VMware® vShield Edge and vShield App Reference Design Guide

TECHNICAL WHITE PAPER
The VMware® vShield family of virtualization security products provides a comprehensive set of security capabilities that help enterprise organizations gain the confidence they need to run business-critical applications in virtual datacenters and virtualized cloud environments. vShield solutions provide better-than-physical security through unique introspection capabilities, change-aware policy enforcement, and seamless integration with existing virtualization and IT security investments. These capabilities make private clouds built with VMware technology more secure than any other platform.

This document describes the architecture and features of vShield Edge and vShield App, and presents some reference designs for solutions built using these products. The designs described are meant to be representative of common business problems that organizations face when they further increase their virtualization footprint and move toward a cloud model of IT. By seeing how these problems are addressed, and mapping them to the actual issues they currently must address, customers should better understand how to deploy vShield Edge and vShield App in their own environments.

This document does not present detailed instructions on how to install and manage the vShield products; for this information, please consult the vShield Administration Guide and the vShield Quickstart Guide.

Introduction

Problems with Physical Security Devices in Virtual and Cloud Environments

Traditionally, network-based security has been implemented in datacenters using various physical appliances placed in strategic locations on an infrequently changing network fabric. However, when this approach is used for a virtualized datacenter, it can lead to a number of problems:

• **Network security devices become chokepoints.** Because network traffic in and out of virtual machines must be routed through physical appliances, the virtual environment must be architected in such a way that all network connections from the physical hosts must eventually pass through one of a small number of devices. This can splinter the virtual environment into isolated network-based silos, thus reducing the potential for sharing and disrupting the cloud vision of a seamless pool of resources.

• **Capacity is never right-sized.** Traditional network security devices like IDS and Firewall appliances are fixed-capacity physical devices, and hence capacity is usually under- or over-provisioned. This is of particular concern in a virtual environment, which can otherwise scale up quickly.

• **There is no intra-host VM visibility.** Traffic flowing between virtual machines (VMs) on the same VMware vSphere™ (“vSphere”) host might never touch the physical network, and so cannot be viewed by a physical security device.

• **Physical topologies are too rigid.** One of the hallmarks of a virtual environment is the ability to change in response to the dynamic needs of an organization. New projects, business cycles, and unpredictable demand can be handled through load-balancing, rapid provisioning, and reconfiguration. Any solution based upon a static network topology is simply not compatible with these capabilities.

With virtualization, and the advent of the cloud model of computing, “static” security will have to be replaced by a more dynamic set of security products. These products should be able to:

• Be compatible with the new paradigm of virtual networks that are not restricted by physical location or boundaries

• Adapt to change, by being able to scale capacity as needed and automatically handle dynamic inventory and configuration changes
The vShield product suite provides protection beyond the limitations of physical security in several significant ways:

• Introspection allows administrators to monitor and control virtual machine networks with comprehensive logging of all security events within the virtual datacenter.
• Change awareness makes it possible to enforce stateful security policies that travel with virtual machines as they migrate from host to host.
• Logical security perimeters protect virtual datacenters and enable safe sharing of network resources in multitenant infrastructures.

vShield Solutions
This document focuses on the network-based security products of the vShield product line, which consists of the following components.

VMware vShield App
VMware vShield App protects applications from network-based threats in the virtual datacenter with a hypervisor-level application firewall and administrator-defined “security groups” to enforce granular segmentation between applications.

VMware vShield Edge
VMware vShield Edge secures the edge of a virtual datacenter with firewalls, VPN, NAT, DHCP, and Web load-balancing capabilities that enable rapid, secure scaling of cloud infrastructures. Along with network isolation, these edge services create logical security perimeters around virtual datacenters and enable secure multitenancy.

