

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

INTERNATIONAL BUSINESS MACHINES CORPORATION,

Petitioner,

v.

CROGA INNOVATIONS LTD.,

Patent Owner.

IPR2025-00379

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 11,178,104**

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	6
II. MANDATORY NOTICES AND FEES	6
A. Real Party in Interest Under 37 C.F.R. §42.8(b)(1)	7
B. Related Matters Under 37 C.F.R. §42.8(b)(2)	7
C. Lead and Back-Up Counsel Under 37 C.F.R. §42.8(b)(3)	8
D. Service Information Under 37 C.F.R. §42.8(b)(4)	8
E. Fees	9
III. REQUIREMENTS FOR IPR	9
A. Grounds for Standing Under 37 C.F.R. §42.104(a)	9
B. Identification of Challenge Under 37 C.F.R. §42.104(b)	9
IV. TECHNICAL OVERVIEW	10
A. Background	10
B. Sandboxed Computing Environments	11
V. THE '104 PATENT	11
A. Overview	11
B. Prosecution History	14
1. Non-Final Office Action and Response	15
2. Final Office Action Dated September 9, 2020	15
3. Response Dated March 8, 2021	16
4. Non-Final Office Action Dated March 23, 2021	17
C. Priority Date	18
VI. LEVEL OF ORDINARY SKILL IN THE ART	18
VII. CLAIM CONSTRUCTION	19
A. “sandboxed computing environment” (claims 1, 10 and 18)	19
1. Proper Construction	19
2. Alternative Construction	19
B. “authentication device” (claims 1, 10 and 18)	20

VIII. INVALIDITY	21
A. Ground 1	21
1. Combination of Hoy and Pratt	21
a. Hoy.....	21
b. Summary of Pratt.....	24
c. Motivation to Combine.....	26
2. Claim 1	27
3. Claim 2	46
4. Claim 3	48
5. Claim 8.....	49
6. Claim 10.....	51
7. Claim 11	53
8. Claim 17	54
9. Claims 18-19.....	55
B. Ground 2.....	55
1. Combination of Hoy and Pratt	55
2. Combination of Hoy-Pratt with Krasin.....	55
a. Summary of Krasin.....	55
b. Motivation to Combine.....	57
3. Claim Analysis.....	58
C. Ground 3.....	60
1. Summary of Benoit	60
2. Claim 1	62
3. Claim 2	78
4. Claim 3	79
5. Claim 8.....	80
6. Claim 10.....	81
7. Claim 11	83
8. Claim 17	84

9.	Claims 18-19	84
D.	Ground 4.....	85
1.	Combination of Benoit and Hunt.....	85
a.	Summary of Hunt	85
b.	Motivation to Combine.....	87
2.	Claim Analysis.....	89
a.	“first memory space” and “second memory space”	89
b.	“isolate the isolated computing environment from the workspace using an internal isolation firewall”	90
c.	Claim 8.....	93
E.	Ground 5.....	94
1.	Combination of Benoit and Hunt.....	94
2.	Combination of Benoit-Hunt with Pratt.....	94
3.	Claim Analysis.....	95
IX.	DISCRETIONARY DENIAL WOULD BE INAPPROPRIATE	97
A.	No Discretionary Denial Under <i>Fintiv</i>	97
1.	No Evidence Regarding a Stay.....	97
2.	Parallel-Proceeding Trial Date	97
3.	Investment in the Parallel Proceeding	98
4.	Overlapping Issues with the Parallel Proceeding	98
5.	Identity of Parties	99
6.	Other Circumstances	99
B.	No Discretionary Denial Under 35 U.S.C. §325(d)	99
X.	CONCLUSION.....	100

EXHIBIT LIST (37 C.F.R. §42.63(E))

EXHIBIT	DESCRIPTION
1001	U.S. Patent No. 11,178,104 to Coleman et al. (“the ’104 Patent”)
1002	Prosecution history of the ’104 Patent
1003	Declaration of Dr. Wenke Lee (“Lee Declaration”)
1004	U.S. Patent Publication No. 2013/0318594 to Hoy et al., published on November 28, 2013 (“Hoy”)
1005	U.S. Patent Publication No. 2015/0096031 to Benoit et al., published on April 2, 2015 (“Benoit”)
1006	U.S. Patent No. 10,798,077 to Pratt et al., filed on January 23, 2015 (“Pratt”)
1007	U.S. Patent Publication No. 2015/0278513 to Krasin et al., published on October 1, 2015 (“Krasin”)
1008	U.S. Patent Publication No. 2012/0017213 to Hunt et al., published on January 19, 2012 (“Hunt”)
1009	Selected pages from MICROSOFT COMPUTER DICTIONARY, FIFTH EDITION (Microsoft Press, 2002)
1010	Plaintiff Croga Innovations Ltd.’s P.R. 4-2 Disclosure, in <i>Croga Innovations Ltd. v. International Business Machines Corporation</i> , No. 2:23-cv-00634-JRG (U.S. District Court, Eastern District of Texas)
1011	First Amended Docket Control Order, Docket No. 24 in <i>Croga Innovations Ltd. v. International Business Machines Corporation</i> , No. 2-23-cv-00634-JRG (E.D. Tex. April 17, 2024)
1012	List of patent trials scheduled before Judge J. Rodney Gilstrap of the U.S. District Court for the Eastern District of Texas on September 22, 2025
1013	Docket sheet for Case No. 2-22-cv-00077 (U.S. District Court, Eastern District of Texas)
1014	Docket sheet for Case No. 2-22-cv-00293 (U.S. District Court, Eastern District of Texas)
1015	Active case statistics for Judge J. Rodney Gilstrap of the U.S. District Court for the Eastern District of Texas

I. INTRODUCTION

Petitioner International Business Machines Corporation (“Petitioner” or “IBM”) requests *inter partes* review of claims 1-3, 8, 10-11, and 17-19 (the “Challenged Claims”) of U.S. Patent No. 11,178,104 (“the ’104 Patent,” Ex-1001), assigned to Croga Innovations Ltd. (“Patent Owner” or “Croga”).

The prior art anticipates or renders obvious the Challenged Claims. The Challenged Claims recite computer systems and methods that (1) implement a “workspace” to run software applications via a first memory space; (2) implement an isolated “sandboxed” computing environment using a second memory space; (3) isolate the sandbox from the workspace using an “internal isolation firewall”; (4) authenticate the sandbox with an “authentication device”; and (5) communicate with a “proxy server” to access an Internet-based cloud service. This functionality has been known since long before the earliest possible priority date of the ’104 patent (September 26, 2017).

II. MANDATORY NOTICES AND FEES

As set forth below and pursuant to 37 C.F.R. §42.8(a)(1), Petitioner provides the following mandatory notices as part of this petition.

A. Real Party in Interest Under 37 C.F.R. §42.8(b)(1)

The real party in interest for Petitioner is International Business Machines Corporation. No other parties directed, controlled, or funded this petition for *inter partes* review (“IPR”).

B. Related Matters Under 37 C.F.R. §42.8(b)(2)

The ’104 patent is presently the subject of a patent infringement lawsuit brought by the assignee, Croga, against IBM and captioned *Croga Innovations Ltd. v. International Business Machines Corporation*, No. 2:23-cv-00634-JRG (U.S. District Court, Eastern District of Texas, filed December 29, 2023) (hereinafter, the “Related Litigation”).

To Petitioner’s best knowledge, the ’104 patent has not previously been challenged in an IPR petition.

The Related Litigation is in its earliest stages. As of the filing of this Petition, more than two months remain for the parties to complete claim construction discovery, with claim construction briefing not set to begin until after that. The parties have engaged in only initial written discovery. No depositions have taken place. The Court has not yet conducted a *Markman* hearing or issued any claim construction order.

C. Lead and Back-Up Counsel Under 37 C.F.R. §42.8(b)(3)

Pursuant to 37 C.F.R. §§42.8(b)(3) and 42.10(a), Petitioner provides the following designation of counsel:

Lead Counsel	Backup Counsel
John R. Keville (Reg. No. 42,723) jkeville@sheppardmullin.com Sheppard, Mullin, Richter & Hampton 700 Louisiana Street, 27th Floor Houston, Texas 77002 Telephone: 713.431.7100 Facsimile: 713.431.7101	Darren M. Franklin (Reg. No. 51,701) dfranklin@sheppardmullin.com Sheppard, Mullin, Richter & Hampton 350 South Grand Avenue, 40th Floor Los Angeles, California 90071-3460 Telephone: 213.620.1780 Facsimile: 213.620.1398 James Young Hurt (Reg. No. 79,121) jhurt@sheppardmullin.com Sheppard, Mullin, Richter & Hampton 12275 El Camino Real, Suite 100 San Diego, California 92130-4092 Telephone: 858.720.8900 Facsimile: 858.509.3691

An appropriate power of attorney is filed concurrently herewith.

D. Service Information Under 37 C.F.R. §42.8(b)(4)

Petitioner consents to service by e-mail addressed to:

jkeville@sheppardmullin.com;
dfranklin@sheppardmullin.com;
jhurt@sheppardmullin.com; and
LegalTM-IBM-Croga@sheppardmullin.com

Petitioner may also be served by mail or hand delivery at: Sheppard, Mullin, Richter & Hampton LLP, 700 Louisiana Street, 27th Floor, Houston, Texas 77002. The telephone and facsimile numbers for lead and backup counsel are shown above.

E. Fees

The Office is authorized to charge fees for this Petition to Deposit Account 50-4561, referencing 0LCL-383832.

III. REQUIREMENTS FOR IPR

A. Grounds for Standing Under 37 C.F.R. §42.104(a)

Petitioner certifies that the '104 Patent is available for IPR, this Petition is timely filed, and Petitioner is not barred or estopped from requesting IPR on the grounds identified herein.

B. Identification of Challenge Under 37 C.F.R. §42.104(b)

Petitioner requests IPR and cancellation of claims 1-3, 8, 10, 11 and 17-19 (the “Challenged Claims”) as follows:

Ground	Claims	Basis	Prior Art
1	1-3, 8, 10-11, 17-19	§103	Hoy and Pratt
2	1-3, 8, 10-11, 17-19	§103	Hoy, Krasin, and Pratt
3	1-3, 8, 10-11, 17-19	§102	Benoit
4	1-3, 8, 10-11, 17-19	§103	Benoit and Hunt
5	1-3, 8, 10-11, 17-19	§103	Benoit, Hunt, and Pratt

The Grounds rely on:

- U.S. Patent Publication No. 2013/0318594 to Hoy et al., published on November 28, 2013 (“Hoy,” Ex-1004);
- U.S. Patent Publication No. 2015/0096031 to Benoit et al., published on April 2, 2015 (“Benoit,” Ex-1005);
- U.S. Patent No. 10,798,077 to Pratt et al., filed on January 23, 2015 (“Pratt,” Ex-1006);
- U.S. Patent Publication No. 2015/0278513 to Krasin et al., published on October 1, 2015 (“Krasin,” Ex-1007); and
- U.S. Patent Publication No. 2012/0017213 to Hunt et al., published on January 19, 2012 (“Hunt,” Ex-1008).

These grounds are supported by the *Declaration of Dr. Wenke Lee* (“Lee Declaration,” Ex-1003).

IV. TECHNICAL OVERVIEW

A. Background

The ’104 patent concerns “a sandbox based network isolation system” that protects computer assets from harmful data on the Internet. Ex-1001, Abstract.

Such harmful data includes virus software, which the ’104 patent calls “malware.”

Ex-1001, 1:13-21.

An “infected host computer system” is one that has downloaded malware.

Ex-1001, 1:22-23. An infected host computer system may result in security losses, reduction of efficiency, and malfunctions. Ex-1001, 1:22-54.

B. Sandboxed Computing Environments

The ’104 patent fails to discuss many solutions that existed before September 26, 2017, to protect computers. Indeed, the network security field was crowded with solutions for protecting network assets before September 26, 2017, including sandbox-based network isolation solutions. Ex-1003 ¶¶8. Such solutions were so well known more than a decade before the ’104 patent’s stated priority date that “sandbox” received its own entry in technical dictionaries. Ex-1003 ¶¶9-10; Ex-1009 at 463. Moreover, people in the network security field before September 26, 2017, were highly familiar with the other concepts described in the ’104 patent, including virtual machines, cloud computing, firewalls, proxies, isolation of computing environments and networks, memory partitioning, virtual private networks (VPNs), authenticating computer environments, and authentication devices. Ex-1003 ¶¶11-26.

V. THE ’104 PATENT

A. Overview

The ’104 patent does not explain what problems, if any, existed in prior solutions to protect network assets from malware. Nor does the patent explain

what problems the alleged invention solves, beyond a high-level statement that the alleged invention protects computer assets from malware. Ex-1003 ¶27.

An example of the alleged invention is shown in Figure 2.

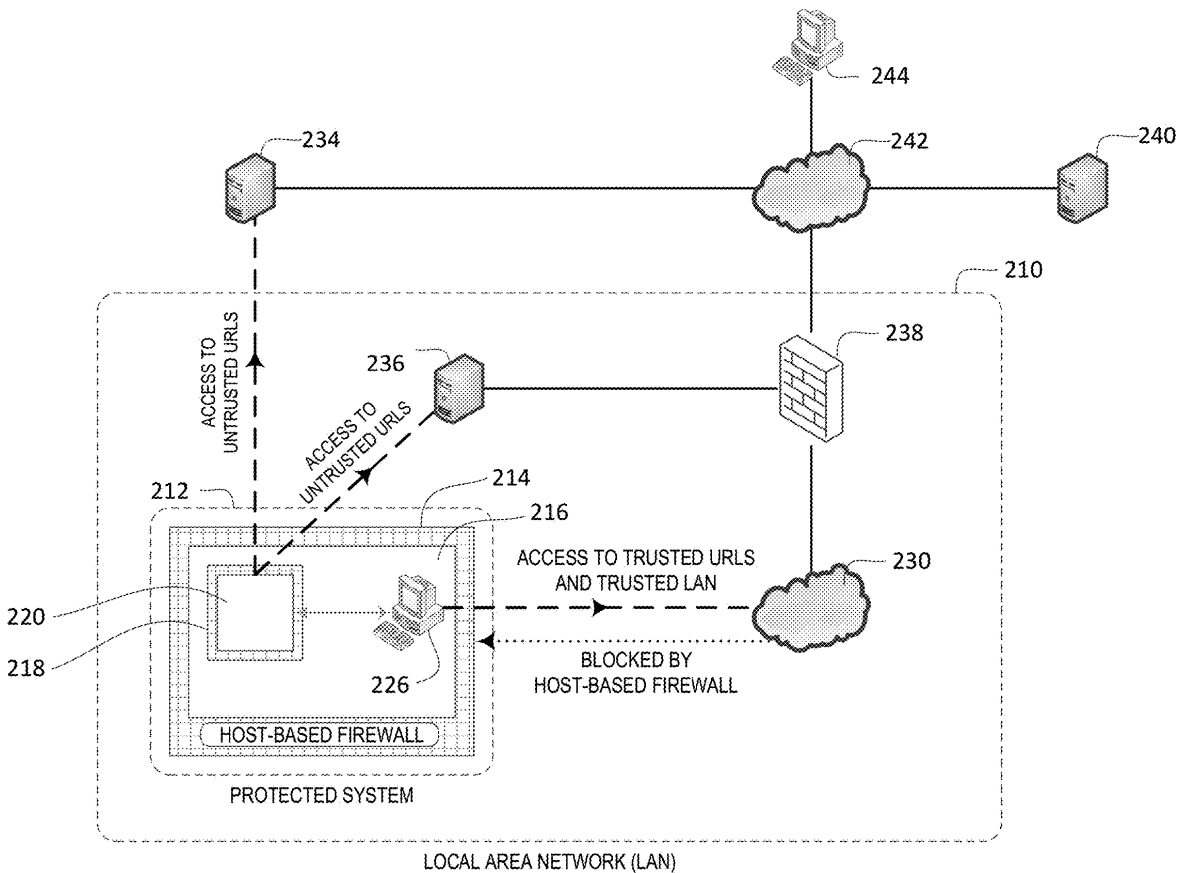


FIG. 2

Figure 2 depicts a host computer system 212 connected to a local area network (“LAN”) 210. Ex-1001, 10:65-11:1. The LAN includes a LAN-based web proxy 236 and a border firewall 238. Ex-1001, 11:7-9. The computer sends traffic to a trusted network 230 within the LAN via an operating system 226. Ex-1001, 11:9-11. The computer also sends traffic to an untrusted network

destination on the Internet 242 using the border firewall, the LAN-based web proxy, a first Internet-based web proxy 234, and/or a second Internet-based web proxy 240. Ex-1001, 11:11-21.

The computer includes a host-based firewall 214, a workspace 216, an internal isolation firewall 218, and a sandboxed computing environment 220. Ex-1001, 11:22-26. The computer isolates itself from untrusted network destinations using the firewalls, proxies, and/or a segregation of untrusted memory space. Ex-1001, 11:49-56.

The '104 patent admits that none of these components was new: “the host-based firewall 214 may be implemented using software that is commercially available, for example, such as Symantec Endpoint Protection, MacAfee [sic] Host Based Security Systems, etc.” Ex-1001, 12:7-11, 16:12-16. The patent incorporates the other firewalls and various web proxies as conventional components well known to a POSITA. Ex-1003 ¶32.

The sandboxed computing environment separates the sandbox's resources from the resources for a trusted workspace. Ex-1001, 12:29-35. The '104 patent admits that sandboxing was not new: “[T]he sandboxed computing environment 220 and/or the sandbox container process may be implemented using software that is commercially available, for example, such as Invincea Endpoint Protection,

Tanium Endpoint Platform, Bromium Advanced Endpoint Security, etc.”

Ex-1001, 16:49-54.

The various proxies and firewalls isolate the computer from untrusted network destinations while giving access to applications operating within the sandbox. Ex-1001, 12:54-61, 13:8-15. When the sandbox has successfully authenticated, it may access the untrusted network destination. Ex-1001, 12:62-13:7, 13:28-42.

The '104 patent provides little description of the authentication process. The LAN-based web proxy server and Internet-based web proxy servers are the only structures described that perform the authentication function. At most, the patent states that the sandbox may authenticate with the proxies “using preconfigured credentials stored, for example, within an encrypted configuration file.” Ex-1001, 12:66-13:2, 13:32-36. Performing authentication using preconfigured credentials stored in an encrypted configuration file was well known to people in the network security field before September 26, 2017. Ex-1003 ¶36.

B. Prosecution History

The '104 patent was filed with twenty claims in the U.S. Patent and Trademark Office (“USPTO”) as U.S. Application No. 16/141,378 (“the '378 application”) on September 25, 2018, with L3 Technologies, Inc. as the applicant (“Applicant”). Ex-1002, 62 (Filing Receipt). The '378 application asserted the

benefit of U.S. Provisional Application No. 62/563,237 (“the ’237 provisional application”), filed on September 26, 2017. *Id.*

1. Non-Final Office Action and Response

On May 21, 2020, the USPTO rejected all claims over the prior art. Ex-1002, 254-263 (Office Action, 3-12). Among other things, claims 1, 2, 4-9 and 19 were rejected as anticipated by U.S. Patent Publication No. 2013/0318594 to Hoy et al. (“Hoy”).

On August 14, 2020, Applicant amended independent claims 1 and 19 to state that the recited “isolated computing environment” uses “an operating system associated with the host computing system and compris[es] a sandboxed computing environment.” Ex-1002, 278, 282 (Reply, 2, 6). Applicant argued that Hoy does not disclose these limitations. Ex-1002, 284-285 (Reply, 8-9).

2. Final Office Action Dated September 9, 2020

On September 9, 2020, the USPTO again rejected all claims over the prior art. Ex-1002, 294-300 (Office Action, 3-9). Specifically, claims 1-17, 19 and 20 were rejected as obvious over Hoy in view of the Comodo Internet Security Software Version 7.0 User Guide (“Comodo”). Ex-1002, 294 (Office Action, 3).

Although the Examiner based the rejection on 35 U.S.C. §103 (obviousness), the Examiner found that Hoy taught all the limitations of independent claims 1, 10 and 19. Ex-1002, 294-296, 299 (Office Action, 3-5, 8).

In particular, the Examiner found that Hoy teaches a sandboxed environment in the form of a virtual guest system that “has no connection whatsoever to the LAN, and cannot access any address on the LAN.” Ex-1002, 296 (Office Action, 5); Ex-1004 ¶0027. The Examiner stated that this disclosure “is essentially a definition of sandboxed environment as known in the art.” Ex-1002, 296 (Office Action, 5). As a backup “[t]o exclude any doubt,” the Examiner cited Comodo, which the Examiner noted “explicitly teaches a sandboxed computing environment....” *Id.*

The Examiner also rejected Applicant’s assertion that Hoy’s virtual machine is not associated with the host operating system. Ex-1002, 294 (Office Action, 3). The Examiner stated that Hoy “explicitly and clearly disclosed” an “isolated computing environment using an operating system associated with the hosting computing system.” *Id.*

3. Response Dated March 8, 2021

On March 8, 2021, Applicant amended independent claims 1, 10 and 19. Ex-1002, 2092, 2094, 2096 (Reply, 2, 4, 6). Among other things, Applicant simplified the limitation “the isolated computing environment using an operating system associated with the host computing system” in claims 1 and 19 as “the isolated computing environment using a host operating system.” Ex-1002, 2092, 2096 (Reply, 2, 6). Applicant also added “using a host operating system” to claim 10. Additionally, Applicant amended claims 1, 10 and 19 to recite

“authenticat[ing] the isolated computing environment with an authentication device” and to clarify that communication with the Internet cloud service or resource is allowed “when the isolated computing environment has been authenticated.” Ex-1002, 2092, 2094, 2096 (Reply, 2, 4, 6). This limitation had been in the prior versions of claims 1 and 19 but had been phrased differently.

In response, the Applicant only argued against “authenticat[ing] the isolated computing environment with an authentication device.” Ex-1002, 2097-2098 (Reply, 7-8). Applicant did not dispute the Examiner’s finding that Hoy teaches a sandboxed environment. Nor did Applicant dispute the Examiner’s finding that Hoy discloses an isolated computing environment using an operating system associated with the hosting computing system.

On the “authenticate” limitation, Applicant noted only that Hoy is silent with respect to authenticating the isolated computing environment and does not contain the term “authentication device.” *Id.*

4. Non-Final Office Action Dated March 23, 2021

On March 23, 2021, the USPTO rejected all claims for non-statutory double patenting but stated that the claims were allowable over the prior art. Ex-1002, 2702-2704 (Office Action, 3-5). The Examiner did not explain his reasoning for finding the claims to be allowable, other than “[n]one of the cited references teaches claims limitations as currently amended.” Ex-1002, 2704 (Office

Action, 5). After ministerial prosecution activities, the USPTO issued a *Notice of Allowance* on October 5, 2021. Ex-1002, 3501.

