Introduction to vShield Zones

vShield Zones 1.0 Update 1

EN-000188-00

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About This Book

This manual, *Introduction to vShield Zones*, provides information about the features and functionality of VMware® vShield Zones.

Intended Audience

This manual is intended for anyone who needs to familiarize themselves with the components and capabilities of vShield Zones. The information in this manual is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

Document Feedback

VMware welcomes your suggestions for improving our documentation. If you have comments, send your feedback to docfeedback@vmware.com.

vShield Zones Documentation

The following documents comprise the vShield Zones documentation set:

- *vShield Zones Administration Guide*
- *vShield Zones Quick Start Guide*
- *Introduction to vShield Zones*

Technical Support and Education Resources

The following sections describe the technical support resources available to you. To access the current version of this book and other books, go to http://www.vmware.com/support/pubs.

Online and Telephone Support

To use online support to submit technical support requests, view your product and contract information, and register your products, go to http://www.vmware.com/support.

Customers with appropriate support contracts should use telephone support for the fastest response on priority 1 issues. Go to http://www.vmware.com/support/phone_support.

Support Offerings

To find out how VMware support offerings can help meet your business needs, go to http://www.vmware.com/support/services.

VMware Professional Services

VMware Education Services courses offer extensive hands-on labs, case study examples, and course materials designed to be used as on-the-job reference tools. Courses are available onsite, in the classroom, and live online. For onsite pilot programs and implementation best practices, VMware Consulting Services provides offerings to help you assess, plan, build, and manage your virtual environment. To access information about education classes, certification programs, and consulting services, go to http://www.vmware.com/services.

vShield Zones Introduction

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.

This chapter includes the following topics:

vShield Zones Components

vShield Zones includes components and services essential for analyzing traffic and protecting virtual machines. vShield Zones can be configured through a Web-based user interface and a command line interface (CLI).

vShield Zones components are packaged as Open Virtualization Format (OVF) files. To run vShield Zones, you need one vShield Manager OVF and one vShield agent OVF.

vShield Manager

The vShield Manager is the centralized network management component of vShield Zones, and is installed as a virtual machine on any ESX™ host in your vCenter Server environment. A vShield Manager can run on a different ESX host from your vShield agents.

You can access the vShield Manager user interface by using a Web browser. The user interface lets administrators install, configure, and maintain the entire vShield Zones deployment. The vShield Manager user interface leverages the VMware Infrastructure SDK to display a copy of the vSphere Client inventory panel, and includes the Hosts & Clusters and Networks views.

You can connect to the vShield Manager user interface using one of the following supported Web browsers:

- Internet Explorer 5.x and later
- Mozilla Firefox 1.x and later
- Safari 1.x or 2.x

vShield Agent

The vShield agent is the active security component of vShield Zones. Each vShield agent provides application-aware traffic analysis and stateful firewall protection by inspecting network traffic and determining access based on a set of rules. A vShield agent regulates traffic based on zones of trust, separating traffic into unprotected and protected zones. The virtual machines protected by a vShield agent reside in the protected zone. All traffic destined for the protected virtual machines enters from the unprotected zone.

Using the vSphere Client, you can install the vShield agent OVF file as a template or virtual machine. After the package is installed in the vSphere Client, you use the vShield Manager to complete installation. If you installed the vShield agent package as a template, you can reference the template from the vShield Manager to install multiple vShield agents as virtual machines into your vCenter Server environment. You can install a vShield agent on any vSwitch that homes a physical NIC. As an ESX host can have multiple physical NICs, you can install multiple vShield agents on a single ESX host.

When installed from a referenced template, the vShield agent installation process performs the following steps:

1 Creates a clone of the vSwitch host.

   This vSwitch clone does not include a NIC. The name of the vSwitch clone includes the name of the vSwitch host with _VS appended: vSwitch1_VS.

2 Creates a protected zone port group, VSprot_*vShield-name*, and attaches this port group to the vSwitch host.

3 Creates a management port group, VSmgmt_*vShield-name*, on the vSwitch host for the vSwitch agent's management interface.

