

VIRTUAL SERVER

VIRTUAL DESKTOP

DATA CENTER

BRIANMADDEN

CHANNEL

CLOUD

**SearchVMware.com**

The Web's independent resource for managing VMware environments

ADVERTISEMENT

HOME

NEWS

TOPICS

ITKNOWLEDGE EXCHANGE

TIPS

BLOGS

MULTIMEDIA

WHITE PAPERS

EVENTS

SEARCH this site and the web

SEARCH

Search Powered by Google

SITE INDEX

ADVERTISEMENT

[Home](#) > [VMware Tips](#) > [VMware management, migration and performance](#) > [VMware vShield Zones: What it is and how it works](#)

VMware Tips:

[EMAIL THIS](#)

TIPS & NEWSLETTERS TOPICS

VMWARE MANAGEMENT, MIGRATION AND PERFORMANCE

VMware vShield Zones: What it is and how it works

Eric Siebert, Contributor

07.29.2009

Rating: -4.60- (out of 5)

[Digg This!](#)[StumbleUpon](#)[Del.icio.us](#)[VMware Migration Tips - White Papers](#)

VMware addressed the growing virtual machine (VM) security concern with two vSphere releases: VMsafe and vShield Zones. While VMsafe's application programming interfaces are designed to help third-party vendors create virtualization security products that better secure VMware ESX, vShield Zones is a security tool targets the VMware administrator.

vShield Zones is essentially a virtual firewall designed to protect VMs and analyze virtual network traffic. This three-part series describes vShield Zones, explains how to install it and provides useful management tips. To begin, let's get started with the basics: what vShield Zones is and how it works.

Overview of vShield Zones

vShield Zones is essentially a virtual firewall designed to protect virtual machines and analyze virtual network traffic built on VMware's Blue Lane Technologies acquisition in 2008. The current 1.0 version of vShield Zones is not yet integrated with VMware's new VMsafe technology but VMware plans on using the VMsafe APIs in vSphere in a future release of vShield Zones. vShield Zones is available as a free download with the Advanced, Enterprise and Enterprise Plus editions of ESX and ESXi.



Click to enlarge.

VMware developed vShield Zones to provide some basic capabilities to protect virtual networks in its core product. vShield Zones provides the same basic protection and analysis as some of similar third-party products such as Reflex Systems Virtualization Management Center, Altor Networks Virtual Firewall and Catbird's V-Security, but vShield Zones is not as complex and is a simpler product. The plus side of this is that VMware administrators should find vShield Zones easier to use – you don't have to become a security expert in order to run the security component of your VMware environment. Here is a list of what functionality vShield Zones adds to your virtual network:

- Firewall protection – vShield Zones provides firewall protection across vSwitches using rules that allow and block specific ports, protocols and traffic direction. The firewall function is termed "VM Wall" and provides a centralized, hierarchical access control list at the data center and cluster level. Layer 4 and Layer 2/3 rules are configurable; these are the data link, network and transport layers of the [OSI networking protocol model](#).
- Traffic analysis – All traffic that passes through vShield appliances is inspected. Information on source, destination, direction and service is gathered and aggregated into the vShield Manager. The traffic analysis data is termed "VM Flow" and can be

used for network troubleshooting, investigating suspicious traffic, and to create access rules.

- Virtual Machine Discovery – The vShield agents utilize a discovery process when analyzing traffic which notes the operating system, application and ports in use. Once this information is collected and analyzed it can be used for firewall rule configuration.

VShield Manager and vShield agents

VShield Zones consists of two components, the vShield Manager and vShield agents, both of which are deployed as virtual appliances from the included Open Virtualization Format (OVF) files. VShield Manager is the centralized management device that is used to manage the vShield agents. It configures rules and monitors network traffic. A single vShield Manager can manage vShield agents on multiple ESX/ESXi hosts and is accessed using a Web-based interface. Once you select a vSwitch to protect with vShield Zones, the vShield Manager will deploy the vShield agent on to the host that the vSwitch is located on. The vShield agent is what provides the firewall protection, performs the network traffic analysis and utilizes trust zones which separate traffic into protected and unprotected zones. Network traffic enters from the unprotected zone and goes through the vShield agent to get to the protected zone where the virtual machines reside.

Think of a group of houses that are accessible via an open road that anyone can access. To protect those houses so only authorized visitors can get to them, the houses are moved to an isolated island. To get the island, you have to cross a single bridge. At the bridge entrance is a guard (vShield agent) that only allows visitors on the guest list (firewall rules) to cross the bridge. Additionally he inspects and logs all traffic that passes across the bridge to look for anything suspicious (traffic analysis).

In more technical terms, here's what happens when you deploy a vShield agent.

