Overview

The new virtual datacenter (vDC) infrastructure deployments enable IT to provide on-demand infrastructure services to its customers on a common, shared infrastructure while maintaining isolation, security and flexibility of resources. This deployment is also termed cloud infrastructure or multitenant infrastructure, where instead of providing internal organizations with siloed physical infrastructures, IT delivers isolated virtual datacenters that are hosted on a common physical infrastructure. By pooling the physical resources on the back end, hardware utilization and consolidation is increased. Similarly, underlying infrastructure can be pooled into tiers and offered to users at discrete service levels and prices. From the end-user point of view, each system is still separate, with its own network, storage and services offering. However, the separation and isolation between tenants/customers are not provided through separate physical racks but through secure multitenancy architecture using a VMware® vShield Edge firewall. Figure 1 provides a simplified illustration of a multitenant virtual datacenter hosting three tenants. Each tenant is allocated with its compute, storage and network resources. The resources are carved out to each tenant from a common pool of physical infrastructure. The isolation and security between tenants are provided through a vShield Edge firewall.

The goal of this document is to help customers understand where and how a vShield Edge firewall can be deployed to secure and isolate tenants/organizations, while providing some reference designs along the way. This document will also help VI administrators and network administrators understand the deployment of security and other network services in virtual datacenters using a vShield Edge firewall.

First, a brief explanation of the multitenant infrastructure use case is provided. Subsequently, the needs of such an environment are discussed along with the traditional design approaches and challenges. Finally, three reference designs are provided to help customers understand the security and other network services deployment in a virtual datacenter using the vShield Edge firewall product, as well as the advantages of these designs.

Figure 1. Virtual Datacenter
Multitenancy Use Case Description

Multitenancy environments might differ from each other based on specific services and SLA requirements from tenants as well as special security requirements from regulatory environments they operate in. Following are the typical tenant requirements that service providers have to be able to fulfill.

1) NAT, load balancing, IPSec VPN services support
2) Secure separation from other tenants
3) Predictable service quality and high availability
4) Scalability of services
5) Rapid provisioning and on-demand deployments

Let us first look at the traditional multitenant design approaches and their challenges before diving into the virtual datacenter or cloud-based multitenant architecture deployments based on vShield Edge.

Traditional Multitenant Designs

As shown in Figure 2, a traditional multitenant design requires three physical siloed infrastructures in order to provide services to three different organizations or companies. Each silo has its own set of equipment (storage, network, server) that addresses specific needs of that organization. To support secure remote access to different users of an organization, separate VPN devices are installed per organization. Also, additional services—such as load balancers, IPS devices and other network and security services if required—are incorporated in the aggregation layer of the design.

---

Figure 2. Siloed Multitenancy Deployment
Isolation between different organizations in traditional design is achieved through physical separation of devices as well as through the firewall rules and separate routing domains. This physical separation reduces the complexity of the deployment but adds rigidity to the infrastructure. The following are key disadvantages of the traditional design:

- Underutilized resources.
- Less flexibility and scalability of the solution.
- Deployment of physical devices takes time and adds to CAPEX and OPEX.

Figure 3 shows another deployment where the customer has successfully consolidated the server infrastructure and is achieving a better consolidation ratio by serving different tenants on one cluster. In this design, traffic isolation between different tenants is through VLANs, and security is introduced by deploying separate physical firewalls at the aggregation layer for each tenant. The following are some disadvantages of this design option:

- VLAN complexity of provisioning and managing.
- Longer provisioning cycle with deployment of hardware firewall devices.
- The firewalls become choke points, as all tenant traffic flows through the security device.

To overcome these challenges with traditional designs, and to meet business requirements mandating increased agility and efficiency, IT departments are embracing the new cloud computing strategy. According to NIST, cloud computing is defined as a model for enabling on-demand network access to a shared pool of computing resources (network, storage, servers, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This model is sometimes referred to as the Infrastructure as a Service (IaaS) model, where the service provider offers the compute, storage and network infrastructure to the customer/consumer on demand. These cloud computing models are categorized as follows, based on who is the service provider and who is the customer/consumer:

- Private cloud: IT department acting as a service provider and providing cloud infrastructure to several internal organizations
Public cloud: Service provider selling the cloud infrastructure to an industry or the general public (VMware vCloud™ Express)

Hybrid cloud: IT department of a company with private cloud deployment makes use of public cloud infrastructure to satisfy the instantaneous infrastructure need (cloud bursting) of its internal organizations

Many enterprises are deploying cloud service (private cloud) offerings to their internal organization and taking advantages of increased operational efficiency and agility over shared infrastructure. However, leveraging shared infrastructure introduces additional challenges in terms of how security and isolation can be maintained across internal organizational resources and how service level agreements (SLAs) can be provisioned and administered based on particular organizational needs. The VMware vShield product family helps address the security and isolation challenges faced in the multitenant, or cloud, infrastructure.