C. Priority Date

The effective filing date of the '104 patent is not earlier than September 26, 2017.

VI. LEVEL OF ORDINARY SKILL IN THE ART

The field of the '104 patent is network security. Ex-1003 ¶62. A person of ordinary skill in the art (“POSITA”) in the field of the '104 patent at the time of the alleged invention would have been a person with a bachelor’s degree in computer science, computer engineering, electrical engineering, or a similar field of study, plus at least two years of professional experience working in the field of network security, or a person with a master’s degree in computer science, computer engineering, electrical engineering, or a similar field of study plus a specialization in network security.¹ Ex-1003 ¶64. A person with less education but more relevant practical experience or technical training may also meet this standard, while advanced education might substitute for experience. *Id.*

¹ Reference herein to what a POSITA would have known, understood, or been motivated to do, and the like, refers to the time of the alleged invention.

VII. CLAIM CONSTRUCTION

The Challenged Claims must be construed under *Phillips* according to the ordinary and customary meaning as understood by a POSITA in light of the prosecution history. *See* 37 C.F.R. §42.100(b). Any claim terms not defined below are presumed to have their plain and ordinary meaning.²

A. “sandboxed computing environment” (claims 1, 10 and 18)

1. Proper Construction

This term should be construed to mean “computing environment that does not require its own separate operating system.” Ex-1003 ¶71. The ’104 patent states that “the sandbox container process may permit isolation of the sandboxed computing environment without requiring the sandboxed computing environment to boot a separate operating system.....” Ex-1001, 7:10-15.

2. Alternative Construction

Croga’s assertions in the Related Litigation are relevant to this claim term. *See General Elec. Co. v. Vestas Wind Sys. A/S*, IPR2018-00928, 2018 WL 5819727, *7 (PTAB Nov. 5, 2018). In its preliminary proposed constructions, Croga proposed “[n]o construction necessary” for “sandboxed computing environment,” but also identified the definition of “sandbox” in the Microsoft

² Petitioner does not concede that any claim terms meet the requirements of 35 U.S.C. § 112.

Computer Dictionary, Fifth Edition. Ex-1010, 6. That dictionary defines

“sandbox” in relevant part as follows:

Java Virtual Machine security area for downloaded (remote or untrusted) applets, an area in which such applets are confined and prevented from accessing system resources.

Ex-1009 at 463; Ex-1003 ¶73.

Croga’s position appears to be that “sandboxed computing environment” broadly means “an area in which software is confined and prevented from accessing system resources.” This Petition and the supporting Lee Declaration apply this alternative construction in addition to the proper construction to show that the prior art anticipates or renders obvious the Challenged Claims under either construction. Ex-1003 ¶74.

B. “authentication device” (claims 1, 10 and 18)

The outer boundary of the term “authentication device” in the ’104 patent would have been unclear to a POSITA. Ex-1003 ¶75. The ’104 patent makes clear that, at a minimum, an authentication device can be a LAN-based or Internet-based web proxy server. These are the only structures described in the ’104 patent that perform the function of authenticating a computing environment. Ex-1001, 2:16-24; Ex-1003 ¶76.

A POSITA would have understood that “authentication device” includes, at a minimum, a proxy server that performs the function of authenticating a computing environment. Ex-1003 ¶77. Because this Petition shows that the Challenged Claims would have been anticipated or obvious under any construction for “authentication device” that includes a proxy server within its scope, it is unnecessary to determine the outer boundary of “authentication device.”

VIII. INVALIDITY

A. Ground 1

1. Combination of Hoy and Pratt

a. Hoy

Hoy was published on November 28, 2013, almost four years before the ’104 patent’s stated priority date. Ex-1004. Hoy therefore is prior art under 35 U.S.C. §102(a)(1).

Hoy teaches a networked computer system as shown in Figure 1.

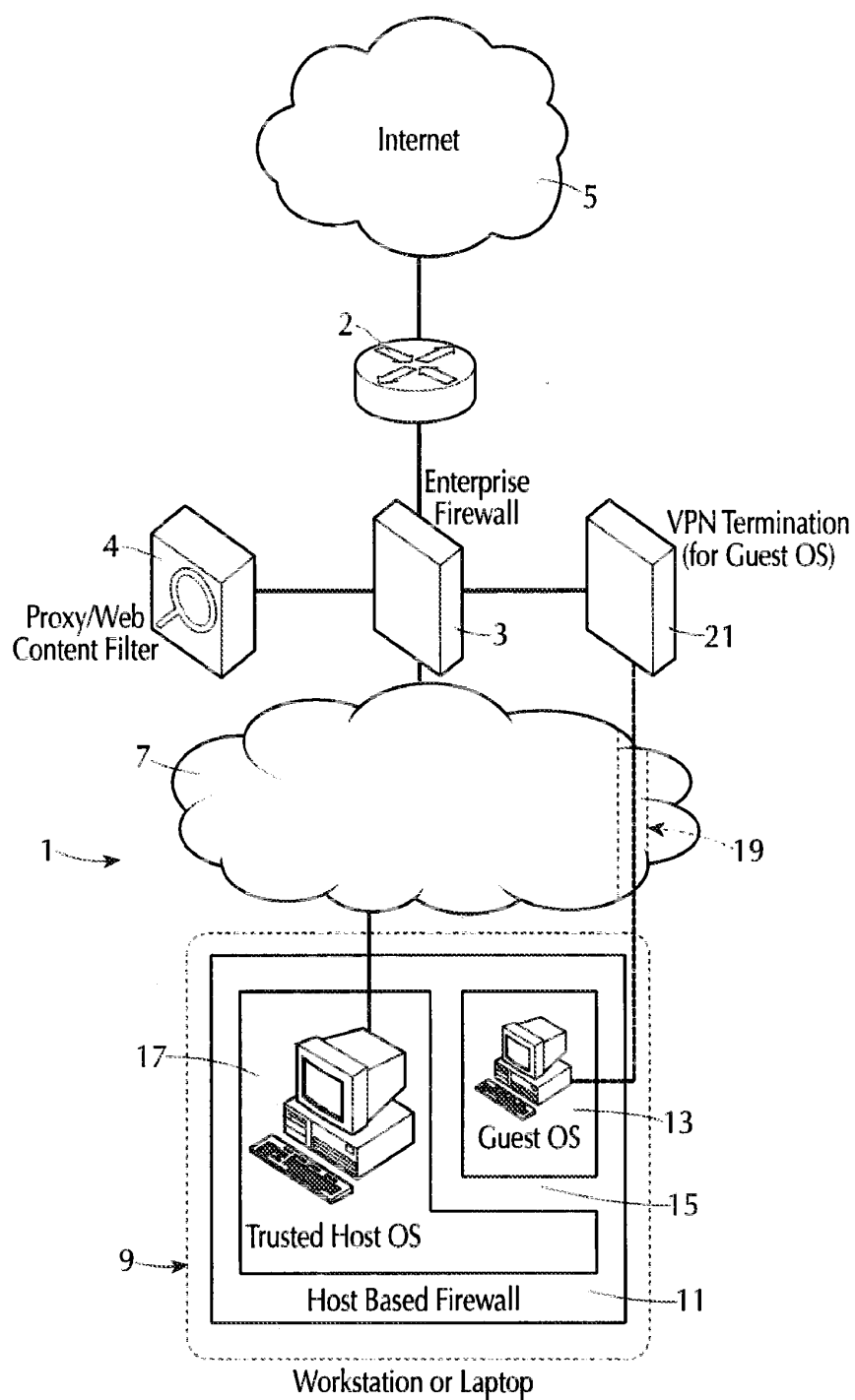


FIG. 1

Hoy's proxy/web-content filter 4 cooperates with a firewall 3 to control the data permitted to pass from the Internet 5 into the local system 1, which includes a LAN 7. Ex-1004 ¶0038. The LAN transmits data between a plurality of computers, including a workstation 9. *Id.*; Ex-1003 ¶82.

The workstation's host-based firewall 11 restricts egress from the workstation. Ex-1004 ¶¶0039-0040. Like the host-based firewall in the '104 patent, Hoy's host-based firewall may be implemented using Symantec Endpoint Protection or McAfee Host-Based Security Systems. *Id.* Hoy's host-based firewall blocks all communications from the workstation except for LAN communications. Ex-1004 ¶0041; Ex-1003 ¶83.

The workstation's hypervisor creates a virtual machine on the workstation, illustrated in Figure 1 as the virtual guest system or guest OS 13. Ex-1004 ¶0042; Ex-1003 ¶84. The hypervisor also provides an additional internal host-supported firewall 15 that separates and restricts interaction between the guest system and the trusted-host operating system ("OS") 17. Ex-1004 ¶¶0043-0047; Ex-1003 ¶85.

The trusted-host OS displays a desktop that includes an icon which initiates an Internet browser running in the guest system. Ex-1004 ¶0052. Traffic between the Internet and the guest system's browser travels through a sealed "virtual conduit" 19 passing through the LAN. *Id.*; Ex-1003 ¶86. The virtual conduit is a standard VPN tunnel. Ex-1004 ¶0053; Ex-1003 ¶¶87-89.

b. Summary of Pratt

Pratt was filed on January 23, 2015, more than two-and-a-half years before the '104 patent's stated priority date. Ex-1006. Pratt therefore is prior art under at least 35 U.S.C. §102(a)(2).

Pratt teaches a device 110 having operating environments, including sandboxed computing environments that may be securely authenticated, as shown in Figure 1 below. Ex-1006, 2:15-22, Fig. 1; Ex-1003 ¶92.

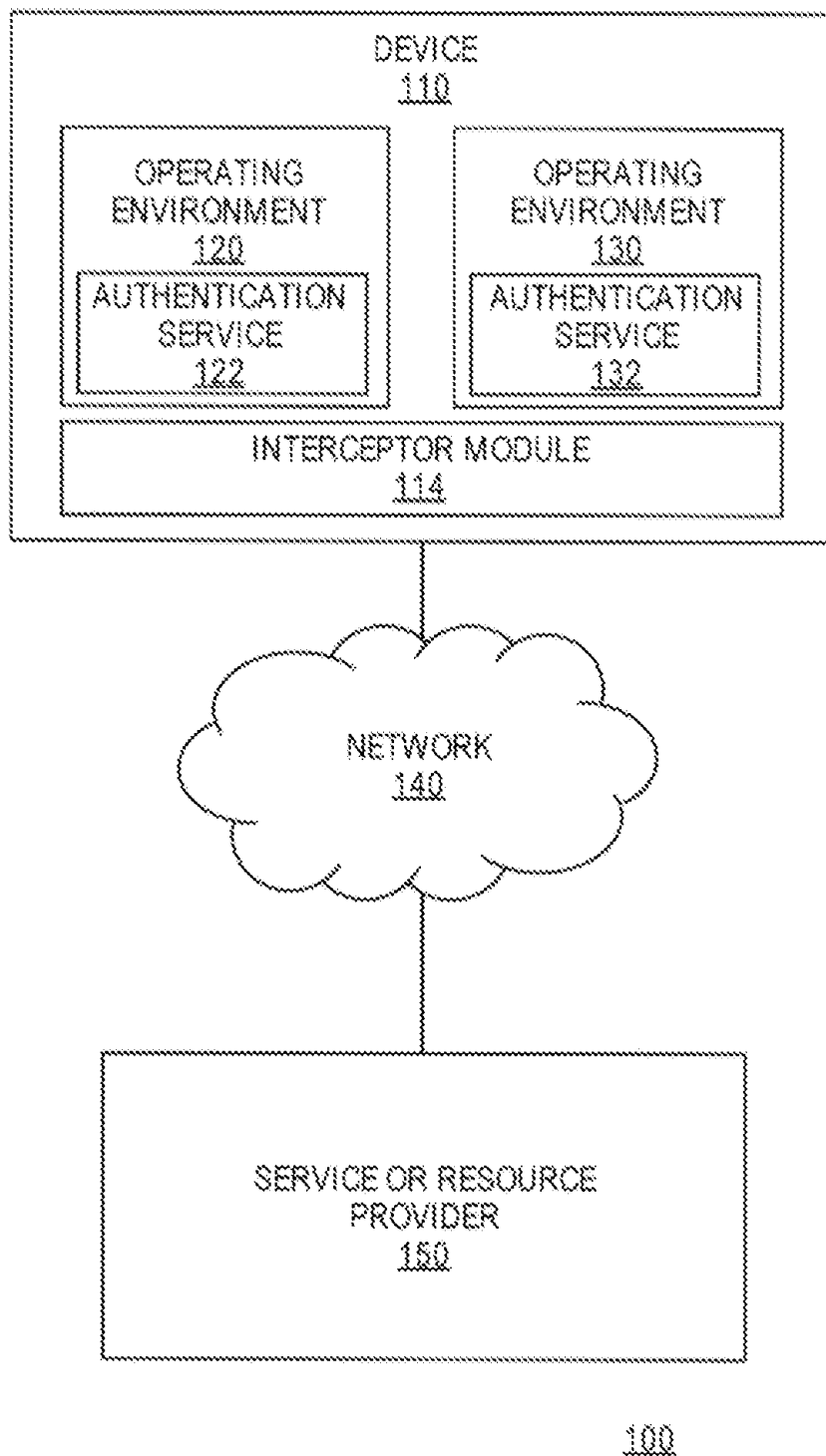


FIG. 1

Figure 1 depicts two operating environments—120 and 130. Ex-1006, 2:37-38; Ex-1003 ¶94. Each operating environment comprises an authentication service, labeled 122 and 132 in Figure 1. Ex-1006, 2:59-63; Ex-1003 ¶¶95-96.

c. Motivation to Combine

Pratt recognizes that a system requesting Internet access may be an isolated computer environment like Hoy’s guest system. Ex-1006, 2:29-36, 4:4-8. Hoy teaches transmitting data using IPsec or SSL, which include authenticating computer environments, but Hoy does not discuss the details, indicating that this was within a POSITA’s knowledge. Ex-1004 ¶0054. Pratt explicitly provides an authentication process for an isolated environment like Hoy’s guest system. Ex-1003 ¶98.

The ability for Hoy’s isolated guest system to authenticate itself would have motivated a POSITA to combine Pratt’s authentication process with Hoy. Ex-1003 ¶99. This combination would involve a POSITA combining prior-art elements according to known methods to yield a predictable result—the proxy or other network device determines that Hoy’s guest system is authentic. *Id.*

A POSITA would have been further motivated to combine Pratt’s authentication process with Hoy because of the stated advantages of Pratt’s process. Ex-1003 ¶100. Pratt teaches that “[a]dvantageously, operating environment 120 is able to authenticate itself to provider 150 without exposing ...

any malicious code which may be inadvertently introduced or present within operating environment 120 to the authentication mechanism capable of authenticating to provider 150.” Ex-1006, 5:54-58; *see also id.*, 5:59-62. This stated advantage (allowing an untrusted operating environment like Hoy’s guest system to authenticate itself without exposing malicious code) would have further motivated a POSITA. Ex-1003 ¶¶100-101.

Additionally, a POSITA would have been familiar with Hoy’s VPN tunnels and would have known that such VPN tunnels require systems to authenticate themselves to gain access to the VPN termination point. Ex-1003 ¶102. Pratt confirms that this commonly-known authentication process can be extended to isolated, untrusted computing environments operating within a device that also operates a trusted computing environment. The ability to authenticate Hoy’s isolated guest system in order to establish the VPN tunnel would have further motivated a POSITA. *Id.*

2. Claim 1

[1pre] A host computer system:

Hoy discloses a **host computer system**. The workstation 9 is shown in Figure 1. Hoy teaches that “[t]he workstation 9 can be virtually any **host computer system**....” Ex-1004 ¶0039; *see also id.* ¶0021; Ex-1003 ¶106.

[1a] a memory; and

Hoy discloses a **memory**.

Hoy's workstation "may be a PC sold by Dell, with 4 GB **RAM**...." Ex-1004 ¶0039. A POSITA would have understood "RAM" to mean random-access memory. Ex-1003 ¶108.

[1b] a processor configured to:

Hoy's workstation would necessarily have included a **processor**. Hoy teaches that "[t]he workstation 9 can be virtually any host computer system, including a **PC**

or a laptop...." Ex-1004 ¶0039. A POSITA would have understood that a PC or laptop would necessarily have included a processor. Ex-1003 ¶110.

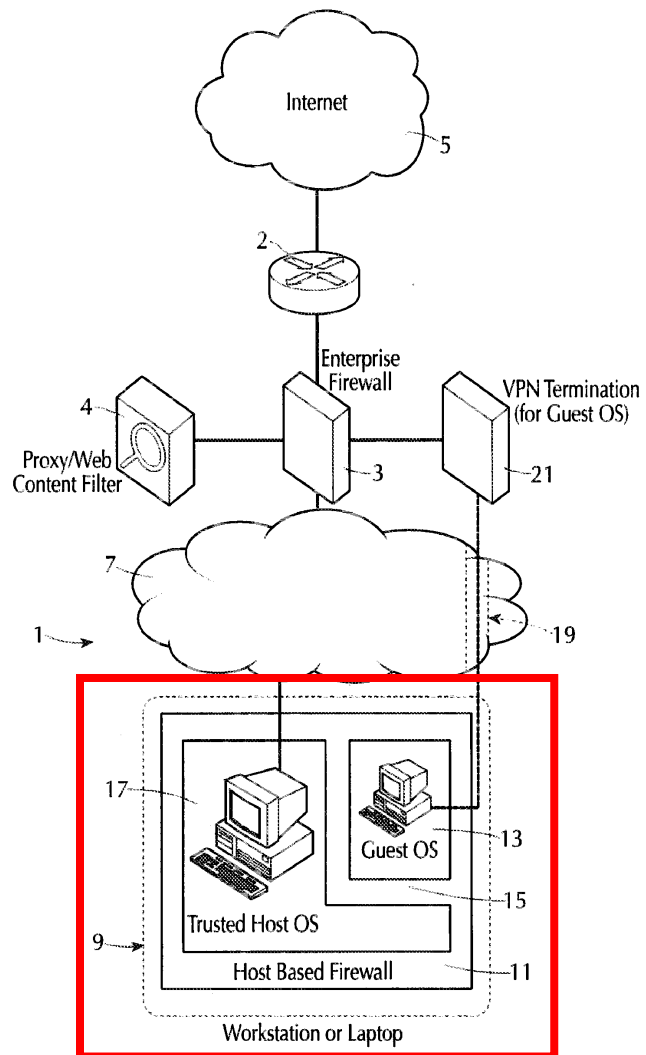


FIG. 1

[1c] **implement a workspace, wherein the workspace is configured to enable operation of a first set of one or more applications or processes via a first memory space;**

In the '104 patent, “workspace” is used to mean a computer environment in which one or more applications may run. *See, e.g.*, Ex-1001, 1:60-63; Ex-1003 ¶113.

Hoy discloses **implement[ing] a workspace** in the form of a trusted-host OS that runs an operating system and software applications like a browser and an email program. Ex-1004 ¶¶0043, 0057, 0058, 0080. The trusted-host OS 17 is shown in Figure 1. The trusted-host OS can also display a desktop, direct the transfer of files, and access trusted websites. Ex-1004 ¶¶0047, 0052, 0057, 0080. Accordingly, the trusted-host OS is a **workspace** and is **configured to enable operation of a first set of one or more applications or processes,**

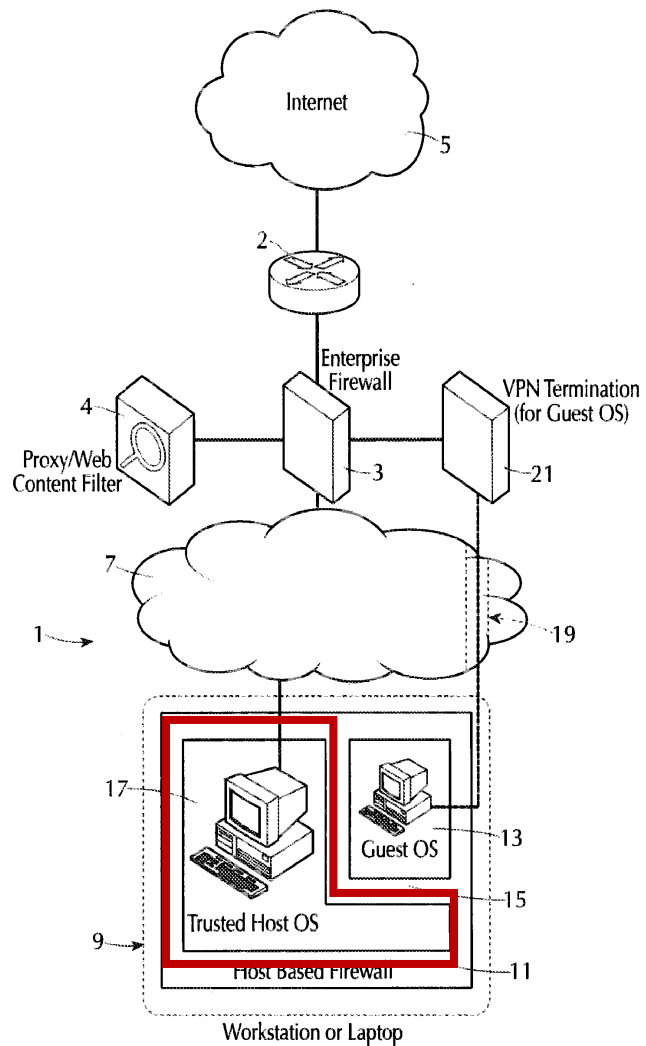


FIG. 1

such as Internet Explorer and Mozilla Firefox. Ex-1003 ¶114.

The trusted-host OS runs the applications or processes **via a first memory space**. Hoy teaches that un-isolated malicious software “allows its creators to simply capture and reuse directly from random access memory of the infected host computer, or from a network data stream, the security token or hash of the user....” Ex-1004 ¶0009. Hoy discloses a solution in which “[t]he guest is separated and completely isolated by an internal firewall from the host, and the guest cannot access any of the resources of the host computer....” Ex-1004 ¶0019; Ex-1003 ¶115.

A POSITA would have understood that isolating the guest from accessing the resources of the host, as taught in Hoy, would have included isolating the guest from accessing the memory space of the host (since memory is a resource), thus creating a first memory space for the trusted-host OS and a second memory space for the guest. Ex-1003 ¶116. That is how internal isolation firewalls, like the internal host-supported firewall 15 taught in Hoy, worked as of Hoy’s filing date. *Id.* Without the RAM of Hoy’s workstation being partitioned into first and second memory spaces, the guest would be able to access the memory being used by the trusted-host OS, and vice-versa, which is the problem that Hoy was trying to solve. Accordingly, Hoy teaches a workspace (the trusted-host OS) that runs applications or processes via a first memory space. *Id.*

Additionally, Hoy teaches “a **computer memory area** (such as a respective desktop) or data storage accessible to the host OS 17.” Ex-1004 ¶0047. A POSITA would have understood Hoy’s reference to “a computer memory area” to encompass both volatile random access memory and non-volatile memory like solid-state and hard drives. Ex-1003 ¶117. Such an interpretation is supported by the ’104 patent itself, which recognizes that:

Memory 14 may include volatile and/or non-volatile memory. Memory 14 may include read-only memory (ROM), random access memory (RAM), a register, cache memory, **semiconductor memory devices**, magnetic media such as, but not limited to, **internal hard disks** and removable disks, magneto-optical media, and/or optical media such as CD-ROM disks, and/or digital versatile disks (DVDs), and/or the like.

