

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,

Petitioner,

v.

CROGA INNOVATIONS LTD.,

Patent Owner.

Case IPR2024-01283

Patent 11,223,601

PATENT OWNER'S RESPONSE TO THE PETITION

Mail Stop "PATENT BOARD"
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

	Page
I. Introduction	1
II. Challenged Claims.....	1
III. Background.....	3
IV. Jeffries	4
V. Ground 1: Petitioner has not shown that Jeffries renders obvious “ <i>a processor configured to . . . isolate the isolated computing environment from the workspace using an internal isolation firewall</i> ”	6
A. Jeffries does not use an “ <i>internal isolation firewall</i> ”	7
B. Jeffries’ Container Manager and Secure Kernel do not “ <i>isolate the isolated computing environment</i> ”	11
VI. Grounds 2 and 3.....	15
VII. Conclusion	15

TABLE OF AUTHORITIES

Regulations

37 C.F.R. § 42.104.....	7
-------------------------	---

PATENT OWNER'S EXHIBIT LIST

Exhibit No.	Description
2001	Docket Sheet, <i>Croga Innovations Limited v. Cisco Systems, Inc.</i> , No. 2:24-cv-00065-JRG (Lead Case) (E.D. Tex. Nov. 20, 2024)
2002	Order, <i>MyPort, Inc. v. Samsung Electronics Co., Ltd., et al.</i> , No. 2:22-cv-00114-JRG (E.D. Tex. June 12, 2023)
2003	Defendants' Invalidation Contentions, <i>Croga Innovations Limited v. Cisco Systems, Inc.</i> , No. 2:24-cv-00065-JRG (Lead Case) (E.D. Tex. August 6, 2024)
2004	<i>Curriculum Vitae</i> of Dr. Eric Cole
2005	Declaration of Dr. Eric Cole
2006	U.S. Patent Application Publication 2014/0344912 to Chapman et al.
2007	U.S. Patent Application Publication 2009/0249472 to Litvin et al.
2008	U.S. Patent No. 7,150,040

I. Introduction

Patent Owner Croga Innovations Ltd. (“Patent Owner”) submits this response to Petitioner Cisco Systems Inc.’s (“Ppetitioner”) Petition for *inter partes* review of U.S. Patent No. 11,223,601 (“the ’601 patent”). Petitioner has failed to demonstrate unpatentability of any challenged claim and has not shown that the prior art it relies upon discloses or renders obvious “a processor configured to . . . isolate the isolated computing environment from the workspace using an internal isolation firewall.”

II. Challenged Claims

Petitioner challenges the patentability of claims 1-4, 7, 9-12, and 15 in ground 1. Petitioner challenges claims 5-6 and 13-14 in ground 2. Petitioner challenges claims 8 and 16 in ground 3. Claims 2-8 depend from claim 1, and claims 10-16 depend from claim 9.

[1.0]	A system comprising:
[1.1]	a memory; and
[1.2]	a processor configured to:
[1.3]	implement a workspace that uses a host operating system, wherein the workspace enables operation of a first set of one or more applications or processes via a first memory space;
[1.4.1]	implement an isolated computing environment that uses the host operating system, wherein the isolated computing environment enables operation of a second set of one or more applications or processes via a second memory space, and

[1.4.2]	wherein the second set of one or more applications or processes comprises a multi-user interactive software application;
[1.5]	isolate the isolated computing environment from the workspace using an internal isolation firewall;
[1.6]	authenticate the isolated computing environment with an authentication device; and
[1.7]	send data to an untrusted destination from the multi-user interactive software application via a proxy device when the isolated computing environment has been authenticated.

[9.0]	A method comprising:
[9.1]	implementing a workspace that uses a host operating system, wherein the workspace enables operation of a first set of one or more applications or processes via a first memory space;
[9.2.1]	implementing an isolated computing environment that uses the host operating system, wherein the isolated computing environment enables operation of a second set of one or more applications or processes via a second memory space,
[9.2.2]	wherein the second set of one or more applications or processes comprises a multi-user interactive software application;
[9.3]	isolating the isolated computing environment from the workspace using an internal isolation firewall;
[9.4]	authenticating the isolated computing environment with an authentication device; and
[9.5]	sending data to an untrusted destination from the multi-user interactive software application via a proxy device when the isolated computing environment has been authenticated.