VMware vShield Manager
vShield Manager is the central point of control for all vShield solutions and integrates seamlessly with VMware vCenter™ to offer role-based access control and administrative delegation in a unified framework for managing virtualization security.

vShield Architecture and Deployment Considerations
The following section describes vShield Edge and App in more detail, and presents some important considerations for their deployment.

vShield Edge
vShield Edge provides network-edge security and gateway services to isolate the virtual machines in a port group. The vShield Edge virtual appliance connects isolated, stub networks to the shared (uplink) networks and provides common gateway services such as DHCP, VPN, NAT, and Load Balancer. Common deployments of vShield Edge include

• DMZs
• Extranets
• Multitenant cloud environments, where the vShield Edge provides perimeter security for the Virtual Datacenters (VDCs)
vShield Edge is compatible with port groups on the vNetwork Standard Switch (VSS), vNetwork Distributed Switch (VDS), and the Cisco Nexus 1000v. vShield Edge can be managed through the vShield Manager Web interface, as well as the vShield Manager plug-in to vCenter Server, which places most vShield Edge features in dedicated tabs as well as context-sensitive menus. vShield provisioning and configuration of all features is also supported through the vShield Manager REST APIs.

vShield Edge virtual appliance has External and Internal Network interfaces. The internal interface connects to the secured port group and is the gateway for all protected virtual machines in this port group. The external interface of the vShield Edge connects to an “uplink” port group that has access to a shared corporate network or a service provider access layer network.

![vShield Edge Deployment Architecture](image)

**Figure 1.** vShield Edge Deployment Architecture.

vShield Edge can be used with one of two architectures. You can deploy vShield Edge with Port Group Isolation, which is a feature that creates a secure, isolated network without using VLANs or PVLANs. After Port Group Isolation is enabled, virtual machines can only communicate within the port group and use the vShield Edge as the gateway. Port Group Isolation installs as a hypervisor module and service virtual appliance on each VMware ESX® host in the cluster hosting the protected virtual machines, and is only available on a vNetwork Distributed Switch (vDS).
A service virtual appliance to be deployed on all hosts that home the internal port group. Deployment requires selection of a datastore on host to locate this virtual machine.

vShield hypervisor module to be deployed on all hosts that home the internal port group.

**Figure 2.** Port Group Isolation Component Architecture.

vShield Edge can also be used to secure port groups with a standard VLAN configuration. In this case, the isolation of virtual machines in the port group is provided exclusively by the VLAN, and it is up to the administrator to ensure that these are configured properly across all hosts. vShield Edge isolation with VLANs may be used on a VSS, VDS, or Cisco Nexus 1000v.

vShield Edge requires at least one IP address to identify the external interface. Multiple external IP addresses can be configured for services like Load Balancer, VPN, or NAT, or these may all be overlaid onto a single IP address. The internal interface can have a private IP address block that can overlap with other vShield Edge-protected isolated port groups, and can be RFC1918 private space.

All vShield Edge services can be configured using the vSphere Client with the vShield Manager plug-in, or directly on the vShield Manager, including the REST APIs. The specific services that vShield Edge provides are:

- **Firewall** — Supported rules include IP-based 5-tuple configurations, with IP and port ranges, for stateful inspection of TCP, UDP, and ICMP traffic. You can add destination and source port ranges to a rule for dynamic services such as FTP and RPC, which require multiple ports to complete a transmission. If you do not allow all of the ports that must be opened for a transmission, the transmission is blocked.

- **Network Address Translation (NAT)** — Separate controls include those for Source and Destination IP address and TCP/UDP port translation. A Source NAT rule translates a private internal IP address from the protect subnet into a public IP address on the External Network for outbound traffic. A Destination NAT rule maps a public IP address to a private internal IP address.
• **Dynamic Host Configuration Protocol (DHCP)** — The service includes configuration of IP pools, gateway, DNS servers, and search domains, as well as one-to-one static IP address allocation based upon virtual machine name and vNIC (instead of MAC address). DHCP rule enforcement prevents MAC spoofing attacks. vShield Edge DHCP listens on the vShield Edge internal interface for DHCP discovery, and uses the IP address of the internal interface, as the default gateway assigned to virtual machines in the container network are also configurable.