Ex-1001, 9:4-11. Accordingly, Hoy’s disclosure of “a computer memory area ... accessible to the host OS 17” teaches a workspace (the trusted-host OS) that is configured to enable operation of a first set of one or more applications or processes **via a first memory space**. Ex-1004 ¶0047; Ex-1003 ¶117.

[1d] **implement an isolated computing environment, the isolated computing environment using a host operating system and comprising a sandboxed computing environment that uses a second memory space to enable operation of a second set of one or more applications or processes,**

“implement an isolated computing environment”

Hoy discloses **implement[ing] an isolated computing environment** in the form of the guest system. Ex-1003 ¶120. This guest system 13 is shown in Figure 1.

Hoy teaches that the guest system is separated from the trusted-host OS by an internal host-supported firewall 15 and that interaction between the two systems is restricted. Ex-1004 ¶0043. Specifically, “data from sites that are opened by the virtual guest system browser remains **isolated** in the virtual system behind the internal firewall 15, and can only be moved by ... limited types of transfer....” Ex-1004 ¶0083. The guest system thus is an isolated

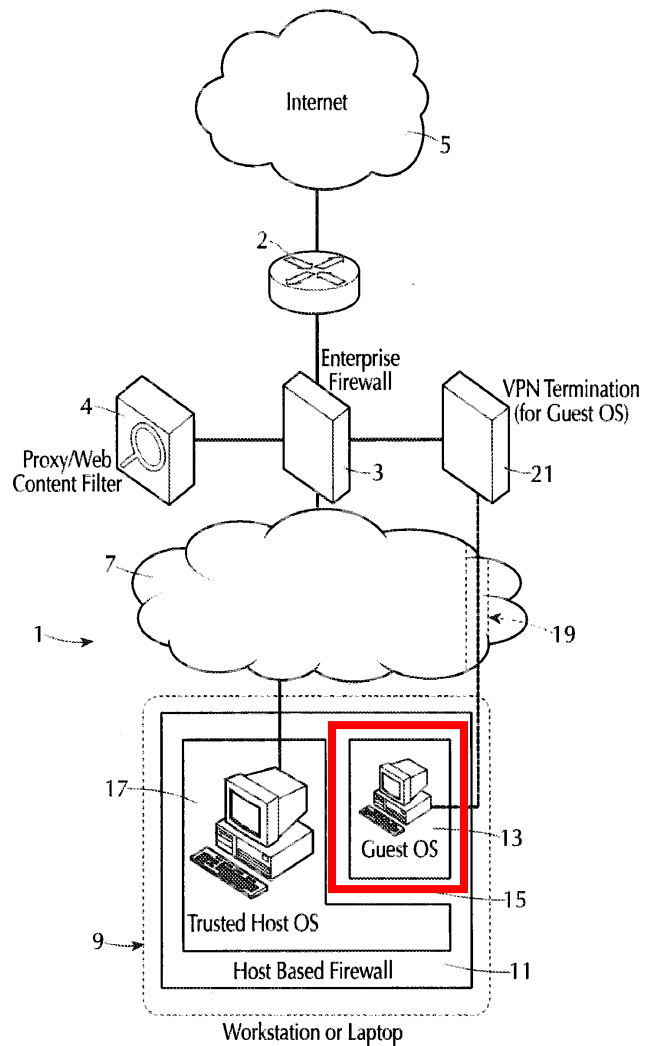


FIG. 1

computing environment—“a secure isolated service that can access the Internet, but not the internal trusted LAN sites.” Ex-1004 ¶0014; *see also id.* ¶¶0019 (“The guest is separated and completely isolated by an internal firewall from the host...”), 0020, 0031; Ex-1003 ¶121.

“the isolated computing environment using a host operating system”

Hoy’s guest system (an isolated computing environment) uses a host operating system. As found by the Examiner, Hoy’s virtual machine environment uses an operating system that is associated with the host operating system architecture, citing paragraph 26 of Hoy. Ex-1002 at 294. The Examiner correctly stated that this disclosure “explicitly and clearly disclosed” an “isolated computing environment using an operating system associated with the hosting computing system.” *Id.* While the Applicant later simplified the limitation to be “the isolated computing environment using a host operating system,” Ex-1002 at 2092, 2096 (Mar. 8, 2021 Reply at 2, 6), this simplification would not have changed the meaning of the claim language to a POSITA. Ex-1003 ¶122.

Additionally, Hoy discloses that a hypervisor creates the guest system. Ex-1004 ¶0042. This hypervisor may be “**a software module that operates based on the underlying operating system, e.g., Windows 7, of the computer 9.**” *Id.* This teaching describes an isolated computing environment using a host operating system. A POSITA would have known that a hypervisor is responsible for

creating, monitoring, and terminating a virtual machine; that is, a virtual machine depends on a hypervisor. Ex-1003 ¶123. When a hypervisor is a software module that operates based on the underlying host operating system, the hypervisor depends on the host operating system, and thus the virtual machine created by the hypervisor also depends on or uses the host operating system. *Id.*

Hoy refers to the guest system in several places as a “guest OS,” but the teachings discussed above would have made clear to a POSITA that this “guest OS” operates based on the underlying host operating system. Ex-1004 ¶¶0042-0043; Ex-1003 ¶124. Indeed, it is the host operating system that initiates the browser running in the guest system through an icon included in the host OS desktop. Ex-1004 ¶0052; Ex-1003 ¶124. Hoy does not require that the guest system actually boot a separate OS. Ex-1003 ¶126. Instead, Hoy’s hypervisor creates “a virtual machine operating on the host computer that has a virtual configuration different from the real hardware and software configuration of the computer 9.” Ex-1004 ¶0042. A POSITA would have known that such a virtual configuration could be accomplished with the same operating system as the host. Ex-1003 ¶126.

Similarly, Pratt teaches that “[a] host operating system or a guest operating system may execute within each of a virtual machine, a container, and a sandbox

environment,” further confirming the understanding of a POSITA. Ex-1006, 2:34-36; Ex-1003 ¶126.

“and comprising a sandboxed computing environment”

Hoy teaches its guest system comprises a sandboxed computing environment, as the Examiner found during prosecution. Ex-1002 at 296; Ex-1003 ¶125. The Examiner found that Hoy’s disclosure, including Hoy’s teaching that “[t]he virtual guest system also has no connection whatsoever to the LAN, and cannot access any address on the LAN” is “essentially a **definition of sandboxed environment** as known in the art.” Ex-1002 at 296; Ex-1004 ¶0027.

Moreover, under the proper construction of a “sandboxed computing environment,” a POSITA would have understood that Hoy’s guest system is a computing environment that does not require its own separate OS. Ex-1003 ¶126. Indeed, as discussed above, Hoy teaches that the hypervisor may be “a software module that operates based on the underlying operating system, e.g., Windows 7, of the computer 9.” Ex-1004 ¶0042. A POSITA would have known that a hypervisor can create a guest system that does not run a full-fledged operating system but rather runs a “stripped down” operating system that uses the host operating system to perform activities like file access and network communications; requests by the guest system to perform these activities are

passed to the hypervisor in the host operating system, which can grant or deny such requests. Ex-1003 ¶126; *see also* Ex-1006, 2:34-36.

Hoy's guest system is also a sandboxed computing environment under the alternative construction discussed in the claim-construction section above ("an area in which software is confined and prevented from accessing system resources").

Ex-1003 ¶127. In particular, Hoy teaches that "[t]he guest is separated and completely isolated by an internal firewall from the host, and the guest **cannot access any of the resources of the host computer....**" Ex-1004 ¶0019.

"that uses a second memory space to enable operation of a second set of one or more applications or processes"

Hoy discloses a **second memory space**. Ex-1003 ¶128. Hoy teaches that "[t]he guest is separated and completely isolated by an internal firewall from the host." Ex-1004 ¶0019. As discussed for element 1c, a POSITA would have understood this to mean that any applications running on the guest system are running in the separate memory space of the guest system. Ex-1003 ¶129.

Additionally, Hoy teaches "a **computer memory area** (such as a respective desktop) or virtual data storage accessible to the virtual guest OS 13." Ex-1004 ¶0047. Hoy distinguishes between this memory area and the memory area accessible to the trusted-host OS, which is isolated from the guest system as discussed above. *Id.* As discussed for element 1c, a POSITA would have

understood Hoy’s “computer memory area” to encompass both volatile RAM and non-volatile memory like solid-state and hard drives. Ex-1003 ¶130; *see also* Ex-1001, 9:4-11. Accordingly, Hoy’s disclosure of “a computer memory area ... accessible to the virtual guest OS 13” further teaches an isolated computing environment (the guest system) that **uses a second memory space** to operate applications. Ex-1004 ¶0047; Ex-1003 ¶130.

As discussed above, the guest system operates a **set of one or more applications or processes**. These applications or processes include “a browser and possibly some related supportive software, such as Adobe or Windows Media Player ..., and potentially an email program such as Microsoft Outlook...” Ex-1004 ¶0048; *see also id.* ¶0052. Accordingly, Hoy teaches using the second memory space to enable operation of a second set of one or more applications or processes. Ex-1003 ¶131.

[1e] wherein the isolated computing environment is configured to access an Internet-based cloud service via at least one application of the second set of one or more applications or processes;

Hoy teaches element 1e. The Internet-based cloud service is illustrated in Figure 1 as a cloud with the word “**Internet**” inside.

Hoy explains that “[t]he Internet provides access to a large number of computer systems,” which a POSITA would have understood as **Internet-based cloud services.**

Ex-1003 ¶134. Hoy teaches that these computer systems may include a file service (upload/download), websites that provide access to online software certificates and online help, and an Internet-based email service. Ex-1004 ¶¶0031, 0050, 0051, 0057, 0058, 0075. A POSITA would have recognized these as Internet-based

cloud services. To access these services, the guest system has an Internet browser or email program (**at least one application of the second set of one or more applications or processes**). *Id.*; see also *id.* ¶¶0048, 0052; Ex-1003 ¶¶134-135.

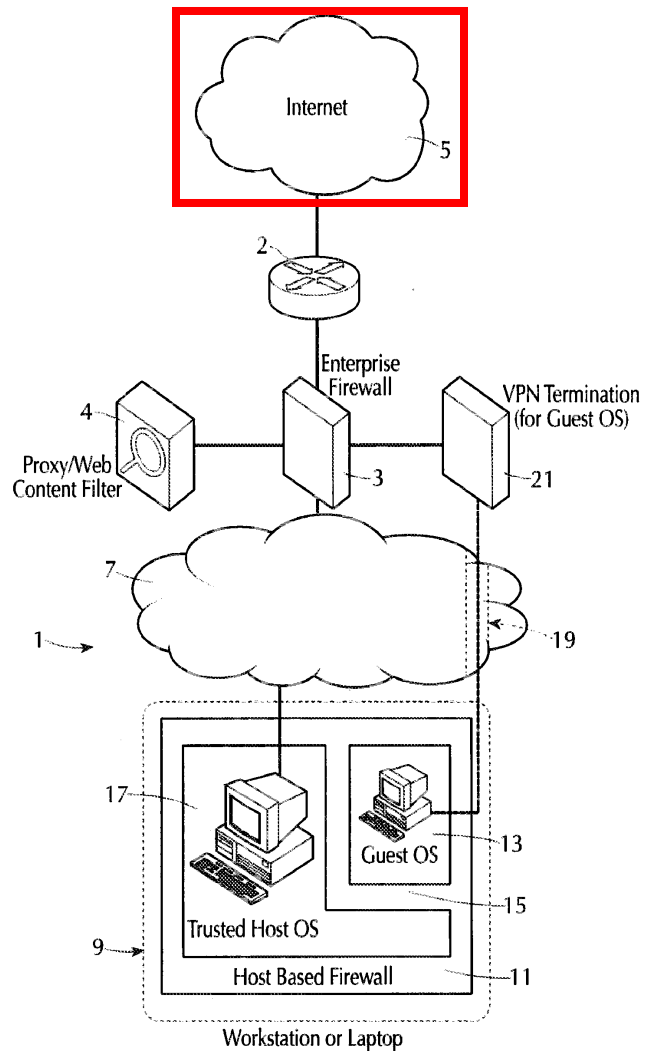


FIG. 1

[1f] **isolate the isolated computing environment from the workspace using an internal isolation firewall;**

As discussed for element 1d, Hoy discloses **isolat[ing]** the guest system (an **isolated computing environment**) from the trusted-host OS (a **workspace**).

Isolation is accomplished **using an internal isolation firewall** in the form of an internal host-supported firewall 15. The internal firewall 15 is in addition to the host-based firewall 11 and is shown in Figure 1. Ex-1003 ¶138.

The internal firewall 15
“separates and restricts interaction
between virtual guest system 13 and
the trusted-host operating system 17,”
thus isolating the guest system from
the trusted-host OS. Ex-1004 ¶0043;
Ex-1003 ¶139. In particular, “data
from sites that are opened by the
virtual guest system browser remains
isolated in the virtual system behind
the internal firewall 15....” Ex-1004
¶0083; *see also id.* ¶0019 (“The
guest is separated and completely

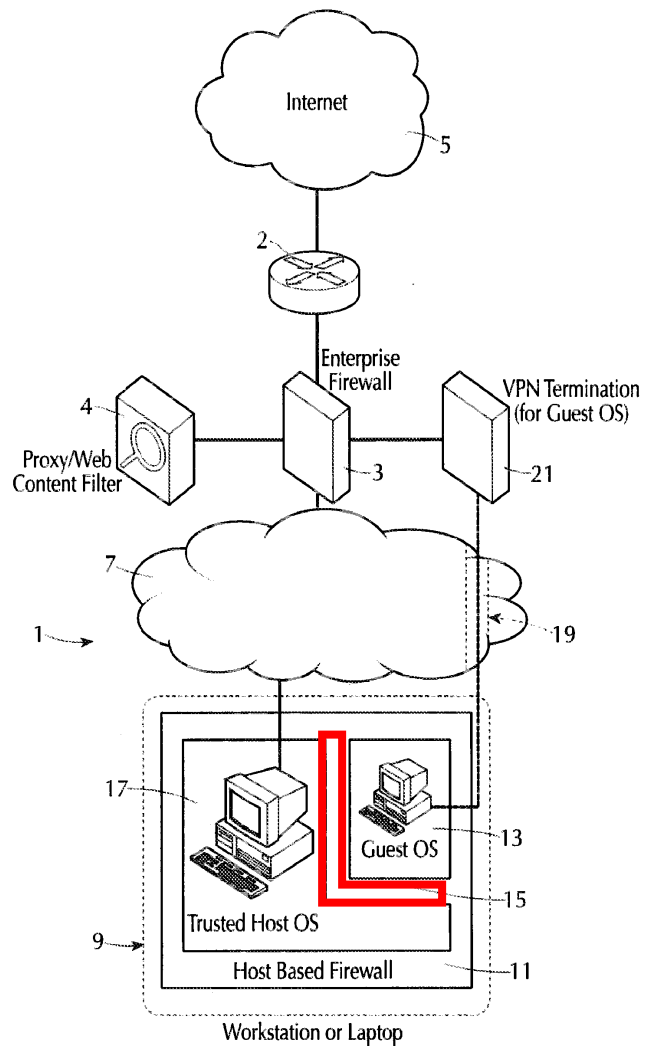


FIG. 1

isolated by an internal firewall from the host, and the guest cannot access any of the resources of the host computer.”), 0021, 0030, 0074 (“[T]he firewall 15 of the first embodiment restricts communication between its host and guest systems.”), 0083.

[1g] authenticate the isolated computing environment with an authentication device; and
--

Hoy combined with Pratt teaches element 1g. Ex-1003 ¶141.

Hoy teaches that “[t]he VPN transmits data packets that are encrypted according to an IPSEC or SSL VPN tunnel construct protocol.” Ex-1004 ¶0054. Both the IPsec and SSL standards include authenticating computer environments that are sending the data packets, Ex-1003 ¶¶21, 23-25, 55, 142, but Hoy does not discuss the specific details.

Pratt teaches authentication: “System 100 may be used to securely **authenticate operating environment** 120 to service or resource provider 150....” Ex-1006, 2:15-22. Like Hoy’s guest system, Pratt’s operating environment 120 is an isolated, sandboxed computing environment that can use a host operating system. Ex-1006, 2:29-36 (“The term ‘operating environment’ broadly refers to any kind of isolated software computer environment.... A host operating system or a guest operating system may execute within each of a virtual machine, a container, and a sandbox environment.”). And like Hoy’s guest system, Pratt’s

operating environment 120 is an operating environment wherein malicious code may be present. Ex-1006, 2:38-40; Ex-1003 ¶143.

Pratt's operating environments comprise an authentication service, labeled 122 and 132 in Figure 1. Ex-1006, 2:59-63. Each authentication service is "a component capable of providing authentication data to an operating system." Ex-1006, 2:63-65. Pratt explains that "many types of schemas and approaches for performing authentication" of an operating environment existed. Ex-1006, 2:65-3:2; Ex-1003 ¶144.

In operation, an interceptor module 114 intercepts a message from a provider 150 that requires the untrusted operating environment 120 to authenticate itself. Ex-1006, 4:14-16. Instead of notifying the untrusted operating environment 120 of the intercepted message, the interceptor module notifies the trusted

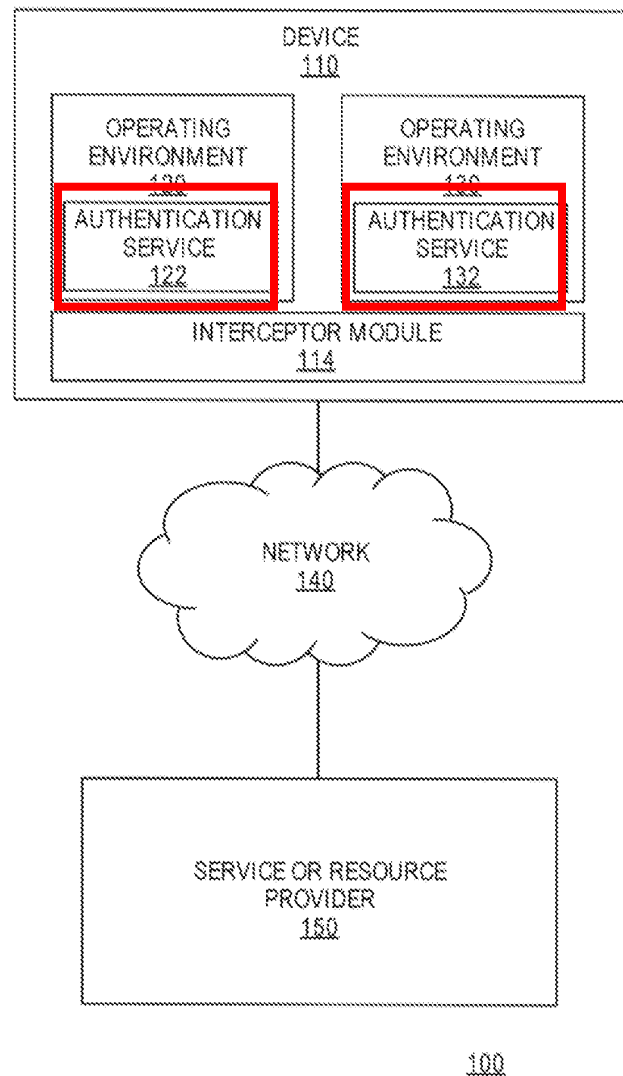


FIG. 1

operating environment 130. Ex-1006, 4:40-41. Through its authentication service 132, the trusted operating environment 130 provides authentication data to the untrusted operating environment 120, which then “authenticates itself to provider 150 using the authentication data.” Ex-1006, 5:1-3, 5:43-53. In this way, “operating environment 120 is able to authenticate itself to provider 150 without exposing ... any malicious code which may be inadvertently introduced or present within operating environment 120 to the authentication mechanism...” Ex-1006, 5:54-58; Ex-1003 ¶145.

As discussed above, a POSITA would have been motivated to combine Pratt’s authentication process with Hoy’s computer system. To accomplish this, a POSITA would have configured Hoy’s guest system to authenticate itself in a manner similar to Pratt’s untrusted operating environment. Ex-1003 ¶146. Both Hoy’s guest system and Pratt’s untrusted operating environment are isolated, sandboxed computing environments, and Hoy’s computer system would be

adapted to include Pratt's interceptor module and authentication services in an arrangement similar to what is shown in Figure 1 of Pratt. *Id.*

Below is Figure 1 of Hoy, modified to show Pratt's interceptor module 114 positioned to intercept authentication messages originating from beyond the trusted LAN 7. Hoy's guest system includes Pratt's authentication service 122, while the trusted-host OS includes Pratt's authentication service 132. The interceptor module of the combined system intercepts the authentication messages and notifies the authentication service 132 in the trusted-host OS, which then provides authentication data to the guest system so that it can authenticate itself. As in Pratt, the guest system can authenticate itself without exposing any malicious code to the authentication service 132 in the trusted-host OS. Ex-1003 ¶147.

