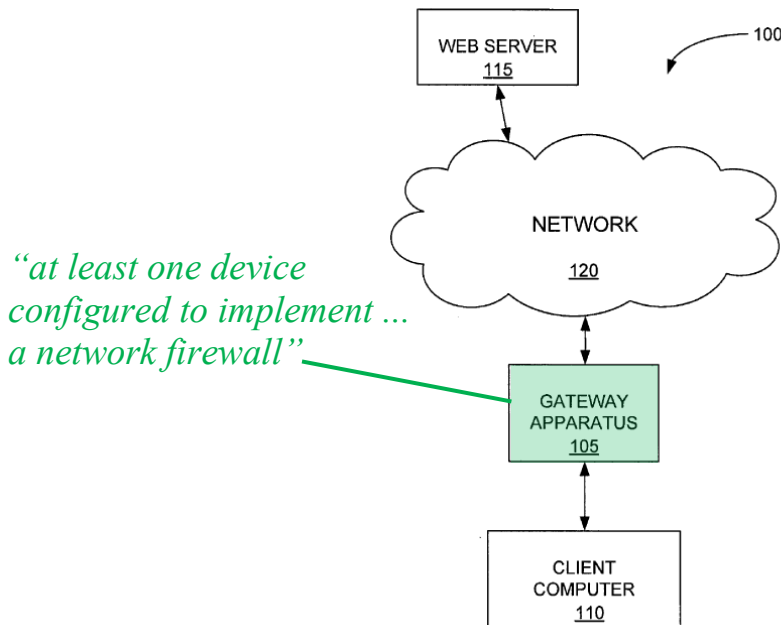
firewall appliance.” Ex.1006, [0021]. In view of Adams’ disclosure, it would have been obvious for Delco’s firewall system 30 to additionally, or alternatively, implement a *web proxy*. Ex.1003, ¶105.

[1.8] *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.*

First, to the extent it is not inherent, a POSITA would have found it obvious for Delco’s firewall system 30 to include a processor and a memory, as evidenced by Adams. Ex.1003, ¶106.

Delco does not provide details regarding the structure of the firewall system 30, i.e., whether it is a device that includes *a processor and a memory*. However, in combination with Adams, a POSITA would have understood that a firewall, such as the firewall system 30, would include *a processor and a memory configured to implement network isolation between one or more untrusted network destinations and the networked computer system*. See *supra* X.B.3; Ex.1003, ¶107.

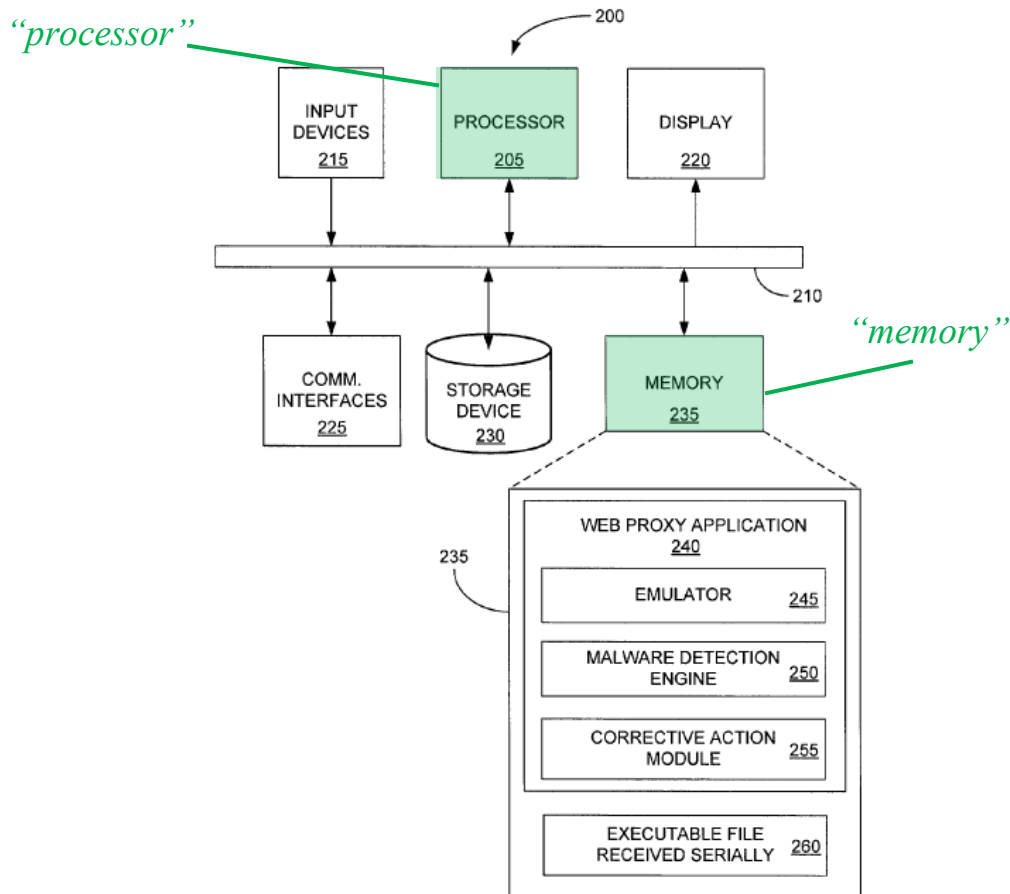
Adams describes a firewall that includes a processor and a memory to perform its intended functions. Adams illustrates a “gateway apparatus 105” in Fig. 1, reproduced below.



Ex.1006, Fig. 1 (annotated); Ex.1003, ¶108.

Adams’ “gateway apparatus 105” may be any of “a Web proxy, a router, and a firewall appliance.” Ex.1006, [0021]. Just as the firewall system 30 in Delco is positioned between the internet 24 and the intranet 22, the gateway apparatus 105 is positioned between the network 120 “which, in some embodiments, includes the Internet” and the client computer 110. Ex.1006, [0021].

Adams’ Fig. 2 is “a functional block diagram of one type of gateway apparatus” such as the gateway apparatus 105 of Fig. 1. Ex.1006, [0022]. The gateway apparatus can include a “processor 205” and a “memory 235” as show in Fig. 2 below.



Ex.1006, Fig. 2 (annotated); Ex.1003, ¶110.

Adams’ gateway apparatus also teaches a “web proxy” as alternatively claimed. Adams explains that its gateway apparatus includes a web proxy application stored in memory. “In FIG. 2, memory 235 includes Web proxy application 240.” Ex.1006, [0025].

Adams’ gateway apparatus isolates the client computer 110 from the network 120. For example, the gateway “tests [executable files] for the presence of malware.” Ex.1006, [0027]. If a file contains malware, the gateway “prevent[s] the executable file 260 from propagating further over network 120. That is, corrective

action module 255 can block an executable file 260 that includes malware, thereby preventing it from reaching a client computer 110.” Ex.1006, [0033].

In summary, it would have been obvious for Delco’s firewall system 30 to include a processor and memory as evidenced by Adams.

