EXHIBIT D-5

Microsoft contends that the asserted claims of the '209 Patent are invalid as obvious by Warfield, "Isolation of Shared Network Resources in XenoServers" ("Warfield"), Matthews, "Data Protection and Rapid Recovery From Attack With a Virtual Private File Server and Virtual Machine Appliances" ("Matthews"), U.S. Patent No. 8,161,475 ("Araujo"), U.S. Patent No. 8,107,370 ("Chandika") prior art references under various subsections of 35 U.S.C. § 102 in view of other prior art references under 35 U.S.C. § 103 as set forth in Microsoft's invalidity contentions.

As Warfield was published in November 2002, Microsoft contends that it is prior art to the '209 Patent under at least pre-AIA 35 U.S.C. § 102(b).

As Matthews was published in 2005, Microsoft contends that it is prior art to the '209 Patent under at least pre-AIA 35 U.S.C. § 102(b).

As Araujo filed on September 29, 2006 and published on April 3, 2008, Microsoft contends that it is prior art to the '209 Patent under at least pre-AIA 35 U.S.C. § 102(e).

As Chandika was filed on April 6, 2005 and published on October 12, 2006, Microsoft contends that it is prior art to the '209 Patent under at least pre-AIA 35 U.S.C. § 102(e).

Patent No. 8,381,209 Claim Limitation(s)	Disclosures
"setting firewalls to permit a network traffic for the virtual machine to go to the second device at the hypervisor layer" (Claim element 2[b]) "updating traffic filters for said virtual machine at the hypervisor level" (Claim element 4[b])	**Warfield, "Isolation of Shared Network Resources in XenoServers" ("Warfield")** Warfield discloses setting firewalls to permit a network traffic for the virtual machine to go to the second device at the hypervisor layer and updating traffic filters for a virtual machine at the hypervisor level. For example, Warfield states: "The network system within Xen consists of a virtual firewall router, which is a rule-based packet classification/forwarding engine (based on Linux netfilter/IPTables code) responsible for simple, fast packet handling. Additionally, Xen's network system incorporates a network address translation (NAT) module that provides functions such as address translation and port forwarding. Packet scheduling in Xen is at the granularity of virtual interfaces. A soft real-time scheduler moves transmit packets from virtual interface send queues through Xen's routing tables. Received packets are delivered on arrival and appropriate RX scheduling is deferred on to the CPU scheduler as VMs are

Patent No. 8,381,209 Claim Limitation(s)	Disclosures
	responsible for emptying their own inbound message buffers. VMs which do not empty their receive queues at the inbound packet rate will have extraneous packets dropped. Rules may be installed into classification engine through an interface provided within a privileged VM (known as domain zero). These rules are tuples of the form (pattern, action). Note that rules may be prioritized and a particular packet may match multiple rules upon classification. This means that, for instance, an arriving packet bound for a VM may be routed to that VM and trigger the generation of a logging event to domain zero." Warfield at 4-5. Warfield at Fig. 3:

Patent No. 8,381,209 Claim Limitation(s)	Disclosures

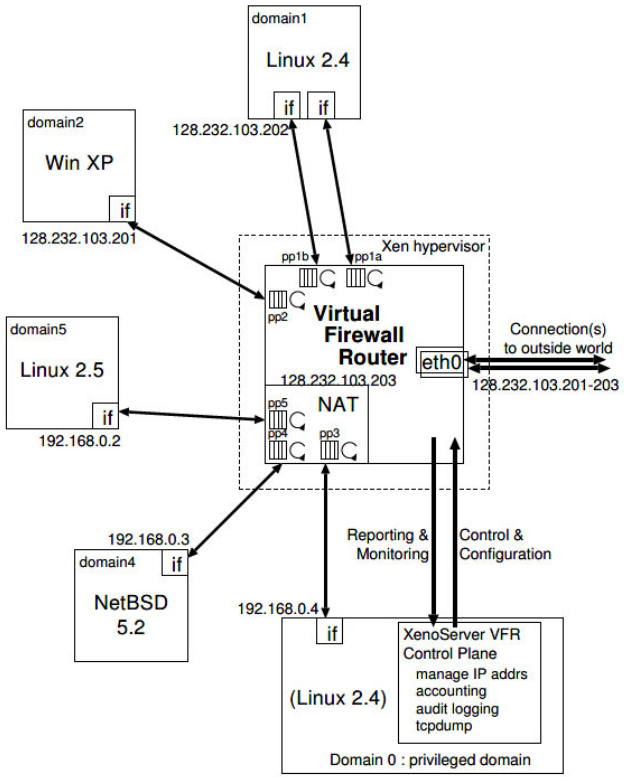

Figure 3: Network virtualization in Xen.