Hoy teaches that “[t]he host monitors the guest browser at all times and screens any destination resource or address that the guest

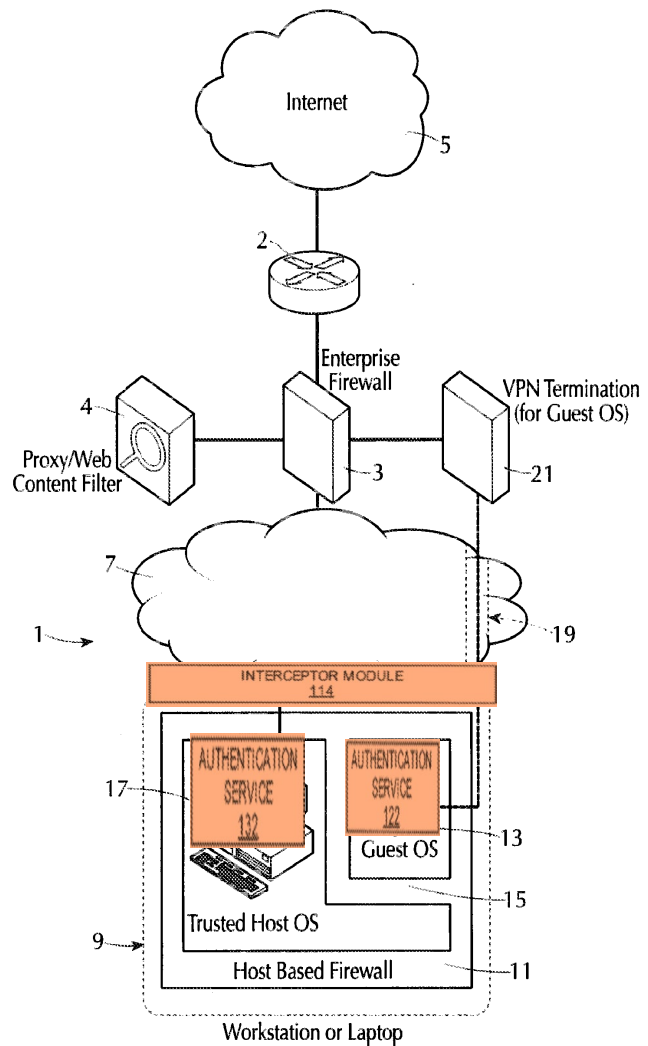


FIG. 1

browser tries to access.” Ex-1004 ¶0082. It would have been straightforward for a POSITA to add Pratt’s interceptor module, which would similarly monitor the guest browser’s communications with entities beyond the LAN and screen them for authentication requests, without changing Hoy’s principle of operation. Ex-1003 ¶149.

Hoy and Pratt combined thus teach **authenticating an isolated computing environment** (Hoy’s guest system) **with an authentication device**. The authentication device is the entity that ultimately receives the authentication data from the guest system and authenticates it. In the Hoy-Pratt system, the authentication device would be Hoy’s proxy/web-content filter, as Pratt discloses that the provider 150 requesting authentication may be a proxy server, such that Hoy’s guest system is authenticated with a proxy. Ex-1006, 3:52-54; Ex-1003 ¶150.

[1h] communicate with a proxy server to access the Internet-based cloud service to allow communication between the at least one application and the Internet-based cloud service when the isolated computing environment has been authenticated.

Hoy combined with Pratt teaches element 1h. Ex-1003 ¶152.

Hoy teaches **communicat[ing] with the proxy/web-content filter (a proxy server) to access an Internet-based cloud service to allow communication between at least one application (e.g., a browser or an email program) and the Internet-based cloud service.** The

proxy/web-content filter 4 is shown in Figure 1 of Hoy. Ex-1003 ¶153.

Hoy teaches that “[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....” Ex-1004 ¶0038; *see also id.* ¶0073. Hoy’s workstation thus communicates with the proxy/web-content filter to access the

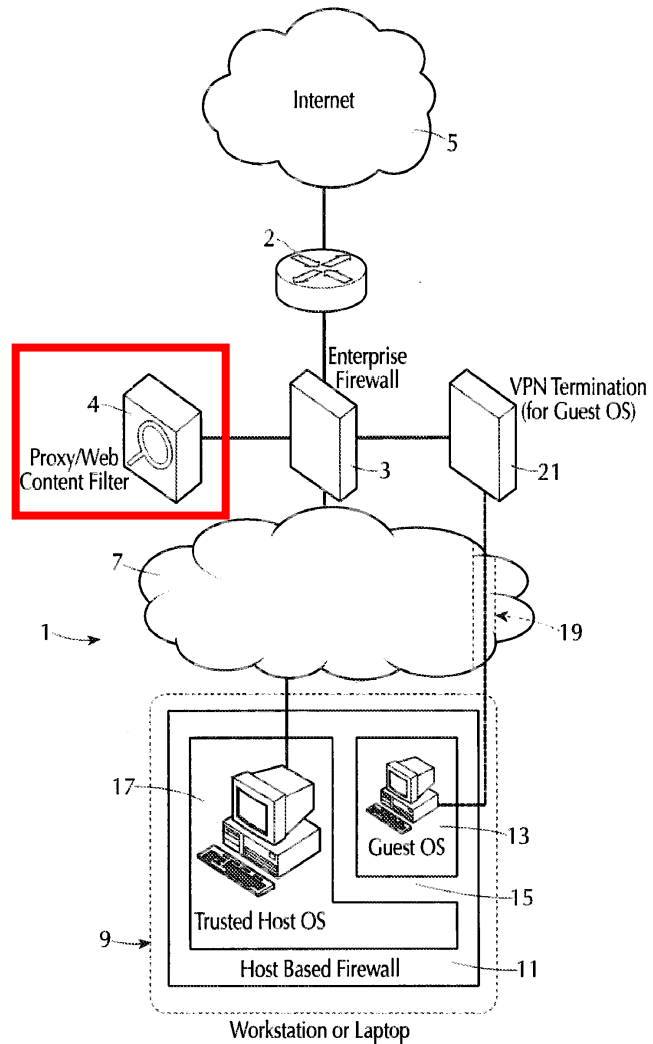


FIG. 1

Internet and the cloud services thereon, discussed in connection with element 1e.

If the proxy/web-content filter permits the data to pass, then communication is allowed between the requesting application operating in the workstation's guest system and the Internet-based cloud service. Ex-1003 ¶¶154-155.

Hoy combined with Pratt discloses that the communication between the requesting application and the Internet-based cloud service is allowed when the guest system (the isolated computing environment) has been **authenticated**. Pratt explains authenticating an isolated operating environment like Hoy's guest system might be needed for a service or resource provider (like Hoy's Internet-based cloud services) to provide its services or resources to an application running in the isolated operating environment. Ex-1006, 3:49-52. As discussed for element 1g, Pratt teaches authenticating the isolated operating environment, after which communication between the application running in the isolated operating environment and the provider is allowed. Pratt also teaches authentication with a proxy. Ex-1006, 3:52-54; Ex-1003 ¶156.

Accordingly, Hoy combined with Pratt teaches claim 1.

3. Claim 2

[2pre] The host computer system of claim 1,

See claim 1.

[2a] wherein the processor is configured to access the Internet-based cloud service via one or more of a local area network (LAN), a wide area network (WAN), a cellular network, a Wi-Fi network, a digital subscribers line (DSL) network, a cloud computing network, a data center, or a satellite network.

As discussed for element 1e, Hoy's guest system is **configured to access an Internet-based cloud service**. Ex-1003 ¶160.

Hoy teaches that the access is done **via one or more of a local area network (LAN), a wide area network (WAN), or a Wi-Fi**

network. Hoy discloses a LAN 7 and the Internet (which a POSITA would have recognized as a WAN), as illustrated in Figure 1. Ex-1003 ¶161. Hoy explains that "the traffic between the **Internet** and the browser of the virtual guest system 13 is routed through a sealed 'virtual conduit' 19 passing through the **LAN**." Ex-1004 ¶0052; *see also id.*

¶¶0054-0055, 0064 (teaching a **Wi-Fi** network); Ex-1003 ¶161-162.

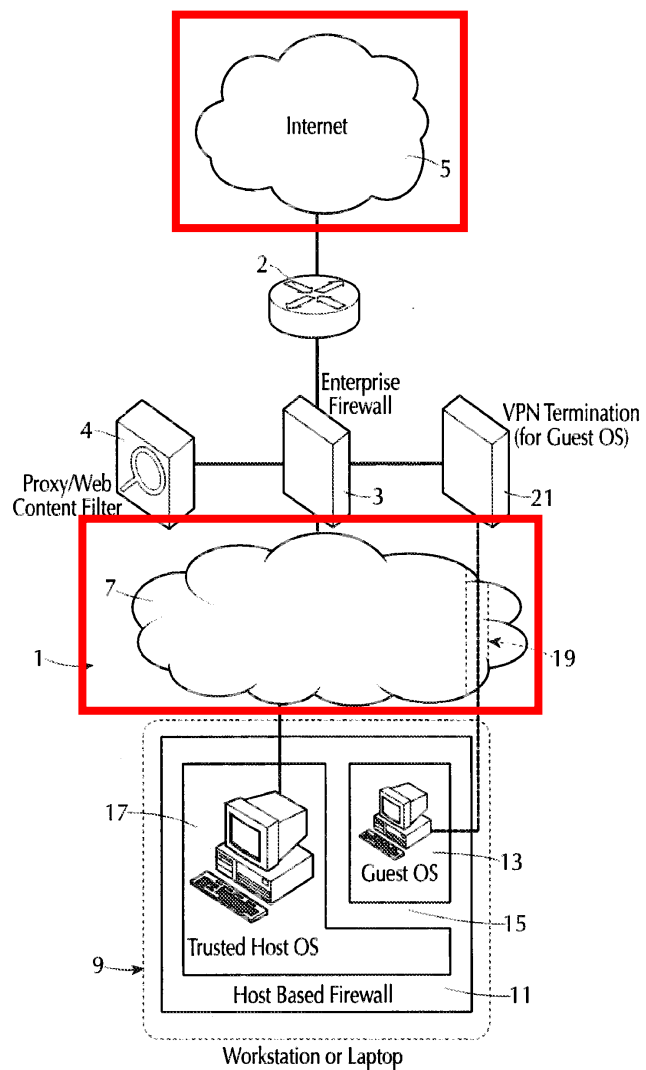


FIG. 1

4. Claim 3

[3pre] The host computer system of claim 1,

See claim 1.

[3a] wherein the Internet-based cloud service comprises one or more of an Infrastructure as a Service (IaaS), a Software as a Service (SaaS), or a Platform as a Service (PaaS).

As discussed for element 1e, Hoy teaches an **Internet-based cloud service** such as a file service (upload/download), websites that provide access to online software certificates and online help, and an Internet-based email service. Ex-1004 ¶¶0031, 0050, 0051, 0057, 0058, 0075; Ex-1003 ¶166.

A POSITA would have recognized the file service (uploading/downloading) as an example of **Infrastructure as a Service (IaaS)**. Ex-1003 ¶167. IaaS is a type of cloud service that offers computing, storage, or networking resources over the Internet. *Id.* A POSITA would have understood file uploading/downloading to be cloud services that offer storage resources over the Internet. *Id.*

A POSITA would have further recognized websites that provide access to online software certificates and online help, and the Internet-based email service, as examples of **Software as a Service (SaaS)**. Ex-1003 ¶168. SaaS is a type of cloud service that offers software resources over the Internet. *Id.* Additionally, A POSITA would have recognized the email service as an example of IaaS, since

such email services at the time normally stored the user's email on a cloud server.

Id.

5. Claim 8

[8pre] The host computer system of claim 1,

See claim 1.

[8a] wherein the internal isolation firewall is configured to segregate the first memory space from the second memory space, and

As discussed above, Hoy teaches a **first memory space** (element 1c), a **second memory space** (element 1d), and an **internal isolation firewall** (element 1f).

Hoy's internal isolation firewall is **configured to segregate the first memory space from the second memory space**. Ex-1004 ¶¶0043; Ex-1003 ¶172. Hoy teaches that “[c]ommunications between the trusted host OS 17 and the guest OS 13 pass through the hypervisor firewall 15, and are limited to ... [t]ransfer of files ... between a computer memory area ... accessible to the virtual guest OS 13 and a computer memory area ... accessible to the host OS 17....” Ex-1004 ¶¶0043, 0047. To a POSITA, this disclosure would have meant that the files accessible by the guest system are not accessible by the trusted-host OS, and vice versa, and that the memory space for storing the files of the guest system is therefore segregated from the memory space for storing the files of the trusted-host

OS. Otherwise, the files would not need to be transferred between the two systems. Ex-1003 ¶173.

Additionally, Hoy teaches that the segregation is performed by the internal firewall 15, which is the gatekeeper for transferring files between the guest system and the trusted-host OS. Ex-1003 ¶173. Hoy explains that the “hypervisor also provides an additional internal host-supported firewall indicated at 15 that separates and restricts interaction between virtual guest system 13 and the trusted operating system.” Ex-1004 ¶0043.

[8b] wherein the processor is configured to enforce policies for communication between the first memory space and the second memory space using the internal isolation firewall.
--

Hoy discloses that “[c]ommunications between the trusted host OS 17 and the guest OS 13 pass through the hypervisor firewall 15, and are limited” to four particular functions, including the transfer of files as discussed above. Ex-1004 ¶¶0043-0047. These four functions, listed in paragraphs 0044-0047 of Hoy, are **policies for communication enforced by the processor using the internal isolation firewall.** Ex-1003 ¶175.

Additionally, Hoy teaches that communications between the memory space for the guest system and the memory space for the trusted-host OS are limited to the transfer of files, and only when directed by trusted-host OS, which a POSITA

would also have understood as **policies for communication enforced by the processor using the internal isolation firewall**. Ex-1003 ¶176.

6. Claim 10

Hoy combined with Pratt renders claim 10 obvious. Ex-1003 ¶178.

Claim 10 largely repeats claim 1. Petitioner incorporates by reference the relevant analysis above for the limitations repeated from claim 1 and does not re-state that analysis, it being understood that the analysis would be the same. In particular:

- Hoy teaches 10b; *see* 1c.
- Hoy teaches 10c; *see* 1d.
- Hoy teaches 10d; *see* 1f.
- Hoy combined with Pratt teaches 10e; *see* 1g.
- Hoy teaches 10f; *see* 1h.
- Hoy combined with Pratt teaches 10g; *see* 1h.

[10pre] A cloud computing system comprising:

Hoy discloses a **cloud computing system** in the form of the networked computer system 1. Ex-1004, Fig. 1; *see also id.* ¶0038 (“Referring to FIG. 1, a networked computer system generally indicated at 1 is linked to the Internet 5....”). As discussed for element 1e, the workstation in the networked

computer system can access an Internet-based cloud service, making the networked computer system a cloud computing system. Ex-1003 ¶179.

[10a] a cloud computing network comprising a server,

The networked computer system 1 in Hoy comprises a **server** in the form of the workstation 9, shown in Figure 1. Ex-1004, Fig. 1; *see also id.* ¶0038; Ex-1003 ¶¶181-182.

A POSITA would have recognized the workstation as a type of server, since the workstation can provide information to other devices on the LAN 7. Ex-1003 ¶183. Hoy explicitly mentions “servers or devices in the LAN.” Ex-1004 ¶0016.

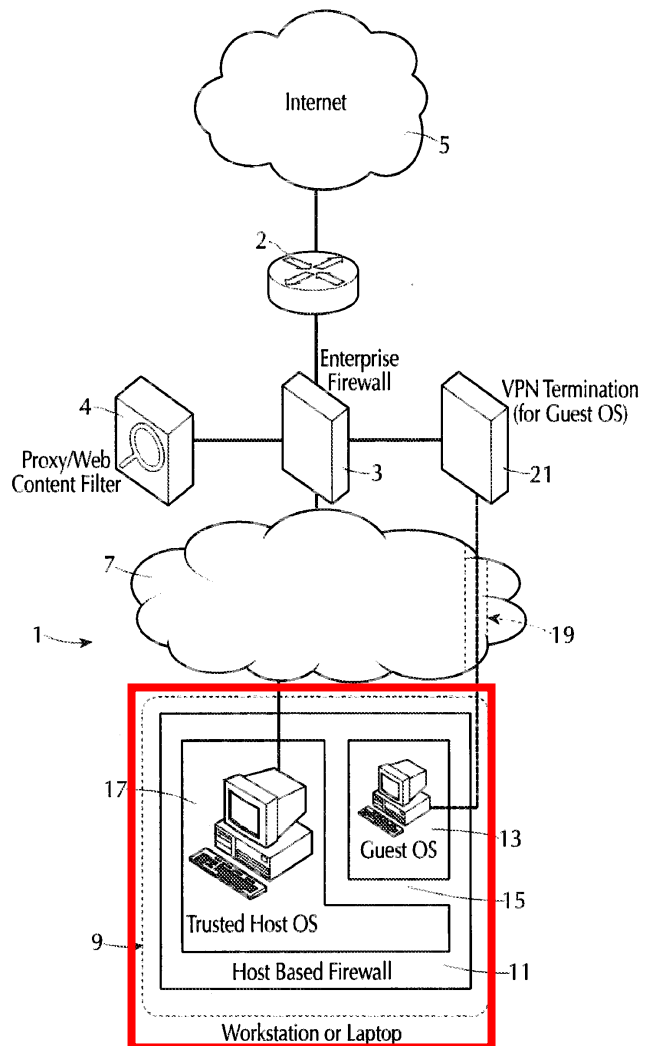


FIG. 1

[10h] to block communication between the first set of one or more applications or processes running in the workspace and the Internet resource.

Hoy discloses that the proxy/web-content filter 4 can **block communication between applications or processes running in the workspace** (the trusted-host OS) and **Internet resources**. Ex-1003 ¶193. Hoy describes that the “proxy/web-content filter 4 ... **blocks communications** from users on the LAN trying to reach disallowed sites....” Ex-1004 ¶0038; *see also id.* ¶0073.

Additionally, Hoy teaches that the “proxy/web-content filter 4 cooperates with the firewall hardware 3,” which in turn “is configured to **block all host-based egress** for all ports, protocols and destinations” with limited exceptions. Ex-1004 ¶¶0038, 0068. Through the cooperation of the proxy/web-content filter and the firewall hardware 3, applications or processes running in the trusted-host OS (the workspace) are blocked from communicating with Internet resources. Ex-1003 ¶194.

7. Claim 11

[11pre] The cloud computing system of claim 10,

See claim 10.

[11a] wherein the server is configured to perform at least one processing task on behalf of a client device.

As discussed for elements 1e and 3a, Hoy teaches an Internet-based cloud service, including file services (upload/download), online software certificates, online software help, and an online email service. Ex-1004 ¶¶0031, 0050, 0051, 0057, 0058, 0075. These are examples of where **the server is configured to perform at least one processing task on behalf of a client device**. The '104 patent describes the server performing a task for the client in the same manner:

The server may perform a processing task on behalf of a client device. For example, the server may receive input data from the client device and may send data to the client device. The processing task may include one or more of an Infrastructure as a Service (IaaS), a Software as a Service (SaaS), and/or a Platform as a Service (PaaS).

Ex-1001, 2:57-62. In each of Hoy's examples, the server receives input data from the client device, e.g., file upload. Ex-1003 ¶197.

Additionally, Hoy teaches an example of an email server that processes a task on behalf of a client device. Ex-1003 ¶198.

8. Claim 17

For the reasons discussed above for claim 3, Hoy teaches claim 17, which recites that the Internet-based cloud service comprises IaaS, SaaS, and/or PaaS.

9. Claims 18-19

Claims 18 and 19 are the method counterparts of claims 1 and 3, with the same elements phrased as method steps. Claims 18 and 19 contain no additional limitations beyond the fact that they recite a method instead of a system. For the reasons stated above for claims 1 and 3, Hoy combined with Pratt teaches the methods of claims 18 and 19.

A POSITA therefore would have found the Challenged Claims obvious based on Hoy combined with Pratt.

B. Ground 2

1. Combination of Hoy and Pratt

As discussed for Ground 1, a POSITA would have been motivated to combine Pratt's authentication process with Hoy. Ex-1003 ¶211.

2. Combination of Hoy-Pratt with Krasin

a. Summary of Krasin

Krasin was published on October 1, 2015, almost two years before the '104 patent's stated priority date. Ex-1007. Krasin therefore is prior art under 35 U.S.C. §102(a)(1).

Krasin teaches sandboxed computing environments, an example of which is shown in Figure 4B. Ex-1007 ¶0077. In Krasin's nomenclature, a "worker" is a software process created from application code to complete an assigned work

assignment. Ex-1007 ¶0041. Krasin's system ensures that each worker executes separately, with access limited only to appropriate input and output files. Ex-1007 ¶0077; Ex-1003 ¶217.

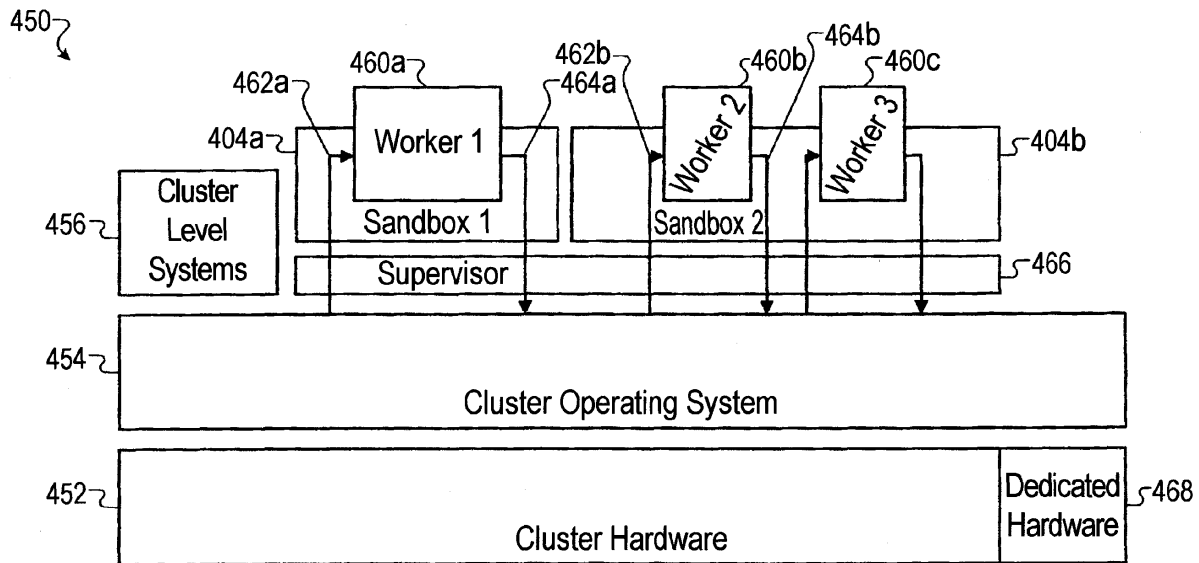


FIG.4B

The workers execute in sandboxes and are subject to tight control on available input and output. Ex-1007 ¶0079. The sandboxes provide limited communications functionality to the workers. *Id.*

Krasin teaches the advantages of using a sandbox over virtual machines:

[T]he sandbox environments 404 are light weight computational structures that require less resource overhead than, for example, virtual machines. Virtual machines, unlike a sandbox environment, emulate physical computer hardware or a full physical machine. Virtual machines **often also instantiate a full or partial operating system, which the sandbox environments 404 need not do.**

Id.; see also *id.* ¶0087; Ex-1003 ¶219.

b. Motivation to Combine

A POSITA would have been motivated to combine Krasin’s sandbox environment with the Hoy-Pratt computer system. As explained for element 1d in Ground 1, Hoy teaches a guest system comprising a sandboxed computing environment that uses a host operating system.

