

VMware vShield Edge

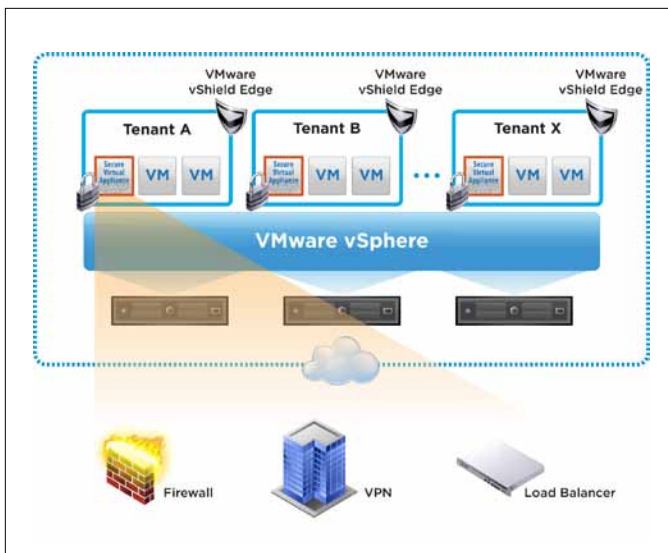
Secure the Edge of the Datacenter

AT A GLANCE

VMware vShield™ Edge, part of the VMware 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 or 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.



vShield Edge secures traffic between virtual datacenters with built-in perimeter security.

What is vShield Edge?

vShield Edge is an edge network security solution for virtual datacenters. It provides essential security capabilities such as 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 multitenant cloud infrastructures. Separation of duties for security and virtual infrastructure administrators limits access only to authorized resources.

How Does vShield Edge Work?

Deployed as a virtual appliance, vShield Edge provides firewall, VPN, Web load balancer, network address translation (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 or destination port and protocol type (TCP or UDP).

How is vShield Edge Used?

- **Consolidate edge security hardware** – vShield Edge allows customers to provision edge security services using existing vSphere resources, eliminating the need for edge security hardware to “air-gap” vSphere hosts.
- **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 multitenant 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 with edge security, or separately.

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

Key Features

Firewall

- Perimeter (Layer 3) firewall, which does not require network address translation
- Stateful inspection firewall, with inbound and outbound connection control 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 and 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 (such as address pools, lease times, dedicated IP addresses)

Site-to-Site VPN

- Secure communication between virtual datacenters (or edge security virtual machines)
- IPsec VPN with support for certificate authentication, as well as shared key, based on the Internet Key Exchange (IKE) protocol

Web Load Balancing

- Inbound load balancing for all traffic including Web traffic (HTTP)
- Round-robin algorithm
- Support for “sticky” sessions

Edge Flow Statistics

- Metering of virtual datacenter resource utilization, with attribution back to the tenant
- Statistics accessible through Representational State Transfer (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 user interface
- Administrator-defined logging on and 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 or folder
 - DHCP: at service level, bindings (release and renewals)

Supported Releases

For information on supported releases of vSphere environments, visit <http://vmware.com/products>.

Related Products

The vShield family of security products also includes VMware vShield App with Data Security to protect applications from network-based attacks and discovery of sensitive data; VMware vShield Endpoint for enhanced endpoint security and performance; vShield Manager; vShield Bundle, which includes all products.

Find Out More

For information or to purchase VMware products, call 877-4-VMWARE (outside North America, +1-650-427-5000), visit <http://www.vmware.com/products>, or search online for an authorized reseller. For detailed product specifications and system requirements, refer to the VMware vShield Administration Guide at http://www.vmware.com/pdf/vshield_41_admin.pdf.

For additional information on vShield products, visit <http://vmware.com/products>.

