BEST PRACTICES

Network Segmentation in Virtualized Environments

vmware®

Table of Contents

Network Segmentation in Virtualized Environments

Introduction

As virtualization becomes the standard infrastructure for server deployments, a growing number of organizations want to consolidate servers that belong to different trust zones. A trust zone is loosely defined as a network segment within which data flows relatively freely, whereas data flowing in and out of the trust zone is subject to stronger restrictions. Examples of trust zones include:

- Demilitarized zones (DMZs)
- Payment card industry (PCI) cardholder data environment
- Site-specific zones, such as segmentation according to department or function
- Application-defined zones, such as the three tiers of a Web application

The introduction of virtual technology does not have to significantly change the network topology. As with other parts of the network, virtual technology merely enables server consolidation by replacing physical servers with virtual servers that function exactly the same way — and need to be configured in much the same way — as their physical equivalents. You can consolidate servers using virtual technology without mixing trust zones and continue to rely on your existing security infrastructure.

However, replicating a purely physical network topology with virtual machines can greatly limit the benefits that virtualization can provide. If you do not run virtual machines of different trust zones together on one host, the degree of consolidation you achieve can remain low. In addition, you might not realize operational benefits from more advanced virtualization capabilities, such as live migration and high availability.

VMware customer experience and independent analyst research demonstrate that a virtualized trust zone configuration option can be secured. However, some network security professionals are concerned that trust zone virtualization might decrease security. This is understandable, because virtualization involves new terminology and technology.

Fortunately, as a network security professional, you already have the critical knowledge necessary to ensure the proper configuration of virtual networks with a segmented infrastructure. Enforcement policies on a virtual network are the same as those on a physical network. The difference is that the way in which these policies are enforced can be different in a virtual environment. Gartner research supports this view by suggesting that security risks primarily emanate from administrative misconfiguration and not from the virtual infrastructure. (See the Resources section for information on this Gartner report.)

This paper provides information that will enable you to configure virtualized trust zones correctly and deploy them seamlessly. It provides detailed descriptions of three different virtualized trust zone configurations and identifies best practice approaches that enable secure deployment. It is very important to understand that the biggest risk to the virtual environment is misconfiguration, not the technology. Thus you need strong audit controls to ensure that you avoid misconfiguration, either accidental or malicious.

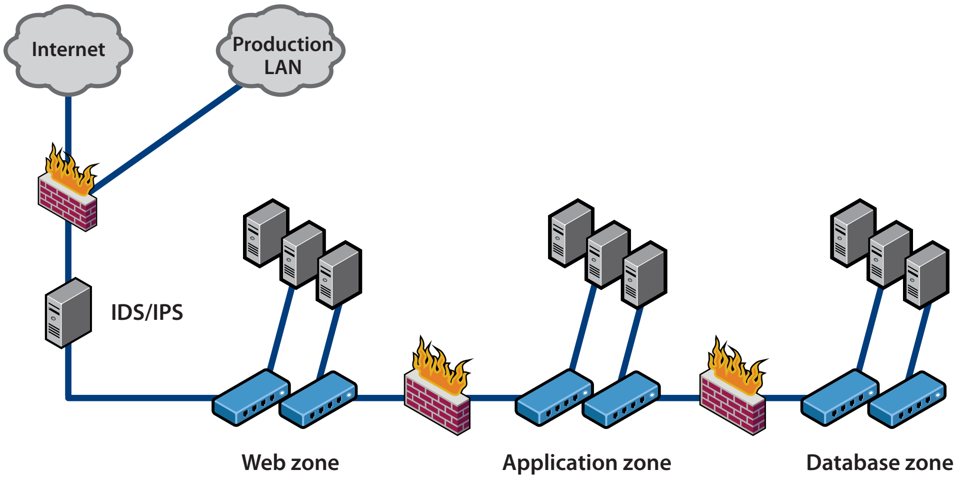

Figure 1 — Example of trust zones in a physical environment

Three Typical Virtualized Trust Zone Configurations

A virtualized network can fully support and enforce a wide range of configurations to separate trust zones. The three options described in this section are typical.