To exclude any doubt, however, the combination of Hoy, Pratt, and Krasin teaches all elements of the Challenged Claims, including a sandboxed computing environment that uses a host operating system. Krasin shows that a POSITA would have been highly familiar with isolated, sandboxed computing environments using a host OS well before the stated priority date of the ’104 patent. Ex-1003 ¶221.

A POSITA would have been motivated to combine Hoy and Pratt with Krasin. Ex-1003 ¶222. Krasin recognizes that sandboxes can protect the parts of the system outside the sandbox from untrusted applications executing in the sandbox, providing a motivation for a POSITA to use such sandboxes in Hoy’s computing system. Ex-1007 ¶0005. Krasin’s sandboxes provide “a secure and light-weight execution environment for untrusted code,” (Ex-1007 ¶0014), in addition to other advantages, such as “supporting efficient use of resources and speed of execution due to decreased number of system calls.” *Id.*; Ex-1003 ¶223.

Krasin provides teachings that would have motivated a POSITA to use Krasin's sandboxes in place of virtual machines. Krasin advantageously discloses that "the sandbox environments 404 are light weight computational structures that require less resource overhead than, for example, virtual machines." Ex-1007 ¶0079; Ex-1003 ¶225. The reduced resource overhead of Krasin's sandboxes would have motivated a POSITA, and the combination with Hoy would involve a POSITA combining prior-art elements according to known methods to yield a predictable result—Krasin's sandbox provides the isolated computing environment on Hoy's workstation. Ex-1003 ¶225.

3. Claim Analysis

For Ground 2, the element-by-element analysis for all Challenged Claims is the same as the element-by-element analysis for Ground 1, except that Krasin provides additional disclosure for:

- "isolated computing environment using a host operating system and comprising a sandboxed computing environment"; and
- "configured to enable operation of a first set of one or more applications or processes via a first memory space"; and
- "a second memory space to enable operation of a second set of one or more applications or processes."

As discussed above, Krasin discloses **sandboxed computing environments** throughout its specification and drawings, including the sandboxes illustrated in Figures 4A-4B. Krasin teaches that the workers executing in the sandboxes are subject to tight control on available input and output, thus creating an **isolated computing environment**. Ex-1007 ¶0079. Krasin also discloses that its sandboxes need not instantiate an operating system and thus **use the host operating system**. *Id.* (“Virtual machines often also instantiate a full or partial operating system, which the sandbox environments 404 need not do.”).

Accordingly, Hoy combined with Krasin teaches an “isolated computing environment using a host operating system and comprising a sandboxed computing environment.” Ex-1003 ¶230.

Krasin also teaches a **memory buffer** that a process-level manager can allocate to each sandbox. Ex-1007 ¶0048. These memory buffers are resources that each sandbox uses for running the application code operating

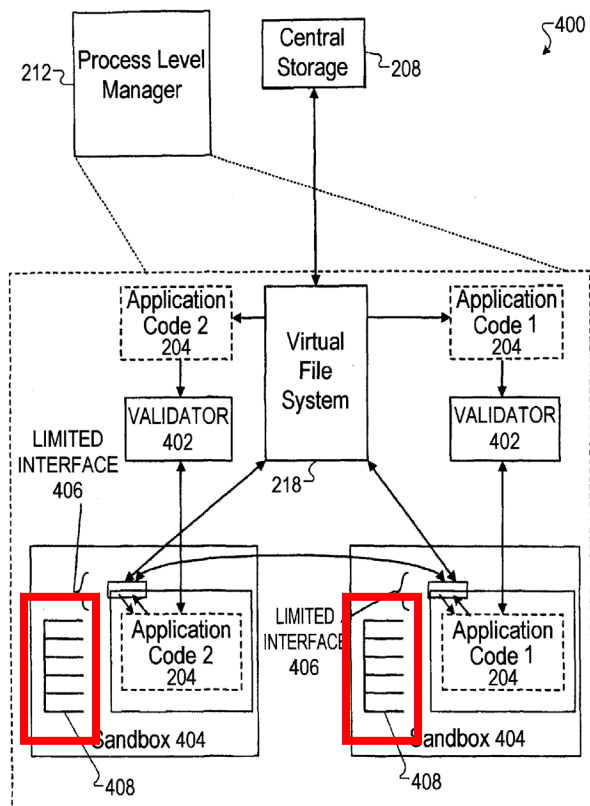


FIG. 4A

in that particular sandbox. *Id.*; Ex-1003 ¶231. The memory buffers 408 are shown in Figure 4A.

Krasin discloses that each computing environment uses its own memory space to enable operation of its own applications or processes. Combined with Hoy, Krasin's memory buffers provide a **first memory space** for the trusted-host OS (a workspace) and a **second memory space** for the guest system (an isolated, sandboxed computing environment). Accordingly, Hoy combined with Krasin also teaches a workspace "configured to enable operation of a first set of one or more applications or processes via a first memory space" and a sandboxed computing environment that uses "a second memory space to enable operation of a second set of one or more applications or processes." Ex-1003 ¶232.

For the foregoing reasons, a POSITA would have found the Challenged Claims obvious based on Hoy combined with Pratt and Krasin.

C. Ground 3

1. Summary of Benoit

Benoit was published on April 2, 2015, more than two years before the stated priority date of the '104 patent. Ex-1005. Benoit therefore is prior art under 35 U.S.C. §102(a)(1).

Benoit teaches a computer device, shown in Figure 2, comprising a host operating system (OS) 201, a typical operating environment (OE) 202, a sandbox

operating environment (OE) 203, and connections between the typical OE and sandbox OE (connections labeled 205 and 206). Ex-1005 ¶¶0041; Ex-1003 ¶¶236-237.

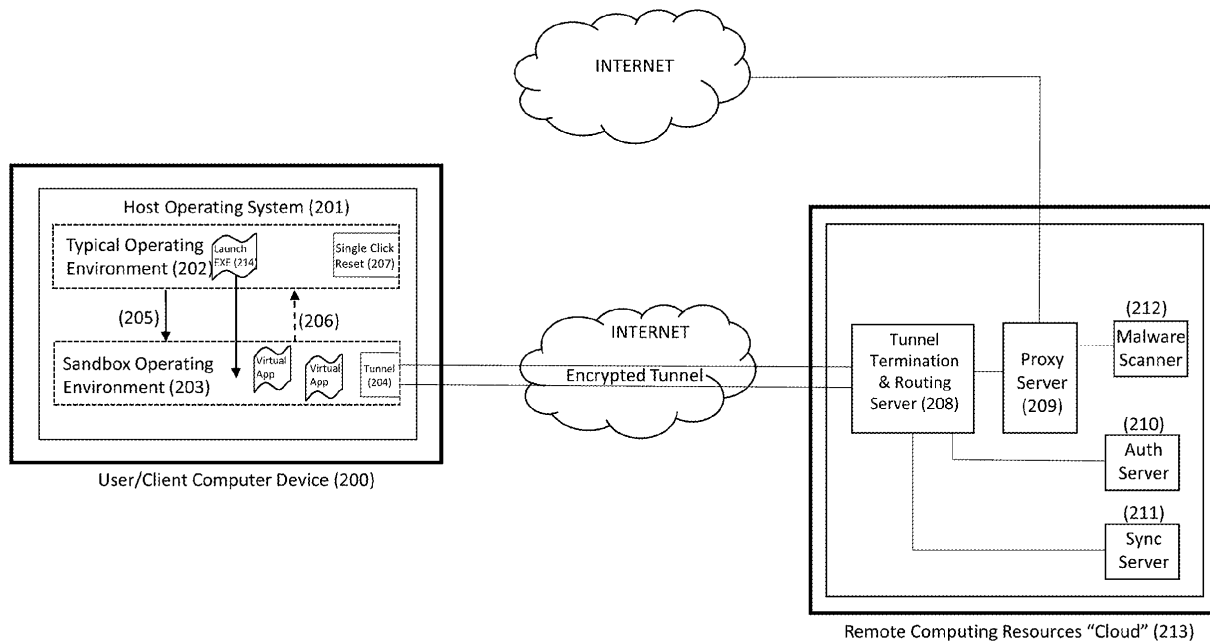


FIG. 2

Connected to the computer through an encrypted tunnel are remote computing resources (RCR) or “cloud” 213. Ex-1005 ¶¶0041. The cloud comprises a tunnel termination and routing server 208, a proxy server 209, an authentication server 210, a synchronization server 211, and a malware scanner 212. *Id.*; Ex-1003 ¶¶238.

Benoit’s system configures pre-defined read and write permissions from the sandbox OE to the host system, launches the tunnel from the sandbox OE to the cloud, and launches a virtualized application inside the sandbox. Ex-1005 ¶¶0042-

0045; Ex-1003 ¶239. Accessing the cloud requires authentication. Ex-1005

¶0046. Upon a successful authentication, a connection is established via the tunnel with the proxy server in the cloud. Ex-1005 ¶0047. The user can then connect to the Internet. *Id.*; Ex-1003 ¶240.

2. Claim 1

[1pre] A host computer system:

Benoit discloses a **host computer system** in the form of a user/client computer device. The computer device is shown in Figure 2. Elsewhere, Benoit specifically calls this computer a “**host computing device.**” Ex-1005 ¶¶0030-0031, 0044, 0046, 0048-0051, 0053, 0054; Ex-1003 ¶243.

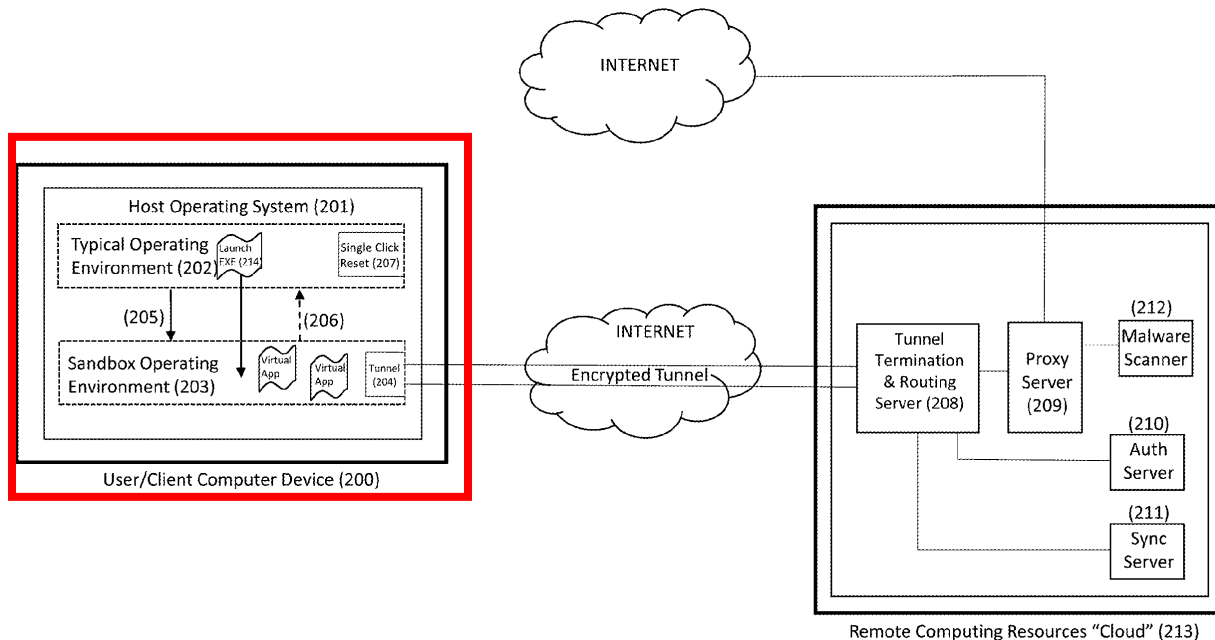


FIG. 2

[1a] a memory; and

Benoit discloses a **memory**. Benoit teaches that “a computing device 100 appropriate for use with embodiments of the present application may generally be comprised of ... **Random Access Memory (RAM) 102**....” Ex-1005 ¶0024; *see also id.* ¶¶0007, 0061, 0065-0066. The RAM 102 is shown in Figure 1. Ex-1003 ¶245.

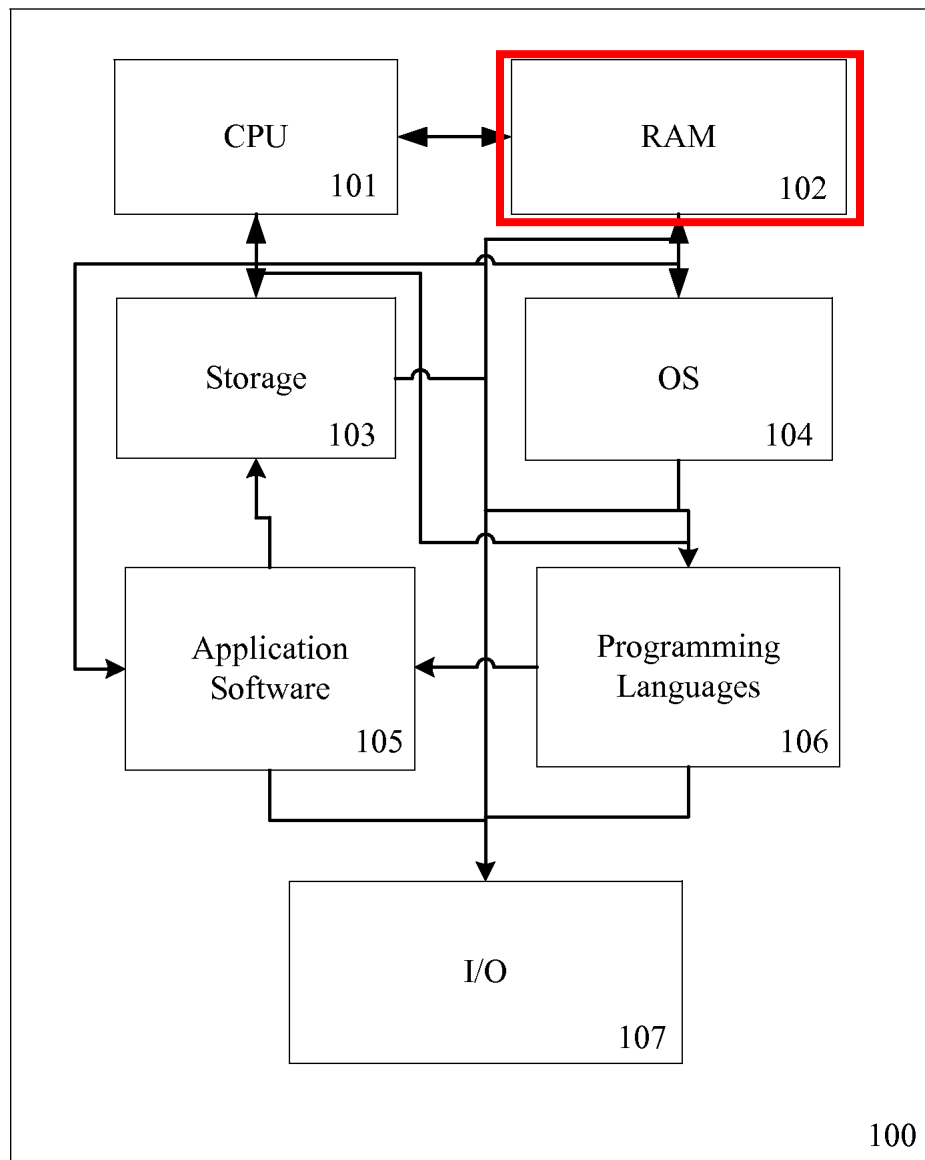


FIG. 1

[1b] a processor configured to:

Benoit discloses **a processor**. In connection with Figure 1, Benoit teaches that “a computing device 100 appropriate for use with embodiments of the present application may generally be comprised of ... a **Central Processing Unit (CPU)**

101....” Ex-1005 ¶0024; *see also id.* ¶¶0007-0009, 0061, 0072. The CPU 101 is shown in Figure 1. Ex-1003 ¶247.

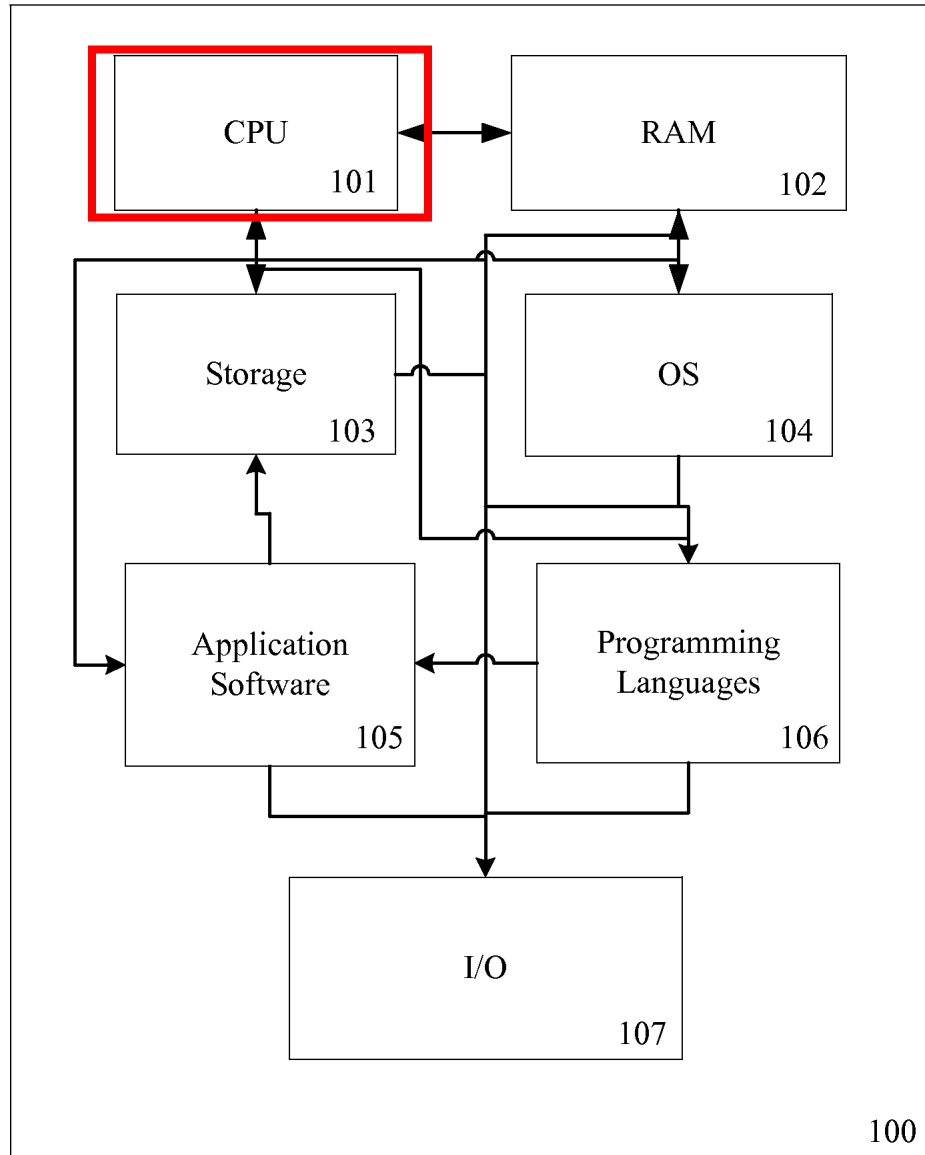


FIG. 1

[1c] implement a workspace, wherein the workspace is configured to enable operation of a first set of one or more applications or processes via a first memory space;

In the '104 patent, “workspace” is used to mean a computer environment in which one or more applications may run. *See, e.g.*, Ex-1001, 1:60-63; Ex-1003 ¶250.

Benoit discloses **implement[ing] a workspace** in the form of a typical operating environment (OE), shown in Figure 2. Ex-1005 ¶0041; Ex-1003 ¶251.

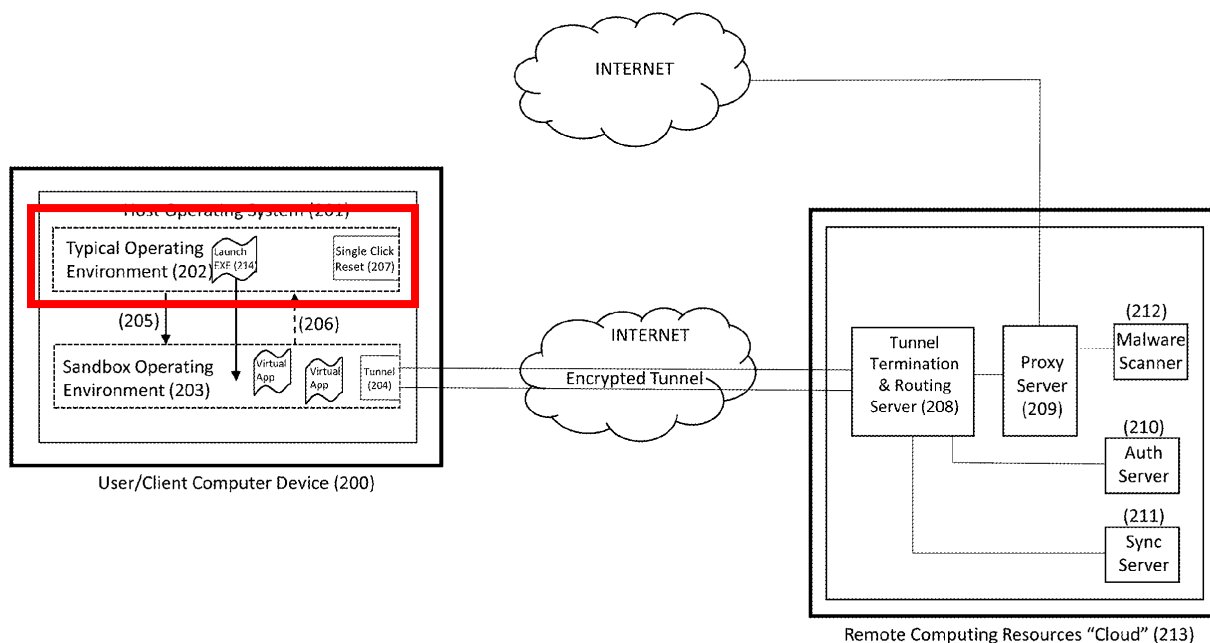
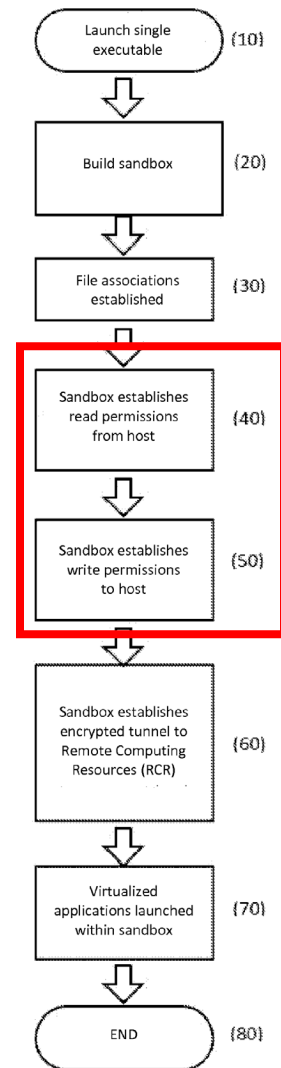


FIG. 2

As shown in Figure 2, the typical OE **configured to enable operation of a first set of one or more applications or processes**, such as a single-click reset process 207 and a launch executable program 214. Ex-1005 ¶0041; Ex-1003 ¶252.

