Trials@uspto.gov
571-272-7822

Paper 11
Entered: November 8, 2021

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MICROSOFT CORPORATION,
Petitioner,

v.

DAEDALUS BLUE, LLC,
Patent Owner.

IPR2021-00832
Patent 8,381,209 B2

Before SALLY C. MEDLEY, HYUN J. JUNG, and ARTHUR M. PESLAK, *Administrative Patent Judges*.

MEDLEY, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

Microsoft Corporation ("Petitioner") filed a Petition for *inter partes* review of claims 1–8 of U.S. Patent No. 8,381,209 B2 (Ex. 1001, "the '209 patent"). Paper 1 ("Pet."). Daedalus Blue, LLC ("Patent Owner") filed a Preliminary Response. Paper 6 ("Prelim. Resp."). In accordance with Board authorization, Petitioner filed a Reply to the Preliminary Response (Paper 9) and Patent Owner filed a Sur-Reply (Paper 10).

Institution of an *inter partes* review is authorized by statute when "the information presented in the petition . . . and any response . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." 35 U.S.C. § 314(a). Upon consideration of the Petition, the Preliminary Response, and the evidence of record, we decline to institute review of the challenged claims of the '209 patent.

A. Related Matters

The parties indicate that related district court litigations are *Daedalus Blue, LLC v. Microsoft Corp.*, No. 6:20-cv-01152 (W.D. Tex.) ("the district court case") and *Daedalus Blue, LLC v. Oracle Corp. et al.*, No. 6:20-cv-00428 (W.D. Tex.) (terminated). Pet. 4; Paper 4, 2.

B. The '209 Patent

The '209 patent relates to "virtual machine migration with filtered network connectivity which includes enforcing network security and routing at a hypervisor layer at which a virtual machine partition is executed and which is independent of guest operating systems." Ex. 1001, 1:11–15. The '209 patent describes that "in order to perform maintenance on or provide a fail-over for a processor device or machine, it is desirable to move or

migrate a virtual machine (VM) from one processor machine or device to another." *Id.* at 2:27–30. The '209 patent seeks to address shortcomings of conventional approaches for VM migration (*id.* at 4:31–40), which include "a complex update scheme to update the ACLs [access control lists] in the real switches and the filters in the firewalls," and "very little network security" (*id.* at 3:6–11).

Figure 4, reproduced below, illustrates an embodiment for "securing a filtered network, including enforcing network security and routing at a hypervisor layer." *Id.* at 8:31–34.