III. Background

The '601 patent relates to a host computer system configured for isolation of a multi-user interactive software. EX1001, 1:58-60. The host computer system may include a workspace (e.g., a trusted memory space) and an isolated computing environment associated with a second memory space that can be isolated from the workspace using, for example, a sandbox container process and/or a virtual machine. EX1001 5:33-43. The '601 patent describes firewalls used for “communication isolation.” For example, it discloses a “*host-based firewall*” that allows communication with “predetermined trusted devices and/or predetermined network ports” while preventing unauthorized communication between applications operating in the workspace and other devices on the network. *Id.*, 6:51-62. The “*host-based firewall*” appears in claim 5, which recites “*host-based firewall [that] isolates the system from communicating with one or more other devices on the network.*” The '601 patent also describes an “*internal isolation firewall*” that can facilitate communication isolation by allowing certain actions—e.g, file transfers, cutting/pasting data, or printing—that require communication between the isolated computing environment (hereinafter “ICE”) and the host system while preventing access to additional resources of the host. *Id.*, 6:63-7:35. The “*internal isolation firewall*” appears in claim 1, which recites “*a processor configured to . . . isolate the isolated computing environment from the workspace using an internal isolation*

firewall” and claim 9, which recites “isolating the isolated computing environment from the workspace using an internal isolation firewall.”

IV. Jeffries

Petitioner relies on Exhibit 1005 (“Jeffries”) in each asserted ground. Jeffries appears to be U.S. Patent No. 10,885,189, titled “Isolated Container Event Monitoring.” EX1005, code (54). Jeffries describes a host operating system running on a computing device that monitors resource access by an application running in a container that is isolated from the host operating system. Jeffries discloses that “[i]n response to detecting resource access by that application, a security event is generated describing malicious activity describing malicious activity that occurs from accessing the resource.” It says that the “security event is analyzed to determine a threat level of the malicious activity” and that “when the threat level satisfies the threat level threshold, the operating system takes corrective action to prevent the malicious activity from spreading beyond the isolated container.” EX1005 at 1 (Abstract).

Figure 4 of Jeffries is a flowchart illustrating a process for implementing a container based on event monitoring.