Partially Collapsed with Separate Physical Trust Zones

Organizations that want to keep trust zones physically separated tend to choose this method, shown in figure 2. In this configuration, each zone uses separate VMware® ESX hosts or clusters. Zone isolation is achieved with air-gap separation of servers and physical network security devices. The physical network does not require any change. The only difference between this configuration and a purely physical datacenter is that the servers within the trust zone are virtualized.

This configuration limits the benefits you can achieve from virtualization because it does not maximize consolidation ratios, but this approach is a good way to introduce virtual technology into a network. Because it has minimal impact on an existing physical network, this configuration avoids certain risks. For instance, it minimizes the impact of the potential loss of separation of duties. This, in turn, greatly reduces the chance that an unqualified individual might be in a position to introduce a vulnerability through misconfiguration.

In this configuration, you do not need to configure dedicated virtual switches or use 802.1q VLANs within the virtual infrastructure. You perform all networking isolation on the physical network, not within the virtual infrastructure.

Advantages

- Simpler, less complex configuration
- Less change to physical environment, and thus less change to separation of duties and less change in staff knowledge requirements
- Less chance for misconfiguration because of lower complexity

Disadvantages

- Lower consolidation and utilization of resources
- Higher costs because of need for more ESX hosts and additional cooling and power
- Incomplete utilization of the operational efficiencies virtualization can provide

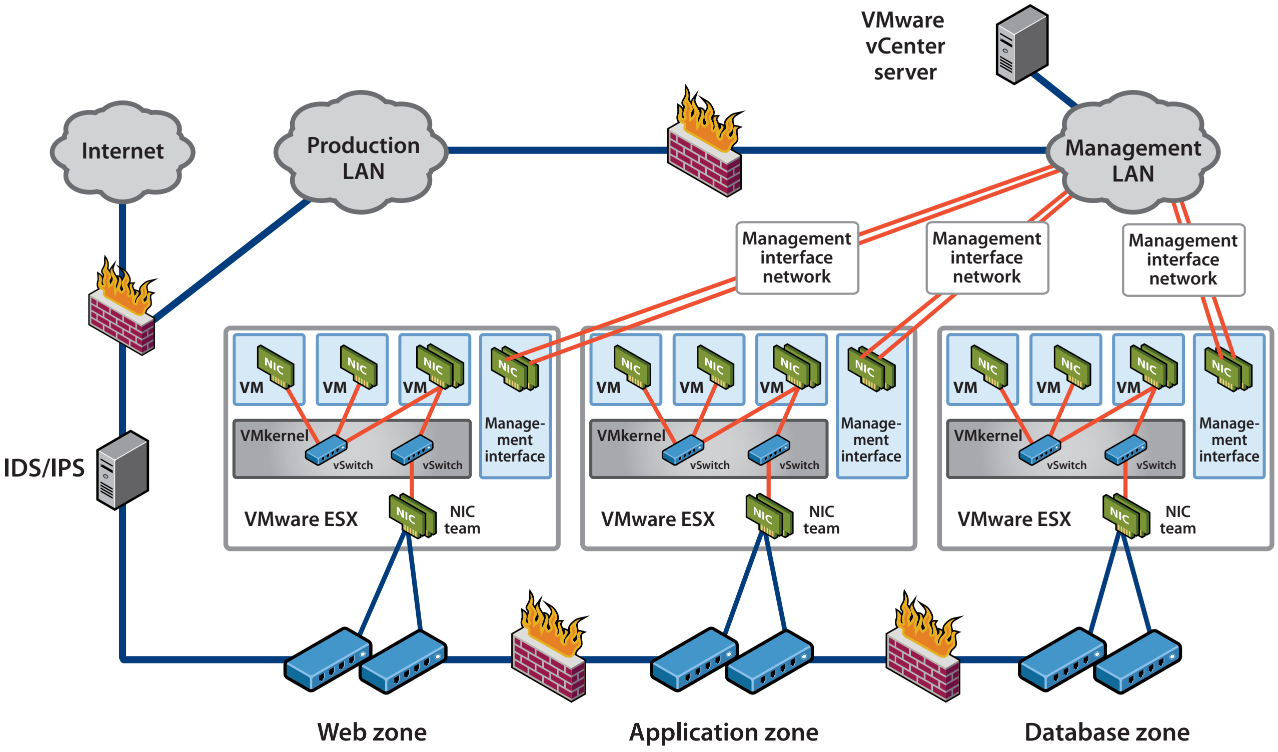

Figure 2 — Partially collapsed with separate physical trust zones

Partially Collapsed with Virtual Separation of Trust Zones

In this configuration, shown in Figure 3, you use virtual technology to enforce trust zone separation. As a result, you can locate virtual servers with different trust levels on the same ESX host. Although physical security devices are part of the configuration, this approach consolidates all virtual machines on the same hosts, thus requiring substantially fewer physical servers. By achieving full server consolidation, you generate significant cost savings for your IT organization.