Second, Delco explains that its firewall system 30 implements network isolation between the Internet 24, which it describes as “a public communications network” and the intranet 22 and host system platform 12 (“*the networked computer system*”). Ex.1005, 4:60. A POSITA would have understood that a destination on the Internet would be considered an *untrusted network destination*, as claimed. Ex.1003, ¶113; Ex.1008, [0006] (“A firewall is a system or combination of systems ... that enforce a boundary between a trusted data network and an **untrusted data network ... such as the internet.**”); Ex.1009, 1:30-32 (“When a computer is connected to **a public network, such as the Internet**, the computer is vulnerable to attack and compromise from other computers on the network.”). Specifically, Delco’s firewall system 30 “selectively filter[s] network traffic to and from the physical computer system.” Ex.1005, 1:63-67.

In addition, “[t]he firewall system 30 is conventionally a network appliance implementing any or all of a variety of packet inspection and control functions.” Ex.1005, 4:62–67. Filtering network traffic and inspecting and controlling functions as described in Delco is *implementing network isolation* as claimed.

Indeed, the function and purpose of a gateway or firewall is to provide isolation between trusted and untrusted networks. *See e.g.*, Ex.1010, [0040] (“[G]ateway 120 may provide **isolation between the untrusted and trusted networks** or network domains ... gateway 120 may include a firewall to allow only certain types of packets or traffic to pass.”); Ex.1003, ¶115.

Thus, because Adams describes the structural details (e.g., processor and memory) of a firewall such as the one described by Delco, which filters packets from the Internet (an untrusted network destination), Delco and Adams render obvious “*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*” as claimed. Ex.1003, ¶¶106-16.

5. Claim 2

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

First, for the reasons explained above at [1.5], Delco’s packet filter layer 74 (“*internal firewall*”) prevents data from being communicated from the guest operating system 58 to the host operating system 42.

Second, Delco describes a “default packet filter configuration” that is configured “*without an explicit user input.*” “Advantageously, the packet filter of a virtual network interface controller 70 is fully initialized prior to any execution of a

guest operating system 58_{1-N} within the corresponding virtual machine 52_{1-N}.”

Ex.1005, 10:9-16. “Even if a zone and controller identity criteria match is not found, an administratively defined default packet filter configuration is established before any possible compromise [sic] of the guest operating system 58_{1-N}.”

Ex.1005, 10:9-16. Because the packet filter has a default configuration upon initialization, it performs its function of preventing communication “*without explicit user input*.”

Additionally, it would have been obvious for Delco’s set of policy rules to be embodied as a “white list” such that only specifically allowed types of communication are allowed to pass. Delco explains that users may change the filtering policy through a management interface. Delco describes “a set of policy rules that define the operational behavior of the packet filter layer 74 is preferably stored as configuration data in an in-memory table 76. A management program interface 78 is preferably provided to allow the setting and updating of the policy rule set held in the table 76.” Ex.1005, 7:19-37. It was known for policy rules—such as the rule set held in table 76—to exist as a white list. *See e.g.*, Ex.1014, [0048] (“[A] policy database may be a block list, a black list, an allowed list, a white list, or the like”). Therefore, Delco’s rule set—embodied as a white list—would have functioned to prevent communication absent “*explicit user input*” as claimed. Ex.1003, ¶¶117-20.

6. Claim 3

[3.1] *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.*

First, Delco’s host operating system utilizes a program execution space (“*host memory space*”). See Ex.1005, 4:53-61 (“memory 16 providing a program execution space”).

Delco’s system stores data within the program execution space. For example, “a packet filter application 32 is conventionally implemented and executed within the program execution space of the host system platform 12.” Ex.1005, 5:9-12. A POSITA would have understood that the packet filter application 32 would process packets for the purpose of filtering packets. Ex.1003, ¶122. The packets themselves are data, and it would have been obvious to a POSITA to *store* the packets in a *host memory space* while the packets are being processed. Accordingly, Delco’s host system “*is configured to store data in a host memory space.*”

Second, Delco’s guest operating systems (each one a “*virtual system*”) store data in their own memory space referred to as the guest operating execution space (“*virtual memory space*”). “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}.” Ex.1005, 6:31-45. “In turn, each virtual machine 54_{1-N}, as executed, then preferably further defines **a guest operating system execution space** above a virtual hardware component layer 60_{1-N}. The guest operating system execution space represents the apparent physical memory address space available to the guest operating system 58_{1-N}.” Ex.1005, 6:46-51. Delco also explains that the “program execution spaces 62_{1-N} [is] held available for the execution of applications by the guest operating systems 58_{1-N}.” Ex.1005, 6:51-60.

Delco’s guest operating systems thus store application data in their respective execution spaces. For example, “program execution spaces 62_{1-N} held available for the execution of applications by the guest operating systems 58_{1-N}.” Ex.1005, 6:46-60. Accordingly, Delco’s guest operating systems are “*configured to store data in a virtual memory space.*”

Third, Delco’s guest operating system execution spaces are “*segregated from*” Delco’s host program execution space. Delco explains that “[a]s 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}.” Ex.1005, 6:46-60. “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}.” Ex.1005, 6:31-45.

Thus, because Delco describes the conventional arrangement in which the guest operating systems utilize their own separate program execution space that is segregated from the host’s memory space, Delco renders this limitation obvious. Ex.1003, ¶¶121-26.

7. Claim 4

[4.1] *The networked computer system of claim 1, wherein malware introduced to the computer system is prevented from moving to another computer system of the networked computer system.*

As explained above at [1.5], Delco’s host system platform 12 includes a host-based firewall in the form of packet filter application 32. Delco’s packet filter is configured to prevent malware from moving from the host machine to an external system. For example, Delco explains that its firewalling techniques are designed to overcome flaws in previous systems in which malware could spread. See Ex.1005, 2:48-58.

Delco further explains the function of its packet filters: “For purposes of describing the present invention, the term packet filter is used to encompass packet filtering packages, such as exemplified by the conventional IPTables and IPChains packages, content filters, such as the well-known SpamAssassin and Clam AntiVirus (ClamAV) packages, deep packet analysis and scrubbing packages, and

other packages implementing network packet security functions.” Ex.1005, 4:67-5:7. Thus, by filtering out spam and computer viruses, Delco’s packet filters 32 prevent malware from spreading from the host system to other systems on the intranet 22 (“*network*”) as claimed. And a POSITA would have found it obvious that the intranet 22 would include other systems. Delco explains that the intranet is a “protected, typically corporate, network.” Ex.1005, 2:15-16. The purpose of such a corporate network is to connect multiple systems together. Ex.1003, ¶¶127-29.