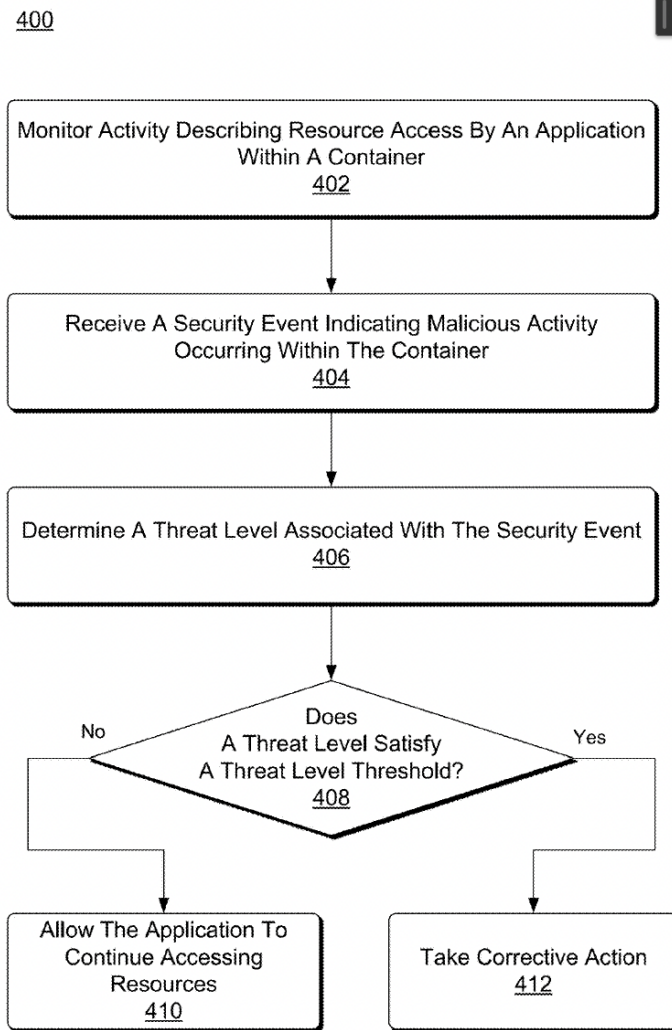


Fig. 4

EX1005, Fig. 4. As illustrated here, Jeffries monitors activity within the container to determine whether malicious activity meeting a threat level has occurred. If a threat level satisfies a threat level threshold, Jeffries takes “corrective action.” For example, “if a user starts visiting numerous websites that the user has not previously visited, . . . [or] if an application begins downloading and installing software that the application has not previously downloaded and installed, this activity is logged in or

more security events and compared against a threat level threshold to determine whether corrective action is needed.” EX1005, 5:25-33. When “corrective action is needed,” Jeffries discloses “the host operating system may quarantine the container to prevent the container from accessing any resources or data outside the container” and “may add the identified resource to a list of untrusted resources so that other computing devices are aware of possible negative effects.” EX1005, 5:51-58 (emphasis added). Jeffries also discloses that “corrective action” can include “terminating the container 122 and rebuilding a new container.” EX1005, 16:38-42. Thus, when Jeffries determines that activity satisfies a threat level threshold, access by the container to all outside resources or data can be blocked, the container can be terminated, or the accessed resource can be added to a list of untrusted resources to make other computing devices aware of them.

V. Ground 1: Petitioner has not shown that Jeffries renders obvious “*a processor configured to . . . isolate the isolated computing environment from the workspace using an internal isolation firewall*”

Petitioner relies on Jeffries for “*a processor configured to . . . isolate the isolated computing environment from the workspace using an internal isolation firewall*” (claim 1) and “*isolating the isolated computing environment from the workspace using an internal isolation firewall*” (claim 9). Pet. 63-65, 87. Petitioner’s argument is that Jeffries’ container manager **118** “quarantine[s] the container 122” and “prevents malicious activity occurring in the container from gaining . . . access

to shared resources.” Pet. 64-65 (citing EX1005, 16:24-37, 16:38-46, 14:40-44). Petitioner also contends that Jeffries secure kernel helps to enforce the separation between the host system and the container by “caus[ing] an exception or interrupt to occur” when malicious activity is detected. Pet. 65. These contentions are insufficient, because (1) Petitioner has not shown that container manager 118 or the secure kernel utilize an “*internal isolation firewall*” to perform their functions, and (2) Petitioner has not shown that any of the functions performed serve to “*isolate*” the ICE from the workspace as claimed.

A. Jeffries does not use an “*internal isolation firewall*”

Petitioner does not provide a claim construction for any term in the ’601 patent, including “*firewall*” or “*internal isolation firewall*,” ignoring its obligation under 37 C.F.R. § 42.104(b) to identify how the challenged claim is to be construed. Pet. 15. Instead, Petitioner attempts to demonstrate that Jeffries discloses an “*internal isolation firewall*” by showing that a combination of Jeffries’ container manager 118 and secure kernel “perform the same **functions** of the internal isolation firewall described by ’601 patent.” Pet. 65 (emphasis added). Without any showing as to the meaning of “*internal isolation firewall*,” Petitioner’s argument here is insufficient on its face.

Claim 1 recites both a function of “*isolat[ing] the isolated computing environment*” and “*an internal isolation firewall*” that is “*us[ed]*” to perform that

function. Petitioner appears to argue that the ICE is “*isolate[d]*” when Jeffries’ secure kernel generates an exception or interrupt that triggers container manager **118** to “quarantine” container **122**. But Petitioner ignores that the claimed “*isolat[ion]*” must be done by “*an internal isolation firewall.*” Under any reasonable construction, Jeffries’ container manager **118** and secure kernel are not an “*internal isolation firewall.*” EX2005, ¶¶ 46-50.