The typical OE runs the applications or processes **via a first memory space**. To a POSITA, Benoit’s sandbox having “pre-defined read (40) and write (50) permissions to the host system,” is a sandbox having its own memory space separate from the memory spaces for other operating environments, including the typical OE. Ex-1003 ¶253. Benoit also teaches that “the sandbox is designed to ‘deny all’ software code from accessing host resources outside of the sandbox,” further indicating that the sandbox and the typical OE have separate resources, including separate memory spaces. Ex-1005 ¶0032; Ex-1003 ¶253.



[1d] implement an isolated computing environment, the isolated computing environment using a host operating system and comprising a sandboxed computing environment that uses a second memory space to enable operation of a second set of one or more applications or processes,

“implement an isolated computing environment”

Benoit discloses **implement[ing] an isolated computing environment** in the form of the sandbox OE, shown in Figure 2. Ex-1005 ¶0041; Ex-1003 ¶256.

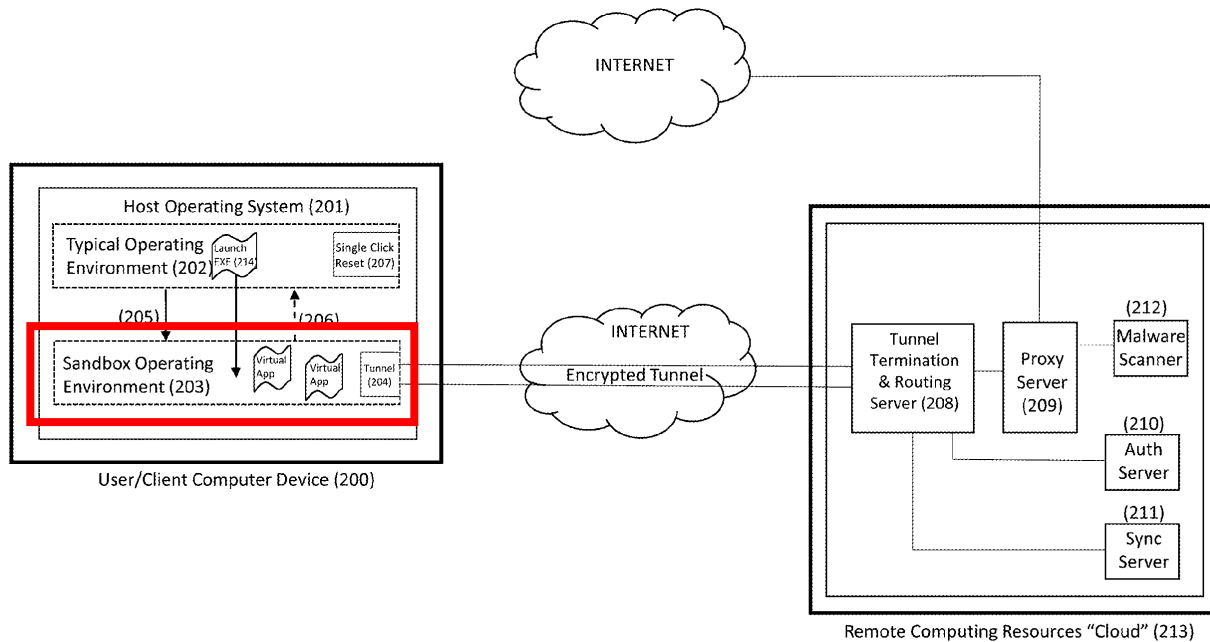


FIG. 2

Benoit teaches that the sandbox OE is separated from the typical OE and that interaction between the two operating environments is restricted to certain “connections between the typical OE 202 and the sandbox OE 203 (connections labeled 205, 206).” Ex-1005 ¶0041, Fig. 2; Ex-1003 ¶257. Benoit also teaches that “a sandbox is utilized and configured to reduce the ability for computer code to access the host computing device to the maximum amount possible....” Ex-1005 ¶0031. Notably, “the sandbox is designed to ‘deny all’ software code from accessing host resources outside of the sandbox.” Ex-1005 ¶0032; *see also id.* (“[N]othing occurs outside of the resources belonging to the sandbox (e.g., virtual host resources)....”); Ex-1003 ¶258.

“the isolated computing environment using a host operating system”

Benoit’s sandbox OE (an isolated computing environment) uses a host operating system. In Figure 2 (reproduced below with the host OS 201 highlighted), both the typical OE 202 and the sandbox OE 203 are within the host OS 201. Because Benoit teaches only one operating system (the host OS) and because this host OS is shown as including both the typical OE and the sandbox OE, a POSITA would have understood that the sandbox OE was using the host OS. Ex-1003 ¶259.

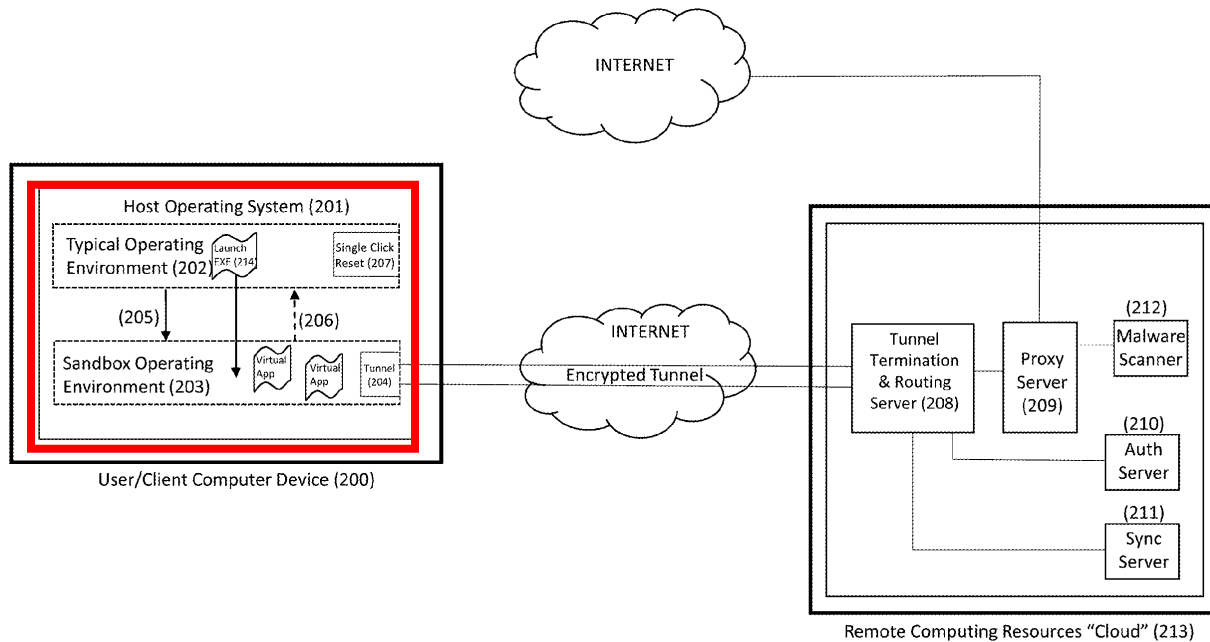


FIG. 2

“and comprising a sandboxed computing environment”

As discussed above, Benoit teaches a **sandboxed computing environment**.

Ex-1005 ¶0041, Fig. 2; Ex-1003 ¶260.

Moreover, under the proper construction of a “sandboxed computing environment,” a POSITA would have understood that Benoit’s sandbox OE is a computing environment that does not require its own separate operating system. As discussed above, Benoit teaches that the sandbox OE uses the host OS. Ex-1003 ¶261. Figure 2 illustrates both the typical OE and the sandbox OE as being within the host OS. Ex-1003 ¶261.

Benoit’s sandbox OE also meets the definition of a sandboxed computing environment under the alternative construction discussed in the claim-construction section above (“an area in which software is confined and prevented from accessing system resources”). Benoit teaches that the sandbox OE is separated from the typical OE and that interaction between the two operating environments is restricted to certain “connections between the typical OE 202 and the sandbox OE 203 (connections labeled 205, 206).” Ex-1005 ¶0041, Fig. 2; *see also id.* ¶0032 (“[T]he sandbox is designed to ‘deny all’ software code from accessing host resources outside of the sandbox.”); Ex-1003 ¶262.

“that uses a second memory space to enable operation of a second set of one or more applications or processes”

As discussed above, a POSITA would have understood that the sandbox OE would necessarily have had its own **memory space**. To a POSITA, Benoit’s sandbox having “pre-defined read (40) and write (50) permissions to the host

system” is a sandbox having its own memory space separate from the memory spaces for other operating environments, including the typical OE. Ex-1003 ¶264. Benoit also teaches that “the sandbox is designed to ‘deny all’ software code from accessing host resources outside of the sandbox,” further confirming that the sandbox and typical OE have separate resources, including separate memory spaces. Ex-1005 ¶0032; *see also id.* (“[N]othing occurs outside of the resources belonging to the sandbox (e.g., virtual host resources)...”); Ex-1003 ¶264.

Benoit also teaches the **operation of a second set of one or more applications or processes** through “launching one or more **virtual applications** from the sandbox,” which is illustrated in Figure 2 (reproduced below with the virtual applications highlighted). Ex-1005 ¶0014; *see also id.* ¶¶0007 (same), 0008; Ex-1003 ¶265.

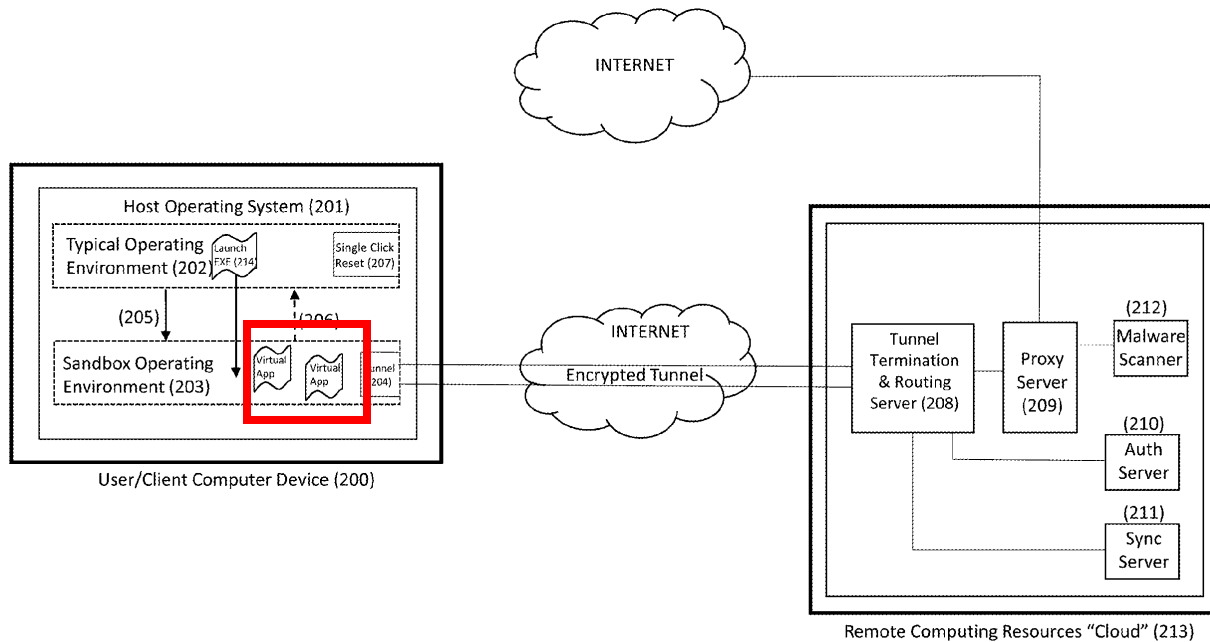


FIG. 2

[1e] wherein the isolated computing environment is configured to access an Internet-based cloud service via at least one application of the second set of one or more applications or processes;

Benoit's Figure 2 illustrates an **Internet-based cloud service** as a set of remote computing resources (RCR) or "cloud" 213 connected to the virtual applications (the **second set of one or more applications or processes**) in the sandbox OE 203 (an **isolated computing environment**) via an encrypted tunnel through the Internet. Ex-1003 ¶267.

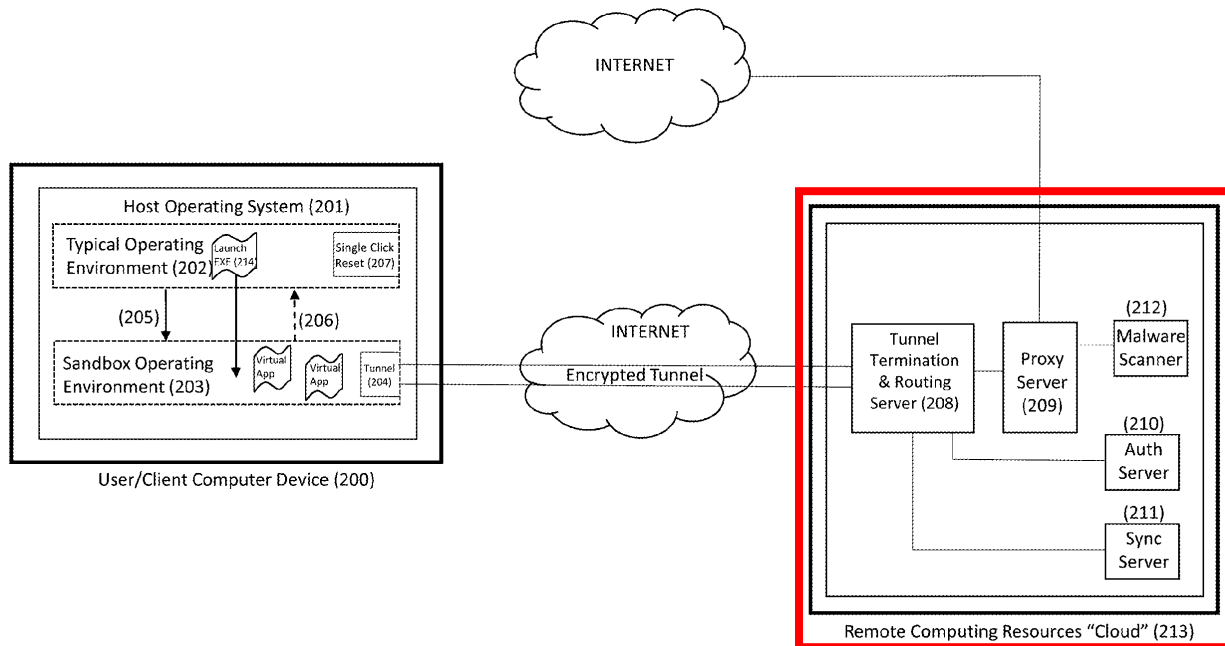


FIG. 2

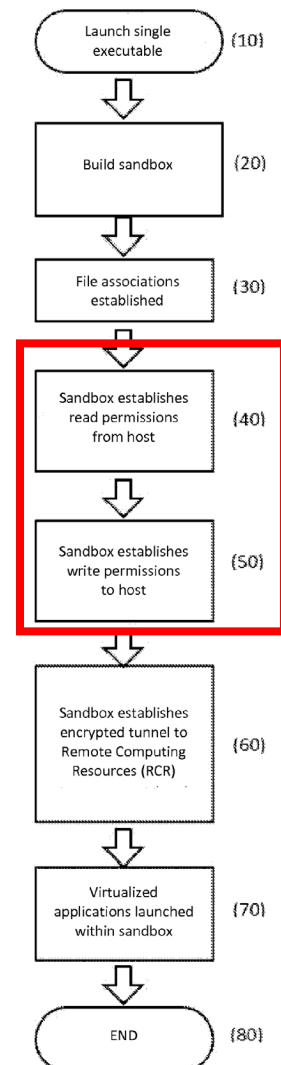
Benoit teaches that “the RCR (i.e., cloud component) 213, compris[es] one or more of a tunnel termination & routing server 208, a proxy server 209, an authentication server 210, a synchronization server 211 and a malware scanner 212.” Ex-1005 ¶0041. A POSITA would have understood each of these servers and the malware scanner as **Internet-based cloud services**. Ex-1003 ¶268. Benoit also teaches Internet-based cloud services in the form of the second cloud labeled “Internet” in Figure 2.

The Internet-based cloud services are accessed via the virtual applications (the **second set of one or more applications or processes**) in the sandbox OE. Ex-1003 ¶269. Figure 3B explains in step 120 that the “user initiates Internet bound traffic via virtual app(s) in sandbox.”

[1f] **isolate the isolated computing environment from the workspace using an internal isolation firewall;**

As discussed above, Benoit discloses a sandbox OE that is **isolated** from the typical OE (a **workspace**). Ex-1003 ¶272.

A POSITA would have understood that Benoit’s host OS implements an internal isolation firewall between the typical OE and the sandbox OE. Ex-1003 ¶273. To a POSITA, Benoit’s sandbox having “pre-defined read (40) and write (50) permissions to the host system” is a sandbox isolated from the host system **using an internal isolation firewall** (the pre-defined read and write permissions). Ex-1005 ¶0043; Ex-1003 ¶273. A POSITA would have known that, to enforce the permissions policy on a sandbox, the host OS needs a module to monitor sandbox activities such as access requests and determine whether to permit such activities, and that this module would be an internal isolation firewall. Ex-1003 ¶¶273-274; *see also id.* ¶0032 (“[T]he sandbox is designed to ‘deny all’ software code from accessing host resources outside of the sandbox.”).



[1g] authenticate the isolated computing environment with an authentication device; and

Benoit discloses **authentica[ing]** the sandbox OE (an **isolated computing environment**) with an authentication server (an **authentication device**). Benoit describes “request[ing] **authentication** from the user to provide access to the remote system via the encrypted connection, which request may also be automated, requiring no user input.” Ex-1005 ¶0007. The authentication is performed with an **authentication server**, illustrated in Figure 2 (reproduced below with the authentication server 210 highlighted). Ex-1005 ¶0041, Fig. 2; Ex-1003 ¶275. A POSITA would have understood that the sandbox OE was being authenticated, since the sandbox OE contains the tunnel termination. Ex-1003 ¶277; *see also* Ex-1005 ¶0046.

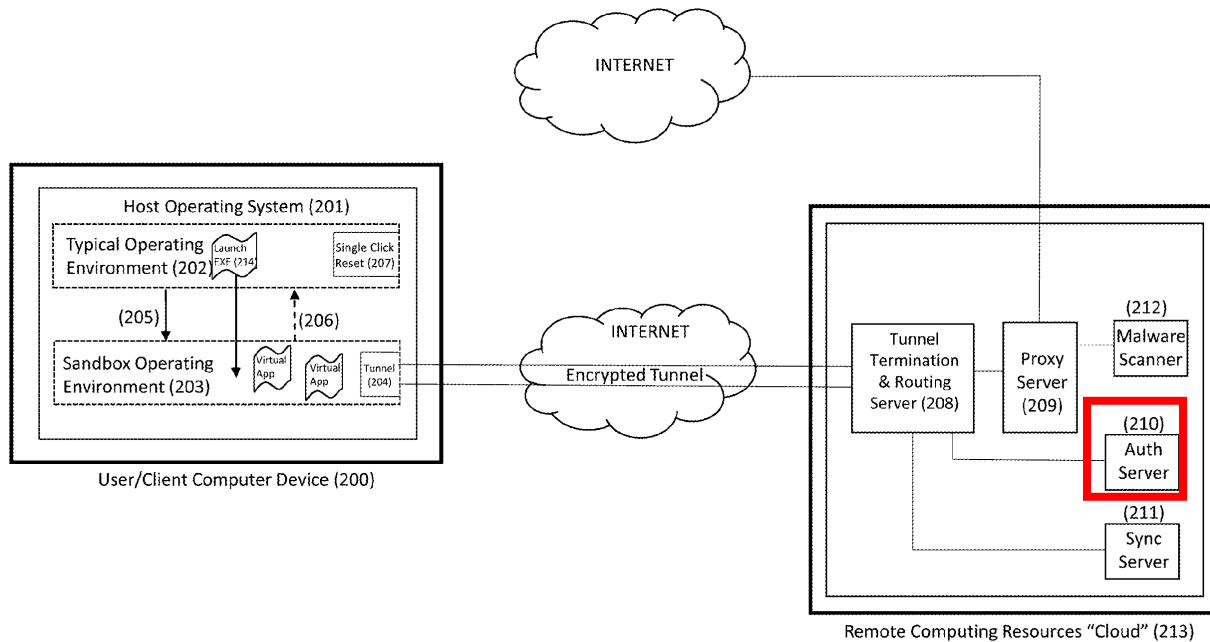


FIG. 2

[1h] communicate with a proxy server to access the Internet-based cloud service to allow communication between the at least one application and the Internet-based cloud service when the isolated computing environment has been authenticated.

Benoit's Figure 2 shows a **proxy server 209**. Ex-1003 ¶279.

