

VMware vShield Zones

Policy-Based Network Monitoring and Enforcement for Virtual Machines

AT A GLANCE

VMware® vShield Zones enables network compliance with security policies and industry regulations while adopting the efficiency and flexibility of cloud computing. VMware vShield Zones creates logical zones in the virtual datacenter that span shared physical resources, with each zone representing a distinct level of trust and confidentiality.

BENEFITS

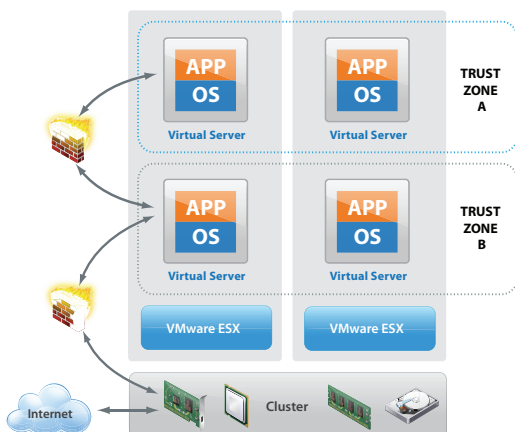
- Gain network visibility over communication between virtual machines without diverting traffic to physical appliances
- Ease administration and reduce policy errors with simple zone-based access rules
- Assure consistent policies throughout VMware VMotion™ and virtual machine lifecycle events
- Audit security posture within the virtual infrastructure irrespective of physical network

What is VMware vShield Zones?

VMware vShield Zones is a security virtual appliance that provides visibility and enforcement of network activity within a VMware vSphere™ deployment to comply with corporate security policies and industry regulations such as PCI or Sarbanes-Oxley. Previously, this level of visibility and policy enforcement required diverting traffic from VMware ESX™ hosts to external physical appliances, splintering resource pools into smaller, disconnected clusters, disrupting the flexibility and efficiency of a shared computing pool or cloud. VMware vShield Zones allows customers to create logical zones that span all the physical resources of the virtual datacenter, so that distinct levels of trust, privacy and confidentiality can be maintained.

VMware vShield Zones enables customers to:

- Bridge, firewall, or isolate virtual machine zones based on logical trust or organizational boundaries
- Create intuitive network access rules using existing VMware vCenter Server containers
- Log and report on allowed and disallowed activity by application-based protocols
- Easily convert observed network flows into precise access rules



Create logical trust and organizational boundaries within and across VMware ESX hosts and to the Internet.

How is VMware vShield Zones Used in the Enterprise?

With VMware vShield Zones, organizations can:

Collapse the virtualized DMZ. VMware vShield Zones enables demilitarized zones (DMZs) to be not only virtualized, but also to share computing resources with the internal network, while still maintain strict separation of Internet traffic from internal servers. By bringing the DMZ firewall into the virtualized environment, dedicated VMware ESX hosts for the DMZ are no longer required, but can allowing them to be fully used for availability and utilization across an entire cloud.

Meet PCI compliance for network separation of sensitive data. Payment Card Industry (PCI) standards mandate the network segmentation of servers processing credit-card data from other systems in order to protect consumers. VMware vShield Zones enables the firewall policies between virtual machines processing credit card data and other untrusted networks and machines as required by the PCI data security standard. Other industry regulations such as HIPAA and SOX similarly address the privacy of other sensitive data such as patient health care information or corporate financial statements, with firewalling and network segmentation being important controls that can be provided by VMware vShield Zones for the virtual environment.

KEY FEATURES

Enforce multi-tenant isolation for external or private clouds. VMware vShield Zones can create isolated and contained datacenter zones to prevent any network leakage of data or user activity across multiple tenants sharing a single cloud infrastructure. Scale isolation to hundreds of tenants without introducing excessive network complexity or management caused by individual virtual switches and virtual LANs (VLANs).

Monitor for unauthorized access within the virtual datacenter. Wide open internal networks facilitate the spread of malware and illegitimate activity. VMware vShield Zones can monitor and log traffic between virtual machines and to the Internet on an application protocol level. Unusual patterns of activity that may be indicative of worms or unauthorized access can be identified through graphical and tabular reports, and specific network flows can be quickly converted into precise blocking rules at an individual machine or aggregate levels.

How Does VMware vShield Zones Work?

VMware vShield Zones eases the burden of partitioning VMware vSphere™ deployments into multiple secure and contained zones of activity, so that virtualization can deliver efficiency, utilization, and availability into datacenter areas of greater sensitivity or confidentiality without exposing users or data to greater risk or breaching security or compliance mandates around network controls. VMware vShield Zones presents network monitoring and access management in a highly virtualization-aware and application-aware context, so that administrators can define access policies that intuitively map to logical trust or organizational zone boundaries expressed in their existing VMware vCenter Server management hierarchy and network topology.

VMware vShield Zones consists of the VMware vShield Manager, which provides centralized management of monitoring and access policies across an entire deployment, and VMware vShield Zones appliances that provide the runtime enforcement. VMware vShield Manager is deployed as a virtual appliance and integrates automatically with VMware vCenter Server to present policies and events in the context of the existing virtual machines, networks, host, and clusters.

VMware vShield Zones virtual appliances are distributed and deployed inline on the virtual switches on VMware ESX hosts to provide runtime visibility and enforcement of traffic. Network activity between zones and to the outside is logged and classified according to application network protocol, and packets are filtered inline to block any disallowed protocols or access. Events are consolidated back to the VMware vShield Manager, where activity across the entire datacenter can be logged, viewed and exported to third-party management solutions.

Key Features of VMware vShield Zones

Central Management of Logical Zone Boundaries and Segmentation

- Leverage existing virtual infrastructure containers – hosts, virtual switches, VLANs – as logical trust or organizational zones
- Define policies to bridge, firewall, or isolate network traffic between zone boundaries
- Manage and deploy policies across entire VMware vCenter Server deployment
- Integrate with VMware vCenter Server and automatically deploy on existing virtual networks
- Scan and discover existing applications running on virtual machines to identify application protocols

Network Enforcement and Flow Monitoring

- Classify traffic by network or application protocol (e.g. HTTP, RDP, SNMP)
- Performantly filter traffic with stateful packet inspection (SPI)
- Track dynamic port connections for protocols such as FTP
- Track network connections across VMware VMotion migration events.
- Easily convert observed network flows into precise network enforcement rules.
- Monitor both allowed and disallowed activity

Management and Reporting

- Access the Web-based vShield Manager interface remotely from any Web browser
- Configure administrators to be common with VMware vCenter Server or distinct for separation of duties and roles
- View activity hierarchically at individual virtual machine or aggregate levels and generate graphical or tabular reports
- Retain log data for archival and compliance purposes
- Export events and data using syslog format

Find Out More

For information or to purchase VMware products, call 1-877-4VMWARE (outside of North America dial +1-650-427-5000), visit www.vmware.com/products/vshield-zones/, or search online for an authorized reseller. For detailed product specifications and systems requirements, please refer to the VMware vShield Zones install and configure guide.