8. Claim 5

[5.0] *The networked computer system of claim 1, wherein the computer system is configured to:*

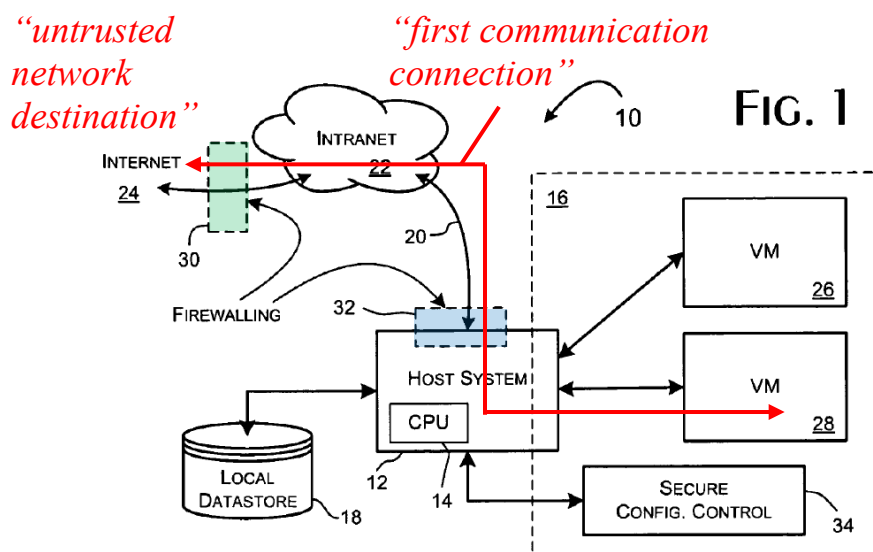
See [1.0]-[1.8]. As will be explained below, Delco’s guest operating system accesses the network through a first connection, and Delco’s host operating system accesses the network through a second, separate connection. Ex.1003, ¶130.

[5.1] *communicate with the one or more untrusted network destinations via a first communication connection,*

Delco’s virtual machines communicate with the Internet 24 (“*one or more untrusted network destinations*”) through a first connection. “The host system platform 12 preferably supports a local datastore 18 and a network interface 20 permitting connection to ... a public communications network 24, such as the Internet.” Ex.1005, 4:53-61.

Delco notes that a “physical computer system may be used in a generally

untrusted network environment.” Ex.1005, 2:10-12. A POSITA would have understood that the Internet is such an untrusted environment. *See e.g.*, Ex.1008, [0006] (“A firewall is a system or combination of systems ... that enforce a boundary between a trusted data network and an **untrusted data network ... such as the internet.**”); Ex.1003, ¶132.



Ex.1005, Fig. 1 (annotated); Ex.1003, ¶138.

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

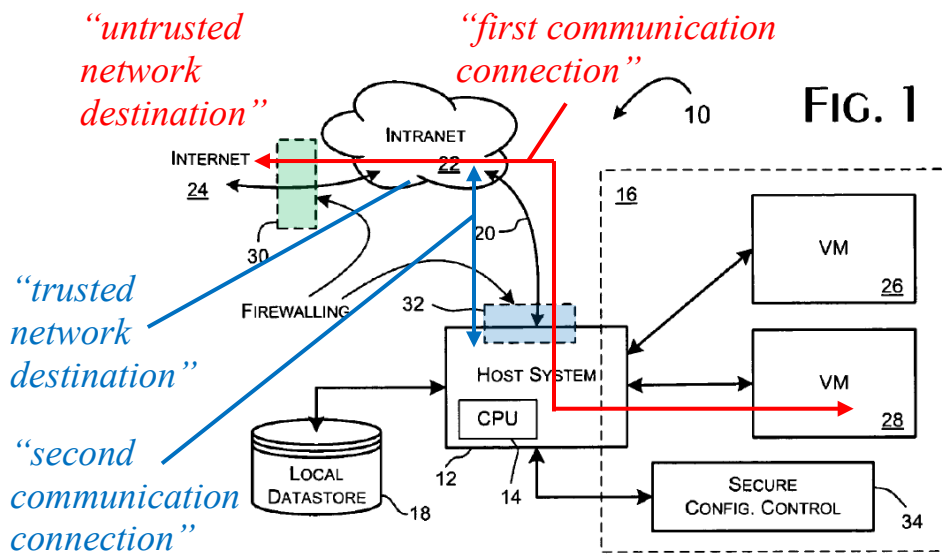
a packet filter layer 74.” Ex.1005, 7:8-10. Delco’s packet filter is intended to filter out harmful packets from untrusted destinations such as the Internet. *See* Ex.1005, 2:26-59; Ex.1008, [0006]. Accordingly, a POSITA would have understood that Delco’s virtual machine communicates with the Internet. Ex.1003, ¶134.

Accordingly, the virtual machines’ connection to the Internet through a VNic of the virtual hardware component layer is a “*first communication connection*” as claimed. Ex.1003, ¶¶131-35.

[5.2] *communicate with one or more trusted network destinations via a second communication connection; and*

Delco’s host computing system accesses the local intranet 22 (“*one or more trusted network destinations*”) through a second connection. “The host system platform 12 preferably supports a local datastore 18 and a network interface 20 permitting connection to **a local intranet 22.**” Ex.1005, 4:53-61.

Delco’s intranet 22 is a “trusted” network because it is behind the firewall system 30. A POSITA would have understood that the intranet 22 is a “protected, typically corporate, network.” Ex.1005, 2:15-16; Ex.1003, ¶137. Delco explains that “In conventional use configurations, an independent firewall system 30 can be installed generally as shown to provide network protection to the intranet 22 including the host system platform 12.” Ex.1005, 4:62-66.



Ex.1005, Fig. 1 (annotated); Ex.1003, ¶137.

The host system platform 12 includes “a network interface 20 permitting connection to a local intranet 22.” Ex.1005, 7:4-18. Accordingly, the host system’s connection to the intranet through the network interface 20 is a “*second connection*” as claimed. Just like the ’780 patent, Delco thus teaches a first connection through a virtual machine and a second connection through the host. See e.g., Ex.1001, Fig. 2. Ex.1003, ¶¶136-39.

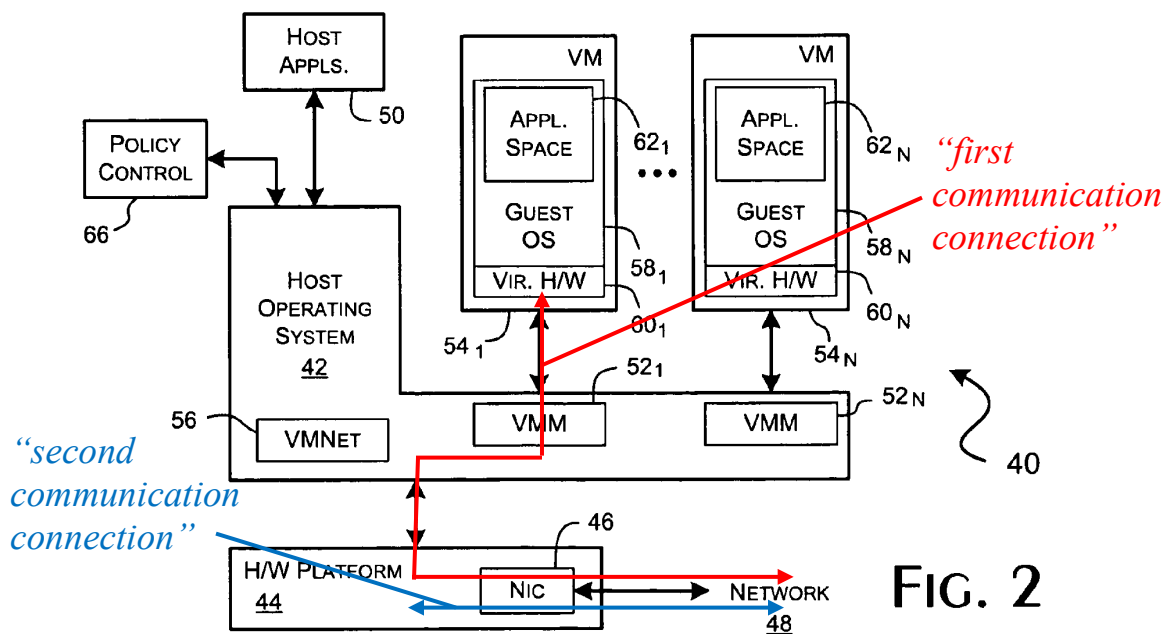
[5.3] enforce separation of the first communication connection from the second communication connection.