• **Site-to-Site Virtual Private Network (VPN)** — This uses standard protocols and settings that interoperate with all major firewall vendors. vShield Edge modules support site-to-site IPsec VPN between a vShield Edge and remote sites. vShield Edge supports pre-shared key mode, AES or 3DES encryption, IP unicast traffic, and no dynamic routing protocol between the vShield Edge and remote VPN routers. Behind each remote VPN router, you can configure multiple subnets to connect to the internal network behind a vShield Edge through IPsec tunnels. These subnets and the internal network behind a vShield Edge must have nonoverlapping address ranges.

• **Web Load Balancer** — These are simple and dynamically configurable virtual IP addresses and server groups, with both IP-hash and round-robin policies. vShield Edge provides load balancing only for HTTP traffic up to layer 7, which enables web application auto-scaling, and listens on port 80.

• **Remote Syslog** — This provides ability to audit selected events to a remote logging server.

You can deploy a vShield Edge virtual appliance behind a NAT device. In this deployment, the NAT device translates the VPN address of a vShield Edge into a publicly accessible address facing the Internet. Remote VPN routers use this public address to access the vShield Edge. Remote VPN routers can be located behind a NAT device as well. You must provide both the VPN native address and the NAT public address to set up the tunnel.

vShield Edge is tightly integrated with vSphere, and therefore works with vSphere features such as VMware Distributed Resource Scheduler (DRS), VMware vMotion™, VMware Distributed Power Management (DPM), and Maintenance mode. The implications are as follows for the different vShield Edge components:

• **vShield Edge Virtual Appliance** — The vShield Edge virtual appliance can be migrated to different ESX hosts automatically by DRS, and can be protected using VMware High Availability (VMware HA) or VMware Fault Tolerance (VMware FT). It can be placed into resource pools and storage locations most optimal for performance.

• **Port Group Isolation** — The Port Group Isolation service virtual appliance will be automatically shut down and restarted by the vShield Manager in response to triggers such as entering and exiting Maintenance mode and DPM power-off and power-on events.

**vShield App**

vShield App provides firewalling capability between virtual machines by placing a firewall filter on every virtual network adapter. It implements an IP-based stateful firewall and application layer gateway for a broad range of protocols including Oracle, FTP, Sun/Linux/MS RPC. This firewall filter operates transparently and does not require network changes or modifications of IP addresses.

Rules can be written using the following vSphere groupings:

• Datacenter
• Cluster
• Resource Pools
• vApps

They can also be written using the following network objects:

• Port Group
• VLAN
vShield App also enables you to create custom containers known as Security Groups, to which you can assign individual vNICs of virtual machines. Similar to the vSphere groupings, Security Groups can be used as a basis for firewall rules.

By writing rules in terms of containers and objects, the number of firewall rules can be dramatically reduced, which makes them easier to track and less prone to configuration error. As membership in these containers can change dynamically, vShield App maintains the state of existing sessions without requiring reconfiguration of firewall rules. When creating App Firewall rules, you can create general rules based on incoming or outgoing traffic at the container level. For example, you can create a rule to deny any traffic from outside of a datacenter that targets a destination within the datacenter.

By default, the App Firewall enforces a set of rules allowing traffic to pass through all vShield Apps. These rules appear in the Default Rules section of the App Firewall table. The default rules cannot be deleted or added to. However, you can change the Action element of each rule from Allow to Deny.

vShield App enforces firewall rules in top-to-bottom ordering. vShield App checks each traffic session against the top rule in the firewall table before moving down the subsequent rules in the table. The first rule in the table that matches the traffic parameters is enforced. In the App Firewall table, the rules are enforced in the following hierarchy:
• Datacenter high-precedence
• Container or network object
• Datacenter low-precedence
• Default

