VMware™ vShield Zones

REVIEWER'S GUIDE

vmware®

Table of Contents

Getting Started

About This Guide

The purpose of this document is to support a self-guided, hands-on evaluation of VMware™ vShield Zones. This document is intended to provide IT professionals with the necessary information to learn the capabilities of vShield Zones and see how they can be used in practical situations.

The content includes a product overview, brief installation instructions, and a walk-through of a scenario that shows the main features of vShield Zones in action.

Help and Support during the Evaluation

This guide is not intended to be a substitute for product documentation. For detailed information regarding installation, configuration, administration, and usage of VMware products, please refer to the online documentation. You may also consult the online Knowledge Base if you have any additional questions. Should you require further assistance, please contact a VMware sales representative or channel partner.

Below are some links to online resources, documentation, and self-help tools:

VMware vSphere and VMware vCenter Server Resources:

- Product Overview
  http://www.vmware.com/products/vsphere/
- Product Documentation
  http://www.vmware.com/support/pubs/vs_pubs.html
- White Papers and Technical Papers
  http://www.vmware.com/resources/techresources/
- VMware vSphere Evaluator's Guide
  http://www.vmware.com/resources/techresources/10020

vShield Zones Resources

- VMware vShield Zones Documentation
  http://www.vmware.com/support/pubs/vsz_pubs.html
- ntroduction to vShield Zones
  http://www.vmware.com/pdf/vsz_10U1_introduction.pdf
- vShield Zones Quick Start Guide
  http://www.vmware.com/pdf/vsz_10U1_quickstart.pdf
- vShield Zones Administration Guide
  http://www.vmware.com/pdf/vsz_10U1_admin.pdf
- VMware Security and vShield Zones Community
  http://communities.vmware.com/community/vmtn/general/security

What is vShield Zones?

vShield Zones is an application-aware firewall built for VMware vCenter™ Server integration. vShield Zones is a critical security component for protecting virtualized datacenters from attacks and misuse helping you achieve your compliance-mandated goals.

vShield Zones Overview

The following components comprise the vShield Zones solution:

- vShield: The active security component of vShield Zones that inspects traffic flows and provides firewall protection. You install a vShield on each ESX server you want to protect. The vShield installs in the traffic path to monitor all traffic into and out of the ESX server, as well as between virtual machines on the ESX server.
- vShield Manager: The vShield Zones management center that manages all of the distributed vShield instances. Provides for monitoring, configuration, and software updating of your vShields. You install one per datacenter.

Once deployed, vShield Zones looks at all network traffic that passes through the vShields and begins building an inventory of the operating systems, applications, and open ports on each guest virtual machine. The vShield Manager presents flow information under the VM Flow tab and virtual machine inventory under the Summary tab.

By default, the vShield Manager inventory tree hierarchy mimics the vSphere Client Hosts & Clusters view. Resources include the root folder, datacenters, clusters, ESX hosts, and virtual machines—including your installed vShields. You can also switch to the Networks view, which displays the VLAN networks and port groups in your inventory. These views are consistent with the same views in the vSphere Client, and the vShield Manager maintains synchronization with your vSphere inventory to present a complete view of your virtual deployment. The vShield Manager itself is the only virtual machine that does not appear in the vShield Manager inventory tree.

Each inventory object has its own set of tabs that appear in the right-side Configuration frame. The inventory tree includes a search function atop the tree. You can type a string in this field to search for a specific resource in the inventory tree.

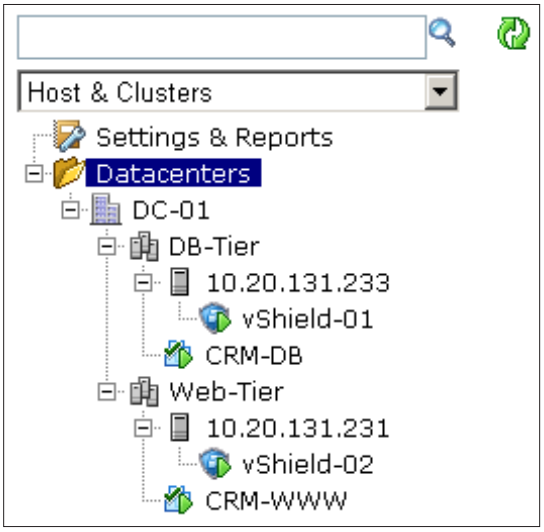


Figure 1. Host and Cluster view

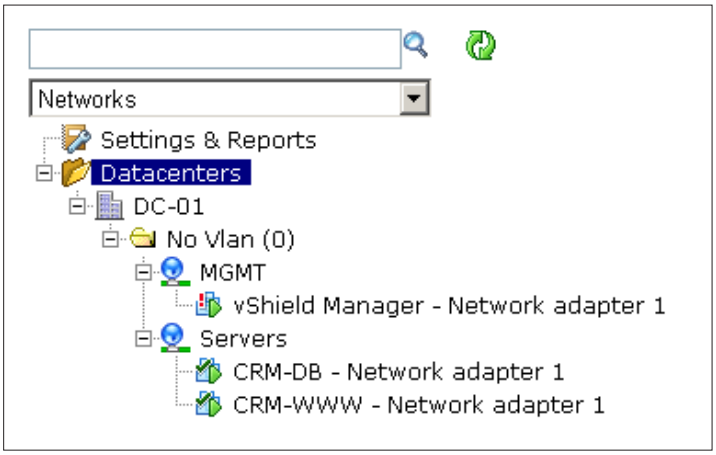


Figure 2. Networks view

vShield Zones profile each virtual machine in your inventory through continuous discovery of the traffic flows to and from them. Once traffic has been inspected by a vShield, a profile is created detailing the operating system, applications, and open ports for each virtual machine. These profiles are presented under the Summary tab.

After initial vShield Zones setup, the Summary tab is empty awaiting continuous discovery by vShields to identify the virtual machines and applications to protect. A vShield discovers all of the supported applications by examining ingress and egress flows, and creates a profile per virtual machine by IP address. The Summary tab displays at the Child Datacenter and Cluster container levels, and at the individual virtual machine level. At the Child Datacenter container level, the Summary tab lists all of the virtual machines being protected by all of the vShields in that container. At the Cluster level, all of the vShields in the cluster container are listed.

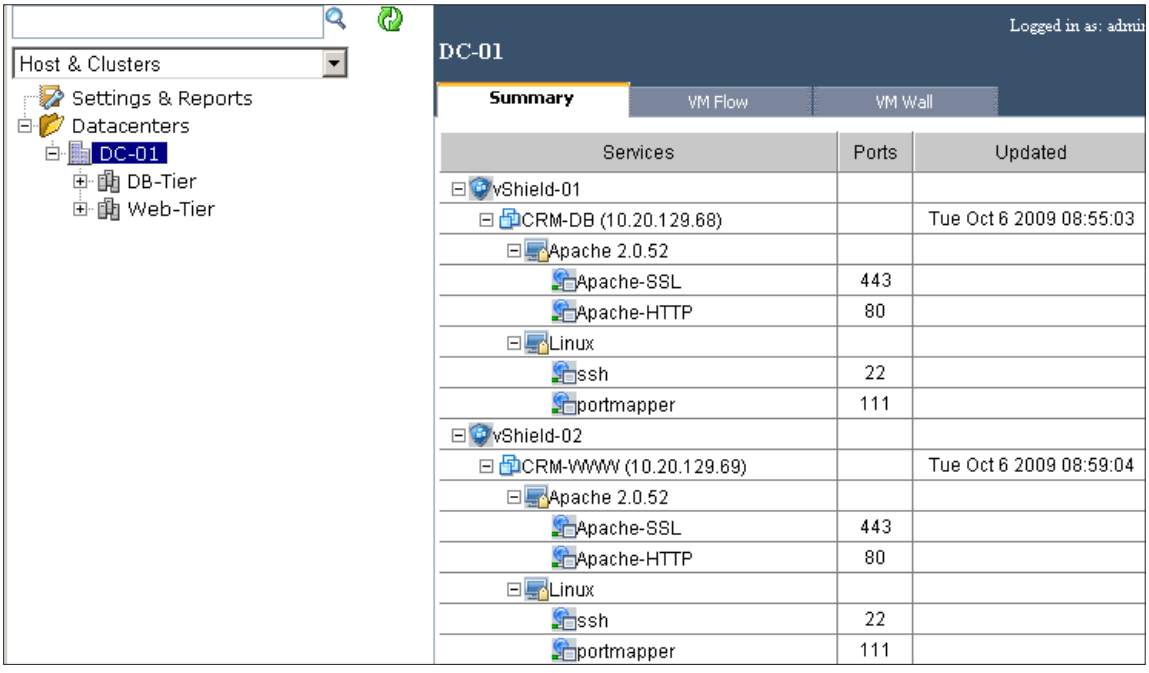


Figure 3. Summary tab

Analyzing Traffic Statistics Using VM Flow

VM Flow is a flow analysis tool that provides a detailed view of the traffic on your virtual network. The VM Flow output defines which machines are talking to each other and over which application. Data includes the number of sessions, packets, and bytes transmitted per flow. VM Flow is useful as a forensic tool to detect rogue services and examine outbound sessions and can be used to create VM Wall rules.