First, the ’601 specification describes an internal isolation firewall that selectively allows or disallows actions to be performed, based on predetermined criteria. As the specification describes, “internal isolation firewall may . . . **allow**[] access to the host system to perform one or more of a cut or copy of data, a paste of data, a printing of data to a local printer, a file transfer, and/or the like” and it “may **prevent** one or more **other transfers** of data between the sandboxed computing environment and the workspace.” EX1001, 7:20-35 (emphasis added). For example, access to specific host resources, transfers of certain data between the ICE and the workspace, and/or execution of predetermined processes within the ICE may be allowed, while other actions are disallowed. The ’601 patent also says “[t]he isolated computing environment may be isolated from the workspace by an internal isolation firewall [that] . . . may **prevent** communication between the isolated computing environment and the workspace, . . . [and] **allow** communication between the isolated computing environment and the workspace.” EX1001, 1:67-2:6 (emphasis

added). It may also “allow a predefined set of processes to be executed within the sandboxed computing environment . . . [and] may prevent execution . . . of any process outside of the predefined set of processes.” EX1001, 13:17-24. In addition, one embodiment shows that the internal isolation firewall “may prevent the host computer system 410 from accessing any of the sandboxed computing environments operating on the host computer system 412.” EX1001 at 21:17-21. Thus, the ’601 patent specification describes an internal isolation firewall serving to prevent access to an isolated computing environment by a host computer system. EX2005, ¶¶ 57-64.

This understanding of a firewall as a component that filters—i.e., selectively allows or blocks, based on predetermined criteria—specific actions or data transmission is also supported by art cited during prosecution of the ’601 patent. For example, U.S. Patent Application Publication 2014/0344912 to Chapman et al. (*see* EX1001 at (56) (“References Cited”)) discloses that a firewall’s “primary objective is to monitor and control the incoming and outgoing network traffic by analyzing the data packets and determining whether each packet should be allowed through or not, based on a predetermined rule set.” EX2006, [0004] (emphasis added). Similarly, U.S. Patent Application Publication 2009/0249472 to Litvin et al. (*see* EX1001 at (56) (“References Cited”)) states “[a] firewall . . . checks incoming and/or outgoing packets of data against an existing list of characteristics that determine

whether the packets should be allowed to continue to their destination or should be blocked.” EX2007, [0009]. And, U.S. Patent No. 7,150,040 to Brownell (*see* EX1001 at (56) (“References Cited”)) states “[f]irewalls are used to screen traffic between . . . networks.” EX2008, 1:29-37. Thus, a rather than **entirely blocking** access to resources outside of an ICE, the ’601 patent describes an “*internal isolation firewall*” that selectively allows certain actions (e.g., data flow, processes, requests, etc.), while prohibiting others, based on predetermined rules. EX2005, ¶ 65.

Petitioner appears to apply a similar meaning to “firewall” in its analysis of claim 5, which recites “*a host-based firewall.*” For example, Dr. Shenoy says that a “*host-based firewall*” that “*isolates the system from communicating with one or more other devices on the network*” is disclosed by a component that “isolates the host computer system by intercepting all incoming and outgoing packets” and “**selectively allow[ing]** packets based on security policies.” EX1003, ¶¶ 255-259 (emphasis added); Pet. 98. Dr. Shenoy also appears to equate a “*firewall*” with a “filter,” when he states “[i]n the combination, **a host-based filter, such as the host-based firewall** component described in Cucinotta, would be implementd with Jeffries’ host operating system 102.” EX1003, ¶ 258 (emphasis added). EX2005, ¶ 66.