Delco’s virtual machine connection (“*first communication connection*”) and host system connection (“*second communication connection*”) are separated at least because they use different network controllers. Delco’s host system establishes the exemplary “*second communication connection*” using the physical

NIC. “A host operating system 42 is executed on a hardware platform 44 including a network interface controller 46.” Ex.1005, 6:15-17. Separately, the virtual machine’s exemplary “*first communication connection*” uses a VNic: “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, 7:4-6. “[E]ach virtual machine 54, as executed, then preferably further defines a guest operating system execution space above a virtual hardware component layer 60_{1-N}.” Ex.1005, 6:46-48.

The VNic of the virtual machine is separate from the NIC on the host system. Ex.1005, 6:31-45. Delco explains that the virtual machines are “managed through separate virtual machine execution processes” and are “effectively isolated from one another and from the host operating system 42 as a function of the applied virtual machine world context switch.” Ex.1005, 6:31-45. Delco explains that “a host operating system 42 is executed on a hardware platform 44 including a network interface controller 46.” Ex.1005, 6:15-17. Separately, “a virtual machine monitor (VMM) 52_{1-N} [is] provided to support a set of one or more virtual machines (VM)54_{1-N} and a virtual network controller (VMNet) 56 that provides coordinated routing of network traffic between the virtual machines 54 and the ... hardware specific network interface controller 46 driver.” Ex.1005, 6:23-30.

Accordingly, because Delco's system relies on the VNic for the virtual machine (using the "*first communication connection*") and relies on only the physical NIC 46 for the host system (using the "*second communication connection*"), Delco's system "*enforce[s] separation of the first communication connection from the second communication connection*" as claimed. The separate connections are illustrated in Fig. 2 below.



Ex.1005, Fig. 2 (annotated); Ex.1003, ¶140.

Additionally, the first and second communication connections are separated in that they use different filters with different policy rules. Delco's packet filter application 32 and packet filters 74 use different policy configurations. "[A]nother advantage of the present invention is that the policy rule sets can be defined to

implement security controls on **a per network interface basis**, including individually for ... individual virtual machines [and] for a defined group of virtual machines, **potentially including the host operating system**, and administratively determined combinations.” Ex.1005, 4:11-18; Ex.1003, ¶¶140-42.

9. Claim 6

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

As explained above at [1.6], Delco’s packet filter application 32 teaches a “*host-based firewall*” as claimed. Because the packet filter application 32 is positioned between the host system platform 12 and the intranet 22, it performs network isolation between the host system platform 12 (“*the computer system*”) and the intranet (“*the network*”). By filtering packets between the host system platform 12 and other devices on the intranet 22, the packet filter application 32 prevents “*lateral communication and movement of malware*” between the host system platform 12 and “*other devices on the networked computer system.*” A POSITA would have understood the term “*lateral communication*” to include communication between devices on the intranet. Ex.1003, ¶143.

Furthermore, as explained above at [4.1], Delco’s packet filters are configured to filter spam, viruses, and other forms of malware. Ex.1003, ¶¶143-45.

10. Claim 7

[7.1] *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.*

First, as explained above at [1.7], Delco’s firewall system 30 teaches the claimed “*device*.”

Second, as explained above at [1.8], Delco’s firewall system 30 provides network isolation between the host system platform on the intranet 22, and the Internet 24 (“*one or more untrusted network destinations*”).

Third, Delco’s firewall system 30 filters unauthorized communication consistent with the known functionality of firewall systems. As Delco explains, “Firewall system architectures are conventionally well-known as implementing various ... network packet processing functions to selectively control the network traffic passed through the firewall system.” Ex.1005, 1:67-2:9. “The packet processing functions typically include discrete packet filtering, such as ... can be performed by various spam filter applications, all conventionally referred to generally as packet filtering.” Ex.1005, 1:67-2:9. Delco also refers to the packet filter functions as “exemplified by the conventional IPTables and IPChains packages, content filters, such as the well-known SpamAssassin and Clam AntiVirus (ClamAV) packages, deep packet analysis and scrubbing packages, and other packages implementing network packet security functions.” Ex.1005, 4:67-

5:7.

Delco's firewall system, which filters for viruses, spam, or other security concerns, prevents "*unauthorized communication*" as claimed. Indeed, Delco describes the same type of firewalls and packet filters as does the '780 patent. *Compare* Ex.1005, 5:11-13 ("Various network security and content filter applications for client system platform configurations are available from Symantec Corporation") *with* Ex.1001, 7:46-47 ("Symantec Endpoint Protection or MacAfee Host-Based Security Systems"). Accordingly, a POSITA would have recognized that Delco's firewall system prevents the same type of unauthorized communications and performs the same types of filtering functions that are described in the '780 patent. Ex.1003, ¶¶146-51.

11. Claim 9

[9.1] *The networked computer system of claim 1, wherein one or more applications or processes are configured to run in the virtual system, and*

Delco describes one or more applications that run on a guest operating system ("*virtual system*"). Ex.1005, 3:67-4:3. Delco also refers to "Applications executing in the other virtual machines co-resident on the physical computer system platform." Ex.1005, 3:67-4:3. Delco further explains that the guest operating systems are configured to support applications. "The individual guest operating system execution spaces are therefore logically coextensive with the

instances of the guest operating systems 58_{1-N}, including **program execution spaces 62_{1-N} held available for the execution of applications by the guest operating systems 58_{1-N}**.” Ex.1005, 6:46-60. Because the applications run on the virtual machine, they are “*configured to run in the virtual system*” as claimed.

Accordingly, because Delco’s virtual machines include execution space for the execution of applications by the guest operating systems, Delco renders this limitation obvious. Ex.1003, ¶¶152-53.

[9.2] *wherein the one or more applications or processes running in the virtual system are configured to communicate with the one or more untrusted network destinations.*

Traffic from the applications running on Delco’s guest operating systems is allowed to communicate with an external network 48, which would include the Internet (an “*untrusted network destination*”). Ex.1005, 10:28-31 (“Network access... is then available 108 to the guest operating system 58_{1-N}.”); Ex.1008, [0006] (“...an untrusted data network ... such as the internet.”). Delco notes there is a “need to provide appropriate security constraints between the **applications** running within the virtual machines, a host operating system if present, **and the connected network environment**.” Ex.1005, 1:59-62. As illustrated in Fig. 1, Delco’s connected network environment includes an intranet 22 and the Internet 24. Indeed, it was known in the art for virtual machine applications to communicate with “untrusted” destinations. *See generally*, Ex.1014.