The VM Flow tab displays throughput statistics as returned by all of the active vShields within a Child Datacenter or Cluster container, or at the individual virtual machine level. Flow statistics display all inspected flows within the time span specified in the Start Date and End Date fields with the last seven days of data displayed by default. VM Flow organizes statistics by the application protocols used in client-server communications with each color in a chart representing a different application protocol. This charting method enables you to track your server resources per application.

Configuring Firewall Settings Using VM Wall

The VM Wall tab presents the firewall function of vShield Zones. VM Wall is a centralized, hierarchical firewall for virtual machine environments. VM Wall acts as a security layer between the hypervisor and virtual machines. VM Wall leverages the rich protocol coverage of vShield Zones to open and close dynamic ports as required. This application-aware knowledge allows VM Wall to represent the protocols and ports more succinctly.

You manage firewall rules at the datacenter and cluster levels to provide a consistent set of rules across multiple vShields under these containers. As membership in these containers can change dynamically, VM Wall maintains the state of existing sessions without requiring reconfiguration of firewall rules. In this way, VM Wall effectively has a continuous footprint on each ESX host under the managed containers.

By default, the VM Wall screen displays a set of default rules allowing traffic to pass through all vShields. The default rules cannot be deleted or added to. However, you can change the Action element of each rule from Allow to Deny. The VM Wall offers two layers of rules: Layer 4 rules and Layer 2/Layer 3 rules. You configure Layer 2/Layer 3 rules at the datacenter level only. You can add Layer 4 rules either manually or based on information from the VM Flow report.

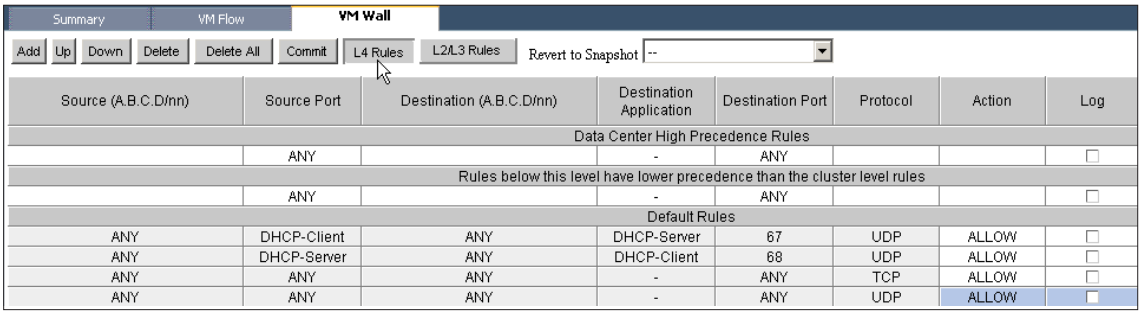


Figure 4. Layer 4 rules

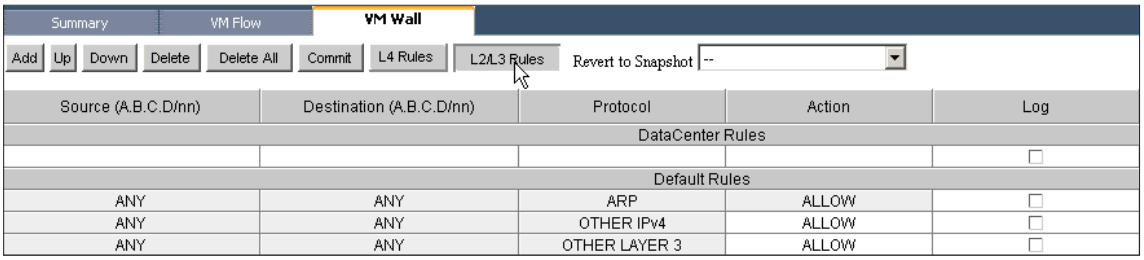


Figure 5. Layer 2 / Layer 3 rules

Evaluation System Requirements

Hardware Requirements

The minimum hardware requirements for a successful evaluation are:

- Two physical servers – These are used to install ESX and the vShield Zones virtual machines, including the vShield Manager, vShield agent. They also run several test virtual machines to demonstrate the product's features.
- One vCenter server. Optionally the vCenter server can also run on the ESX server as a virtual machine. In the examples used in this guide the vCenter servers runs on a separate server.
- One Windows workstation or laptop – This is used to access the applications on the test virtual machines and test the VM Wall and VM Flow functionality.

Note: "ESX" in this document refers to both ESX and ESXi.

For detailed hardware requirements for ESX host(s), refer to the table below:

HARDWARE REQUIREMENTS FOR VSHIELD ZONES EVALUATION USE CASES	MINIMUM
# ESX hosts	2
CPU	2 processors of 1500Mhz
Memory	6GB
Disk Space	8GB vShield Manager; 5GB per vShield Enough space for the two test virtual machines (Local/Network Storage)
Network	2GB NICs on each ESX server hosts

Software Requirements

For the purpose of this evaluation, you will need the latest versions of the following software downloads:

- VMware vSphere (Advanced/Enterprise/Enterprise Plus) Evaluation copy.
- VMware vCenter Evaluation copy.
- vShield Zones Evaluation copy.

VMware offers a free, 60-day evaluation of the VMware software below. Follow the instructions at https://www.vmware.com/tryvmware/index.php?p=vsphere&lp=1, which will walk you through the process to download the necessary licenses and the following binaries:

BINARY	USAGE
ESX 4 (iso file)	You can create a boot CD from this iso file and use this CD to boot your server and install ESX 4.
VMware vCenter Server (zip file)	The zip file includes an installer for VMware vCenter Server 4.
VMware vShield Zones (exe file)	The exe file is a self-extracting executable that includes the .OVF files for the vShield and vShield Manager.

Note that vShield Zones can also be configured in an existing environment and does not require an isolated, dedicated environment for evaluation purposes. The above recommended hardware and software is intended for sites that want to evaluate vShield Zones without having access to an existing virtual infrastructure setup.

vSphere Installations and Configurations

Before you embark on the evaluation exercises, you need to install and configure a basic vSphere installation. The following is a high-level overview of this process. For more detailed information, please consult the vSphere resources listed in Chapter 1.

Step 1. Provision two physical servers with the hardware profile described in the hardware requirements section.

Step 2. Install the ESX Server software on the physical servers. (See ESX Server 4 Installation Guide for more detail).

Step 3. Create a simple networking configuration with 2 vSwitches, each with a physical NIC. The first vSwitch has the Service Console or VMkernel management interface. The second vSwitch has the Virtual Machines port group called "Servers" in this example. Another port group in the second vSwitch is required; its name has to include the word 'mgmt' (not case sensitive). This port group will be noted by the automated installation and will house the management interface of the vShield Zones virtual appliances.

Step 4. Install the VMware vSphere Client on a supported Windows machine (e.g. a laptop).

Step 5. Install VMware vCenter Server on a supported Windows machine. This can be the same machine where the VMware vSphere Client was installed.

Step 6. Start the VMware vSphere Client and connect to the VMware vCenter Server just created in the previous step. Add the ESX hosts provisioned in Step 2 to the VMware vCenter Server inventory.

vShield Zones Installations and Configuration

Before installing VMware vShield on the virtual machine you need to ensure the following prerequisites are met:

PREREQUISITES	DETAILS
Network	Set aside the following network assignments: • One static IP address for vShield Manager. One vShield Manager is required per datacenter. • One static IP address per vShield. One vShield is required per vSwitch per ESX host. • Gateway IP address • Subnet Mask
ESX host networking configuration	A simple networking configuration with 2 vSwitches, each with a physical NIC. First vSwitch has the Service Console or VMkernel interface. Second vSwitch has the Virtual Machines port group called "Servers" and MGMT port group. See Figure 6.

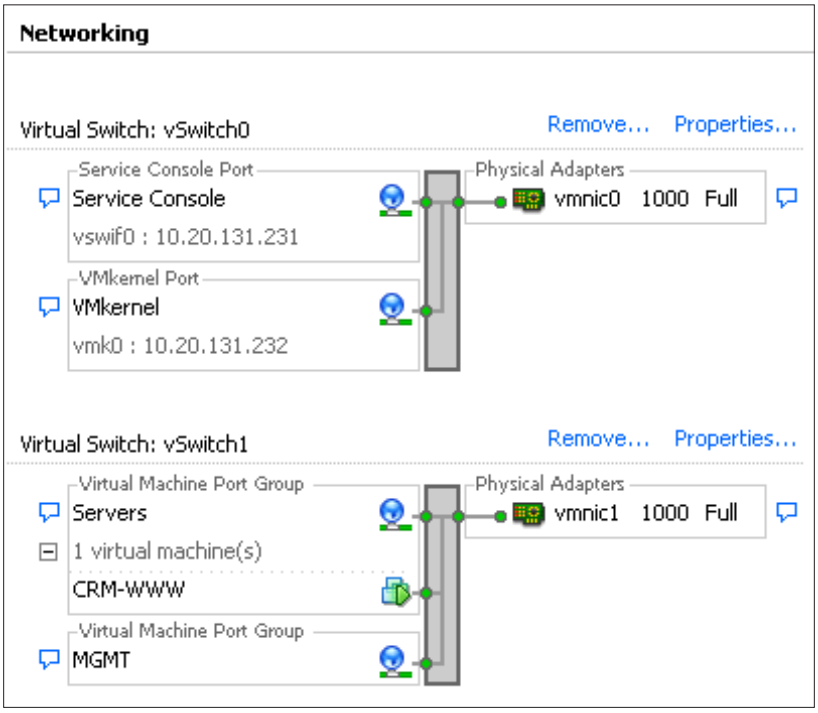


Figure 6. ESX Host networking configuration

To install vShield Zones, please consult the vShield Zones Quick Start Guide, available at http://www.vmware.com/pdf/vsz_10U1_quickstart.pdf.