Although Petitioner contends that Jeffries’ secure kernel in combination with container manager 118 perform a quarantining function, it does not show that they

do so using an “*internal isolation firewall*” as that term would be understood in the ’601 patent. Jeffries expressly states that quarantining the container “prevent[s] the container from accessing any resources or data outside the container.” EX1005, 5:51-54. A firewall does not prevent access to all resources. It selectively allows access to some resources while preventing access to other resources.

B. Jeffries’ Container Manager and Secure Kernel do not “*isolate the isolated computing environment*”

Jeffries’ container manager **118** and secure kernel do not “*isolate the isolated computing environment.*” **First**, the “corrective actions” in Jeffries do not indicate that a firewall is used to “*isolate*” the ICE. In Jeffries, “a determination of whether potentially malicious activity indicated by the security event satisfies a threat level threshold is used by the container manager **118** to either allow an application **124(1)**, . . . , **124(n)** to continue accessing resources or take corrective action to mitigate the malicious activity.” EX1005, 11:18-23. Corrective action in Jeffries includes: “quarantin[ing] the container **122**,” “quarantin[ing] the accessed resource associated with the malicious activity,” “add[ing] the identified resource to a blacklist . . . and propagat[ing] the blacklist to other connected computing devices,” or “terminating the container **122** and rebuilding a new container.” EX1005, 16:4-46. But quarantining an entire container to prevent it from accessing any outside resources is not how the ’601 patent isolates an ICE using an internal isolation firewall.

Instead, the '601 patent selectively allows certain actions while disallowing others. The specification describes that “internal isolation firewall may . . . allow access to the host system to perform one or more of a cut or copy of data, a paste of data, a printing of data to a local printer, a file transfer, and/or the like” and it “may prevent one or more other transfers of data between the sandboxed computing environment and the workspace.” EX1001, 7:20-35 (emphasis added); EX2005, ¶¶ 57-64. The “corrective action” (e.g., quarantining or terminating the container) in Jeffries does not allow any action. It “prevent[s] the container from accessing any resources or data outside the container.” EX1005, 5:51-54. As Dr. Cole explains, “[t]he wholesale restriction in Jeffries, which prevents the container from accessing any resources or data outside the container, is an entirely different process than what the '601 patent describes and claims. As a POSITA would understand, a firewall (and, specifically, the claimed “*internal isolation firewall*” in the '601 Patent) isolates the ICE by filtering specific actions, operations, or data so that some of those actions, operations, or data are allowed to pass through the firewall while others are not.” EX2005 ¶ 54.

Indeed, the claims themselves would be rendered effectively meaningless if “*isolat[ing] the isolated computing environment from the workspace using an internal isolation firewall*” comprised terminating the ICE completely or preventing processes within the ICE from accessing any resources or data outside the ICE. For

example, claim 1 recites “*a multi-user software application*” within the “*isolated computing environment*” that can “*send data to an untrusted destination.*” If, as Petitioner contends for Jeffries, “isolating” the ICE includes a quarantine that prevents access to any resources or data, the “send data” limitation would be meaningless.

Jeffries also includes “terminating the container **122** and rebuilding a new container” as a remedy for malicious behavior. EX1005, 27:34-35. This is also not the behavior of an “*internal isolation firewall*” used to “*isolate*” the ICE. As Petitioner’s expert, Dr. Shenoy, appears to recognize, there is a difference between a firewall’s filtering function and the “correction actions” taken in Jeffries. In his discussion of claim 5, Dr. Shenoy states “using an isolated container or virtual machine to protect against received malware typically requires terminating the container or machine, along with its contents, entirely to prevent the spread of malware. *See* Jeffries, 16: 41-42 (“terminating the container 122 and rebuilding a new container”), 27:34-35. Doing so results in the loss of unsaved or unfinished work and is a lengthy process leading to frustration of the user. A POSITA would have recognized that advantage of **additionally filtering** packets received by the containers/virtual machines to minimize the instances in which an isolated container or virtual machine must be terminated and rebuilt.” EX1003, ¶ 248 (emphasis added). Thus, Dr. Shenoy’s opinions further demonstrate the distinction between

isolating the ICE using an internal isolation firewall and the remedies applied in Jeffries when malicious activity is detected. EX2005, ¶ 56.