Enforcement of the security zones at the network level takes place in both virtual and physical realms. You use virtual switches to enforce which virtual servers are connected to which zone, but you use physical hardware to enforce the network security between the zones. For this reason, virtual servers must use the physical network and pass through physical security devices to communicate between trust zones.

The impact of the potential loss of separation of duties — and the associated risk that an unqualified individual might be in a position to introduce vulnerabilities through misconfiguration — is greater in this case than when you have separate physical trust zones, but the potential impact is minimized by the fact that network security is still physically enforced. In this configuration, you should create and enforce access controls that allow only privileged administrators to assign virtual machines to highly sensitive trust zones, and restrict less privileged administrators to less sensitive zones.

Because the trust zones in this configuration are enforced in the virtualization layer, you should audit virtual switches regularly for consistent policy and settings to mitigate the potential for a virtual machine to be placed on the wrong network.

Although Figure 3 shows separate virtual switches for each zone, you can accomplish the same goal by using 802.1q VLANs. The most important factor in determining which configuration option to choose is typically the number of physical NICs present in the hardware. You should always dedicate at least one physical NIC to the virtualization management network. If possible, use two physical NICs for the virtualization management network to provide redundancy.

Advantages

- Full utilization of resources
- Full utilization of the advantages of virtualization
- Lower cost

Disadvantages

- More complexity
- Greater chance of misconfiguration requires explicit configuration of separation of duties to help mitigate risk of misconfiguration; also requires regular audits of configurations