Scenario – Multi-tier Applications

This section outlines a multi-tier application scenario using vShield Zones. This use case will provide a better understanding of how vShield Zones can be used to segment these two layers. This section will create VM Wall rules for a two-tier application architecture consisting of a web front-end layer and a database back-end layer, with each layer in its own cluster. Next it will create VM Wall rules at each cluster level specific to the access needs of each layer.

In this example, VMware is using Linux virtual machines simulating a two-tier application where the web services and a CRM application are running on the front-end server and the database is running in the back-end server. The applications used to run this are SugarCRM, Apache and MySQL. You can use Windows virtual machines as well, by placing a Windows Server 2003 virtual machine with IIS and FTP enabled on it configured as the server in one cluster and a Windows XP with a web browser to act as the client on the other cluster.

The layered application example is broken down into the following steps:

Step 1. Create a multi-tier application scenario by installing two virtual machines in two separate clusters.

Step 2. Generate traffic to the protected virtual machines.

Step 3. Analyze and learn the type of traffic that is flowing to your virtual machines. Use this information to learn about the type of traffic going and the correct virtual machines are communicating with each other.

Step 4. Edit port mappings - categorize an uncategorized port.

Step 5. Create rules based on your needs.

Step 6. Test rule enforcement.

Step 7. Modify or adjust rules if necessary.

Step 8. Configure and test Layer2/Layer3 rules.

Step 9. Delete a VM Wall Rule.

Step 1: Create multi-tier application scenario

For the example in this guide, VMware is using two Linux virtual machines simulating a two-tier application where the web services and a CRM application are running on the front-end server and the database is running in the back end tier. The applications used to run this should be deployed as follows:

- First Virtual Machine: Web Tier, running SugarCRM and Apache.
- Second Virtual Machine: DB Tier, running MySQL.

You can use Windows virtual machines as well, with one virtual machine acting as the server and the other as a client. The virtual machines should be provisioned as follows.

- First Virtual Machine: Client Tier, running Windows with a web browser.
- Second Virtual Machine: Server Tier, running Windows Server with IIS and FTP enabled and configured.

To start, create two clusters with one ESX host in each. For this guide, the clusters DB-Tier and Web-Tier were created. Next, create the two virtual machines on the ESX host using the VMware vSphere Client, and place them in the appropriate cluster. For all virtual machines, make sure you power them on and you place their NICs in the Servers port group on the respective servers. The deployment should look something like the inventory in Figure 7.

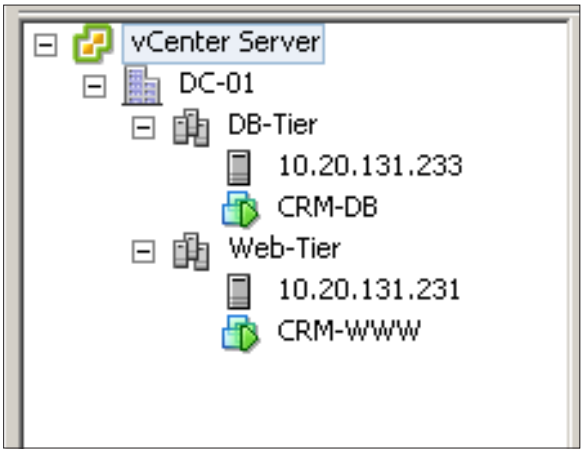


Figure 7. Host and Cluster setup

Step 2: Generate Traffic

If you don't already see traffic in the Summary and VM Flow pages, generate some network activity7 by accessing or connecting to a service/port on the protected virtual machines. In this example, you can generate HTTP/HTTPS and SSH traffic to both virtual machines. You can do this from the outside, using a computer that not being protected by the vShield. You can also generate intra-VM Traffic from one protected virtual machine to the other.

Generate Traffic from Outside

1. From the Windows computer/laptop that is not being protected by the vShield, open a web browser and point it to the IP address of the web server. Alternatively you can use a different application supported by the server such as SSH, telnet, FTP, etc.
2. Log in to the CRM application, navigate the web site, traverse the FTP directory, run a few remote telnet/SSH/FTP commands.

In this example VMware connects to CRM running on the web server via the web browser:

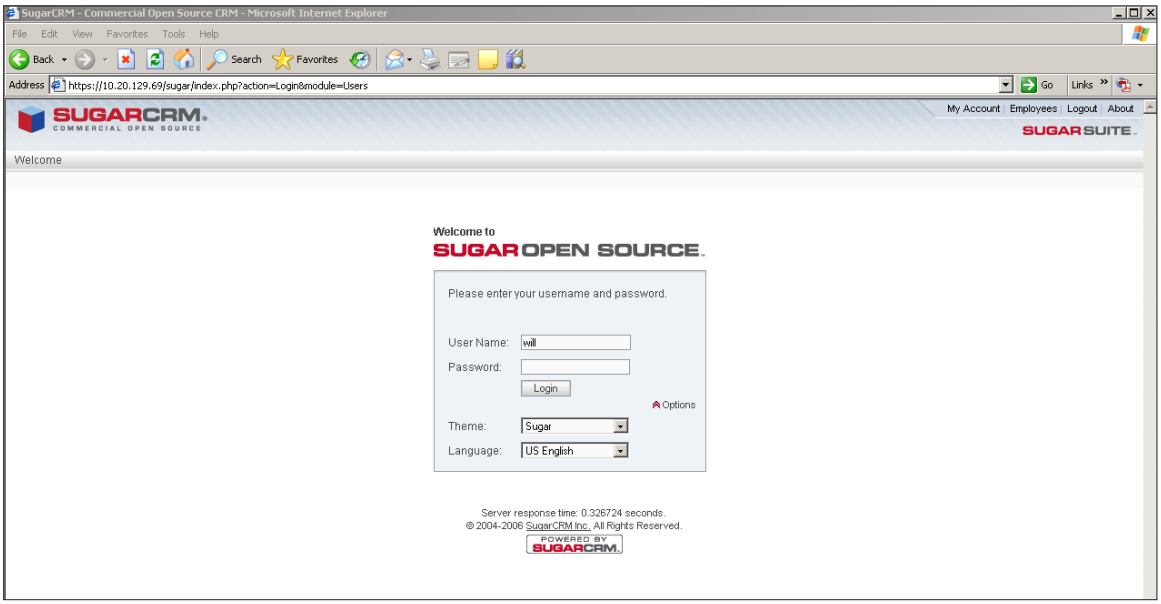


Figure 8. Login page for CRM application

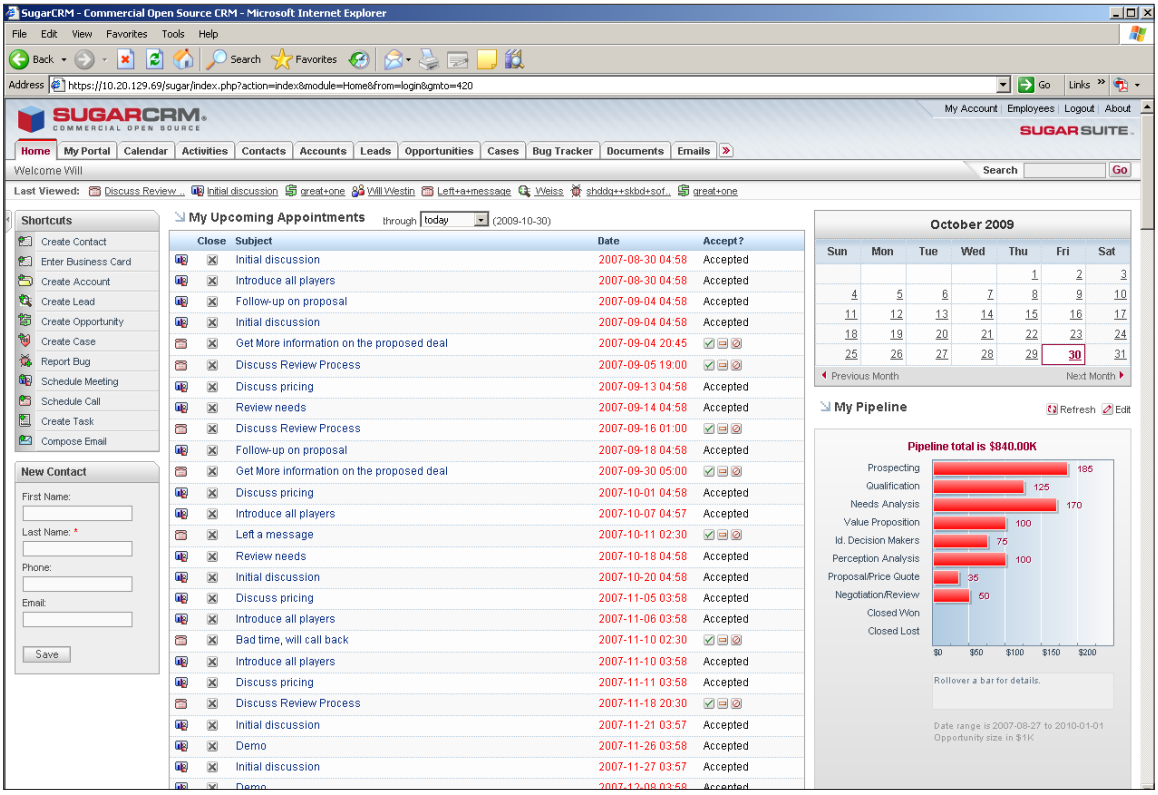


Figure 9. Home screen for CRM application

Generate Intra-VM Traffic from one protected virtual machine to the other

1. Open a console to the protected virtual machine on cluster one and generate application traffic to the other protected virtual machine on cluster two. Use any of the supported applications such as http, SSH, telnet, FTP, etc.
2. Switch to the protected virtual machine on cluster two and generate traffic in the other direction.