Second, Petitioner contends that the secure kernel “helps to enforce the separation between the host operating system 102 and container 122” when it “causes an exception or interrupt to occur.” Pet. 65. Yet, as Dr. Cole explains, an exception or interrupt are notifications to the processor that an event has occurred. They do not block access to resources. They merely inform the processor of an event. EX2005, ¶ 54.

Third, adding a resource to a “blacklist” that is provided to other devices does not indicate that container manager **118** or secure kernel are an internal isolation firewall that isolate the ICE. Petitioner contends that Jeffries discloses that the host operating system may identify a resource causing the malicious activity and add the identified resource to a list of untrusted resources so that other computing devices are aware of possible negative effects. Pet. 64. However, as Dr. Cole notes, “[c]reating a list of untrusted resources does not allow or block any actions from occurring. It merely makes other computing devices aware of those resources.” EX2005 ¶ 55.

For all of these reasons, Petitioner has not shown that Jeffries’ secure kernel or container manager **118** are used to “isolate the isolated computing environment.” Thus, Jeffries does not render obvious claim 1. Petitioner presents no new arguments

for claim 9 as to the “isolating the isolated computing environment from the workspace using an internal isolation firewall.” Pet. 87. Thus, its arguments for claim 9 fails for the same reasons as identified for claim 1.

VI. Grounds 2 and 3

Grounds 2 and 3 challenge claims 5-6, 8, 13-14, and 16, all of which depend from claims 1 or 9. Petitioner presents no new arguments as to the “*isolate the isolated computing environment*” limitation of claim 1 or the “*isolating the isolated computing environment from the workspace using an internal isolation firewall*” limitation of claim 9.

VII. Conclusion

Petitioner has failed to demonstrate unpatentability of any challenged claim because it has not shown that Jeffries discloses or renders obvious “*a processor configured to . . . isolate the isolated computing environment from the workspace using an internal isolation firewall*” (claim 1) or “*isolating the isolated computing environment from the workspace using an internal isolation firewall*” (claim 9), which are required by every challenged claim.

Date: May 22, 2025

Respectfully submitted,

/Brett Cooper/

Brett Cooper, Reg. No. 55,085
Lead counsel for Patent Owner

CERTIFICATE OF WORD COUNT (37 C.F.R. § 42.24(d))

The undersigned hereby certifies that the word count in this Patent Owner Response is 3,167 words, as counted by the word-processing program Microsoft Word that was used to generate this Patent Owner Response, where such word count excludes the table of contents, table of authorities, mandatory notices, certificate of service, appendix of exhibits, claim listing, and this certificate of word count. This Patent Owner Response is in compliance with the 14,000-word limit set forth in 37 C.F.R. § 42.24(b)(1).

Date: May 22, 2025

/Brett Cooper/

BC Law Group, P.C.
200 Madison Avenue, 24th Floor
New York, NY 10016
(212) 951-0100

Brett Cooper
Reg. No. 55,085
Attorney for Patent Owner

CERTIFICATE OF SERVICE (37 C.F.R. § 42.6(e))

The undersigned hereby certifies that the above document was served on May 22, 2025, by filing this document through the Patent Trial and Appeal Case Tracking System as well as delivering a copy via electronic mail upon the following attorneys of record for the Petitioner:

Theodore M. Foster (Reg. No. 57,456)
ipr.theo.foster@haynesboone.com
David L. McCombs (Reg. No. 32,271)
david.mccombs.ipr@haynesboone.com
Eugene Goryunov (Reg. No. 61,579)
eugene.goryunov.ipr@haynesboone.com
Adam Erickson (Reg. No. 77,434)
adam.erickson.ipr@haynesboone.com

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

Date: May 22, 2025

/Brett Cooper/

BC Law Group, P.C.
200 Madison Avenue, 24th Floor
New York, NY 10016
(212) 951-0100

Brett Cooper, Reg. No. 55,085
Attorney for Patent Owner