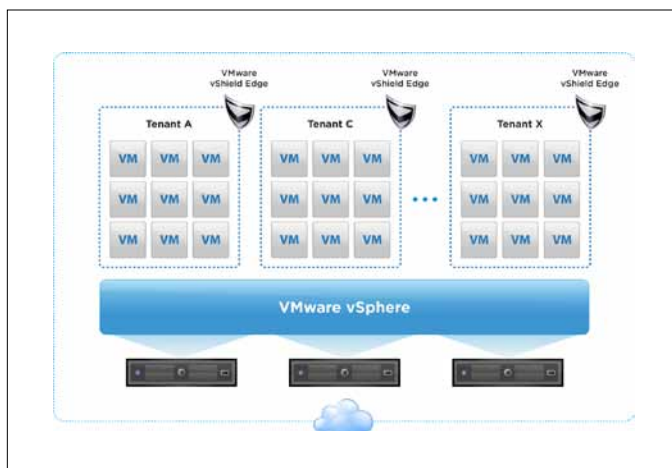# VMware vShield Edge
Secure the Edge of the Datacenter

AT A GLANCE

VMware vShield Edge, part of the vShield family of virtualization security products, provides comprehensive perimeter network security for virtual datacenters. vShield Edge integrates seamlessly with VMware vSphere™ and includes essential network gateway services that organizations can use to quickly and securely scale their cloud infrastructures.

KEY BENEFITS

• Reduce cost and complexity by eliminating multiple special-purpose appliances, and by rapidly provisioning network gateway services.

• Ensure policy enforcement with built-in edge network security and services.

• Increase scalability and performance with one edge per organization/tenant.

• Simplify IT compliance with detailed logging.

• Streamline management using a full-featured interface that integrates with VMware vCenter™ Server and leading enterprise security solutions.

VMware vShield Edge secures traffic between virtual datacenters with built-in perimeter security and port group isolation.

What Is VMware vShield Edge?

VMware vShield Edge is an edge network security solution for virtual datacenters that provides essential security capabilities such as port group isolation, network security gateway services and Web load balancing for performance and availability. The solution plugs directly into vSphere and leverages built-in features such as fault tolerance and high availability for unparalleled resiliency.

Administrators can centrally manage vShield Edge through the included vShield Manager console, which integrates seamlessly with vCenter Server to facilitate unified security management for virtual datacenters. vShield Edge also works in concert with VMware VCloud Director to automate and accelerate the secure provisioning of virtual datacenters in multi-tenant cloud infrastructures.

How Does VMware vShield Edge Work?

Network Security Gateway

Deployed as a virtual appliance, vShield Edge provides firewall, VPN, Web load balancer, NAT, and DHCP services to monitor packet headers for source and destination IP addresses. Depending on policy, it can deny or allow connections, initiate and terminate VPN sessions, perform network address translation, or inspect data by source/destination port and protocol type (TCP or UDP).

Port Group Isolation

When deployed as a loadable kernel module on vSphere, port group isolation creates a barrier between the virtual machines protected by vShield Edge and the external network. This has the same effect as implementing VLANs but without the complexity of trunking switch connections and defining switch port mappings.

How Is VMware vShield Edge Used?

• **Consolidate edge security hardware** – vShield allows customers to provision edge security services using existing vSphere resources, eliminating the need for edge security hardware to "air gap" vSphere hosts.

vmware®

- **Rapidly and securely provision virtual datacenter perimeters** – vShield Edge allows organizations to easily create secure, logical, hardware-independent perimeters ("edges") around virtual datacenter environments, making it easier to leverage shared network resources in multi-tenant IT infrastructures.

- **Protect data confidentiality over shared networks** – vShield Edge provides site-to-site VPN with 256-bit encryption to protect the confidentiality of all data transmitted across virtual datacenter perimeters.

- **Ensure performance and availability of Web services** – vShield Edge efficiently manages inbound Web traffic across virtual machine clusters and includes Web load balancing capabilities that customers can deploy in conjunction with port group isolation and edge security, or on its own.

- **Facilitate compliance management** – vShield Edge provides the necessary controls such as detailed event logging and flow statistics that enterprises need to demonstrate compliance with corporate policies, along with industry and government regulations.

Key Features

Stateful Inspection Firewall

Inbound and outbound connection control with rules based on the following parameters:

- **IP address** – source/destination IP address
- **Ports** – source/destination port
- **Protocol** – type (TCP or UDP)

Network Address Translation

- IP address translation to/from the virtualized environment
- Masquerading of virtual datacenter IP addresses to untrusted locations

Dynamic Host Configuration Protocol

- Automatic IP address provisioning to virtual machines in vSphere environments
- Administrator-defined parameters (e.g., address pools, lease times, dedicated IP addresses, etc.)

Site-to-Site VPN

- Secure communication between virtual datacenters (or edge security virtual machines)
- IPsec VPN, based on the Internet Key Exchange (IKE) protocol

Web Load Balancing

- Inbound load balancing for all traffic including Web traffic (HTTP, HTTPS)
- Round-robin algorithm
- Support for "sticky" sessions

Port Group Isolation

- Enforced at hypervisor layer to restrict traffic within a virtual datacenter to specified port groups
- Same effect as VLANs in virtual or physical switch environments

Edge Flow Statistics

- Virtual datacenter resource utilization metered and attributed back to tenant
- Statistics accessible through REST APIs and leveraged in service provider chargeback applications

Policy Management

- Full-featured management through vShield Manager; many features also accessible through vCenter Server interface
- Customizable interface for management using REST APIs
- Support for integration with enterprise IT security management tools

Logging and Auditing

- Based on industry standard syslog format
- Accessible through REST APIs and vShield Manager UI
- Administrator-defined logging on/off for key edge security events (errors, warnings, etc.):
  - *Firewall: at rule level*
  - *NAT: at rule level*
  - *VPN: site-to-site connection name*
  - *Web load balancer: At pool level, specific Web requests including URL/folder*
  - *DHCP: At service level, bindings (release/renewals)*

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 Edge Administration Guide

vmware®