The Flow Monitoring feature of vShield App displays Allowed and Blocked network flows at an application protocol granularity, and presents the information in the context of various objects such as datacenter, cluster or port group. This can be used to audit network traffic and as an operational troubleshooting tool.

vShield App installs as a hypervisor module and Firewall Service virtual appliance on each ESX host in the cluster hosting the protected virtual machines. The hypervisor module places a vNIC-level firewall enforcement point for the traffic to and from virtual machines. Similar to vShield Edge Port Group Isolation, vShield App is tightly integrated with vSphere, and therefore works with vSphere features such as DRS, vMotion, DPM, and Maintenance mode.
Figure 3. vShield App Component Architecture.
Design Use Cases

The following section presents some idealized but realistic use cases for network security in a virtualization and cloud environment, and describes how vShield Edge and vShield App can be used to solve the business requirements.

Use Case 1: DMZ

A DMZ (demilitarized zone) is a generic term for a subnetwork that contains and exposes an organization’s external services to a larger untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization’s Local Area Network (LAN); an external attacker only has access to equipment in the DMZ, rather than any other part of the network.

In this use case, a hypothetical company decides that they need a DMZ for hosting a public-facing Web application, as well as some collaboration applications that need to be accessed over the Internet by trusted third parties such as external partners and remote office sites. In particular, the technical requirements for the DMZ are as follows:

• There should be network load balancing for the Web servers.
• The DMZ Web servers need to be able to reach out to the public Internet in order to download patches.
• Remote SSH into the Web servers should be allowed, in case remote maintenance is needed.
• In order to allow third-party companies to do uptime monitoring, ICMP ping traffic should be allowed to the Web servers.
• There needs to be automatic IP address assignment within the DMZ, including fixed addresses for specific VMs such as the Web servers. These IP assignments should all be audited.
• Several VPN tunnels are needed for secure connection by outside partners as well as a remote office.

In addition, the following business requirements need to be satisfied:

• The DMZ must be strictly isolated from the rest of the company’s network to contain any malware or malicious behavior inside this enclave. However, the networking team would like to avoid allocating a new VLAN in order to reduce management complexity.
• There needs to be firewall rules to lock down traffic to and from this enclave, as well as to minimize and control inter-VM traffic within it.
• Due to a shortage of internal IP addresses, there is a need to minimize the number of addresses used up on the corporate network.

vShield products provide a solution that can address these business requirements in a cost-effective manner that’s easy to deploy and configure. We will look at a vShield deployment that satisfies each of these requirements.

Layer 2 Network Isolation

The company has two primary internal corporate networks, one for business applications and one for virtual desktops. These are configured as two different port groups on a vDS that spans all the hosts in the vSphere deployment. For the DMZ, a new port group is created on the vDS, which doesn’t have any network adapter bindings. vShield Edge is then deployed so that it bridges the DMZ port group with the corporate business network (see Figure 4).
The Port Group Isolation feature is configured so that no additional VLAN needs to be created. The vShield Edge network settings, such as subnet mask and default gateway, used for the DMZ, can be seen in Figure 5. vShield App is also deployed on all hosts for the purpose of network traffic control inside the DMZ.
IP Address Management

By using the DHCP feature of vShield Edge, IP addresses can be assigned automatically. Static assignments are used for the Web servers as well as an associated database, to make tracking easier. Other transient applications, such as collaboration services, are assigned IP addresses from a pool. All IP assignments are logged for audit purpose. The DHCP configuration is shown in Figure 6.
NAT and Load Balancer

The Source NAT feature of vShield Edge is employed to allow all systems in the DMZ with a router to connect to the outside network (note that some of these systems could still be prevented from communicating out by vShield firewall rules configured elsewhere). A single IP address is used to represent all systems connecting out (so-called IP Masquerading). The NAT configuration is shown in Figure 7, and is described in greater detail in the following paragraph.