4 Creates an unprotected zone port group, VSunprot_*vShield-name*, and attaches this port group to the vSwitch clone.

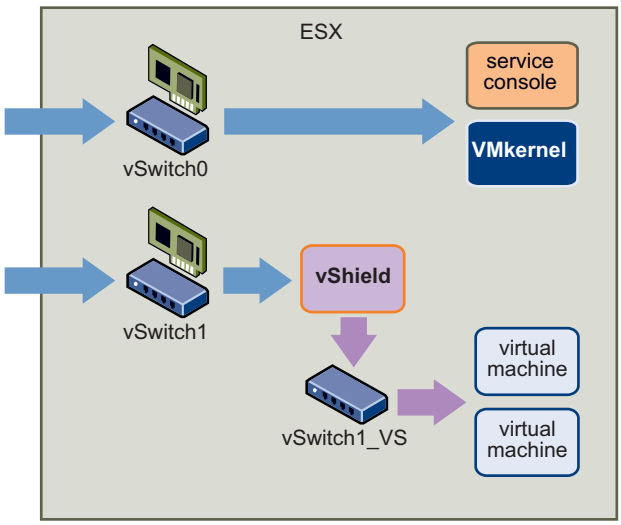
5 Connects and powers on the vShield agent.

6 Attaches the virtual interfaces on the vShield agent to the unprotected and protected port groups.

7 Moves the virtual machines from the vSwitch host to the vSwitch clone.

   If the vShield Manager virtual machine resides on the same vSwitch, it is not moved. During vShield Manager installation, you created a port group called **`vsmgmt`** in which to place the vShield Manager. vShield agent installation recognizes this port group name and ignores any virtual machines in this port group.

Figure 1. Installation of a vShield agent on a vSwitch



Each installed vShield agent monitors all incoming and outgoing traffic on the vSwitch host, including traffic between virtual machines on the vSwitch host and vSwitch clone. As traffic passes through a vShield agent, each session header is inspected to catalog the data. A profile is created for each virtual machine detailing the operating system, applications, and ports used in network communication. Based on this information, the vShield agent allows ephemeral port usage by permitting dynamic protocols such as FTP and RPC to pass through while maintaining lockdown on ports 1024 and higher.

By design, each vShield agent allows up to 40,000 concurrent sessions.

You cannot protect the Service Console or VMkernel components with a vShield agent as these components are not virtual machines.

Key Features

vShield Zones offers a rich set of features aimed at providing information on the traffic to and from your virtual machines and protecting the virtual machines in your virtual datacenter.

Firewall Protection

vShield Zones provides firewall protection by enforcing global and local access control policies across all deployed vShield agents. vShield Zones enables you to build firewall rules based on general traffic direction, application protocols and ports, and specific source-to-destination parameters.

Within the vShield Manager user interface, the **VM Wall** tab presents the firewall function of vShield Zones. VM Wall is a centralized, hierarchical access control list. You can manage VM Wall access rules at the datacenter and cluster levels, providing a consistent set of rules across multiple vShield agents in these containers. As virtual machine membership in these containers can change dynamically, vShield Zones maintains the state of existing sessions without requiring reconfiguration of access rules.

Default Rules

By default, the VM Wall enforces a set of rules allowing traffic to pass through all vShield agents. These rules appear in the **Default Rules** section of the VM Wall table. The default rules cannot be deleted or added to. However, you can change the **Action** element of each rule from **Allow** to **Deny**.

Layer 4 Rules and Layer 2/Layer 3 Rules

The **VM Wall** tab offers two sets of configurable rules: L4 (Layer 4) rules and L2/L3 (Layer 2/Layer 3) rules. Layers refer to layers of the Open Systems Interconnection (OSI) Reference Model.

Layer 4 rules govern TCP and UDP transport of Layer 7, or application-specific, traffic. Most of your interaction with VM Wall rules centers on managing Layer 4 rules.

Layer 2/Layer 3 rules monitor traffic from ICMP, ARP, and other Layer 2 and Layer 3 protocols. By default, the VM Wall rules governing Layer 2 and Layer 3 allow all traffic to pass. Layer 2/Layer 3 rules are enforced at the datacenter level only.

Hierarchy of VM Wall Rules

Each vShield agent enforces VM Wall rules in top-to-bottom ordering. A vShield agent checks each traffic session against the top rule in the VM Wall table before moving down the subsequent rules in the table. The first rule in the table that matches the traffic parameters is enforced.