**Design Approach with VMware vShield Edge**

This section provides details on how to build a multitenant deployment and how to implement isolation and security for individual tenants.

A security design approach using a vShield Edge firewall can be based on the following approaches:

- VLAN isolation
- Cloud network isolation – port group isolation (PGI)

**Common Components**

The following are the common components in the design. This list doesn’t include the external network and storage infrastructure that are required to build the virtual infrastructure. It is assumed that based on the customer environment, there will be iSCSI or FC SAN infrastructure and also network switches and router infrastructure.

**Hosts**

Six physical hardware servers provide compute, memory and network resources based on the configuration of the hardware (for example, an HP ProLiant DL380 rackmountable server with two Intel Xeon CPUs (four cores each), 96GB memory, 2x10GB network interface cards running VMware ESX®/ESXi™ servers). Customers can have different hardware capacities, which will drive the decision on how many virtual machines or workloads can be hosted on a particular hardware.

**Cluster**

A cluster is a collection of VMware ESX/ESXi hosts and associated virtual machines with shared resources. When a host is added to a VMware Distributed Resource Scheduler (VMware DRS) cluster, the host’s resources become part of the cluster’s resources. There is one cluster with six hosts.

**Number of tenants**

Depending on the service provider’s infrastructure resources and its needs, multiple tenants can be hosted. For purposes of illustration, in this design three tenants are considered. They might be three different companies for a service provider or three different organizations for an internal IT deployment. Each tenant gets its own set of compute, storage and network resources from a common resource pool. The number of tenants will depend on the customer’s (in this case, IT or the service provider) need to provide services to different tenants, as well as on the capacity of available resources that can be shared across tenants. These tenants are referred to as company X, company Y and company Z in the designs.

**VMware vShield Edge**

The vShield Edge firewall provides network perimeter security and services to a tenant. It isolates the tenant’s stub network from the shared (uplink) networks and provides common perimeter security services such as DHCP, VPN and NAT. One vShield Edge firewall is deployed per tenant or port group.
Design Option 1: VLAN Isolation

This design approach utilizes a network infrastructure’s ability to provide isolation through VLANs. Each of the three tenants that must be supported in this design must have its own VLAN for its own virtual machine traffic. Additional VLANs are required if tenants want to separate storage and management traffic from normal virtual machine traffic. For purposes of simplified illustration, assume that all storage, network and management traffic of a tenant is assigned to one VLAN. As shown in Figure 4, VLAN 1000 is associated with company X, VLAN 1001 is associated with company Y, and VLAN 1002 is associated with company Z. There is also a provider VLAN, VLAN 100, which is associated with an external network of different companies’ perimeters.

This VLAN separation of traffic between tenants provides layer-2 isolation between tenants but doesn’t provide security from layer-3-and-above attacks. To protect from higher-layer network attacks, one VMware vShield Edge virtual machine, acting as a firewall, is deployed per tenant. The vShield Edge virtual machine has two network interfaces. One of the interfaces is connected to the uplink port through the PG-C (VLAN 100) port group and provides access to the external world. The other interface of the vShield Edge virtual machine is connected to the internal port group, PG-X, which is part of the company X network. All virtual machines of the company X tenant connect to the internal port group, PG-X (VLAN 1000), and these virtual machines are allowed to communicate with each other without going through the vShield Edge firewall virtual machine. However, if the company X virtual machine attempts to access external devices, traffic must flow through the vShield Edge virtual machine. Depending on the security rules defined, the access will be allowed or denied. The vShield Edge firewall is a virtual machine that can be scaled up or down based on the amount of traffic that a particular tenant must handle. Also, the firewall virtual machine is protected through the VMware DRS and VMware High Availability (VMware HA) features of the VMware vSphere™ 4.1 (“vSphere”) platform. So when a host on which vShield Edge is running goes down, that virtual machine restarts immediately on another available host in that cluster.

Similar to the deployment of vShield Edge virtual machine for company X, deploy vShield Edge for company Y and company Z and configure the internal network by creating separate port groups PG-Y and PG-Z where respective-company virtual machines will be connected. As shown in Figure 4, VLANs 1000, 1001 and 1002 are configured on PG-X, PG-Y and PG-Z respectively. The external network infrastructure at the access and aggregation layers requires VLAN configuration that will provide layer-2 isolation at the network level. However, customers that have their network infrastructure architected with separate layer-2 domains and are familiar with the operation can utilize the network design as is and can deploy a vShield Edge firewall to provide layer-3-and-above security.