Communication into the DMZ is only allowed for the Web servers, and for three purposes:

- For users to browse the Web apps, the vShield Edge Load Balancer feature is used. The Load Balancer is configured to listen on the external interface address of the vShield Edge for Web requests, and routes them accordingly. Both Web servers are configured to participate, using a round-robin algorithm. Note that the Load Balancer implicitly handles destination NAT for the Web servers, so this does not need to be configured separately in the NAT section. The Load Balancer configuration is shown in Figure 8.
- Destination NAT is configured so that administrators connecting to the vShield Edge external IP address on special port number (6666 and 6667) are connected to port 22 of the Web servers, allowing remote SSH login for maintenance.
- Destination NAT is also configured so that ICMP ping to the vShield Edge external IP address is forwarded to one of the Web servers, allowing uptime monitoring by a third party.

In all cases, the vShield Edge external IP address is used, so that another IP address on the corporate network is not required.

Figure 7. NAT Configuration for the DMZ.

Figure 8. Load Balancer Configuration for the DMZ.
VPN

A VPN tunnel is configured for external partners to connect to collaboration services running in the DMZ. First, a remote site is configured, and then a specific tunnel is created. The tunnel is encrypted using AES, and the remote site can use any industry standard Site-to-Site VPN product on their side. The vShield Edge external IP address is used to create the tunnel, avoiding the use of any additional IP addresses on the corporate network. The VPN configuration is shown in Figure 9.

![Figure 9. VPN Configuration for the DMZ.](image)

Firewall

There are two separate places where a firewall is configured to block traffic. vShield Edge provides perimeter security for traffic going in and out of the DMZ by monitoring it at the vShield Edge internal interface. vShield App can be used to restrict traffic within the DMZ, to and from individual virtual machines.

At the vShield Edge internal interface, the default policy is to deny all traffic. Exceptions are added to enable Web servers to contact the outside network (in order to download patches), and for remote sites to connect to the Web servers via SSH (for remote maintenance). The firewall rules are applied after the incoming traffic has been translated by the destination NAT mappings described in the previous section. The vShield Edge Firewall configuration is shown in Figure 10.
In order to control traffic within the DMZ, vShield App is used with the Security Groups feature. Security groups are defined for the Web servers as well the associated database, and are assigned membership by virtual machine vNIC, as shown in Figure 11.

vShield App firewall rules are then created using these groups. The point of policy definition is the DMZ Port Group, and this is the context in the vSphere Client UI where the rules would be created. As shown in Figure 12, there are two main kinds of rules:

- Web servers are allowed to connect to database servers but only using Oracle protocols, which is all that is required for this particular business application to function.
- Both TCP and UDP traffic from Web servers to any Web server is disallowed, so that in case one Web server is compromised it will not be able to attempt a compromise on any other Web server. Any such attempt is logged so that administrators can have an audit trail of attack attempts.
Summary of Benefits

By using vShield Edge and vShield App to build the DMZ, the company achieved the following:

- They were able to carve out a fully isolated enclave within the existing vSphere environment, but the infrastructure changes necessary were limited to creating a dedicated internal-only port group, and using up a single IP address on the corporate network.
- They avoided capital expenditure on the purchase of numerous hardware devices, such as firewalls, VPN, and Load Balancer.
- They benefited from extremely quick setup — no racking, stacking, or cabling of equipment was required. The setup is also easy to modify or replicate if required, allowing for rapid provisioning of other DMZs for changing partners, temporary remote offices, and so on.
- They attained additional network security controls, such as traffic blocking and auditing, using firewall zoning within the DMZ without requiring VLANs for routing traffic out to physical firewalls.

Use Case 2: Virtual Desktops with Business Applications

In this use case, a hypothetical company would like to impose better network security controls on an existing environment. They would like to provide better security against both internal and external threats, and better satisfy compliance requirements by implementing security best practices in a comprehensive way. Their specific technical requirements:

- Impose finer-grain controls on virtual desktop networking, which will allow them to extend virtual desktops beyond task workers, who work in tightly locked-down environments, out to knowledge workers, who require greater flexibility.
- Create network security zones while maintaining the existing network configuration, such as topology and LAN segments.