In this example, VMware opens a console on the database server CRM-DB and ping CRM-WWW followed by establishing an SSH session:

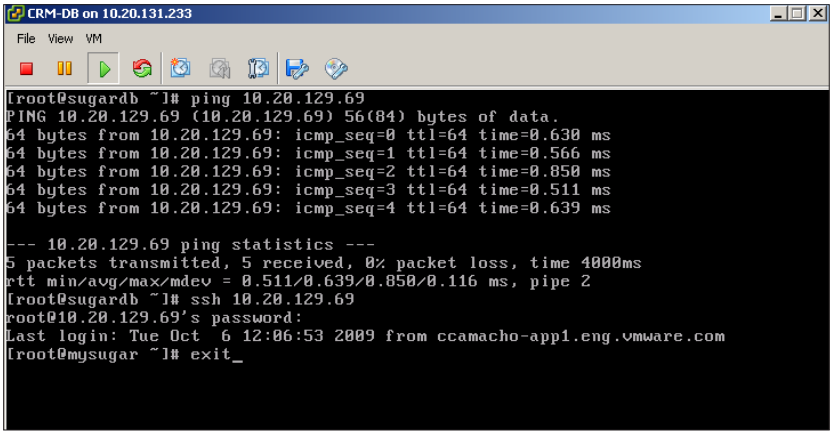


Figure 10. Ping between Web and DB tiers

Next, VMware opens a console on the web server CRM-WWW and ping CRM-DB followed by establishing an SSH session:

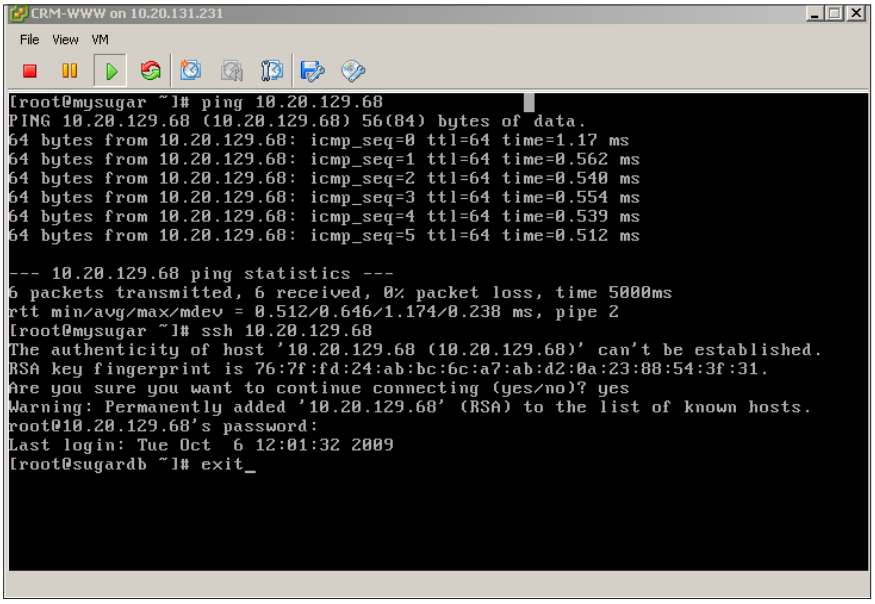


Figure 11. SSH session between Web and DB tiers

Step 3: Analyze traffic flows

Select the top-level datacenter container on the left hand side tree of the vShield Manager. Go to the Summary page and review the Services and ports for each of your virtual machines. They will be categorized by vShield. In this example, you'll see that there are two virtual machines, one in each cluster:

- Virtual machine 10.20.129.69 runs the CRM software and web server.
- Virtual machine 10.20.129.68 is the back-end database server used by the CRM software.

Also note the ports and services running on each virtual machine, in this example, 443, 80, 22, 111.

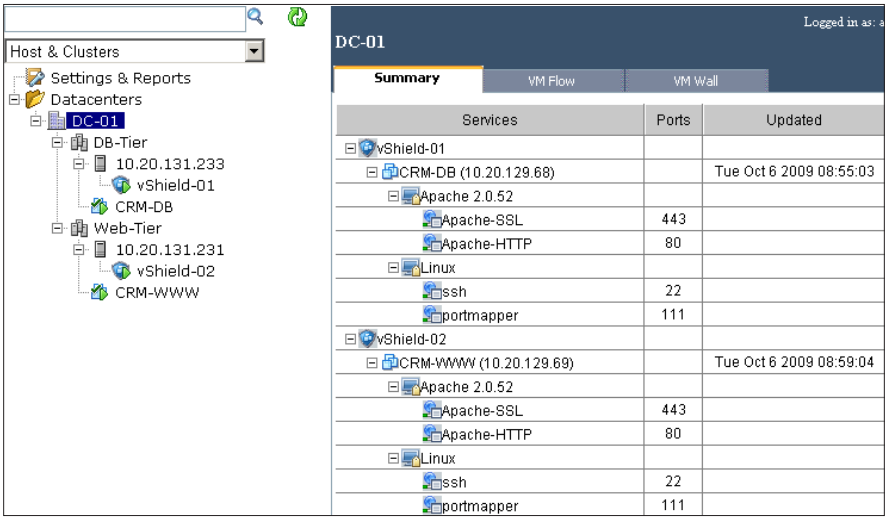


Figure 12. Summary tab for the whole datacenter

While still having the datacenter selected on the left hand side tree, click the **VM Flow** tab. Click **Show Report**, then expand the Allowed, Incoming, Categorized & Uncategorized, Intra Categories to learn the details of all the traffic flowing in and out of your virtual environment.

Application	Sessions	Packets	Bytes	VMWall
ALLOWED	669	17,539	2,402,853	
TCP	158	11,296	2,050,812	
INCOMING	138	8,529	1,197,896	
CATEGORIZED	138	8,529	1,197,896	
HTTP	2	20	2,278	
MS-RPC	0	3,300	145,760	
NBSS	0	284	14,200	
HTTPS	136	2,565	930,114	
CRM-DB(10.20.129.68)	4	59	8,943	
CRM-WWW(10.20.129.6	132	2,506	921,171	
10.20.129.248	132	2,506	921,171	
MS-DS	0	2,360	105,544	
UNCATEGORIZED	0	0	0	
OUTGOING	0	3	180	
INTRA	20	2,764	852,736	
CATEGORIZED	10	744	86,434	
SSH	10	744	86,434	
CRM-DB(10.20.129.68)	2	102	13,266	
CRM-WWW(10.20.12	2	102	13,266	
CRM-WWW(10.20.129.6	8	642	73,168	
CRM-DB(10.20.129.6	8	642	73,168	
UNCATEGORIZED	10	2,020	766,302	
3306	10	2,020	766,302	
CRM-DB(10.20.129.68)	10	2,020	766,302	
CRM-WWW(10.20.12	10	2,020	766,302	
INTRA_HOST	0	0	0	
UDP	511	1,022	213,545	
INCOMING	0	0	0	
OUTGOING	511	1,022	213,545	
CATEGORIZED	511	1,022	213,545	
DNS	511	1,022	213,545	
10.20.148.1	511	1,022	213,545	
CRM-DB(10.20.129.6	400	800	164,602	
CRM-WWW(10.20.12	111	222	48,943	
UNCATEGORIZED	0	0	0	
INTRA	0	0	0	
INTRA_HOST	0	0	0	
ICMP	0	1,544	138,496	
ECHO REPLY	0	772	69,248	
INCOMING	0	0	0	
OUTGOING	0	550	50,600	
INTRA	0	222	18,648	
CRM-DB(10.20.129.68)	0	210	17,640	
CRM-WWW(10.20.129.6	0	210	17,640	
CRM-WWW(10.20.129.69)	0	12	1,008	
CRM-DB(10.20.129.68)	0	12	1,008	

Figure 13. VM Flow report for datacenter

Look for the traffic flows generated earlier. For example, Figure 14 shows the incoming HTTPS traffic coming from the Windows test desktop 10.20.129.248 going to the web server CRM-WWW.