A VMware vShield Edge firewall can successfully provide a perimeter security solution that is scalable, flexible, resilient and secure. If a tenant wants to deploy its own NAT, DHCP and VPN services, the vShield Edge firewall also provides the capability to enable those services per tenant. In design option 3, an extranet use case is described in which partner access to a tenant resource is provided through a secure IPSec tunnel.
Figure 4. Multitenancy with VLAN Isolation

Figure 5, Figure 6 and Figure 7 illustrate in detail the various traffic flows that can occur between the virtual machines of different tenants and how vShield Edge firewall rules can allow or deny these flows based on security policies. To simplify the diagram, a two-host cluster with two different tenants (X and Y) and their virtual machine resources is shown. Three traffic flows are illustrated in the following:

- Tenant Y virtual machine on host 1 communicating to tenant X virtual machine on host 2 (different-host communication). This communication is shown by a green circle with numbers in Figure 5.

Figure 5. Different-Tenant-on-Different-Host Communication
• Tenant X virtual machine on host 1 communicating to tenant X virtual machine on host 2. This communication is shown by a blue circle with numbers in Figure 6.

![Figure 6. Same-Tenant-on-Different-Host Communication](image)

• Tenant Y virtual machine on host 1 communicating to tenant X virtual machine on host 1 (same-host communication). This communication is shown by an orange circle with numbers in Figure 7.

![Figure 7. Different-Tenant-on-Same-Host Communication](image)
The following are the key challenges of the VLAN-backed isolation design:

• Limitation on number of tenants supported due to VLAN limitations (4K VLAN)
• Configuring and managing VLAN across the switching infrastructure

Design Option 2: Cloud Network-Backed Isolation (PGI)

To overcome the challenges faced by the VLAN deployments, VMware has introduced a new approach: providing isolation through traffic encapsulation. With this approach, there is no need for customers to worry about multiple VLANs for isolation. They only must provide a single layer-2 domain. All tenants’ virtual machines will be part of the same layer-2 domain. This design requires customers to use a virtual distributed switch (vDS).

The three tenants that must be supported in this design will be part of one VLAN. As shown in Figure 8, tenants X, Y and Z are part of the same layer-2 domain. Port groups X, Y and Z are the internal port groups on which tenant virtual machines are connected. All traffic from virtual machines that are connected to a port group is allowed to flow through. However, when a virtual machine connected to Port group PG-X attempts to communicate with a virtual machine connected to Port group PG-Y, the traffic is not allowed, even if those virtual machines are in the same layer-2 domain. The vDS keeps track of where the traffic is coming from and where it is headed. It determines whether the traffic can flow directly or whether it must go through a VMware vShield Edge firewall. The isolation between tenants that are in the same layer-2 domain is maintained through the platform, which is aware of the association of virtual machines to the port groups.

The vShield Edge virtual machine has two network interfaces. One of the interfaces is connected to the uplink port through the PG-C port group and provides access to the external world. The other interface of the vShield Edge virtual machine is connected to the internal port group PG-X, which is part of the company X network. All virtual machines of the company X tenant connect to PG-X port group, and these virtual machines are allowed to communicate with each other without going through the vShield Edge firewall virtual machine. However, if the company X virtual machine attempts to access external devices, traffic must flow through the vShield Edge virtual machine. Depending on the security rules defined, the access will be allowed or denied. Also, the vShield Edge firewall virtual machine is protected through the VMware DRS and VMware HA features of the vSphere platform. So when a host on which vShield Edge is running goes down, that virtual machine gets restarted immediately on another available host in that cluster.

Similar to the deployment of the vShield Edge virtual machine for company X, deploy the vShield Edge for company Y and company Z. Configure the internal network by creating separate port groups PG-Y and PG-Z where the respective company Y and company Z virtual machines will be connected. As shown in Figure 8, all the port groups (PG-X, PG-Y and PG-Z) are in the same layer-2 domain, and isolation between different companies is achieved through the method of encapsulation. The advantage of this method over the VLAN-based isolation is that there is no need for complex configuration at the access aggregation layer, thereby simplifying operational challenges. Also, there is no number of VLAN limitations in this deployment.
The following figures illustrate in detail the different traffic flows that can occur between different tenant virtual machines and how vShield Edge firewall rules can allow or deny these flows based on the security policies. To simplify the diagram on a two-host cluster, two different tenants, X and Y, have their resources (virtual machine) running. Three traffic flows are illustrated, as follows:

- Tenant Y virtual machine on host 1 communicating to tenant X virtual machine on host 2 (different-host communication). This communication is shown by a green circle with numbers in Figure 9.