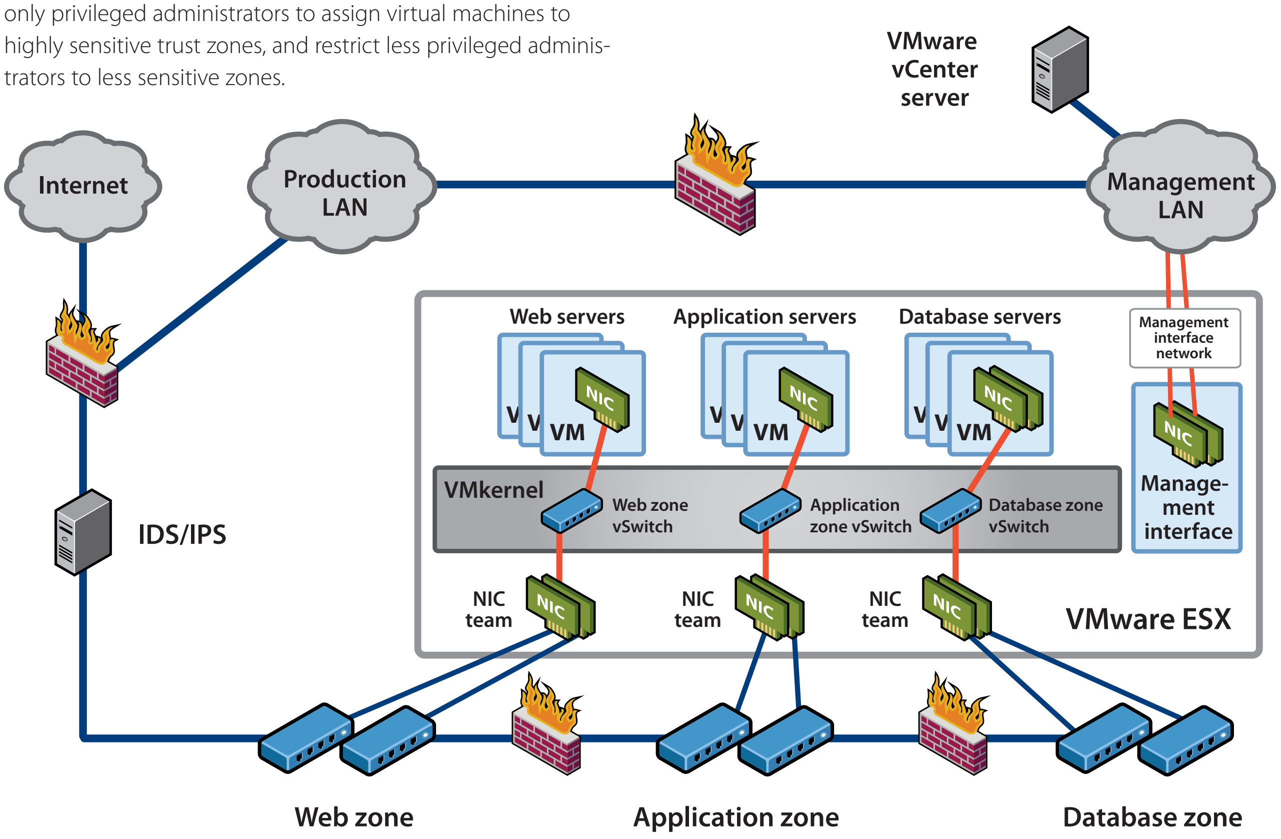

Figure 3 — Partially collapsed with virtual separation of trust zones

Fully Collapsed Trust Zones

Taking full advantage of VMware technology, this approach, shown in Figure 5, virtualizes the entire datacenter — including all network and security devices. For DMZs, this is sometimes described as a "DMZ in a box." This configuration enables you to maximize server consolidation and realize significant cost reductions.

This configuration fully leverages consolidation benefits. All servers and security devices are virtualized in this configuration, enabling you to isolate the virtual servers and the networks while managing communications between the zones with virtual security appliances. This completely virtual infrastructure can fully enforce the isolation and security between zones. You can collocate virtual machines of different security levels on the same physical server or servers and bring network security devices into the virtual infrastructure.

You can choose from an increasing number of virtual network security devices to manage and secure the communication between virtual trust zones. For example, you can use VMware vShield Zones to bridge trust zones and allow only selective communication between them, while monitoring both allowed and disallowed traffic. If trust zones reside on different LAN network segments, Layer 3 routing between trust zones still takes place in the physical part of the network, unless you use a virtual routing device. However, you do not need to use a virtual router to enjoy the consolidation and operational benefits of a fully collapsed trust zone.

This is the most complex configuration of the three. Therefore, risks associated with misconfiguration are higher and you need to take care when planning this configuration. Enforcing separation of duties through the use of roles and permissions is very important. Also, when you plan and deploy your virtual networks, you must make sure that the isolation of those networks is enforced and that any communications between virtual machines on separate networks are properly routed through the virtual firewalls as well as any other in-line security devices you are using.

It is especially important in this configuration to audit the configurations of virtual firewalls and virtual switches for consistent policy and settings, because all of the zone enforcement is performed in the virtual environment. If the policy is different on any of the virtual firewalls or virtual switches, you can encounter such issues as dropped connections — for example, when a virtual machine is moved to a new host using VMotion

You can use 802.1q VLANs in this configuration, but VLANs are not required as they are in the configuration using partially collapsed trust zones with virtual separation. With a fully collapsed trust zone, you need a minimum of three NICs per ESX host — one to connect to the Internet, a second to connect to