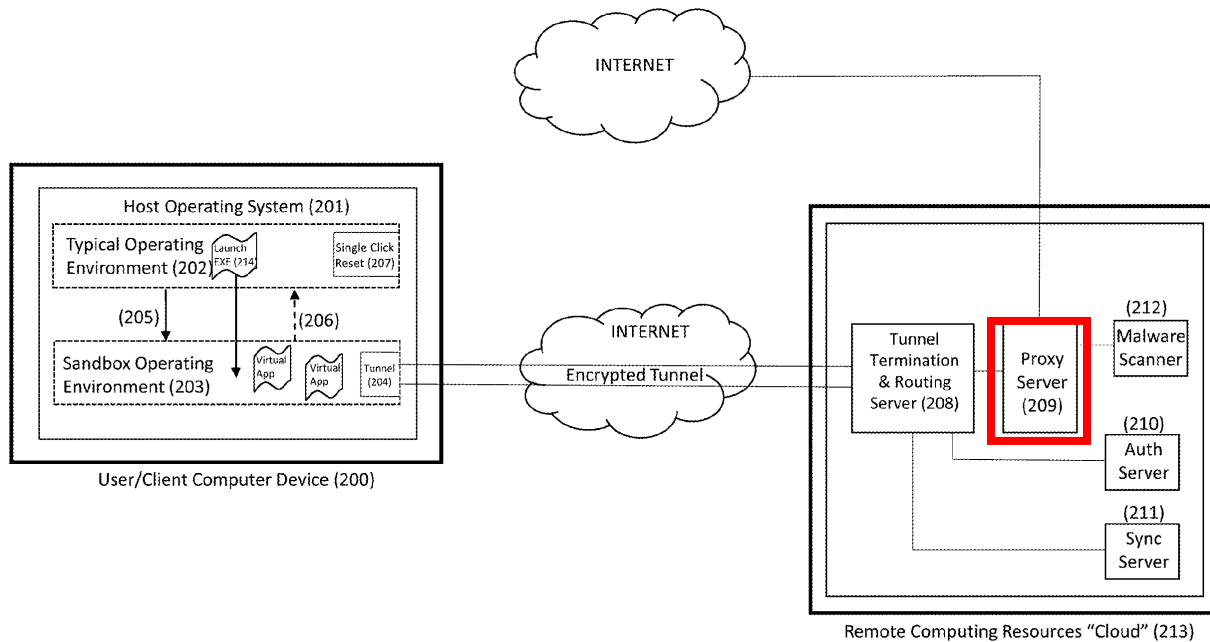


FIG. 2

As shown in Figure 2, the sandbox OE 203 communicates with the proxy server 209 to access services in the cloud 213 via the Internet, as well as to access other Internet-based cloud services via a connection from the proxy server 209 to a second cloud labeled “Internet.” Thus, Benoit teaches **allow[ing] communication between the virtual applications** operating in the sandbox OE and the **cloud 213** or other cloud services. *Id.*; Ex-1003 ¶280.

The communication is allowed **when the isolated sandbox OE has been authenticated** as discussed for element 1g. Benoit explains that “[u]pon successful authentication, the user is allowed to establish a connection, via the secured tunnel, with the proxy server (110) in the RCR component of the system.” Ex-1005 ¶0047; Ex-1003 ¶¶281-282.

3. Claim 2

Benoit teaches claim 2, which as discussed for Ground 1 concerns accessing the Internet-based cloud service via one or more of a LAN, WAN, cloud computing network, etc. Benoit discloses the Internet, which Benoit explicitly recognizes as a **WAN** (Ex-1005 ¶¶0003, 0025), and the RCR or “cloud,” which a POSITA would have recognized as a **cloud computing network**. Ex-1003 ¶287. Benoit’s Figure 2 shows both the Internet and cloud 213.

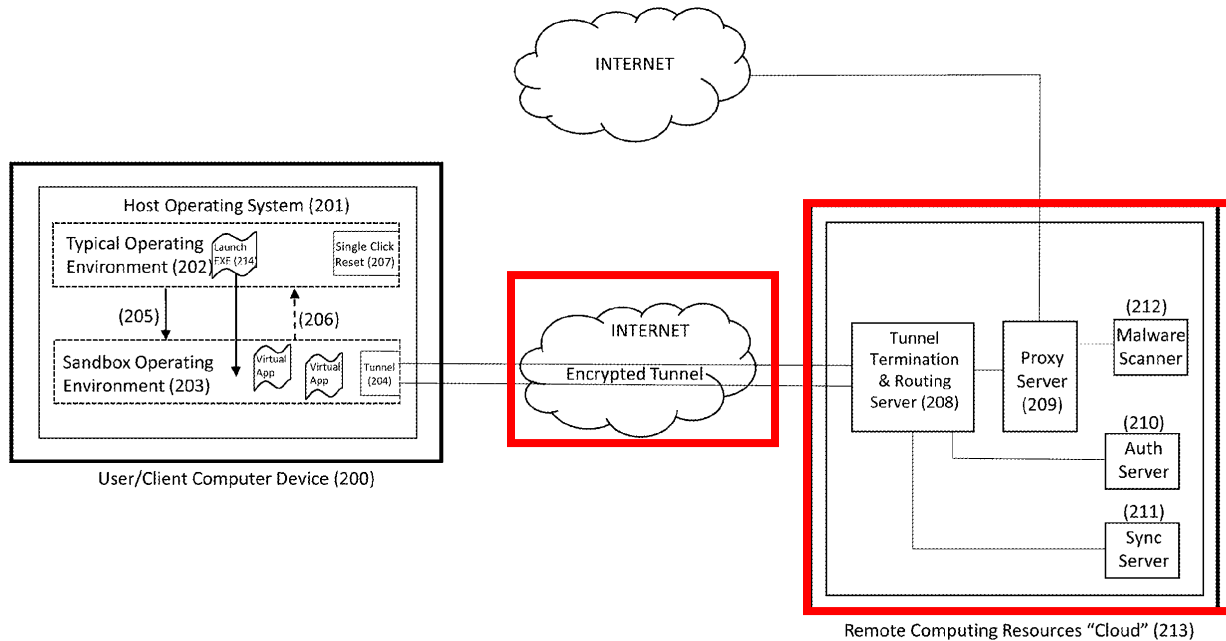


FIG. 2

Benoit further teaches a **LAN**. Benoit discloses that “data may be provided to the system, stored by the system and provided by the system to users of the system across **local area networks (LANs)** (e.g., office networks, home

networks)...” Ex-1005 ¶0025; *see also id.* ¶¶0001, 0007, 0014, 0025; Ex-1003 ¶288.

4. Claim 3

Benoit teaches claim 3, which as discussed for Ground 1 recites that the Internet-based cloud service comprises IaaS, SaaS, and/or PaaS. In particular, Benoit teaches that the connection between the sandbox OE and the RCR/cloud supports “protocols comprising web, mail, video conferencing, and instant messaging.” Ex-1005 ¶0010; *see also id.* ¶¶0036, 0049; Ex-1003 ¶292. A POSITA would have understood that email, video conferencing, and instant messaging are examples of **SaaS**. Ex-1003 ¶293.

Benoit additionally teaches “multi-layered malware protection, multi-protocol encrypted tunnel handling, and proxy capabilities...” Ex-1005 ¶¶0027, 0041; *see also id.* ¶¶0033, 0048. Benoit further teaches restoring synchronized custom settings from the cloud if the sandbox OE becomes infected. Ex-1005 ¶¶0032, 0041. A POSITA would have understood that malware protection, encrypted tunnel handling, proxy, and synchronization services are examples of **SaaS**. Ex-1003 ¶294.

A POSITA would further have understood that the tunnel termination and routing server, proxy server, authentication server, synchronization server, and malware scanner in the cloud are examples of **IaaS**. Ex-1003 ¶295.

5. Claim 8

[8pre] The host computer system of claim 1,

See claim 1.

[8a] wherein the internal isolation firewall is configured to segregate the first memory space from the second memory space, and

As discussed for element 1d, Benoit's sandbox OE would necessarily have had its own **memory space**. Ex-1003 ¶299.

As discussed for element 1f, a POSITA would have understood Benoit's pre-defined read and write permissions to be a form of **internal isolation firewall configured to segregate the memory spaces**. Ex-1003 ¶300. Benoit also teaches that "the sandbox is designed to 'deny all' software code from accessing host resources outside of the sandbox," which would have further indicated to a POSITA that the internal isolation firewall segregates the sandbox's resources, including its memory space, from the host's resources, including its memory space. Ex-1005 ¶0032; Ex-1003 ¶300.

[8b] wherein the processor is configured to enforce policies for communication between the first memory space and the second memory space using the internal isolation firewall.

Benoit's **policies for communication** are the "pre-defined read (40) and write (50) permissions to the host system," which the internal isolation firewall implements. Ex-1005 ¶0043, Fig. 3A. A POSITA would have understood that

these policies govern **communication between the memory space for the typical OE and the memory space for the sandbox OE**. Ex-1003 ¶302.

6. Claim 10

Benoit anticipates claim 10, which largely repeats claim 1. Ex-1003 ¶304. Petitioner incorporates by reference the relevant analysis above for the limitations repeated from claim 1, it being understood that the analysis would be the same. In particular:

- Benoit teaches 10b, *see* 1c.
- Benoit teaches 10c, *see* 1d.
- Benoit teaches 10d, *see* 1f.
- Benoit teaches 10e, *see* 1g.
- Benoit teaches 10f, *see* 1h.
- Benoit teaches 10g, *see* 1h.

[10pre] A cloud computing system comprising:

Benoit discloses a **cloud computing system** in the form of the system illustrated in Figure 2. Ex-1005, Fig. 2; *see also id.* ¶0041 (describing the system of Figure 2 as having a “cloud component” 213). As discussed for element 1e, the computer device in the system can access an Internet-based cloud service in the

form of the RCR or “cloud,” making the system a cloud computing system.

Ex-1003 ¶305.

[10a] a cloud computing network comprising a server,

Benoit’s system comprises a **server** in the form of the user/client computer device 200, shown in Figure 2. Ex-1005, Fig. 2; *see also id.* ¶0041.

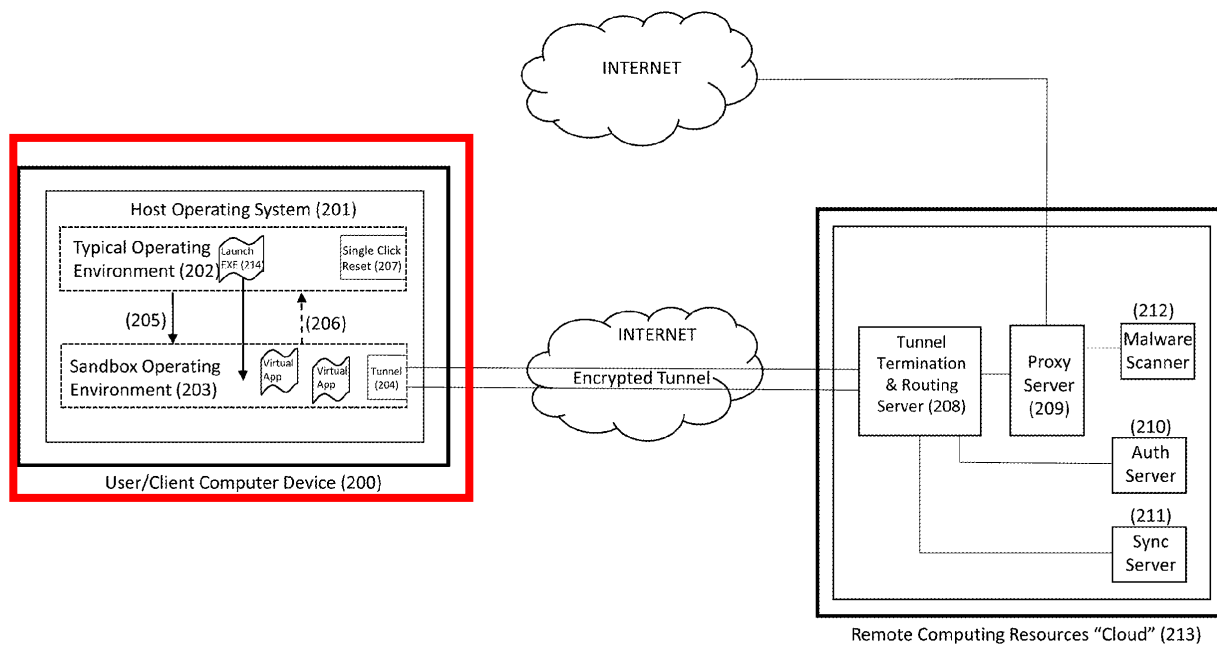


FIG. 2

A POSITA would have recognized the computer 200 as a type of server, since the computer can provide information to other devices on the Internet. Ex-1003 ¶309. Indeed, Benoit states that “[e]xamples of computing devices usable with embodiments of the present invention include ... **servers.**” Ex-1005 ¶0024; *see also id.* ¶0025.

[10h] to block communication between the first set of one or more applications or processes running in the workspace and the Internet resource.

Benoit discloses that the proxy server 209 can block **communication from applications or processes** running in any of the workspaces on the computer device and the Internet resources. Benoit explains that “[i]f the traffic returning from the Internet is not free of malicious code or content, then the traffic is **not returned** to the virtual application running on the system

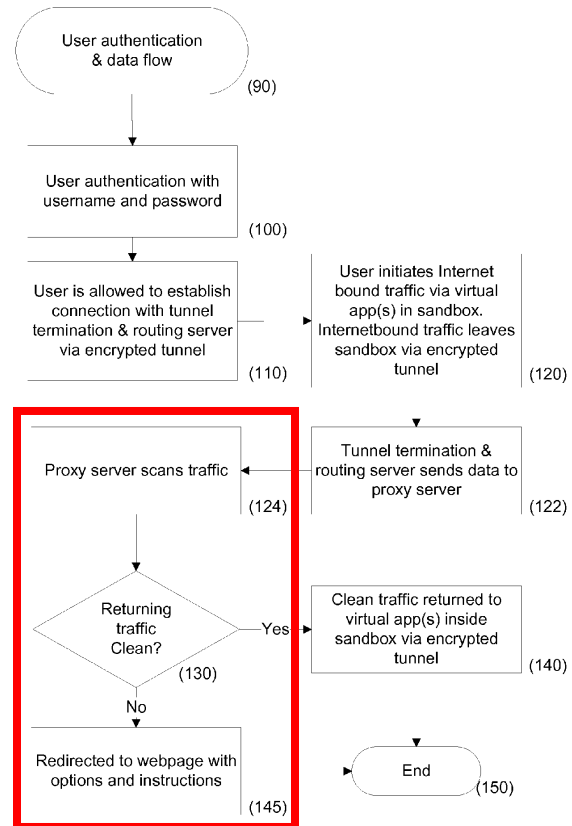


FIG. 3B

components of the user’s host computer....” Ex-1005 ¶0048; Ex-1003 ¶322. Additionally, Figure 3B teaches in step 124 that it is the proxy server which scans and blocks the Internet communications. Ex-1005, Fig. 3B; Ex-1003 ¶323.

7. Claim 11

[11pre] The cloud computing system of claim 10,

See claim 10.

[11a] wherein the server is configured to perform at least one processing task on behalf of a client device.

As discussed for elements 1e and 3a, Benoit teaches an Internet-based cloud service, including mail, video conferencing, and instant messaging. Ex-1005 ¶¶0010, 0036, 0049. These are examples of a **server configured to perform at least one processing task on behalf of a client device**. The '104 patent describes the server performing a task for the client in the same manner. Ex-1001, 2:57-62. In each of Benoit's examples, the server receives input data from the client device, e.g., emails, videos, and instant messages. *See also* Ex-1005 ¶0025; Ex-1003 ¶326.

8. Claim 17

For the reasons discussed above for claim 3, Benoit teaches claim 17, which recites that the Internet-based cloud service comprises IaaS, SaaS, and/or PaaS.

9. Claims 18-19

Claims 18 and 19 are the method counterparts of claims 1 and 3, with the same elements phrased as method steps. Claims 18 and 19 contain no additional limitations beyond the fact that they recite a method instead of a system. For the reasons stated above for claims 1 and 3, Benoit teaches the methods of claims 18 and 19.

A POSITA therefore would have found the Challenged Claims to be anticipated by Benoit.

D. Ground 4

1. Combination of Benoit and Hunt

a. Summary of Hunt

Hunt was published on January 19, 2012, more than five years before the stated priority date of the '104 patent. Ex-1008. Hunt therefore is prior art under 35 U.S.C. §102(a)(1).

Hunt teaches a secure application execution system as shown in Figure 1. Ex-1003 ¶346.

100

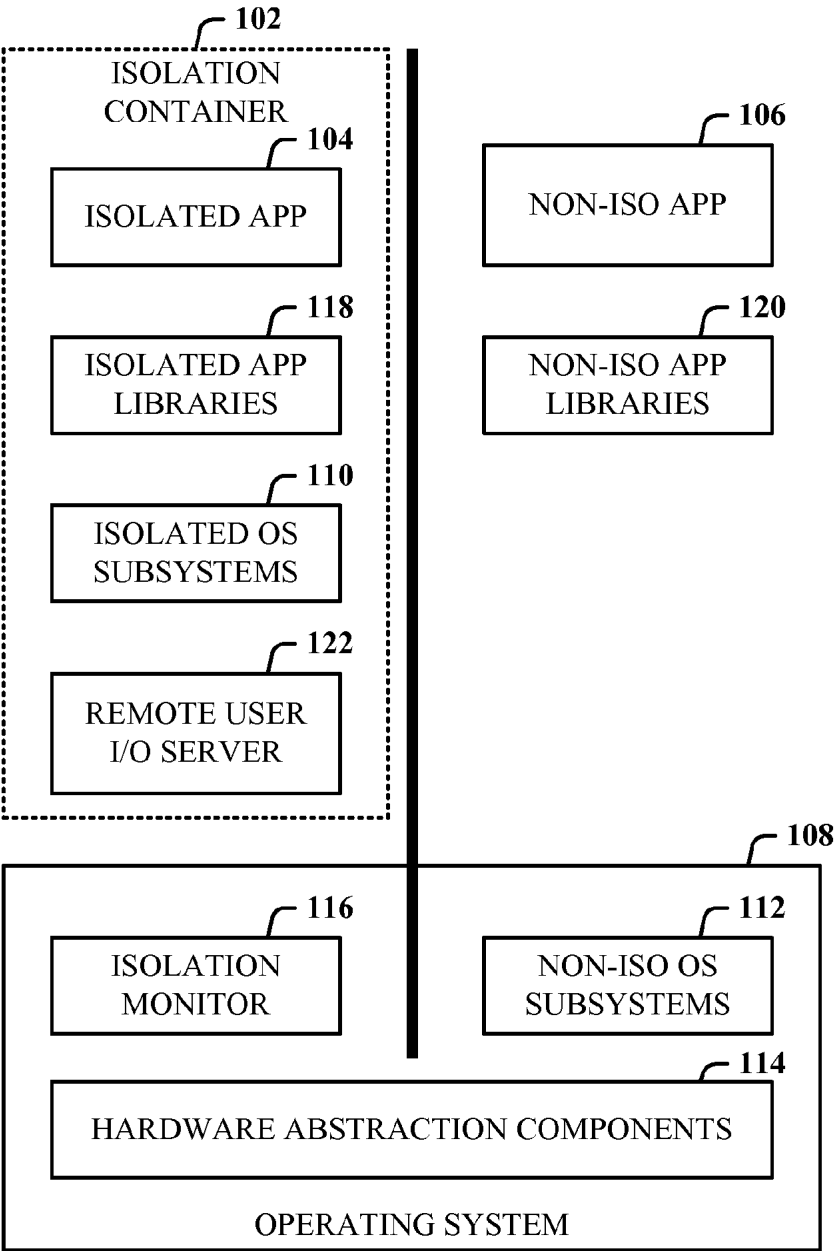


FIG. 1

The system includes an isolation container 102 (a sandbox), in which an application 104 runs in isolation from a non-isolated application 106. Ex-1008 ¶¶0024. The isolated and non-isolated applications both run in association with one operating system (OS) 108. *Id.*; Ex-1003 ¶347. The OS includes an internal isolation firewall in the form of an isolation monitor 116 that provides the interface for services from the OS to the isolation container. Ex-1008 ¶0025; Ex-1003 ¶348.

The isolated and non-isolated applications both use basic computation services provided by the single OS. Ex-1008 ¶0030. The OS also includes hardware abstractions for both the isolated and non-isolated applications. Ex-1008 ¶¶0025, 0029. The code within the isolation container interfaces to the OS kernel through the isolation monitor. Ex-1008 ¶0031; Ex-1003 ¶349. The isolation monitor also isolates abstractions like virtual memory “for use by the sandbox environment.” Ex-1008 ¶0005.

b. Motivation to Combine

A POSITA would have been motivated to combine Hunt’s sandbox implementation, including the firewall and memory isolation processes, with Benoit’s computer system. Hunt describes the benefits of using a low-overhead sandbox instead of a high-overhead solution like a virtual machine. Ex-1008 ¶¶0001-0003, 0005; Ex-1003 ¶353.

As discussed for Ground 3, Benoit discloses an isolated, sandboxed computing environment that uses a host operating system. Ex-1003 ¶354. Benoit, however, does not expressly use the word “firewall” to describe the isolation of the typical OE from the sandbox OE.

To exclude any doubt, the combination of Benoit and Hunt teaches all elements of the Challenged Claims. Hunt demonstrates that a POSITA would have been highly familiar with implementing an isolated computing environment as a sandbox having its own memory space and isolated using an internal isolation firewall. The combination would involve a POSITA combining prior-art elements according to known methods to yield a predictable result—Benoit’s sandbox OE would have its own memory space and be isolated using an internal isolation firewall. Ex-1003 ¶356.

A POSITA would have been further motivated to combine Hunt’s sandbox implementation with Benoit’s computer system because of Hunt’s stated advantages. Ex-1003 ¶357. Hunt advantageously teaches that the disclosed architecture both reduces computing overhead and safely isolates abstractions like virtual memory and threads. Ex-1008 ¶0005. Hunt explains that “[t]he significant reduction in resources and overhead provided by the disclosed architecture now makes it possible to sandbox every application.” Ex-1008 ¶0021; Ex-1003 ¶357.

2. Claim Analysis

For Ground 4, the element-by-element analysis for all Challenged Claims is the same as the element-by-element analysis for Ground 3, except that Hunt provides additional disclosure for:

- “a first memory space” and “a second memory space”;
- “isolat[ing] the isolated computing environment from the workspace using an internal isolation firewall;” and
- Dependent claim 8.

a. “first memory space” and “second memory space”

Benoit combined with Hunt teaches that Benoit’s typical OE operates applications or processes via a **first memory space**, while Benoit’s sandbox OE uses a **second memory space**. Hunt teaches that its isolation monitor isolates abstractions like virtual memory “for use by the sandbox environment.” Ex-1008 ¶0005. These abstractions create a memory space specific to the isolation container (a sandbox). Ex-1008 ¶¶0031, 0037, 0066; Ex-1003 ¶362.

Hunt also describes an interface for creating the sandboxed isolation container that involves allocating virtual memory from a free memory space to a protected memory space. Ex-1008 ¶0092. This memory allocation is performed using the DkVirtualMemoryAllocate and DkVirtualMemoryFree functions. *Id.* A

POSITA would have understood that the free memory space would have been for Hunt's non-isolated applications operating outside the isolation container (a **first memory space**). Ex-1003 ¶363. A POSITA would have also understood that the protected memory space would have been for Hunt's isolated applications operating inside the isolation container (a **second memory space**). *Id.* When combined with Benoit's computer system, Hunt's memory allocation process further confirms that Benoit's typical OE and sandbox OE each have its own memory space.

b. “isolate the isolated computing environment from the workspace using an internal isolation firewall”

Benoit combined with Hunt teaches this limitation in elements 1f, 10d, and 18f. Hunt demonstrates that a POSITA would have been highly familiar with isolating sandboxes (like Hunt's isolation container) from a workspace (Hunt's non-isolated applications) using an **internal isolation firewall** in the form of an isolation monitor. Ex-1003 ¶¶367-368. Hunt's Figure 1 is reproduced below with the isolation monitor 116 highlighted.