Application	Sessions	Packets	Bytes	VMWall
ALLOWED	669	17,539	2,402,853	
TCP	158	11,296	2,050,812	
INCOMING	138	8,529	1,197,896	
CATEGORIZED	138	8,529	1,197,896	
HTTP	2	20	2,278	
MS-RPC	0	3,300	145,760	
NBSS	0	284	14,200	
HTTPS	136	2,565	930,114	
CRM-DB(10.20.129.68)	4	59	8,943	
CRM-WWW(10.20.129.6	132	2,506	921,171	
10.20.129.248	132	2,506	921,171	
MS-DS	0	2,360	105,544	
UNCATEGORIZED	0	0	0	

Figure 14. HTTPS traffic from test system to Web server

Under the outgoing traffic category we can see Intra-VM traffic. Figure 15 shows the SSH sessions established between the protected virtual machines.

OUTGOING	0	3	180	
INTRA	20	2,764	852,736	
CATEGORIZED	10	744	86,434	
SSH	10	744	86,434	
CRM-DB(10.20.129.68)	2	102	13,266	
CRM-WWW(10.20.12	2	102	13,266	
CRM-WWW(10.20.129.6	8	642	73,168	
CRM-DB(10.20.129.6	8	642	73,168	
UNCATEGORIZED	10	2,020	766,302	
3306	10	2,020	766,302	
CRM-DB(10.20.129.68)	10	2,020	766,302	
CRM-WWW(10.20.12	10	2,020	766,302	
INTRA_HOST	0	0	0	

Figure 15. SSH traffic between Web and DB tiers

Figure 16 shows DNS requests coming from the protected virtual machines going out to a DNS server with IP 10.20.148.1 that is located outside the datacenter. It also shows the ping (ICMP) tests done earlier between the protected virtual machines.

UDP	511	1,022	213,545	
INCOMING	0	0	0	
OUTGOING	511	1,022	213,545	
CATEGORIZED	511	1,022	213,545	
DNS	511	1,022	213,545	
10.20.148.1	511	1,022	213,545	
CRM-DB(10.20.129.6	400	800	164,602	
CRM-WWW(10.20.12	111	222	48,943	
UNCATEGORIZED	0	0	0	
INTRA	0	0	0	
INTRA_HOST	0	0	0	
ICMP	0	1,544	138,496	
ECHO REPLY	0	772	69,248	
INCOMING	0	0	0	
OUTGOING	0	550	50,600	
INTRA	0	222	18,648	
CRM-DB(10.20.129.68)	0	210	17,640	
CRM-WWW(10.20.129.6	0	210	17,640	
CRM-WWW(10.20.129.69)	0	12	1,008	
CRM-DB(10.20.129.68)	0	12	1,008	

Figure 16. DNS and ping traffic

Step 4: Edit port mappings to categorize an uncategorized port.

When an application is not using a well-known port, it will be listed under the Uncategorized section of the VM Flow. It is possible to categorize these ports by editing the port mappings. In Figure 17, port 3306 is MYSQL related traffic between the CRM-WWW and CRM-DB.

OUTGOING	0	3	180	
INTRA	20	2,764	852,736	
CATEGORIZED	10	744	86,434	
SSH	10	744	86,434	
CRM-DB(10.20.129.68)	2	102	13,266	
CRM-WWW(10.20.12	2	102	13,266	
CRM-WWW(10.20.129.6	8	642	73,168	
CRM-DB(10.20.129.6	8	642	73,168	
UNCATEGORIZED	10	2,020	766,302	
3306	10	2,020	766,302	
CRM-DB(10.20.129.68)	10	2,020	766,302	
CRM-WWW(10.20.12	10	2,020	766,302	

Figure 17. Uncategorized traffic

To edit port settings:

1. From the **vShield Manager**, click the datacenter in the left hand side tree.
2. Click the **VM Flow** tab.
3. Click **Edit Port Mappings**.

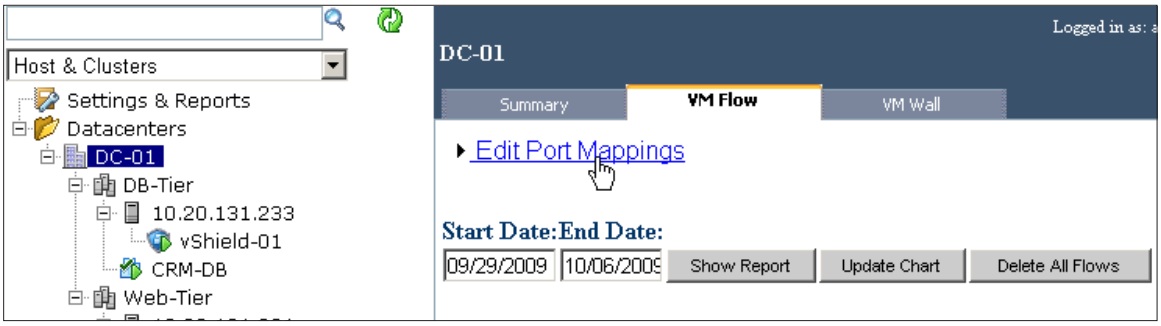


Figure 18. Edit Port Mappings

4. Click any of the rows in the **Port Mappings** table to insert a new port mapping, for example click the FTP row followed by clicking **Add**. A new port mapping appears in red font.

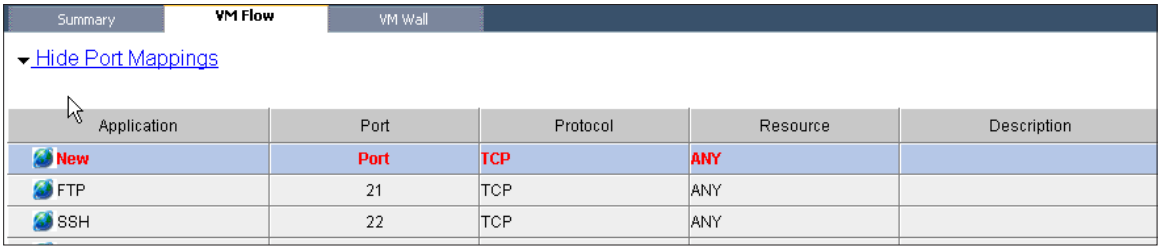


Figure 19. Adding new application protocol

5. Modify this port mapping by double-clicking each column and typing the correct information. In this case the port mapping created is for MySQL on port 3306. A description is also added to clairfy what this is used for.

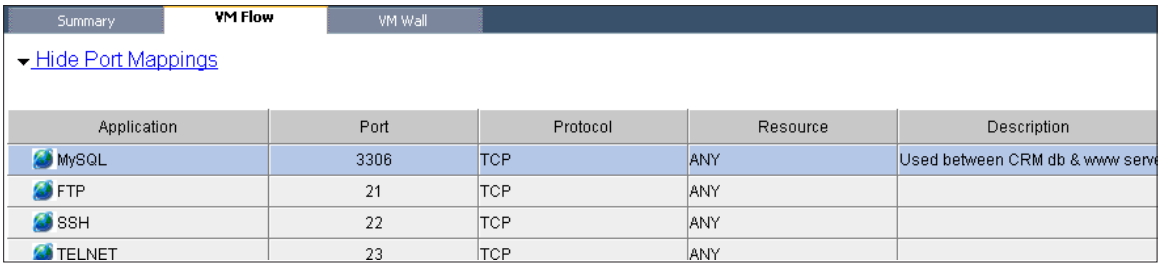


Figure 20. MySQL protocol added

Now the traffic for port 3306 will show up as MySQL in the Categorized section of the VM Flow table. See Figure 21.

ALLOWED	34	2,039	423,472	
TCP	5	1,579	406,221	
INCOMING	5	1,579	406,221	
CATEGORIZED	5	1,579	406,221	
SUNRPC	1	9	540	
MS-RPC	0	294	13,120	
NBSS	0	26	1,300	
MS-DS	0	236	10,540	
MySQL	4	1,014	380,721	
CRM-DB(10.20.129.68)	4	1,014	380,721	
CRM-WWW(10.20.12	4	1,014	380,721	

Figure 21. Newly-categorized traffic

Step 5: Create VM Wall Rules

In this step, VMware will generate firewall rules via the VM Wall tab. These rules can be IP/Subnet based just like you would on a traditional firewall. However by leveraging the container labels such as datacenter and cluster names to create these rules, your configuration is much simpler, less error-prone, and automatically adapts when virtual machines are added or removed from this environment. In previous steps you tested connectivity to and from the virtual machines.

VMware will create rules at different levels of the virtual datacenter to achieve the following:

1. Allow MySQL traffic between the front-end web cluster and the back-end cluster using container-based rules.
2. Allow DNS traffic from outside the virtual datacenter into the web and database servers using IP-based rules.
3. Deny HTTP from outside the virtual datacenter into the virtual datacenter.
4. Allow HTTPS from outside the virtual datacenter into the Web-Tier cluster only.
5. Deny all other incoming traffic into the virtual datacenter.

Allow MySQL traffic

This step will allow MySQL traffic between the front-end web cluster and the back-end cluster using container-based rules.