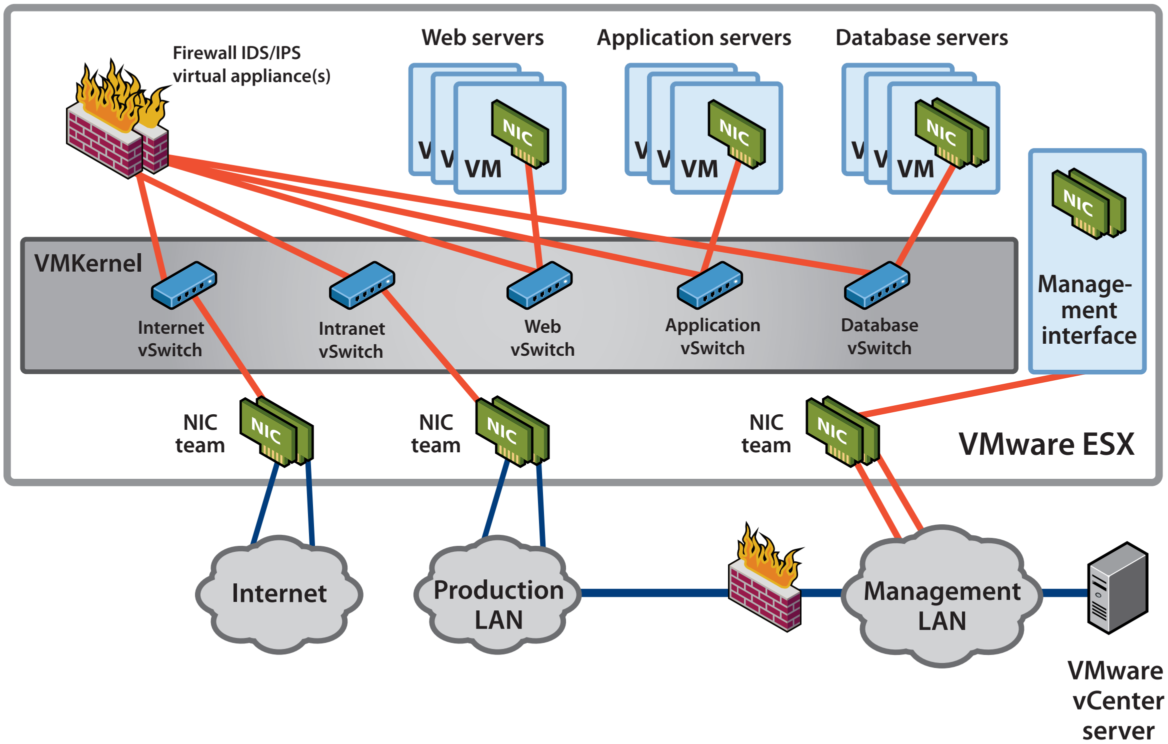

Figure 4 — Fully collapsed trust zones

the internal network, and a third for the management network. VMware strongly encourages NIC teaming for redundancy, so you should consider using enough physical NICs to allow for redundancy of all networks.

Advantages

- Full utilization of resources, replacing physical security devices with virtual
- Lowest-cost option
- Management of entire network from a single management workstation

Disadvantages

- Greatest complexity, which in turn creates highest chance of misconfiguration
- Requirement for explicit configuration of separation of duties to help mitigate risk of misconfiguration; also requires regular audits of configurations
- Loss of certain functionality, such as VMotion, if current virtual security appliances are not properly configured and audited

Best Practices for Achieving a Secure Virtualized Mixed Trust Zone Deployment

Most security issues do not arise from the virtualization infrastructure itself but from administrative and operational challenges. The primary risks are caused by a loss of separation of duties. When this occurs, individuals who lack the necessary experience and capabilities are given an opportunity to introduce vulnerabilities through misconfiguration. For instance, they can accidentally place the virtual NIC of a virtual machine in the wrong trust zone. This risk — which also can also occur in purely physical environments — can breach the isolation between networks and virtual machines of different trust levels.

Although best practice security policies and procedures for introducing virtualization into mixed trust zone environments are not overly complex, you should be aware of the critical challenges and best practice methods in order to mitigate risk.

At every stage, you must remember that virtual machines need the same type of protections as their physical counterparts — including antivirus software, host intrusion protection, configuration management, and patching in a timely manner. In short, virtual machines need to be secured in the same manner as physical machines.

After you decide to either partially or completely collapse trust zones, your first step should be to map out which virtual servers will reside on which physical servers and to establish the level of trust that is required for each system. Afterwards, you should follow the guidelines in this section.

Virtualized Trust Zone Security Checklist

- Harden and isolate the service console and management network
- Enforce consistency of network configuration across all hosts
- Set Layer 2 security options on virtual switches
- Enforce separation of duties
- Use ESX resource management capabilities
- Regularly audit virtualized configuration

Harden and Isolate the Service Console and Management Network

This step is especially important because access to the service console of an ESX host gives a user with root privileges full control over the virtual machines on that host. Although access to the service console is secured through authentication, you can provide additional security against unauthorized access by creating additional layers of security.