Thus, because the applications on Delco’s virtual systems access the Internet, which is understood to be an untrusted network, Delco renders this limitation obvious. Ex.1003, ¶¶154-55.

12. Claim 10

[10.1] *The networked computer system of claim 1, wherein one or more applications or processes are configured to run in the host system, and*

Delco explains that “[t]he host operating system 42 supports the execution of any number of conventional applications 50.” Ex.1005, 6:13-30.

Thus, because Delco’s host system supports conventional applications, Delco renders this limitation obvious. Ex.1003, ¶¶156-57.

[10.2] *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.*

Delco’s applications 50, which run on the host system platform 44, communicate with an external network 48, which a POSITA would understand to include the intranet 22 (“*network*”). Delco’s host system platform 12 uses a “network interface 20 permitting connection to a local intranet 22.” Ex.1005, 4:58-59. A POSITA would have understood that by connecting to the intranet, the host system platform communicates with devices on the network, such as other computers. *See e.g.*, Ex.1007, Fig. 2 (illustrating multiple devices connected to a local network); Ex.1009, Fig. 4A (illustrating multiple client systems on a local network); Ex.1003, ¶157. For example, Delco teaches that “[b]y default, DHCP

protocol packets are enabled through the host-based packet filter.” Ex.1005, 8:46-48. A POSITA would have been familiar with the dynamic host control protocol (DHCP), including the fact that a DHCP request message would be transmitted by the host to a DHCP server (“*one or more devices*”) on intranet 22 (“*the network*”). Ex.1003, ¶158; Ex.1015, 13 (“The client broadcasts a DHCPDISCOVER message on its local physical subnet.”).

Delco also describes evaluating whether “whether a specific DHCP, DNS, or other server is known on or reachable through the network 48.” Ex.1005, 9:10-17. A POSITA would have found it obvious for the host operating system to communicate with a DHCP server or a DNS server on the intranet 22. Ex.1003, ¶158.

Delco’s applications 50 are referred to as “conventional applications.” Ex.1005. A POSITA would have thus understood that conventional applications communicate with other devices on a network. For example, it was known in the art for users to share files over a network: “[E]xemplary scenarios ... as examples of the present technology for a network aware firewall ... Abby attaches her laptop to her home network. Abby then opens the file sharing port on the laptop to share files between her laptop and her desktop.” Ex.1007, 7:40-51. Accordingly, a POSITA viewing the teachings of Delco would have recognized that conventional applications communicate with other devices on a network.

Accordingly, because Delco's applications, which are described as conventional, run on the host system which has a network interface connected to the network, Delco renders this limitation obvious. Ex.1003, ¶¶158-60.

13. Claim 11

[11.0] *A method of network isolation in a networked computer system, the method comprising:*

To the extent the preamble is limiting, Delco renders it obvious.

First, consistent with the discussion above at [1.0], Delco teaches “*a networked computer system*” as claimed.

Second, Delco teaches a method by which a host system platform 12 within the networked computer system executes virtual machines which run guest operating systems in an isolated fashion. *See e.g.*, [1.5]. Thus, Delco teaches “*a method of network isolation.*” Ex.1003, ¶¶161-63.

[11.1] *providing a network and at least one computer system that is configured to connect to the network,*

First, consistent with the discussion above at [1.1], Delco teaches “*a network*” as claimed.

Second, consistent with the discussion above at [1.2], Delco teaches “*at least one computer system that is configured to connect to the network.*” Ex.1003, ¶¶164-65.

[11.2] *the computer system comprising a host system and a virtual system,*

See [1.3]. Ex.1003, ¶166.

[11.3] *wherein the virtual system is a separate operating system or a software module operating on the computer system;*

See [1.4]. Ex.1003, ¶167.

[11.4] *separating the host system from the virtual system using an internal firewall executed on the computer system;*

As explained above at [1.5], 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.

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

As explained above at [1.6], Delco teaches “a host-based firewall executed on the computer system is configured to implement network isolation between the computer system and the network.” For similar reasons, Delco teaches “*implementing network isolation between the computer system and the network using a host-based firewall executed on the computer system*” as claimed. Ex.1003, ¶169.

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

Consistent with the discussion above at [1.7], Delco teaches “*providing at*

least one device configured to implement a network firewall or a web proxy” as claimed. Ex.1003, ¶170.

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

As explained above at [1.8], Delco and Adams teach “*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.*” For similar reasons, at least Delco alone (as well as Delco and Adams) teach “*implementing network isolation, between one or more untrusted network destinations and the networked computer system, via the at least one device.*”

Ex.1003, ¶171.

14. Claim 12

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

See [2.1]. Ex.1003, ¶172.

15. Claim 13

[13.1] *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.*

First, as explained above at [3.1], Delco’s host system, which utilizes a program execution space, teaches “*wherein the host system is configured to store data in a host memory space.*” For similar reasons, Delco’s use of the host program

execution space teaches “*the host system storing data in a host data storage.*”

Second, for the reasons explained above at [3.1], Delco’s virtual machines, which utilize guest execution space, teach “*the virtual system is configured to store data in a virtual memory space.*” For similar reasons, Delco’s use of the guest execution space teaches “*the virtual system storing data in a virtual data storage.*” Ex.1003, ¶¶173-74.

16. Claim 14

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

As explained above at [4.1], Delco teaches “*wherein malware introduced to the computer system is prevented from moving to another computer system of the networked computer system.*” For similar reasons, Delco renders this limitation obvious. Ex.1003, ¶175.

17. Claim 15

[15.0] *The method of claim 11, further comprising:*

See [11.0]-[11.7]. Ex.1003, ¶176.

[15.1] *communicating with the one or more untrusted network destinations via a first communication connection;*

See [5.1]. Ex.1003, ¶177.

[15.2] *communicating with one or more trusted network destinations via a second communication connection; and*

See [5.2]. Ex.1003, ¶178.

[15.3] *enforcing separation of the first communication connection from the second communication connection.*

See [5.3]. Ex.1003, ¶179.

18. Claim 16

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

See [6.1]. Ex.1003, ¶180.

19. Claim 17

[17.1] *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.*

See [7.1]. Ex.1003, ¶181.

20. Claim 19

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

See [9.1]-[9.2]. Ex.1003, ¶182.

21. Claim 20

[20.1] *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.*

See [10.0]-[10.2]. Ex.1003, ¶183.

C. Ground 2: Claims 8 and 18 are obvious in view of Delco, Adams,

and Dadhia.

1. Summary of Dadhia.

Dadhia, entitled “Network Aware Firewall,” describes a technique that uses different security policies based on whether the detected network is public or private. Dadhia explains that “as increasing number of computers become mobile in ‘home’ and ‘enterprise,’ they connect to different types of networks at different times.” Ex.1007, 4:23-26.

