VMware vShield App

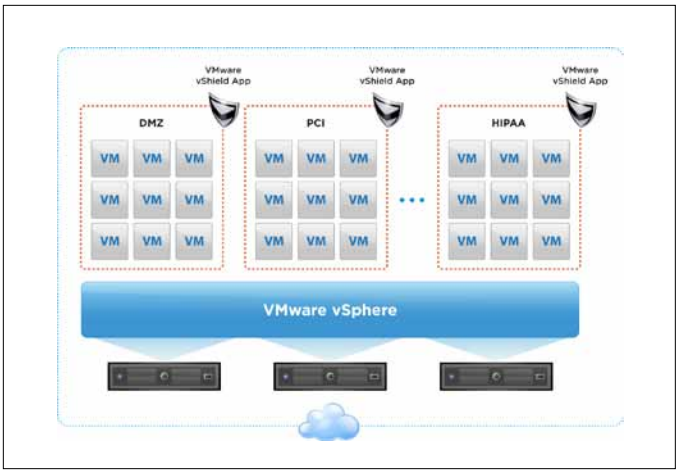
Protect Applications from Network-based Attacks

AT A GLANCE

VMware vShield App, part of the VMware vShield family of virtualization security products, protects applications in the virtual datacenter from network-based threats. vShield App gives organizations deep visibility into network communications between virtual machines and enables granular policy enforcement with security groups. The solution also eliminates the hardware and policy sprawl associated through traditional measures, resulting in a cost-effective solution that helps customers to go beyond the limitations of physical security.

KEY BENEFITS

- Increase visibility and control over network communications between virtual machines.
- Eliminate the need for dedicated hardware and VLANs to separate security groups from one another.
- Optimize hardware resource utilization while maintaining strong security.
- Simplify compliance with comprehensive logging of all virtual machine network activity.



VMware vShield App enables granular policy enforcement using security groups.

What Is VMware vShield App?

VMware vShield App is a hypervisor-based application-aware firewall solution for virtual datacenters. vShield App plugs directly into VMware vSphere™ to protect against internal network-based threats and reduce the risk of policy violations within the corporate security perimeter using application-aware firewalling with deep packet inspection and connection control based on source and destination IP addresses.

vShield helps to simplify policy control by enabling the rapid creation of business-relevant security groups and includes flow monitoring to analyze virtual machine network traffic and dynamically enforce security group policies. Administrators can centrally manage vShield App through the included vShield Manager console, which integrates seamlessly with VMware vCenter™ Server to facilitate unified security management for virtual datacenters.

How Does VMware vShield App Work?

vShield App installs on each vSphere host, controlling and monitoring all network traffic on the host, even for packets that never cross a physical network interface card (NIC). vShield App can create and enforce policies based on administrator-defined, business-relevant security groups instead of physical boundaries or static assumptions about application deployments.

vShield App provides a centralized interface that leverages vCenter Server to consistently apply these policies across multiple vSphere hosts in the virtual datacenter.

How Is VMware vShield App Used?

- **Eliminate blind spots** – vShield App helps administrators define and enforce granular policies for all traffic that crosses a virtual NIC, increasing visibility over internal virtual datacenter traffic while helping to eliminate detours to physical firewalls.
- **Maintain change-aware protection** – vShield App helps to ensure that network topology changes do not impact application security with continuous firewall protection for virtual machines as they migrate from host to host.

- **Efficiently manage dynamic policies** – vShield App helps to simplify policy definition and provides administrators a rich context for defining and refining internal firewall policies as business needs evolve over time.
- **Reduce botnet risks** – vShield App helps security administrators protect against botnets and other attacks by dynamically allocating ports to trusted applications.
- **Control access to shared resources** – vShield App allows security administrators to restrict access to shared services such as storage and backup on vSphere hosts based on IP address.
- **Accelerate IT compliance** – vShield App increases visibility and control over virtual machine network security, providing the logging and auditing controls that enterprises need to demonstrate compliance with internal policies and external regulatory requirements.

Key Features

Hypervisor-Level Firewall

- Inbound/outbound connection control enforced at the virtual NIC level through hypervisor inspection, supporting multihomed virtual machines
- Ability to enforce based on network, application port, protocol type (TCP, UDP), application type
- Dynamic protection as virtual machines migrate
- IP-based stateful firewall and application layer gateway for a broad range of protocols including Oracle, Sun Remote Procedure Call (RPC), Microsoft RPC, LDAP and SMTP; complete list of supported protocols in VMware vShield App Administration Guide

Flow Monitoring

- Ability to observe network activity between virtual machines to help define and refine firewall policies, identify botnets and secure business processes through detailed reporting of application traffic (application, sessions, bytes)

Security Groups

- Administrator-defined, business-relevant groupings of any virtual machines by their virtual NICs

Policy Management

- Management of full-features through vShield Manager; many features also accessible through vCenter Server interface
- Policy enforcement on security groups, vCenter groupings and TCP 5 tuple (source IP, destination IP, source port, destination port, protocol)
- Programmable interface for management and policy enforcement using REST APIs
- Support for integration with enterprise security management tools

Logging and Auditing

- Based on industry-standard syslog format
- Accessible through REST APIs and vShield Manager
- Administrator defined logging on/off for firewalls at rule level

Find Out More

For information or to purchase VMware products, call 877-4-VMWARE (outside of North America dial 650-427-5000), visit www.vmware.com/products, or search online for an authorized reseller. For detailed product specifications and systems requirements, refer to the VMware vShield App Administration Guide.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Copyright © 2010 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_10Q3_DS_PROD_VSHIELD_APP_USLET_EN_R6