Matthews, "Data Protection and Rapid Recovery From Attack With a Virtual Private File Server and Virtual Machine Appliances" ("Matthews")

Matthews discloses setting firewalls to permit a network traffic for the virtual machine to go to the second device at the hypervisor layer and updating traffic filters for a virtual machine at the hypervisor level. For example, Matthews states:

EXHIBIT D-5

Patent No. 8,381,209 Claim Limitation(s)	Disclosures
	"We also use the base machine as a platform for monitoring the behavior of each guest. For example, in our prototype, we run an intrusion detection system on the base machine. (The base machine could also be used as a firewall or NAT gateway to further control access to virtual machine appliances with interfaces on the physical network.) The intrusion detection system can detect both attack signatures in incoming traffic and unexpected behavior in outgoing traffic. For example, it could indicate that all outgoing network traffic from a particular virtual machine appliance should be POP or SMTP. In such a configuration, unexpected traffic such as an outgoing ssh connection that would normally not raise alarms could be considered a sign of an attack." Matthews at Section 2.1. "The base machine creates a set of resource limits for each virtual machine appliance in several ways. First, the base machine can allocate a limited amount of system resources such as memory, disk space or even CPU time to each guest. Second, the base machine can restrict access to the local virtual network and/or the physical network connection. In either case, access can be denied completely or restricted through firewall rules. Third, the intrusion detection system running on the base machine monitors the behavior of the guest for both attack signatures and otherwise "innocent" looking traffic that is simply unexpected given the purpose of the virtual machine appliance." Matthews at Section 2.4. "We can defend against backdoor programs and programs that exploit specific server software by blocking all unneeded ports using firewall software at the base OS or virtual machine monitor level. On a base operating system, this may not always be possible because some ports exploited by viruses must be left open for legitimate reasons. For example, the blaster worm infects systems via the Microsoft Windows DCOM RPC service that listens on TCP port 135. Most VM's will not need access to this port so it will be blocked by default which completely removes any threat that the Blaster virus will infect those VM's. Some VM's may need access to TCP port 135 and on these systems you would not block it. In this case, an intrusion detection system on the base machine could monitor for and recover from many of these attacks." Matthews at Section 4. **U.S. Patent No. 8,161,475 ("Araujo")**

Patent No. 8,381,209 Claim Limitation(s)	Disclosures
	Araujo discloses setting firewalls to permit a network traffic for the virtual machine to go to the second device at the hypervisor layer and updating traffic filters for a virtual machine at the hypervisor level. For example, Araujo states: "A mechanism for the provisioning of virtual machines is desired in order to achieve and maintain a predetermined state or requirement of a system of virtual machines. A virtual machine provisioning system 300 to achieve this goal is illustrated in FIG. 3. Virtual machines 310 are connected to a monitoring agent 320. FIG. 3 illustrates three virtual machines 310 (310 a, 310 b, and 310 c), although the number of virtual machines is not so limited and more or fewer virtual machines 310 may form part of the virtual machine provisioning system 300. The monitoring agent 320 is responsible for collecting data from the virtual machines 310. The monitoring agent 320 may also collect data from a virtual server host 350, connected to virtual machines 310, and/or from a computing device or system 360, also connected to virtual machines 310. The computing device or system 360 may include, for example, a network router, load balancing hardware, a firewall, a software management system, and/or any combination thereof. The collected data may be used to determine a state of the virtual machines 310 and to determine if their state or that of the system, which may be a combination of virtual machines 310 from multiple servers, is at a predetermined state. The provisioning mechanism is employed, as described in further detail below, if the state of the virtual machines 310 is not at or near the predetermined state." Araujo at 7:37-60. "For example, suppose that the policy administrator 340 defines system policies as a target usage of a web server at 1,000 pages per minute per web server for a target of 10 virtual machines 310. The target usage is, in this example, the monitored variable and is used to determine the state (healthy or unhealthy) of the system. The virtual machines 310 provide their respective usage in number of pagers per minute to the monitoring agent 320. Further suppose that the policy administrator 340 defines an unhealthy state as +/−10% change in usage over a 24 hour time period. If the monitoring agent 320 detects in virtual machine 310 a+/−10% change in usage over a 24 hour time period, then the monitoring agent 320 relays such detection to the enforcement agent 330 to take appropriate action. Suppose that the policy administrator 340 defines a violation action as deleting a virtual machine if the usage for the particular virtual machine is −10% below 1,000 pages per minute and adding a virtual machine if the usage is +10% above 1,000 pages per minute. The policy administrator 340

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.