VM Wall offers container-level and custom priority precedence configurations:

- Container-level precedence refers to recognizing the datacenter level as being higher in priority than the cluster level. When a rule is configured at the datacenter level, the rule is inherited by all clusters and vShield agents therein. A cluster-level rule is only applied to the vShield agents within the cluster.

- Custom priority precedence refers to the option of assigning high or low precedence to rules created at the datacenter level. **Data Center High Precedence Rules** work in the same manner as container-level precedence rules. **Data Center Low Precedence Rules** are lower in precedence than **Cluster Level Rules**, while being higher in priority than the pre-configured **Default Rules**. This flexibility allows you to recognize multiple layers of applied precedence.

In the VM Wall table, the rules are enforced according to the following hierarchy:

1 **Data Center High Precedence Rules:** A set of global access rules created at the datacenter level that are highest in priority.

2 **Cluster Level Rules:** A set of cluster-specific access rules that are lower in priority than datacenter high precedence rules.

3 **Data Center Low Precedence Rules:** A set of global access rules created at the datacenter level that are lower in precedence than cluster-level rules.

4 **Default Rules:** Default set of global access rules that are lowest in priority.

As a general policy, make sure lower precedence rules are not in conflict with higher precedence rules.

Planning VM Wall Rule Enforcement

Using VM Wall, you can configure allow and deny rules based on your network policy. The following policies represent common VM Wall configurations:

- You keep the default rules to allow all traffic, and add deny rules at the datacenter and cluster levels based on traffic statistics or manual configuration. In this scenario, if a session does not match any of the custom deny rules, the vShield agent allows the traffic to pass.
- You change the action status of the default rules from **Allow** to **Deny**, and add allow rules at the datacenter and cluster levels for specific systems and applications. In this scenario, if a session does not match any of the custom allow rules, the vShield agent drops the session before it reaches its destination. If you change all of the default rules to deny all traffic without creating allow rules, the vShield agent drops all incoming and outgoing traffic.

Traffic Analysis

A vShield agent inspects each passing packet header to gather information about each session to and from your virtual machines. Session details includes the source, destination, direction, and service being requested. The traffic data gathered by all deployed vShield agents is aggregated in the vShield Manager user interface.

In the vShield Manager, the **VM Flow** tab presents traffic analysis data. This data includes the number of sessions, packets, and bytes transmitted. VM Flow is useful as a forensic tool to detect rogue services, examine inbound and outbound sessions, and create VM Wall access rules. Traffic data can also be used for network troubleshooting, such as detecting high or low traffic usage by a service or client.

The **VM Flow** tab displays throughput statistics as returned by all the active vShield agents within a datacenter or cluster container, or for a single vShield agent at the individual virtual machine level. VM Flow organizes statistics in three charts according to the application protocols used in client-server communications. Each color in the charts represents a different application protocol. This charting method enables you to track your server resources per application.

By default, VM Flow displays traffic statistics for all inspected flows within the last seven days.

VM Flow includes a comprehensive report of traffic data on a session-by-session basis. You can drill down in the report data to view statistics for specific source-to-destination pairs. Based on this data, you can create granular VM Wall allow and deny rules.

Virtual Machine Discovery

After installation, each vShield agent inspects all passing network traffic to build an inventory of the operating systems, applications, and open ports on each virtual machine. This inspecting process is called discovery. The vShield Manager presents discovered virtual machine inventory under the **VM Inventory** tab.