1. Click the **Datacenter** on the left hand side **Inventory** view of the vShield Manager.
2. Click the **VM Wall** tab and under Data High Precedence Rules enter a new rule by double-clicking each field and entering the following:
   - Source: Web-Tier Cluster
   - Destination: DB-Tier Cluster
   - Destination Application: MySQL
   - Destination Port: This is filled in automatically for this application
   - Protocol: TCP in this case
   - Action: ALLOW

3. Click **Commit**.

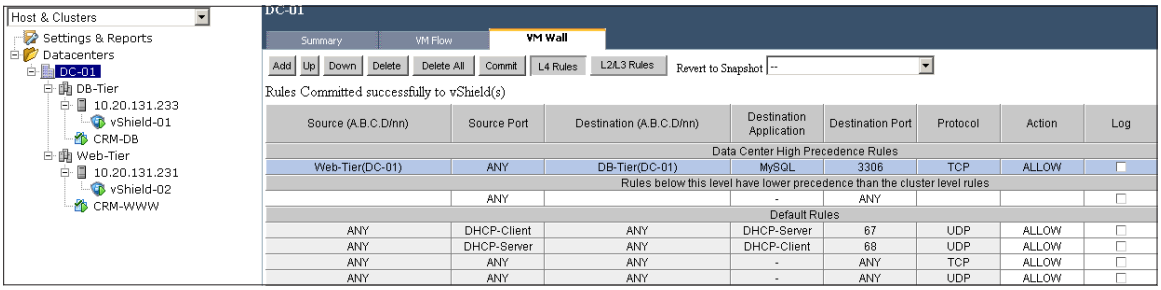


Figure 22. Container-based rule for MySQL

Allow DNS

This step will allow DNS traffic from the virtual datacenter to the physical DNS servers using IP-based rules.

1. At the Datacenter level, highlight the new Datacenter rule that was created and click **Add** in the **VM Wall** table.
2. Enter a new rule by double-clicking each field and entering the following:
   - Source: DC-01
   - Destination: type the IP address of the DNS server
   - Destination Application: DNS
   - Destination Port: This is filled in automatically for this application
   - Protocol: UDP in this case
   - Action: ALLOW
3. Click **Commit**.

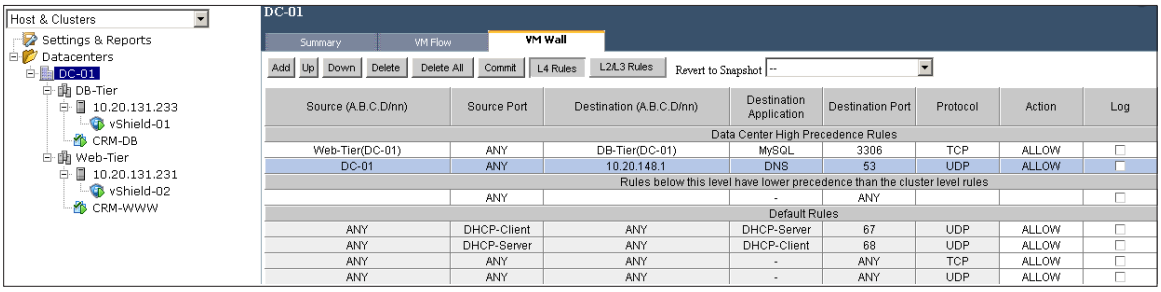


Figure 23. IP-based rule for DNS

Deny HTTP

This step will deny HTTP from outside the virtual datacenter into the virtual datacenter.

1. Still at the Datacenter level, highlight the new Datacenter rule that was created in the previous step and click **Add** in the **VM Wall** table.
2. Enter a new rule by double-clicking each field and entering the following:
   - Source: Outside DC-01
   - Destination: DC-01
   - Destination Application: HTTP
   - Destination Port: This is filled in automatically for this application
   - Protocol: TCP in this case
   - Action: DENY
3. Click **Commit**.

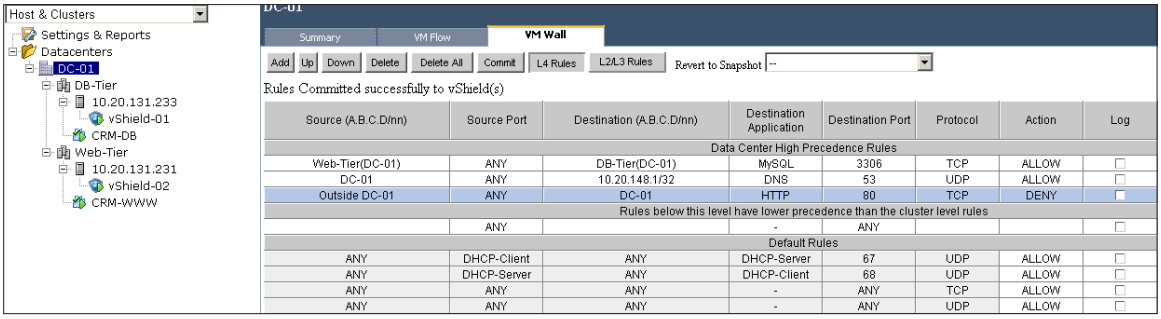


Figure 24. Container-based rule for HTTP

Allow HTTPS

This step will allow HTTPS from outside the virtual datacenter into the Web-Tier cluster only.

1. Click the **Web-Tier** cluster to create a cluster level rule. You will notice the Datacenter rules are present, however, they are grayed out since they cannot be modified at this level.
2. Click the empty cluster level rule and enter a new rule by double-clicking each field and entering the following:
   - Source: Outside DC-01
   - Destination: Web-Tier (DC-01)
   - Destination Application: HTTPS
   - Destination Port: This is filled in automatically for this application
   - Protocol: TCP in this case
   - Action: ALLOW
3. Click **Commit**.

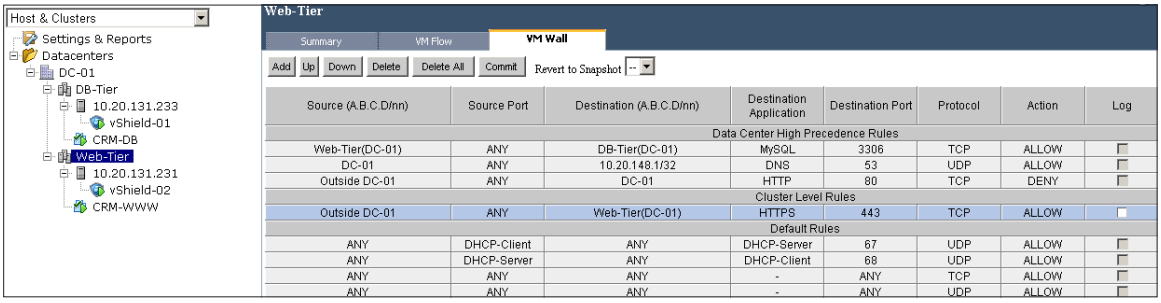


Figure 25. Container-based rule for HTTPS

Default Deny

This step will deny all other incoming traffic into the virtual datacenter.

1. Select the **Datacenter DC-01** from the left hand side Inventory tree to go back to the Datacenter level rules.
2. Look for the Any/Any TCP and UDP default rules and change both of them from ALLOW to DENY.
3. Click **Commit**.

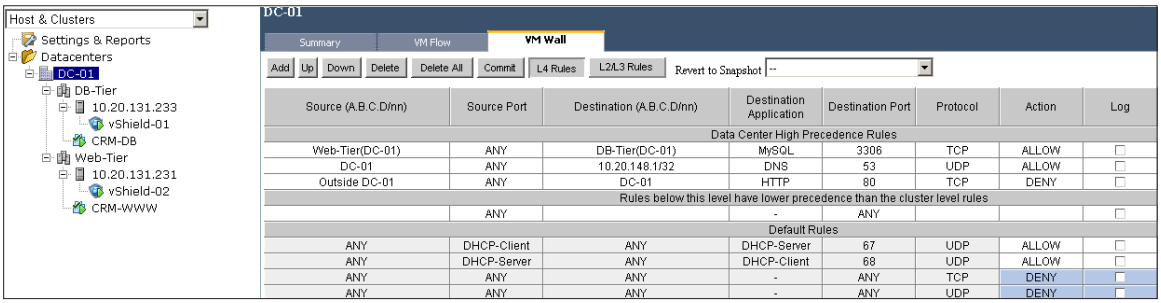


Figure 26. Default Deny rule

The rules created should look like Figure 27 from the Datacenter level:

Source (A.B.C.D/nn)	Source Port	Destination (A.B.C.D/nn)	Destination Application	Destination Port	Protocol	Action	Log	Notes
Data Center High Precedence Rules								
Web-Tier(DC-01)	ANY	DB-Tier(DC-01)	MySQL	3306	TCP	ALLOW	☐	
DC-01	ANY	10.20.148.1/32	DNS	53	UDP	ALLOW	☐	
Outside DC-01	ANY	DC-01	HTTP	80	TCP	DENY	☐	
Rules below this level have lower precedence than the cluster level rules								
	ANY		-	ANY			☐	
Default Rules								
ANY	DHCP-Client	ANY	DHCP-Server	67	UDP	ALLOW	☐	
ANY	DHCP-Server	ANY	DHCP-Client	68	UDP	ALLOW	☐	
ANY	ANY	ANY	-	ANY	TCP	DENY	☐	
ANY	ANY	ANY	-	ANY	UDP	DENY	☐	

Figure 27. Datacenter level rules

From the DB-Tier Cluster level, they should look like Figure 28:

Source (A.B.C.D/nn)	Source Port	Destination (A.B.C.D/nn)	Destination Application	Destination Port	Protocol	Action	Log
Data Center High Precedence Rules							
Web-Tier(DC-01)	ANY	DB-Tier(DC-01)	MySQL	3306	TCP	ALLOW	☐
DC-01	ANY	10.20.148.1/32	DNS	53	UDP	ALLOW	☐
Outside DC-01	ANY	DC-01	HTTP	80	TCP	DENY	☐
Cluster Level Rules							
	ANY		-	ANY			☐
Default Rules							
ANY	DHCP-Client	ANY	DHCP-Server	67	UDP	ALLOW	☐
ANY	DHCP-Server	ANY	DHCP-Client	68	UDP	ALLOW	☐
ANY	ANY	ANY	-	ANY	TCP	DENY	☐
ANY	ANY	ANY	-	ANY	UDP	DENY	☐

Figure 28. DB tier rules

From the Web-Tier Cluster level they, should look like Figure 29:

Source (A.B.C.D/nn)	Source Port	Destination (A.B.C.D/nn)	Destination Application	Destination Port	Protocol	Action	Log
Data Center High Precedence Rules							
Web-Tier(DC-01)	ANY	DB-Tier(DC-01)	MySQL	3306	TCP	ALLOW	☐
DC-01	ANY	10.20.148.1/32	DNS	53	UDP	ALLOW	☐
Outside DC-01	ANY	DC-01	HTTP	80	TCP	DENY	☐
Cluster Level Rules							
Outside DC-01	ANY	Web-Tier(DC-01)	HTTPS	443	TCP	ALLOW	☐
Default Rules							
ANY	DHCP-Client	ANY	DHCP-Server	67	UDP	ALLOW	☐
ANY	DHCP-Server	ANY	DHCP-Client	68	UDP	ALLOW	☐
ANY	ANY	ANY	-	ANY	TCP	DENY	☐
ANY	ANY	ANY	-	ANY	UDP	DENY	☐

Figure 29. Web tier rules

Step 6: Test rule enforcement

Now that all rules have been created, ensure the rules are being enforced by sending traffic to, from and within the virtual machines. Refer to the final rules configurations in Figures RULES_DATACENTER, RULES_DB, RULES_WEB.

Test the HTTP datacenter rule

This rule can be tested by launching a web browser from a computer outside of the datacenter and pointing it to the IP address of the CRM-WWW server using the HTTP protocol. You should NOT be able to reach the web page.

Test the HTTPS Cluster rule

This rule can be tested by launching a web browser from a computer outside of the datacenter and pointing it to the IP address of the CRM-WWW server using the HTTPS protocol. You should be able to reach the login web page for the CRM application.

Test the DNS Datacenter IP based rule

To test this rule, open a console to one of the protected virtual machines and run an nslookup for a domain or host.

The domain name service lookup should be successful.

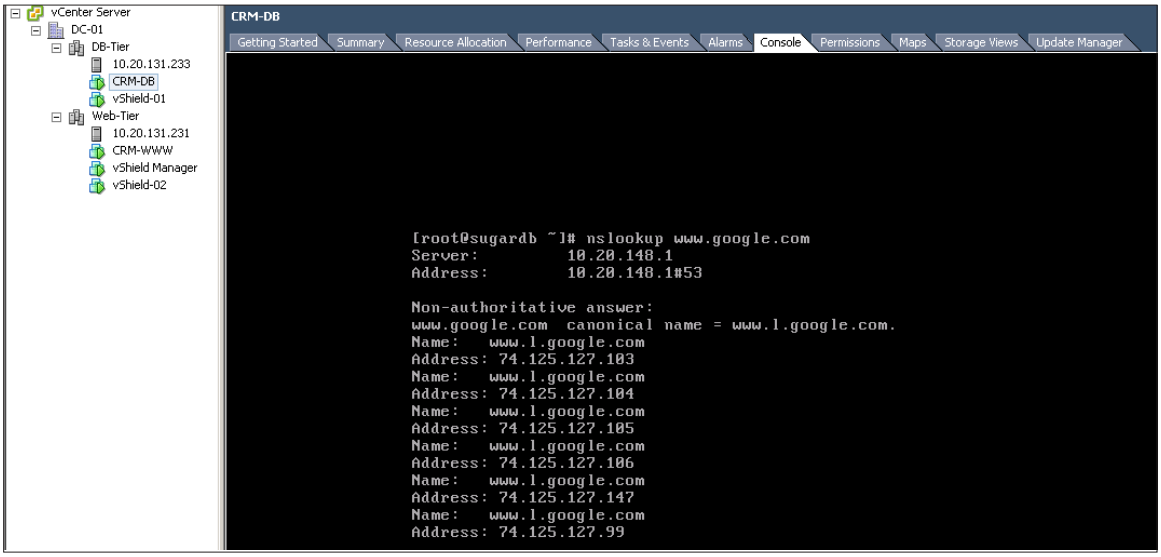


Figure 30. Testing DNS rule

Test the MySQL Datacenter rule

The connectivity of the CRM software to the back-end MySQL database can be tested by logging in to the CRM software, which establishes the MySQL connection. Launch a web browser from a computer outside of the datacenter and pointing it to the IP address of the CRM-WWW server using the HTTPS protocol. At the login web page for the CRM application, enter the proper credential to log in. You should be able to log in successfully, thus indicating connectivity to the MySQL database.

Test the Default Deny rule

This rule can be tested by trying to connect to one of the protected virtual machines on a service or port that would normally be open. Try to SSH from the remote test machine to any of the virtual machines. The connection should fail since SSH is not explicitly allowed in any rule.

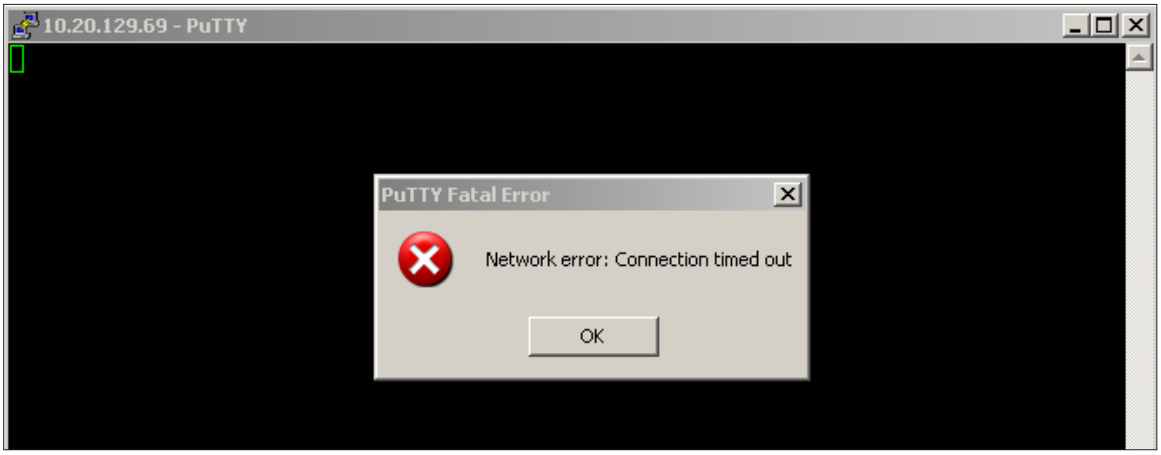
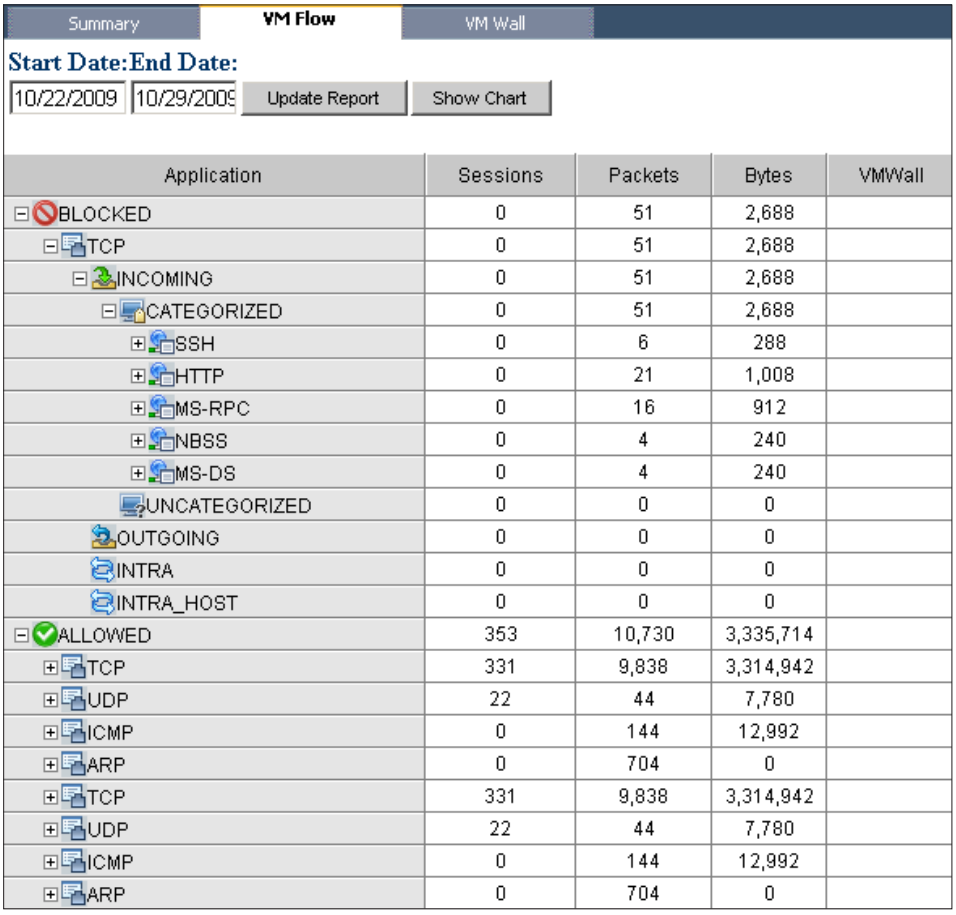


Figure 31. Testing Default Deny rule

After having done all the rule testing, the VM Flow page should be populated with 'Blocked' traffic as well as 'Allowed' traffic.