Additional business requirements:

- Impose datacenter-wide network policies that are absolute, while allowing individual zones or clusters to have additional independent policies.
- Create datacenter-wide network policies that are optional, so that security best practices are implemented but can be overridden for specific virtual business purposes if required.
- Monitor and audit network traffic, particularly for the virtual desktops.

In this example the company has both virtual desktops and business applications already running and located on the internal corporate network. They would like to maintain this existing networking setup, but layer on security controls to meet their business and technical objectives, and so vShield App was chosen as the solution.
Creation of Logical Groupings

In the previous use case we saw how custom security groups could be created to provide logical groupings where none existed. For this use case, we can take advantage of pre-existing vSphere containers for the logical grouping. In particular, the company already makes use of resource pools to group virtual desktops and business services, as well as vApps to contain all virtual machines belonging to the same application. Figure 13 shows a diagram of the resource pools and vApps in use at this company, including those for the DMZ.

![Figure 13. vSphere Containers for Logical Grouping.](image)

Datacenter-Wide Policies

vShield App allows for the creation of high- and low-precedence datacenter policies. In this example, the following high-precedence rules were created:

- Web browsing to public Internet by all desktops is allowed.
- All other traffic to public Internet from desktops is disallowed.

These rules are written in terms of the VDI resource pool, which means they apply to every single virtual desktop that is created (provided the administrator adheres to the policy of placing all virtual desktops inside this resource pool).

In addition, a low-precedence rule was created to block NetBIOS traffic from any virtual machine to any other virtual machine, in order to contain the effects of a recent worm outbreak. This rule provides a way of instituting a security best practice, but can be overridden for specific virtual machines or groups at a later time. Finally, the default rules are set to deny-all, again as a security best practice.
Virtual Desktop Policies

In order to provide greater control over virtual desktops, the company has employed nested resource pools. Inside the top-level VDI resource pool, there is a resource pool for task workers and another one for knowledge workers. In addition to using these to control server resource utilization, for example, using shares or limits on CPU and memory usage, the resource pools are repurposed to provide finer-grained control of network policies. The following rules were created at the cluster level:

- DNS protocol access from the VDI resource pool to a physical DNS server located at a specific IP address is allowed.
- AD protocols access from the VDI resource pool to the virtual AD vApp is allowed.
- All attempts by any desktop to directly communicate with any other desktop is blocked and also logged.
- Desktops in the knowledge worker resource pool are allowed to communicate with the virtual Sharepoint vApp; this is not permitted for the task worker resource pools.

The entire set of vShield App rules for this example can be seen in Figure 14.
Summary of Benefits

By using vShield App to provide network controls, the company achieved the following:

• They were able to impose network controls where none existed before, without excessive cost, and without requiring changes to virtual network topology or physical network infrastructure.
• They can take advantage of vSphere groupings to define rules. Many of these groupings already exist in the virtual datacenter. Others are easy to create.
• By basing them on groupings, the rules become “write-once, apply everywhere,” in other words, they apply to any VM that joins that group.
• Since rules can also be written using IP addresses, they work with existing physical or legacy servers.
• They were able to control and audit virtual desktop network traffic, which is something that is simply not practical with other security solutions.

Conclusion

VMware vShield leverages the unique advantages virtualization brings to security—such as introspection, hardware independence, and change awareness—and integrates seamlessly with VMware vSphere, VMware vCenter Server, and virtualization-ready security solutions from VMware partners, giving customers a single framework for securing hosts, networks, applications, data and endpoints against internal and external threats. These capabilities make cloud infrastructures built with VMware technology more secure than any other platform, providing the defense-in-depth that enterprises need to achieve the benefits that cloud computing has to offer without compromising security, control or compliance management efforts.