To address this, Dadhia’s “firewall keeps two sets of firewall policies locally. The first policy is associated with private (e.g., trusted) networks.” Ex.1007 4:59-61. “The second policy is associated with public (e.g., untrusted) networks.” Ex.1007, 4:63-64. Dadhia’s network aware firewall is configured to “dynamically modify security settings on the laptop 120 in response to the network the computer is connected to.” Ex.1007, 5:36-38.

Dadhia provides an example in which file sharing is enabled on trusted networks but blocked or disabled on untrusted networks. When the computing system is on a home network that is “considered safe” (i.e., a trusted network), “a user may enable file sharing so that files may be shared between a laptop computer system 120 and a home PC desktop computer system 115.” Ex.1007, 5:20-23. But “[w]hen the laptop computer system 120 is then used in a public network (e.g., at a local coffee house), the file sharing ... should be disabled to prevent other computer

systems 160 from accessing information and/or applications on the laptop computer system 120.” Ex.1007, 5:26-30.

Accordingly, Dadhia provides evidence of the obviousness of using different firewall policies depending on whether the computing system is connected to a trusted or an untrusted network. Ex.1003, ¶¶184-87.

2. Reasons to Combine Dadhia with Delco and Adams

A POSITA would have found it obvious for Delco’s firewall (e.g., packet filter 32) to use different policies based on whether the host computing system is connected to a trusted or an untrusted network as taught by Dadhia. Doing so furthers Delco’s goal of providing “a network traffic management system capable of performing firewall operations securely for multiple virtual machines and host operating system.” Ex.1005, 3:13-15. Indeed, Delco already provides the capability for changing firewall policy based on the detected network. Ex.1003, ¶188.

Delco explains that “the selection of policy rule sets by the policy controllers 64, 66 is preferably further qualified by defined zones of application.” Ex.1005, 9:5-7. “[A] network zone is defined by the unique characteristics of the network 48 then accessible through the network interface controller 46.” Ex.1005, 9:7-9. Based on the detected network zone, a specific policy ruleset for the packet filters is used. “[S]tored configuration files are retrievable upon request by the policy controllers 64, 66 from the local datastore 18. The files or identifiers within the files allow

policy rule sets to be identified by zone.” Ex.1005, 9:25-28. Delco’s system “also actively monitors the network 46 for changes that might affect zone criteria matches.” Ex.1005, 10:44-46. Thus, if Delco’s host computer system were to switch to a different network, the system would detect that change and update the firewall policy accordingly. Ex.1003, ¶189.

Delco’s Fig. 1 illustrates the host system platform 12 connected to an intranet 22. That intranet is a protected network because it is behind firewall system 30. *See* Ex.1007, 5:23-25 (explaining that a “home network can be considered safe, because the home router 125 may have a firewall that blocks malicious access attempts from the Internet 101.”). But, if Delco’s host platform system 12 were to connect to a different network (i.e., a different zone) that was not protected, a POSITA would have found it obvious for the policy for that network or zone to be more restrictive. Ex.1003, ¶190.

Dadhia provides an example in which on a protected network, file sharing is enabled. However, on a public or unprotected network, file sharing is disabled. *See* Ex.1007, 5:17-41. A POSITA would have thus found it obvious for Delco’s host system platform to similarly allow file sharing on the intranet (i.e., protected network) and disallow file sharing on a public or untrusted network. Doing so provides the benefit of allowing desired functionality such as file sharing when on a trusted network while automatically blocking such features when connected to

public, unsafe networks. Ex.1003, ¶191.

A POSITA would have had a reasonable expectation of success when combining the teachings of Dadhia with those of Delco. Ex.1003, ¶192. Dadhia explains that its network aware firewall “can be local to a computer system and can be implemented in hardware as well as software.” Ex.1007, 5:45-46. Delco’s host system platform 12 is such a computer system: “A host system platform 12 includes a local processor 14 and memory 16 providing a program execution space.” Ex.1005, 4:55-56. Additionally, Delco’s packet filter application is implemented in software: “a packet filter application 32 is conventionally implemented and executed within the program execution space of the host system platform 12.” Ex.1005, 5:8-11. Thus, a POSITA would have expected that Dadhia’s different firewall policies for different networks would be compatible with Delco’s system. Ex.1003, ¶192.

Moreover, like Dadhia’s system, Delco’s system includes a mechanism for accessing the network to which the host computer system is attached. Dadhia describes “a network accessor 302 for accessing a network connection. A connection determiner 304 determines the type of the connection.” Ex.1007, 5:47-50. Delco similarly includes a mechanism that determines the zone (i.e., network) to which the computer system is attached. “The current zone characteristics are preferably determined by the policy controller 64, 66 upon initialization, at

periodic intervals, and in response to notices of a potentially significant change in the connected network as may be conventionally generated by the host operating system 42 and dedicated kernel 82.” Ex.1005, 9:17-23. Accordingly, a POSITA would have expected success when combining the teachings of Delco and Dadhia to result in a network aware firewall that uses more strict policies on untrusted networks. Ex.1003, ¶193.

The resultant combination of Delco and Dadhia—Delco’s packet filter application 32 employing stricter policies when connected to an untrusted network—is predictable because Dadhia’s network aware firewall technique performs the same function within Delco that it does in Dadhia. For example, Dadhia explains that “the firewall on the laptop 120 would disable file sharing when the laptop 120 is connected to the public network 150 and enable file sharing when the laptop 120 is connected to the home network 110.” Ex.1005, 5:38-42. It would have been obvious that this technique would work similarly in Delco. For example, the packet filter application 32 on Delco’s host system platform 12 would disable file sharing when connected to a public, untrusted network and enable file sharing when connected to the trusted intranet 22. Ex.1003, ¶194.

A POSITA would have thus been motivated to implement Delco’s host-based firewall to have different policies for different environments as taught by Dadhia. Accordingly, the combination of Delco and Dadhia is merely the use of a

known technique (Dadhia’s different firewall policies for different networks) to improve similar devices (Delco’s packet filter application 32) in the same way (using stricter policies when connected to an untrusted network). Ex.1003, ¶195.

3. Claim 8

[8.1] *The networked computer system of claim 1, wherein the host-based firewall is configured to implement a first policy when the computer system is connected to the network and a second policy when the computer system is connected to another network,*

First, as explained above at [1.6], Delco’s host system platform includes a packet filter application 32 (“host-based firewall”). The packet filter application 32 is controlled by policy controllers: “In the currently preferred embodiments of the present invention, **the individual policy controller components 64, 66 operate independently of one another in managing the various virtual network interface controller components 70 and host platform packet filter.**” Ex.1005, 8:7-11. The policies used by Delco’s policy controllers 64, 66 are dependent on the detected “network zone.” Ex.1005, 9:5-9. “**The selection of policy rule sets by the policy controllers 64, 66 is preferably further qualified by defined zones of application.**” Ex.1005, 9:5-22. Delco’s system looks at the “current zone characteristics” and uses a “policy rule set” that matches those zone characteristics. Ex.1005, 9:63-10:8.