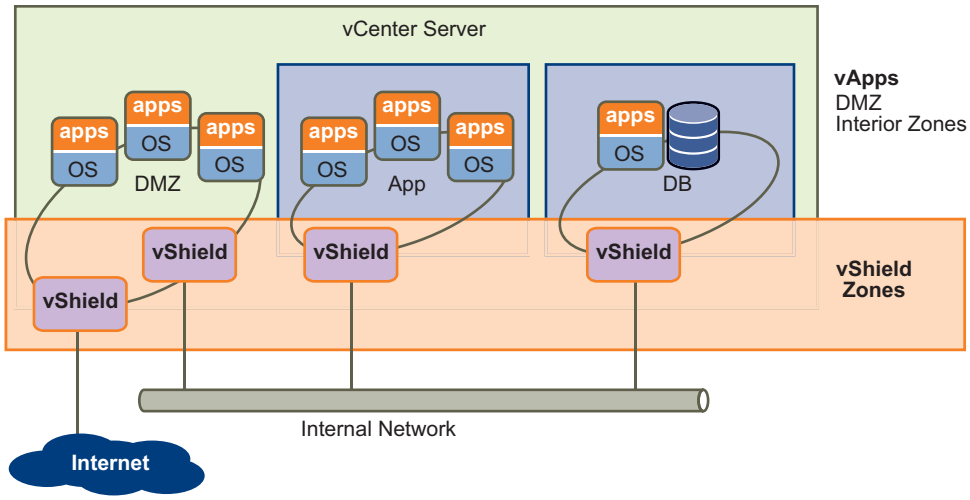
If traffic to an unprotected virtual machine is discovered by a vShield agent, that virtual machine is highlighted in red in the inventory panel of the vShield Manager user interface. This enables you to quickly identify vulnerable servers and protect them with a new or existing vShield agent. Each virtual machine that is identified as unprotected by the discovery process is outlined in red in the inventory panel of the vShield Manager. This enables you to identify and protect all of your virtual machines.

The vShield agent discovery operation can also be used to scan virtual machines, identifying open applications which might present security risks.

Deployment Scenarios

Using vShield Zones, you can build secure zones for a variety of virtual machine deployments. You can isolate virtual machines based on specific applications, VLAN segmentation, or custom compliance factors. Once you determine your zoning policies, you can deploy vShield Zones to enforce access rules to each of these zones.

Figure 2. Securing Specific Zones in Your Virtual Network with vShield Zones



Protecting the DMZ

The DMZ is a mixed trust zone. Clients enter from the Internet for Web and email services, while services within the DMZ might require access to services inside the internal network. A common example of a DMZ service requiring an internal service is Microsoft Exchange. Microsoft Outlook Web Access (OWA) commonly resides in the DMZ cluster, while the Microsoft Exchange back end is in the internal cluster. On the internal cluster, you can create VM Wall rules to allow only Exchanged-related requests from the DMZ, identifying specific source-to-destination parameters. From the DMZ cluster, you can create rules to allow outside access to the DMZ only to specific destinations using HTTP, FTP, or SMTP.

Isolating VLANs

If you utilize VLAN tags to segment traffic, you can use VM Wall to create smarter access policies. Using VM Wall instead of a physical firewall allows you to collapse or mix trust zones in shared ESX clusters. By doing so, you gain optimal utilization and consolidation from features such as DRS and HA, instead of having separate, fragmented clusters. Management of the overall ESX deployment as a single pool is less complex than having separately managed pools.

For example, you use VLANs to segment virtual machine zones based on logical, organizational, or network boundaries. Leveraging the Virtual Infrastructure SDK, the vShield Manager inventory panel displays a view of your VLAN networks under the Networks view. You can build access rules for each VLAN network to isolate virtual machines and drop untagged traffic to these machines.

Segmenting VMware View™ Users

VMware View users can also benefit from VM Wall access policies. You can create access rules based on directional (for example, outside-to-inside) traffic, dynamic applications such as RDP, or another such requirement to provide access control across different View port groups. For example, you can create port groups to isolate users based on employee status as either permanent or contract. You can then determine access using VM Wall rules from these port groups to the internal network as well as attempts to reach the Internet from virtual machines.

Integrating with Cisco Nexus 1000V Series Switches

You can deploy vShield Zones with Cisco® Nexus™ 1000V Series Switches. vShield Zones provides firewall protection to the virtual machines in Nexus 1000V Virtual Service Domains.

Refer to the *vShield Zones Administration Guide* for more information on integrating vShield Zones with the Cisco Nexus 1000V Series.

Where to Go from Here

Table 1 provides references to vShield Zones documentation and the tasks covered therein.

Documentation for all VMware products is located on the Web at http://www.vmware.com/support/pubs.

Table 1. Documentation

Task	Document
Install vShield Zones.	*vShield Zones Quick Start Guide*
Configure, monitor, and maintain vShield Zones. Install vShield Zones in a vNetwork Distributed Switch environment.	*vShield Zones Administration Guide*