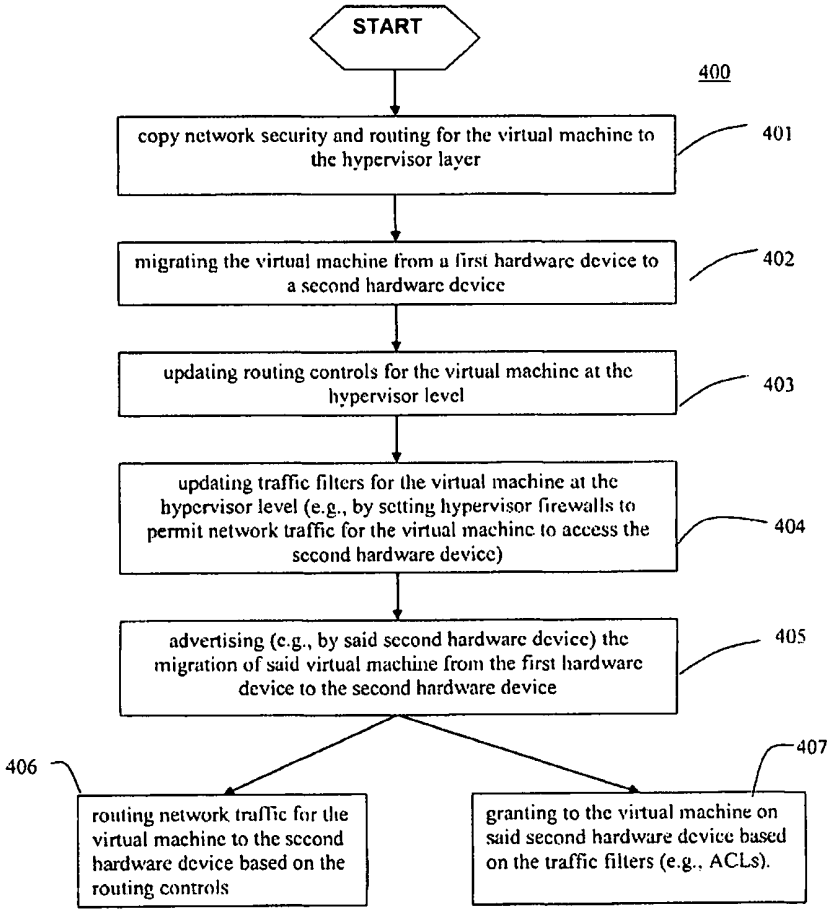

FIGURE 4

Figure 4 shows a method, beginning with step 401, which "copies network security and routing for the virtual machine to the hypervisor layer." *Id.* at 8:37–39. Then, the method "migrates the virtual machine from a first hardware device to a second hardware device" in step 402, "updates routing controls for the virtual machine at the hypervisor level" in step 403, "updates traffic filters for the virtual machine at the hypervisor level" in step 404, "and advertises the migration of the virtual machine from the first hardware device to the second hardware device" in step 405. *Id.* at 8:39–46. In steps 406 and 407, network traffic for the virtual machine is routed to the second hardware device based on the routing controls and access is granted to the virtual machine on the second hardware device based on the traffic filters. *Id.* at 8:47–51.

The '209 patent describes that by copying security and routing to the hypervisor layer, "the user will see no difference in operation." *Id.* at 9:25–28. For example, "the first and second device . . . would each act the same, and preferably, would each have the same internet protocol (IP) address." *Id.* at 9:29–31. Moreover, because "the hypervisor layer provides traffic filtering and routing updating," "the real switches do not need to be updated at the first and second hardware devices." *Id.* at 9:39–42.

C. Illustrative Claim

Petitioner challenges claims 1–8 of the '209 patent. Claim 1 is independent, and claims 2–8 depend therefrom. Claim 1 is reproduced below.

> 1. A computer implemented method of controlling network security of a virtual machine, the method comprising enforcing network security and routing at a hypervisor layer via dynamic updating of routing controls initiated by a

migration of said virtual machine from a first device to a second device.

Ex. 1001, 15:39–43.

D. Asserted Grounds of Unpatentability

Petitioner asserts that claims 1–8 are unpatentable based on the following grounds (Pet. 7):[1]

Claims Challenged	35 U.S.C §	References/Basis
1, 3, 6	103(a)[2]	Dhawan[3], Clark[4]
2, 4, 5	103(a)	Dhawan, Clark, Warfield[5]
7, 8	103(a)	Dhawan, Clark, Chandika[6]

[1] Although Petitioner adds the general knowledge of a person of ordinary skill in the art to the express statement of each alleged ground of unpatentability (Pet. 7, 36, 45, 55), that is not necessary. Obviousness is determined from the perspective of one with ordinary skill in the art. We leave out the express inclusion of the general knowledge of one with ordinary skill.

[2] The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) ("AIA"), amended 35 U.S.C. § 103. The '209 patent was filed on January 3, 2007. Ex. 1001, code (22). Because the filing date is before the effective date of the applicable AIA amendments, we refer to the pre-AIA version of 35 U.S.C. § 103.

[3] U.S. Pat. App. Pub. No. US 2007/0079307 A1, published Apr. 5, 2007 (Ex. 1005, "Dhawan").

[4] "Live Migration of Virtual Machines" (Ex. 1006, "Clark"). Petitioner asserts a publication date of May 3, 2005, and a public accessibility date of February 28, 2006. Pet. 6 (citing Ex. 1009).

[5] "Isolation of Shared Network Resources in XenoServers" (Ex. 1007, "Warfield"). Petitioner asserts a publication date of November 2002, and a public accessibility date of December 2002. Pet. 7–10 (citing Exs. 1024–1045).

[6] U.S. Patent No. 8,107,370 B2, filed Apr. 6, 2005, issued Jan. 31, 2012 (Ex. 1008, "Chandika").

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.