Application	Sessions	Packets	Bytes	VMWall
BLOCKED	0	51	2,688	
TCP	0	51	2,688	
INCOMING	0	51	2,688	
CATEGORIZED	0	51	2,688	
SSH	0	6	288	
HTTP	0	21	1,008	
MS-RPC	0	16	912	
NBSS	0	4	240	
MS-DS	0	4	240	
UNCATEGORIZED	0	0	0	
OUTGOING	0	0	0	
INTRA	0	0	0	
INTRA_HOST	0	0	0	
ALLOWED	353	10,730	3,335,714	
TCP	331	9,838	3,314,942	
UDP	22	44	7,780	
ICMP	0	144	12,992	
ARP	0	704	0	
TCP	331	9,838	3,314,942	
UDP	22	44	7,780	
ICMP	0	144	12,992	
ARP	0	704	0	

Figure 32. Blocked and Allowed traffic

Step 7: Modify or adjust rules if necessary

If there are any rules that are not working as expected, you can use the VM Flow page to assist in the troubleshooting of VM Wall rules. Identify a server you can test with, follow its traffic flows, and look for its categorization under either 'Blocked' or 'Allowed' traffic. Create or modify rules accordingly.

Step 8. Configure and test Layer2/Layer3 rules

Even if all the configured rules work as expected, you are still able to ping the protected servers. This can be confirmed by pinging one of the protected virtual machines from the external computer. The reason is that all the rules configured thus far are Layer 4 rules, while ping operates using a different layer protocol. In order to block ping and other ICMP traffic, create a Layer2/Layer3 rule.

While pinging one of the protected virtual machines, perform the following steps.

1. Click the **Datacenter DC-01** on the left hand side inventory tree.
2. From the **VM Wall** page click **L2/L3 Rules**.
3. Click the empty datacenter level rule and enter a new rule by double-clicking each field and entering the following:
   - Source: Outside DC-01
   - Destination: DC-01
   - Protocol: ICMP ANY
   - Action: DENY
4. Click **Commit**.

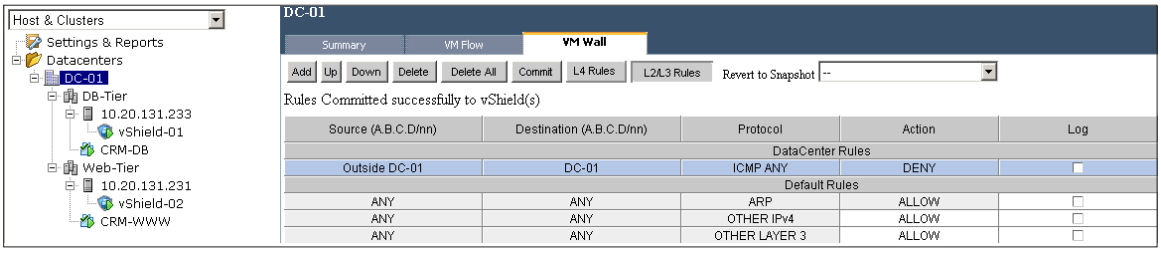


Figure 33. Rule for blocking ping

You should see ping start to time out shortly afterwards.

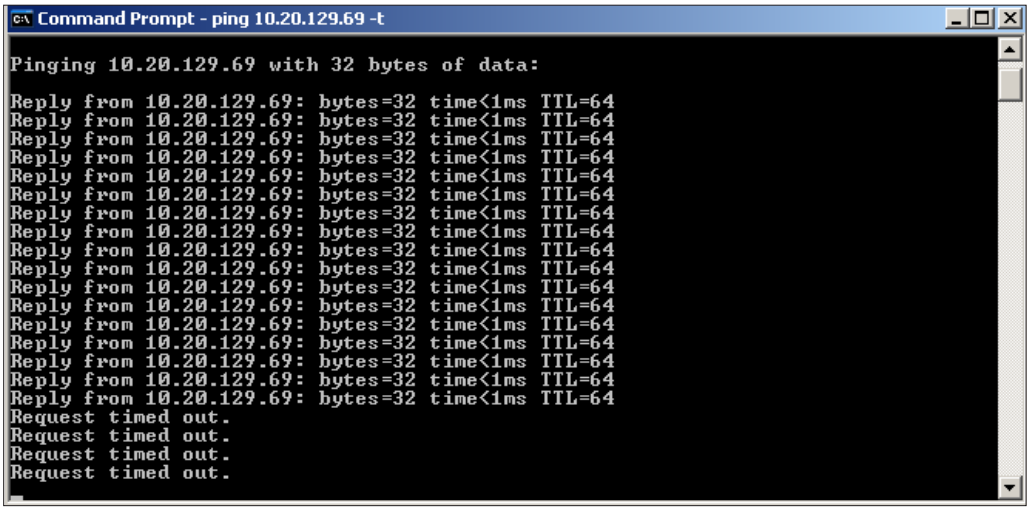


Figure 34. Testing ping rule

Step 9. Delete a VM Wall Rule

To delete a rule, select it from the VM Wall table, click **Delete** followed by **Commit**. You can confirm the rule no longer applies by attempting the connection that the rule had previously governed. If you need to start all over you can use the 'Delete All' button to remove all rules.

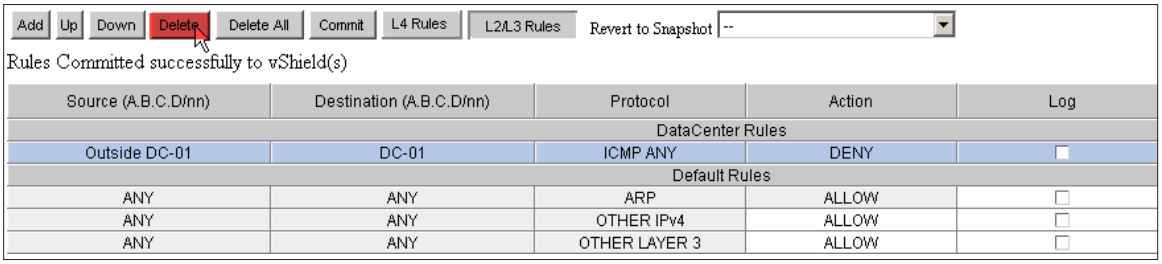


Figure 35. Deleting a rule

Other Exercises

You can use the VM Flow and Summary table to answer the following questions in real-world deployments.

What Are the Busiest Applications?

Identify resource utilization by using the VM Flow chart to determine which applications are the busiest. The Sessions/hr chart displays the number of sessions for the Top 10 busiest applications. Once you identify busy applications, you can use the VM Flow report to view the relevant details for each transaction.

What Are the Busiest Clients?

Similarly to testing for busiest applications, you can view the applications most requested by clients at different periods in time in the VM Flow Client Kbytes/hr chart. In the VM Flow report, you can view granular details on application use from a source to a destination. You can use this data to create a VM Wall rule to allow or deny traffic from a client to a specific virtual machine.

What Virtual Machines Participate in an Application?

Knowing that you have an application deployed within your datacenter does not always mean there is a clear mapping of which virtual machines serve it. The VM Flow report provides mapping of applications to virtual machines allowing you to determine utilization of your individual virtual machines based on number of sessions, packets, and bytes served.

What Applications Run on My Virtual Machines?

Due to the ease of deploying new virtual machines, often there is limited knowledge of the applications deployed within a virtual environment. The Summary table lists your guest virtual machines with the applications discovered to be active on each. Using this information, you can determine if an application should or should not be active on a virtual machine.

Next Steps

In this guide, the key-use cases of vShield Zones have been presented. Please refer to the VMware vShield Zones User's Guide for more details.

VMware Contact Information

For additional information or to purchase VMware vShield Zones, VMware's global network of solutions providers are ready to assist. If you would like to contact VMware directly, you can reach a sales representative at 1-877-4VMWARE (650-475-5000 outside North America) or email sales@vmware.com. When emailing, please include the state, country, and company name from which you are inquiring.

Providing Feedback

VMware appreciates your feedback on the material included in this guide, and in particular, would be grateful for any guidance on the following topics:

- How useful was the information in this guide?
- What other specific topics would you like to see covered?
- Overall, how would you rate this guide?

Please send your feedback to the following address: tmdocfeedback@vmware.com, with "VMware vShield Zones Reviewer's Guide" in the subject line. Thank you for your help in making this guide a valuable resource.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Copyright © 2009 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: VMW_09Q4_RG_vShield_EN_P27_R1