For the reasons explained above at X.C.2, it would have been obvious for

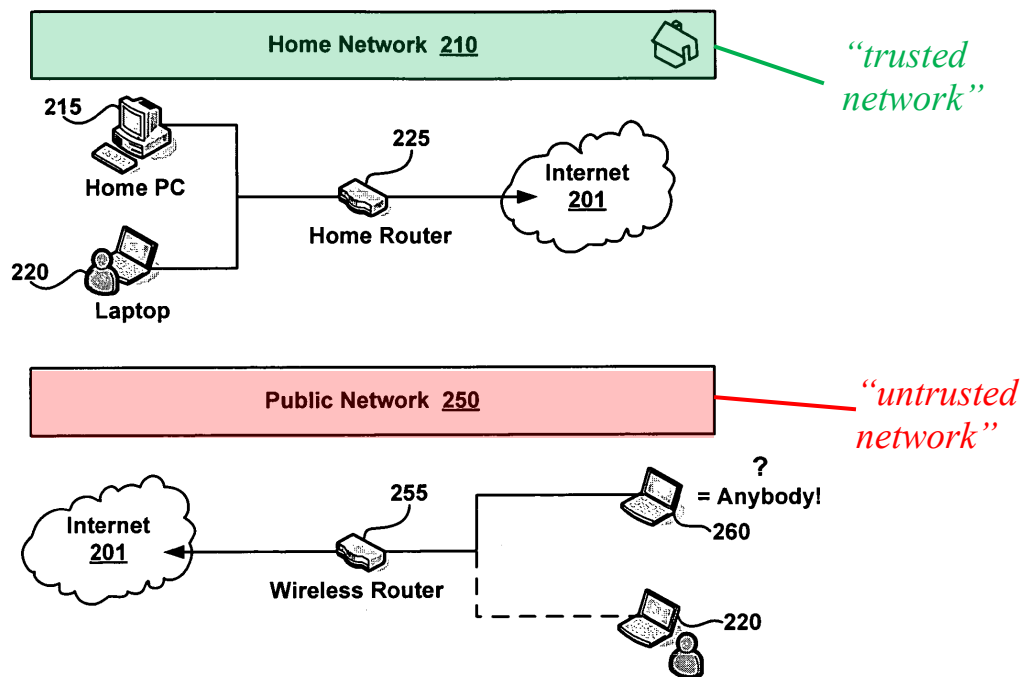
Delco's packet filter to use different policies for trusted networks versus untrusted networks. Dadhia provides an example of such a model. Dadhia describes an example in which "a firewall keeps two sets of firewall policies locally." Ex.1007, 4:59-5:7. "The first policy is associated with private (e.g., trusted) networks" such as "a trusted Intranet, etc." Ex.1007, 4:59-5:7. "The second policy is associated with public (e.g., untrusted) networks," such as "WiFi at a local coffee shop, [or] an airport connection." Ex.1007, 4:59-5:7.

Accordingly, Dadhia describes a "*first policy*" when connected to a trusted Intranet ("*the network*") and a "*second policy*" when connected to a coffee shop or airport Wifi network ("*another network*"). Ex.1003, ¶¶196-199.

[8.2] *wherein the first policy permits one or more communications between the host system of the computer system and one or more resources on the network and*

Dadhia gives an example in which the "*first policy*" for the trusted network allows file sharing. "When connected to a home network 110, a user may enable file sharing so that files may be shared between a laptop computer system 120 and a home PC desktop computer system 115." Ex.1007, 5:17-25. Thus, Dadhia's system "enable[s] file sharing when the laptop 120 is connected to the home

network 110.” Ex.1007, 5:35-42. This is shown in Fig. 2 below.⁶



Ex.1007, Fig. 2 (annotated); Ex.1003, ¶200.

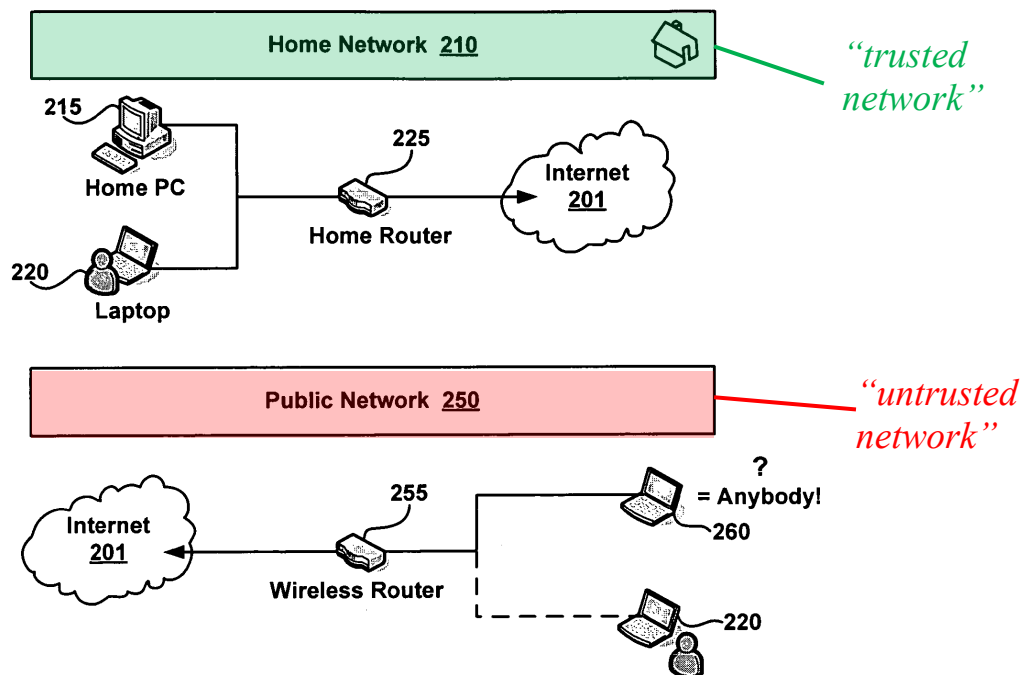
Accordingly, by enabling file sharing with another system on the trusted network, “the first policy permits one or more communications between the host system of the computer system and one or more resources on the network” as claimed. Ex.1003, ¶¶200-02.

[8.3] the second policy blocks communications egressing from the host system of the computer system but allows communications egressing from the virtual

⁶ Dadhia’s description uses different reference numerals in the figures than it does in the text. For example, the described home network 110 and laptop 120 are illustrated as home network 210 and laptop 220.

system.

First, Dadhia gives an example in which the “*second policy*” for the untrusted network disables file sharing. “When the laptop computer system 120 is then used in a public network (e.g., at a local coffee house), the file sharing enabled within the home network 110 should be disabled to prevent other computer systems 160 from accessing information and/or applications on the laptop computer system 120.” Ex.1007, 5:26-34. Thus, “the firewall on the laptop 120 would disable file sharing when the laptop 120 is connected to the public network 150 and enable file sharing when the laptop 120 is connected to the home network 110.” Ex.1007, 5:35-42.



Ex.1007, Fig. 2 (annotated); Ex.1003, ¶203.