Hunt's isolation monitor

“employs a collection of rules that map the approval or denial of requests to access resources to an application manifest.” Ex-1008 ¶0029. Hunt's isolation monitor is an internal isolation firewall, which Hunt calls an “application firewall.” Ex-1008 ¶0053; Ex-1003 ¶369.

As discussed above, a POSITA would have been motivated to combine

Hunt's sandbox implementation, including the isolation monitor, with Benoit. To accomplish this, a POSITA would have implemented Hunt's isolation monitor between Benoit's typical OE and sandbox OE. Ex-1003 ¶371. Hunt's isolation monitor would provide the interface for services from Benoit's host OS to Benoit's sandbox OE, akin to the function that the isolation monitor performs in Hunt. Ex-1008 ¶0025. The isolation monitor would also employ a collection of rules that govern the approval or denial of requests by Benoit's sandbox OE to access resources, again akin to the function that the isolation monitor performs in Hunt. Ex-1008 ¶0029. The result would be a separation of the state of the isolated

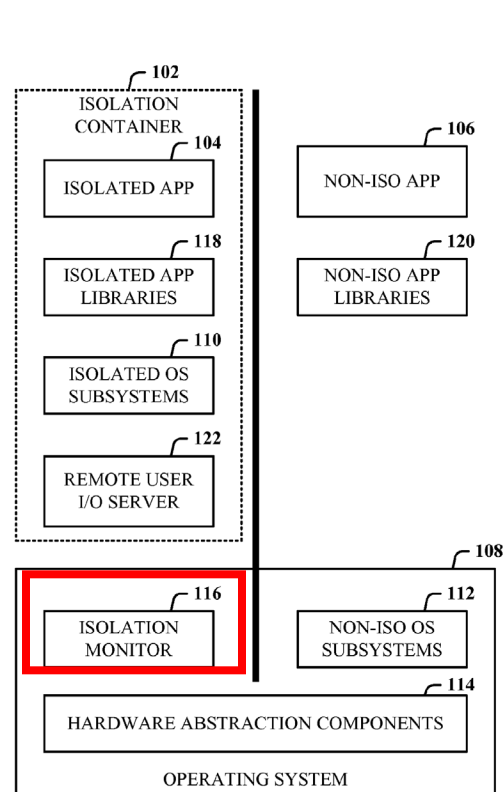


FIG. 1

applications in Benoit's sandbox OE from the state of the non-isolated applications in Benoit's typical OE. Ex-1008 ¶0025; Ex-1003 ¶371.

Below is Figure 2 of Benoit, modified to show Hunt's isolation monitor positioned to provide the interface for communications between Benoit's host OS and typical OE, on the one hand, and Benoit's sandbox OE, on the other. So adapted, Hunt's isolation monitor approves and denies requests by Benoit's sandbox OE to access resources on the computer. Ex-1003 ¶372.

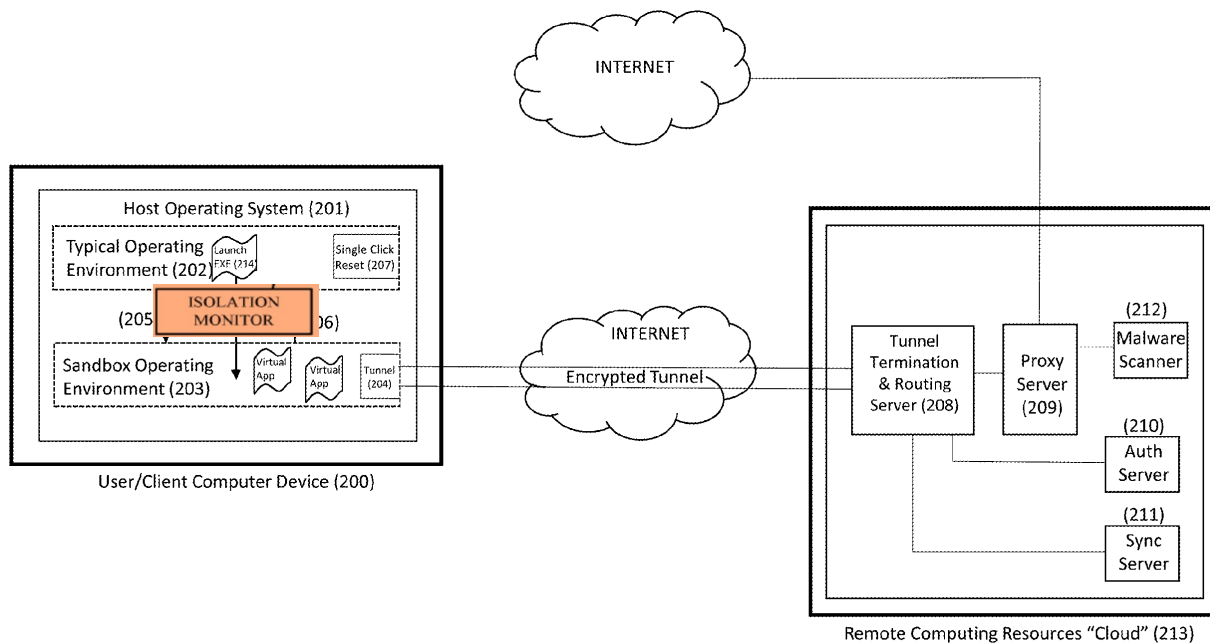


FIG. 2

Benoit combined with Hunt teaches isolating an isolated computing environment (Benoit's sandbox OE) from a workspace (Benoit's typical OE) using an internal isolation firewall (Hunt's isolation monitor). Ex-1003 ¶374.

c. Claim 8

[8a] wherein the internal isolation firewall is configured to segregate the first memory space from the second memory space, and

Benoit combined with Hunt teaches element 8a. Ex-1003 ¶376. As discussed above, Hunt teaches that the isolation monitor isolates abstractions like virtual memory for use by the sandboxed isolation container. Ex-1008 ¶0005. These abstractions create a memory space specific to the isolation container. Ex-1008 ¶¶0031, 0066; Ex-1003 ¶379.

A POSITA thus would have understood that the isolation monitor (an internal isolation firewall) segregates the isolation container’s memory space. Ex-1003 ¶380. In Benoit, a POSITA would have used Hunt’s isolation monitor to **segregate the memory space** for Benoit’s sandbox OE (a second memory space) from the memory space for Benoit’s typical OE (a first memory space). *Id.*

[8b] wherein the processor is configured to enforce policies for communication between the first memory space and the second memory space using the internal isolation firewall.

Benoit combined with Hunt teaches element 8b. Ex-1003 ¶382. Hunt’s **policies for communication** are the “collection of rules that map the approval or denial of requests to access resources to an application manifest.” Ex-1008 ¶0029; *see also id.* ¶¶0053, 0055, 0094. A POSITA would have understood that such resources include **memory spaces**. Ex-1003 ¶383. In Benoit, a POSITA would

have used Hunt's isolation monitor (an internal isolation firewall) to enforce policies for Benoit's sandbox OE. Ex-1003 ¶384.

A POSITA therefore would have found the Challenged Claims obvious based on Benoit in view of Hunt.

E. Ground 5

1. Combination of Benoit and Hunt

As discussed for Ground 4, a POSITA would have been motivated to combine Hunt's sandbox implementation, including the firewall and memory allocation processes, with Benoit. Ex-1003 ¶391.

2. Combination of Benoit-Hunt with Pratt

A POSITA would have been further motivated to combine Pratt's authentication process with Ground 4's Benoit-Hunt system. As explained for Ground 3, Benoit already teaches an authentication process. Ex-1003 ¶392. To exclude any doubt, however, Benoit, Hunt, and Pratt combined teach all elements of the Challenged Claims, including the authentication process. Ex-1003 ¶393.

A POSITA would have been motivated to combine Benoit and Hunt with Pratt. Ex-1003 ¶394. The combination would involve a POSITA combining prior-art elements according to known methods to yield a predictable result—a proxy or other network device determines that Benoit's sandbox OE is authentic using Pratt's authentication process. Ex-1003 ¶395.

A POSITA would have been further motivated to combine Pratt's authentication process with the Benoit-Hunt system because of the stated advantages of Pratt's process, discussed in connection with Ground 1. Ex-1006, 5:54-62; Ex-1003 ¶¶396-397.

3. Claim Analysis

For Ground 5, the element-by-element analysis for all Challenged Claims is the same as the element-by-element analysis for Grounds 3 and 4, except that Pratt provides additional disclosure for the limitation "authentica[ing] the isolated computing environment with an authentication device."

Like Benoit's sandbox OE, Pratt's operating environment 120 is an isolated sandbox environment that uses a host operating system. Ex-1006, 2:29-36. To combine Pratt's authentication process with the Benoit-Hunt system, a POSITA would have configured Benoit's sandbox OE to authenticate itself in a manner similar to Pratt's operating environment 120. Ex-1003 ¶402. The Benoit-Hunt system would include Pratt's interceptor module and authentication services in an arrangement similar to what is shown in Pratt's Figure 1. *Id.*

Below is Benoit's Figure 2, modified to show Pratt's interceptor module positioned to intercept authentication messages from Benoit's cloud 213 or from the second cloud labeled "Internet." Benoit's sandbox OE includes Pratt's authentication service 122, while Benoit's typical OE includes Pratt's

authentication service 132. As discussed for Ground 4, Hunt's isolation monitor is positioned to provide the interface for communications between Benoit's host OS and typical OE, on the one hand, and Benoit's sandbox OE, on the other. Ex-1003 ¶403.

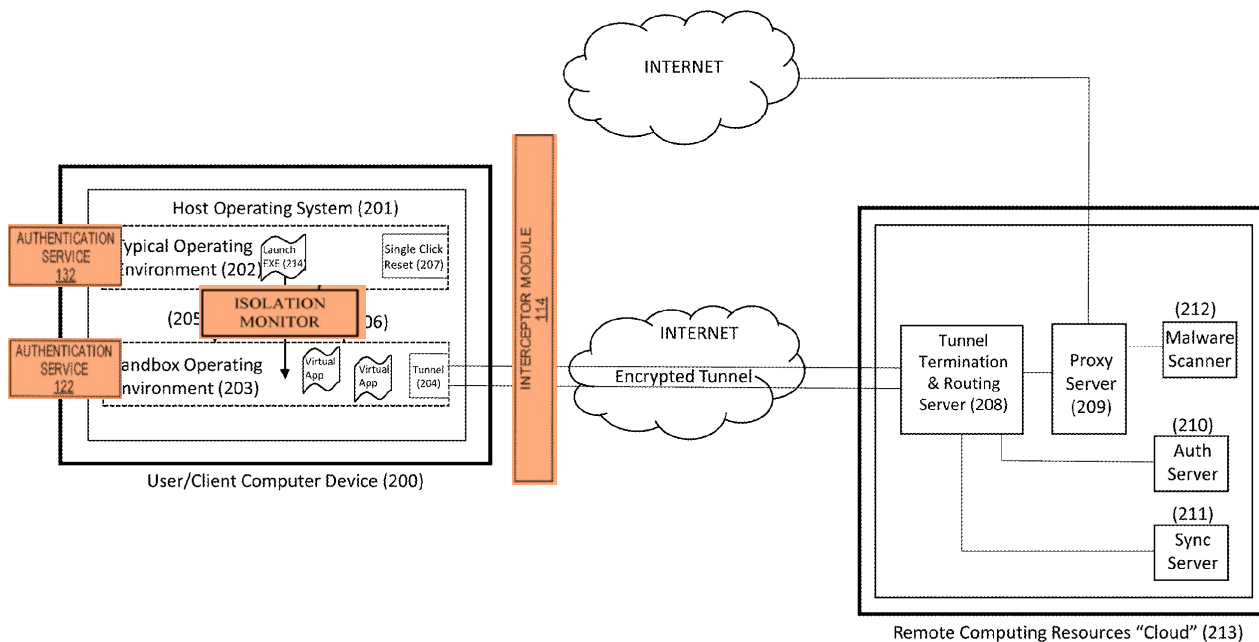


FIG. 2

As in Pratt, the interceptor module of the combined system intercepts the authentication messages and notifies the authentication service 132 in the typical OE, which then provides authentication data to the sandbox OE so that it can authenticate itself. Ex-1003 ¶404.

A POSITA therefore would have found the Challenged Claims obvious based on Benoit combined with Hunt and Pratt.

IX. DISCRETIONARY DENIAL WOULD BE INAPPROPRIATE

A. No Discretionary Denial Under *Fintiv*

The *Fintiv* factors strongly favor institution. In particular, Petitioner is offering a *Sotera* stipulation (see factor 4, below).

1. No Evidence Regarding a Stay

No motion to stay has been filed, and the Board should not infer the outcome of such a motion. *See Sand Revolution II LLC v. Continental Intermodal Group – Trucking LLC*, IPR2019-01393, Paper 24 at 7 (PTAB June 16, 2020) (informative). Thus, this factor is neutral.

2. Parallel-Proceeding Trial Date

The Related Litigation was filed in the Eastern District of Texas on December 29, 2023, and is currently set for trial before Judge Rodney Gilstrap on September 22, 2025. Ex-1011. However, “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). Here, Judge Gilstrap has ten other patent trials—plus two other trials—scheduled to begin on September 22, 2025. Ex-1012.

Although the scheduled trial date is about ten months before a final written decision is expected here (July 2026), Judge Gilstrap’s trial dates have slipped recently, as reflected in Case No. 2-22-cv-00077 (Ex-1013—jury selection delayed

from October 30, 2023, docket no. 31, to March 4, 2024, docket no. 67) and Case No. 2-22-cv-00293 (Ex-1014—jury selection delayed from April 15, 2024, docket no. 55, to November 12, 2024, docket no. 791). Further, Judge Gilstrap has 682 active cases and a median time-to-trial of 23 months—pushing the realistic trial date here to at least November or December, 2025. Ex-1015. While this is 7-8 months before a final written decision is expected, the Board has granted institution in similar circumstances. *See, e.g., NetNut Ltd. v. Bright Data Ltd.*, IPR2021-01492, Paper 12 (PTAB March 21, 2022) (granting institution when trial was scheduled six months before the final written decision deadline).

3. Investment in the Parallel Proceeding

The Related Litigation is in its early stages, with major activities including *Markman* briefing not having started as of the filing of this Petition. Ex-1011. The court has not issued any substantive orders, Ex-1011, and the parties have not yet invested substantial time in the litigation. Thus, this factor favors institution.

4. Overlapping Issues with the Parallel Proceeding

There is no present overlap of prior-art issues with the Related Litigation. Moreover, Petitioner offers the following stipulation: If the Board institutes this Petition, Petitioner will not pursue the grounds raised or reasonably could have been raised in this Petition in the Related Litigation with respect to the claims for which trial is instituted. *See Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019,

Paper 12 (PTAB Dec. 1, 2020) (precedential for §II.A). Consequently, this factor favors institution.

5. Identity of Parties

Petitioner is a defendant in the Related Litigation. That is true of most IPR petitioners. Accordingly, this factor should not be grounds for denying institution.

6. Other Circumstances

This Petition presents a compelling case. The Examiner allowed the '104 patent only after Applicant argued that Hoy does not teach authentication.

Ex-1002, 2097-2098 (Mar. 8, 2021 Reply, 7-8). As explained above, however, Pratt teaches a system “to securely **authenticate** operating environment 120.” Ex-1006, 2:15-22. Ex-1003 ¶¶22-26. The Examiner allowed the claims without evaluating Pratt.

The Board’s policy is to “not deny institution of an IPR or PGR under *Fintiv* (i) when a petition presents compelling evidence of unpatentability.” June 21, 2022 USPTO Memorandum, 9. The evidence of unpatentability is compelling here, and the Board should not deny institution under *Fintiv*.

B. No Discretionary Denial Under 35 U.S.C. §325(d)

The challenges presented are neither cumulative nor redundant to the prosecution of the '104 patent. Only Hoy was cited by the Examiner,³ and not in

³ Hunt is listed on the '104 patent but was not cited by the Examiner.

combination with Pratt or another reference teaching authentication of isolated computer environments. Moreover, the challenges are non-cumulative because the references presented describe the limitations that Applicant distinguished to gain allowance.

X. CONCLUSION

The Challenged Claims are anticipated or rendered obvious for the reasons discussed above. Petitioner accordingly requests IPR.

Respectfully submitted,
SHEPPARD, MULLIN, RICHTER & HAMPTON LLP

By /John R. Keville/

John R. Keville (Registration No. 42,723)

Darren M. Franklin (Registration No. 51,701)

James Young Hurt (Registration No. 79,121)

Attorneys for Petitioner

INTERNATIONAL BUSINESS MACHINES CORPORATION

CLAIM APPENDIX

[1pre] A host computer system:

[1a] a memory; and

[1b] a processor configured to:

[1c] implement a workspace, wherein the workspace is configured to enable operation of a first set of one or more applications or processes via a first memory space;

[1d] implement an isolated computing environment, the isolated computing environment using a host operating system and comprising a sandboxed computing environment that uses a second memory space to enable operation of a second set of one or more applications or processes,

[1e] wherein the isolated computing environment is configured to access an Internet-based cloud service via at least one application of the second set of one or more applications or processes;

[1f] isolate the isolated computing environment from the workspace using an internal isolation firewall;

[1g] authenticate the isolated computing environment with an authentication device; and

[1h] communicate with a proxy server to access the Internet-based cloud service to allow communication between the at least one application and the Internet-based cloud service when the isolated computing environment has been authenticated.

[2pre] The host computer system of claim 1,

[2a] wherein the processor is configured to access the Internet-based cloud service via one or more of a local area network (LAN), a wide area network (WAN), a cellular network, a Wi-Fi network, a digital subscribers line (DSL) network, a cloud computing network, a data center, or a satellite network.

[3pre] The host computer system of claim 1,

[3a] wherein the Internet-based cloud service comprises one or more of an Infrastructure as a Service (IaaS), a Software as a Service (SaaS), or a Platform as a Service (PaaS).

[8pre] The host computer system of claim 1,

[8a] wherein the internal isolation firewall is configured to segregate the first memory space from the second memory space, and

[8b] wherein the processor is configured to enforce policies for communication between the first memory space and the second memory space using the internal isolation firewall.

[10pre] A cloud computing system comprising:

[10a] a cloud computing network comprising a server,

[10b] wherein the server is configured to:

implement a workspace configured to enable operation of a first set of one or more applications or processes;

[10c] implement an isolated computing environment using a host operating system and comprising a sandboxed computing environment and being configured to enable operation of a second set of one or more applications or processes;

[10d] isolate the isolated computing environment from the workspace using an internal isolation firewall; and

[10e] authenticate the isolated computing environment with an authentication device; and

[10f] a proxy configured to control communication between the server and an Internet resource,

[10g] wherein the proxy is configured to allow communication between the second set of one or more applications or processes running in the isolated computing environment and the Internet resource when the isolated computing environment has been authenticated and

[10h] to block communication between the first set of one or more applications or processes running in the workspace and the Internet resource.

[11pre] The cloud computing system of claim 10,

[11a] wherein the server is configured to perform at least one processing task on behalf of a client device.

[17pre] The cloud computing system of claim 11,

[17a] wherein the at least one processing task performed on behalf of the client device comprises a processing task for an Infrastructure as a Service (IaaS), a Software as a Service (SaaS), or a Platform as a Service (PaaS).

[18pre] A method implemented in a host computer system, the method comprising:

[18a] implementing a workspace,

[18b] wherein the workspace is configured to enable operation of a first set of one or more applications or processes via a first memory space;

[18c] implementing an isolated computing environment,

[18d] the isolated computing environment using a host operating system and comprising a sandboxed computing environment using a second memory space to enable operation of a second set of one or more applications or processes,

[18e] wherein the isolated computing environment is configured to access an Internet-based cloud service via at least one application of the second set of one or more applications or processes;

[18f] isolating the isolated computing environment from the workspace using an internal isolation firewall;

[18g] authenticate the isolated computing environment with an authentication device; and

[18h] communicating with a proxy server to access the Internet-based cloud service to allow communication between the at least one application and the Internet-based cloud service when the isolated computing environment has been authenticated.

[19pre] The method of claim 18,

[19a] wherein the Internet-based cloud service comprises one or more of an Infrastructure as a Service (IaaS), a Software as a Service (SaaS), or a Platform as a Service (PaaS).

**CERTIFICATE OF COMPLIANCE WITH
TYPE-VOLUME LIMITATION, TYPEFACE REQUIREMENTS,
AND TYPE-STYLE REQUIREMENTS**

1. Pursuant to 37 C.F.R. §42.24(d), I certify that the foregoing Petition complies with the type-volume limitation of 37 C.F.R. §42.24 and contains 13,992 words based on the word count indicated by the word-processing system used to prepare the paper, excluding the parts exempted by 37 C.F.R. §42.24(a).
2. The foregoing Petition complies with the general format requirements of 37 C.F.R. §42.6(a) and has been prepared using Microsoft Word in 14-point Times New Roman.

/John R. Keville/

John R. Keville (Registration No. 42,723)

Counsel for Petitioner

INTERNATIONAL BUSINESS MACHINES CORPORATION

Date: January 2, 2025

Sheppard, Mullin, Richter & Hampton LLP

700 Louisiana Street, 27th Floor

Houston, TX 77002

Telephone: 713.431.7100

Facsimile: 713.431.7101

Email: jkeville@sheppardmullin.com

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§42.6 and 42.105, I hereby certify that on January 2, 2025, true and correct copies of the foregoing Petition for *Inter Partes* Review of U.S. Patent No. 11,178,104 and Exhibits 1001-1015 were served in their entirety on the Patent Owner at the following correspondence address of record as listed on Patent Center, by FedEx:

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

I further certify that on January 2, 2025, true and correct copies of the foregoing Petition for *Inter Partes* Review of U.S. Patent No. 11,178,104 and Exhibits 1001-1015 were also sent in their entirety by FedEx to the attorneys of record for Patent Owner in the Related Litigation, *Croga Innovations Ltd. v. International Business Machines Corporation*, No. 2:23-cv-00634-JRG (U.S. District Court, Eastern District of Texas):

Brett E. Cooper
Seth Raymond Hasenour
Drew Bennett Hollander
Jonathan Randy Yim
BC Law Group, P.C.
200 Madison Ave., 24th Fl.
New York, NY 10016

/John R. Keville/

John R. Keville (Registration No. 42,723)
Counsel for Petitioner
INTERNATIONAL BUSINESS MACHINES
CORPORATION

Date: January 2, 2025

Sheppard, Mullin, Richter & Hampton LLP
700 Louisiana Street, 27th Floor
Houston, TX 77002