In addition, you should isolate the service console. To do so, make sure that the network to which the service console is isolated is firewalled and accessible only to authorized administrators. You can use a VPN or other access control methods to restrict access to the management network.

Although VMware ESXi does not have a service console, you should nonetheless isolate the management interface, which provides access to the ESXi APIs, and you should harden the server.

For details on how to harden both ESX and ESXi, read "VMware Infrastructure 3 Security Hardening" (see Resources for a link).

Enforce Consistency of Network Configuration Across All Hosts

Ensuring that the virtual network is configured in a consistent manner across all hosts is particularly critical because accidentally connecting virtual servers to the wrong networks can undermine all other security efforts. By clearly labeling the networks, you make it less likely that a virtual machine can be connected to an unauthorized network accidentally.

You can use automated tools, such as VMware Host Profiles or other third-party tools, to enforce and monitor configuration consistency. Another approach is to use distributed switch technology, such as the VMware vNetwork Distributed Switch, or a third-party switch such as the Nexus 1000V. This enables you to manage and configure virtual networking on a cluster of ESX or ESXi hosts in a single place, thus avoiding the possibility of configuration inconsistency altogether.

Set Layer 2 Security Options on Virtual Switches

Protect against attacks such as data snooping, sniffing, and MAC spoofing by disabling the promiscuous mode, MAC address changes, and forged transmissions capabilities on the virtual network interfaces. These capabilities are very rarely needed and create opportunities for exploitation. Fortunately, in the VMware virtual network layer you have full control over these options, something that is not the case in purely physical environments.

Enforce Separation of Duties

Mitigate configuration mistakes by using vCenter to define roles and responsibilities for each administrator of the vSphere infrastructure. By distributing rights based on skills and responsibilities, you can significantly reduce the chance of misconfiguration. As an added benefit, this method also limits the amount of authority any one administrator has over the system as a whole.

In particular, you should restrict privileges for performing the following actions:

- Reconfiguring virtual networks
- Assigning virtual machines to sensitive networks
- Changing firewall or other network security policies

Best practice also dictates that you use administrator or root access only in emergency situations. This practice mitigates the potential for accidental or malicious misconfiguration by an administrator. It also helps further limit the number of people who know the password for this type of account, which provides full control.

Use ESX Resource Management Capabilities

Denial of service within a virtual environment can occur if an individual virtual machine is allowed to use a disproportionate share of ESX host resources. In so doing, it starves other virtual machines running on the same ESX host. Such denial of service can occur as the result of malicious intent or accidentally, but you can guard against this possibility by setting resource reservations and limits for virtual machines using vCenter. You should use the same resource controls to ensure that sufficient resources are available to virtual network security devices.

Regularly Audit the Virtualized Configuration

Regular audit of configurations is essential in both physical and virtual environments. When virtualizing any part of your infrastructure, it is important to audit the configurations of all of the components — including vCenter, vSwitches, virtual and physical firewalls, and any other security devices —regularly. You must conduct these audits to make sure that changes to configurations can be controlled and that the changes do not cause a security hole in the configuration. The use of configuration management and compliance tools can greatly assist with the audit process. Audits are especially important for the second and third options discussed in this paper because the risk of misconfiguration is much higher in those topologies.

Conclusion

You can take advantage of the benefits of virtualization in setting up mixed trust zones, and you can do so securely, maintaining compliance with your organization's policies. There are a number of configurations you can use to achieve this goal.

As part of continuing efforts to keep customers informed of best practice approaches to security, VMware has generated a number of technology briefs that enable you to further harden ESX hosts and vCenter and to ensure the overall security of your vSphere Infrastructure. For a list of technical documents that fully detail insights gained from deploying virtual technology at over 20,000 IT organizations worldwide, go to the VMware Security Center on the Web (see References for a link).

Resources

- "Server Virtualization Can Break DMZ Security," by Neil MacDonald and Greg Young, Gartner Research
- "VMware Infrastructure 3 Security Hardening" http://www.vmware.com/resources/techresources/726
- VMware Security Center http://www.vmware.com/security

Revision: 20090519 Item: BP-059-INF-02-01

VMware, Inc. 3401 Hillview Ave. Palo Alto CA 94304 USA Tel 650-475-5000 Fax 650-475-5001 www.vmware.com

vmware®