![Figure 8. Multitenancy with PGI Isolation](image)

![Figure 9. Different-Tenant-on-Different-Host Communication](image)
• Tenant X virtual machine on host 1 communicating to tenant X virtual machine on host 2. This communication is shown by a blue circle with numbers in Figure 10.

![Figure 10. Same-Tenant-on-Different-Host Communication](image)

• Tenant Y virtual machine on host 1 communicating to tenant X virtual machine on host 1 (same-host communication). This communication is shown by an orange circle with numbers in Figure 11.

![Figure 11. Different-Tenant-on-Same-Host Communication](image)
Comparison of Two Options

The following table compares the two design options of multitenancy deployments described in previous sections on operational and scalability parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>VLAN Isolation</th>
<th>Cloud Network Isolation</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Limitations</td>
<td>Maximum 4K VLANS</td>
<td>No VLAN limitations</td>
</tr>
<tr>
<td>Complexity</td>
<td>High</td>
<td>Lower</td>
</tr>
<tr>
<td>Scalability</td>
<td>Not scalable</td>
<td>Simple to scale</td>
</tr>
<tr>
<td>Management</td>
<td>Complex</td>
<td>Simple</td>
</tr>
<tr>
<td>Provisioning</td>
<td>Time consuming</td>
<td>Automated</td>
</tr>
</tbody>
</table>

Design Option 3: Extranet – Partner Access

The partner access use case is very prominent in today's collaborative work environment. Companies work with different partners to take advantage of their unique skills, and they all must share information. So if an organization wants to take advantage of a service that is provided by a partner, it must establish a secure communication channel that enables them to communicate securely. IT or the service provider must provision this secure tunnel that can be used by this organization, by deploying physical devices on local and remote site. The deployment of physical devices across two sites, along with the configuring of tunnels, results in considerable time before communication service can be enabled between the partner and the organizations. However, the following design using a VMware vShield Edge firewall shows how simple it is to deploy and configure a site to a site virtual private network (VPN). The following section provides some details on how to enable the VPN service for a typical use case.

The vShield Edge firewall product provides NAT, DHCP, load balancing and VPN services along with firewall capability. This design depicts a use case where a tenant or organization wants to provide access to its resources to a partner over a secure link. As shown in Figure 12, Org X and Org Z are providing access to their respective resources through an IPSec tunnel. Customers can enable these services on the fly without the complexity of the physical infrastructure deployment.
The following simple steps are required to configure the VPN tunnel from Org X to the partner of Org X:

1. In the vSphere Client, go to Inventory > Networking.
2. Select an internal port group that is protected by a vShield Edge. In this case, it is PG-X.
3. Click the vShield Edge tab.
4. Click the VPN link.
5. Type an External IP Address for the VPN service on the vShield Edge.
6. Type the NATed Public IP that represents the External IP Address to the external network.
7. Select the Log check box to log VPN activity.
8. Click Apply.

Next, identify a peer site.

Click the VPN link after choosing the PG-X port group and vShield Edge tab.

1. Under Peer Site Configuration, click Create Site.
2. Type a name to identify the site in Site Name.
3. Type the IP address of the site in Remote EndPoint.
4. Type the Shared Secret.
5. Type an MTU threshold.
6. Click Add.
Next, add a tunnel to connect to the site.

Click the VPN link after choosing the PG-X port group and vShield Edge tab.

1. Under Peer Site Configuration, select the appropriate peer from the Select or create a site drop-down list.
2. Click Add Tunnel.
3. Double-click the Tunnel Name cell and type a name to identify the tunnel.
4. Double-click the Remote Site Subnet cell and enter the IP address in CIDR format (A.B.C.D/M).
5. Double-click the Encryption cell and select the appropriate encryption type.
6. Click Commit.

Similarly, IT can configure a tunnel for Org Z and its partner. The vShield Edge agent can be deployed 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. In this case, IT must provide both the VPN native address and the NAT public address to set up the tunnel. On both ends, static one-to-one NAT is required for the VPN address.

Conclusion

VMware vShield Edge is a key component of the cloud, or multitenant, architecture. It provides perimeter security to tenants, as well as additional services (NAT, DHCP, load balancing and VPN) that are easy to deploy and manage. The simplified isolation through vDS technology is a key differentiator that enables customers to deploy scalable private/public cloud services without the complexity of a VLAN implementation.