Accordingly, by disabling file sharing with another system on the untrusted network, “*the second policy blocks communications egressing from the host system of the computer system*” as claimed.

Second, while Delco’s packet filter application 32 (“*host-based firewall*”) disables file sharing for the host, the filter application 32 is not responsible for communication between the virtual machine and Internet—thus allowing incoming and outgoing communication between the virtual machine and external networks. In other words, even when the packet filter 74 of the virtual machine prevents egress, the filter application 32 on the host would still “*allow[] communications egressing from the virtual system.*”

To the extent the claim requires that there be an actual egress through the virtual machine, it would have been obvious for the virtual machine to allow communication over the untrusted network, even when communication from applications running directly on the host system are blocked by the host’s packet filter application. Ex.1003, ¶206. As explained above at [5.0]-[5.3], Delco uses different communication sessions for the host system and the virtual systems. Thus, disabling file sharing on the communication session for the host system does not affect the policies of the virtual system. Indeed, Delco explains that “The policy rule sets can be further individualized based variously on the identity, role, and other operative characteristics of the **virtual machines**, **the host computer**

system, and the connected network, thereby allowing different levels of qualified security.” Thus, Delco allows for different policies between the host computer system and the virtual machines.

A POSITA would have understood that in Delco’s system, the virtual machine packet filter policy may be more or less restrictive than the host packet filter policy. Ex.1003, ¶207. Delco explains that “[p]rograms executed in one virtual machine are essentially unaffected by and, conversely, essentially unable to affect the execution of programs in other virtual machines.” Ex.1005, 1:40-43. Similarly, Delco’s virtual machines are “managed through separate virtual machine execution processes” and are “effectively isolated from one another and from the host operating system 42 as a function of the applied virtual machine world context switch.” Ex.1005, 6:31-45. This separation between the virtual machines and the host system thus allows for variation in permissiveness of their respective packet filters. Ex.1003, ¶207. A POSITA would have appreciated that the risks associated with contacting an untrusted destination are reduced by performing that communication from a virtual machine (e.g., if a virus is acquired, it will infect only that individual virtual machine and not the other virtual machines or the host system itself). Ex.1003, ¶207. As a result, it would have been obvious for Delco’s virtual machine to have a more permissive security policy than the host system, such that an application running in Delco’s virtual machine would be able to

communicate with an untrusted destination even when an application running directly on the host system would be prevented from such communications.

Ex.1003, ¶207.

In summary, Delco's multiple packet filters act independently to restrict or allow different types of traffic. Delco's "policy controllers 64 preferably operate to initially and dynamically direct the configuration of the different packet filter layer 74 instances as implemented in the virtual machines 54_{1-N}." Ex.1005, 8:25-57.

Since it would be obvious for a virtual machine packet filter to be more permissive than the packet filter for the entire host system, Delco and Dadhia render obvious that the "*second policy blocks communications egressing from the host system of the computer system but allows communications egressing from the virtual system.*" Ex.1003, ¶¶203-08.

4. Claim 18

[18.0] *The method of claim 11, further comprising:*

See [11.0]-[11.7]. Ex.1003, ¶209.

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

See [8.1]. Ex.1003, ¶210.

[18.2] *implementing a second policy for the host-based firewall when the computer system is connected to another network, the second policy for the host-*

based firewall blocking communications egressing from the host system of the computer system but allowing communications egressing from the virtual system.

See [8.2]. Ex.1003, ¶211.

XI. CONCLUSION

Accordingly, Petitioner has established a reasonable likelihood that the Challenged Claims are unpatentable.

Respectfully submitted,

Dated: July 25, 2024
HAYNES AND BOONE, LLP
2801 N. Harwood St., Suite 2300
Dallas, Texas 75201
Customer No. 27683

/Theodore M. Foster/
Theodore M. Foster
Lead Counsel for Petitioner
Registration No. 57,456

XII. MANDATORY NOTICES

A. Real Party-in-Interest

Pursuant to 37 C.F.R. § 42.8(b)(1), Petitioner certifies that the real party-in-interest is Cisco Systems, Inc.

B. Related Matters

Pursuant to 37 C.F.R. § 42.8(b)(2), to the best knowledge of the Petitioner, the '780 patent is involved in the following cases:

Case Heading	Number	Court	Date
<i>Croga Innovations Ltd. v. Cisco Systems, Inc.</i>	2-24-cv-65	EDTX	February 1, 2024
<i>Croga Innovations Ltd. v. International Business Machines Corporation.</i>	2-23-cv-00634	EDTX	December 29, 2023
<i>Croga Innovations Ltd. v. Fortinet, Inc.</i>	2-24-cv-00206	EDTX	March 22, 2024
<i>Croga Innovations Ltd. v. Amazon Web Services, Inc.</i>	1-24-cv-00398	WDTX	April 16, 2024

C. Lead and Back-up Counsel and Service Information

Lead Counsel

Theodore M. Foster
HAYNES AND BOONE, LLP
2801 N. Harwood St., Suite 2300
Dallas, TX 75201

Phone: (303) 382-6205
Fax: (214) 200-0853
ipr.theo.foster@haynesboone.com
USPTO Reg. No. 57,456

Back-up Counsel

David L. McCombs
HAYNES AND BOONE, LLP
2801 N. Harwood St., Suite 2300
Dallas, TX 75201

Phone: (214) 651-5533
Fax: (214) 200-0853
david.mccombs.ipr@haynesboone.com
USPTO Reg. No. 32,271

Calmann J. Clements
HAYNES AND BOONE, LLP
2801 N. Harwood St., Suite 2300
Dallas, TX 75201

Phone: (972) 739-8638
Fax: (214) 200-0853
calmann.clements.ipr@haynesboone.com
USPTO Reg. No. 66,910

Please address all correspondence to lead and back-up counsel. Petitioner consents to service in this proceeding by email at the addresses above.

CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. § 42.24(d), Petitioner hereby certifies, in accordance with and in reliance on the word count provided by the word-processing system used to prepare this Petition, that the number of words in this paper is 13,999.

Pursuant to 37 C.F.R. § 42.24(d), this word count excludes the table of contents, table of authorities, mandatory notices under § 42.8, certificate of service, certificate of word count, appendix of exhibits, and any claim listing.

Dated: July 25, 2024

/Theodore M. Foster/

Theodore M. Foster
Lead Counsel for Petitioner
Registration No. 57,456

CERTIFICATE OF SERVICE

The undersigned certifies that, in accordance with 37 C.F.R. § 42.6(e) and 37 C.F.R. § 42.105, service was made on Patent Owner as detailed below.

Date of service July 25, 2024

Manner of service FEDERAL EXPRESS

Documents served Petition for *Inter Partes* Review Under 35 U.S.C. § 312 and 37 C.F.R. § 42.104 of U.S. 10,601,780; Petitioner's Exhibit List; All Exhibits; Petitioner's Power of Attorney.

Persons served Atlantic IP
c/o Lombard Geliebter LLP
1325 Avenue of the Americas, 28th Floor
New York, NY 10019

/Theodore M. Foster/
Theodore M. Foster
Lead Counsel for Petitioner
Registration No. 57,456