1. A new VM is created for the vShield agent from the template. This virtual machine (VM) has three virtual network interface cards (vNICs) assigned to it, one for its management interface to talk to the vShield Manager, one to connect to the original vSwitch (vSwitch1) for unprotected traffic (entrance) and the other to connect to the new vSwitch (vSwitch2) that is created for protected traffic (exit) to reach the VMs.
2. A new vSwitch (vSwitch2) is created that has no physical NICs assigned to it.
3. A new port group is created on vSwitch1 for unprotected traffic and a new port group is created on vSwitch2 for protected traffic. The vShield agent's vNICs are connected to both these port groups.
4. All VM port groups from vSwitch1 are created on vSwitch2, the settings for each VM are edited and the NICs are moved to the new port groups on vSwitch2.
5. Once the VMs are all moved to vSwitch2 the original port groups are removed from vSwitch1.

Here is what the vSwitch configuration looks like before the vShield Zones deployment:



[Click to enlarge.](#)

Here's what it looks like after vShield Zones deployment:



[Click to enlarge.](#)

As you can see all traffic must go through the physical NIC on vSwitch1, then through the vShield agent VM, then to the new protected vSwitch1_VS vSwitch where the VMs are located.

The basic requirements for vShield Zones are that you need to have VMware ESX or ESXi 4.0 hosts and vCenter Server 4.0. Beyond that you need to have permission to add and power-on VMs, and you'll need static IP addresses for the vShield Manager and each vShield agent that you deploy

There is, however, an additional requirement that is currently not documented. The vShield Manager VM is created with 2 GB of memory and also has a preset memory reservation of 2 GB. The vShield agents are created with 1 GB of memory and have 1 GB preset memory reservations. Because of these reservations you must ensure you have enough available free physical host memory to satisfy the reservations when the Manager and agents are powered on. While it is possible to edit the VM settings and remove the reservations, it is not recommended, because this can affect the performance of the appliances which can affect their functionality.

Do not increase the amount of memory assigned to the vShield Manager and agents as this will not increase their performance.

There are also [port requirements](#) for the few ports that vShield uses which are listed below:

- Port 22 – Secure Shell, or SSH (Transmission Control Protocol, or TCP) – Used for all communication between the vShield Manager and agents
- Port 123 – Network Time Protocol (User Datagram Protocol, or UDP) – Used for time synchronization of the vShield Manager and agents
- Port 443 – HTTP Secure (TCP) – Used for PCs to access to the web UI for administration of the vShield Manager
- Port 1162 – Simple Network Management Protocol, or SNMP (UDP) – Used to send SNMP trap messages from vShield agents to the vShield Manager. All other statistics, including memory and CPU, use port 22.

Both the vShield Manager and agents use host resources and while the memory and disk usage is static, the CPU usage will vary based on the amount of network traffic that is passing through the agent. There is also some very slight network latency for the traffic passing through the agent due to the additional hops the traffic is taking to pass through the agent en route to the destination VMs. By design, each vShield agent allows up to 40,000 concurrent sessions and there are no throughput limitations as it uses the hardware on which it runs and the resources that are assigned to the agent. The resource usage and overhead for both the vShield Manager and the agents is listed below:

Restore	vShield Manager	vShield Agents
Disk space usage	8 GB	5 GB
Memory usage	2 GB (reserved)	1 GB (reserved)
CPU usage	3-7 %	3-10%
Network latency	N/A	500 microseconds

The vShield Manager can manage up to 50 vShield agents and a single vShield Zones agent can protect up to 500 virtual machines.

In the next part of this tip series, we will cover [how to install and configure the vShield Zones Manager and agent components](#).



Eric Siebert is a 25-year IT veteran with experience in programming, networking, telecom and systems administration. He is a guru-status moderator on the [VMware community VMTN forums](#) and maintains [VMware-land.com](#), a V13 information site.

Rate this Tip

(BAD) ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 (EXCELLENT)

[Digg This!](#) [StumbleUpon](#) [Del.icio.us](#)

DISCLAIMER: Our Tips Exchange is a forum for you to share technical advice and expertise with your peers and to learn from other enterprise IT professionals. TechTarget provides the infrastructure to facilitate this sharing of information. However, we cannot guarantee the accuracy or validity of the material submitted. You agree that your use of the Ask The Expert services and your reliance on any questions, answers, information or other materials received through this Web site is at your own risk.

[HOME](#) | [NEWS](#) | [TOPICS](#) | [ITKNOWLEDGE EXCHANGE](#) | [TIPS](#) | [BLOGS](#) | [MULTIMEDIA](#) | [WHITE PAPERS](#) | [EVENTS](#)

[About Us](#) | [Contact Us](#) | [For Advertisers](#) | [For Business Partners](#) | [Site Index](#) | [RSS](#)

TechTarget provides technology professionals with the information they need to perform their jobs - from developing strategy, to making cost-effective purchase decisions and managing their organizations' technology projects - with its network of [technology-specific websites, events and online magazines](#).

[TechTarget Corporate Web Site](#) | [Media Kits](#) | [Reprints](#) | [Site Map](#)



All Rights Reserved, [Copyright 2007 - 2010](#), TechTarget | [Read our Privacy Policy](#)