BEST PRACTICES

DMZ Virtualization with VMware Infrastructure

vmware®

Table of Contents

DMZ Virtualization with VMware Infrastructure

Virtualized DMZ Networks

As virtualization of network DMZs becomes more common, demand is increasing for information to help network security professionals understand and mitigate the risks associated with this practice. This paper provides detailed descriptions of three different virtualized DMZ configurations and identifies best practice approaches that enable secure deployment.

VMware customer experience and independent analyst research demonstrate that it is possible to set up a DMZ in a virtualized environment that is as secure as a DMZ in a physical environment. However, some network security professionals are concerned that DMZ 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 a DMZ using virtual network infrastructure. Enforcement policies on a virtual network are the same as those on a physical network. Gartner research supports this view by suggesting that security risks primarily emanate from administrative misconfiguration and not from the virtual infrastructure. (See the References section for information on this Gartner report.)

This paper provides information that will enable you to configure a virtualized DMZ correctly and deploy it seamlessly.

The biggest risk to a DMZ in a virtual environment is misconfiguration, not the technology. Thus you need strong audit controls to ensure that you avoid misconfiguration, either accidental or malicious.

As shown in figures 1 and 2, the introduction of virtual technology into a DMZ does not have to change the DMZ topology significantly. As with other parts of the network, virtual technol-

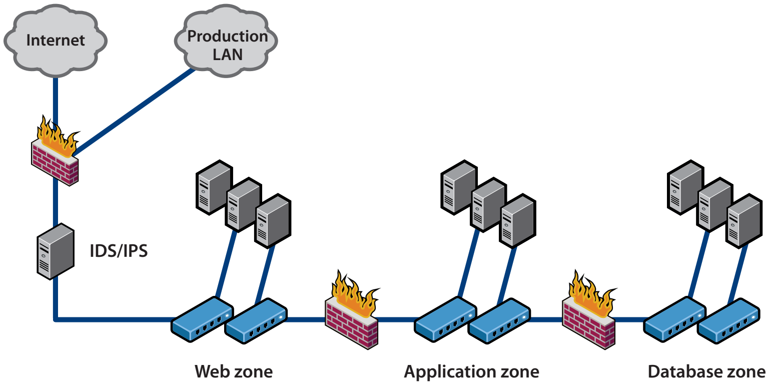

Figure 1 — A typical DMZ in a physical environment

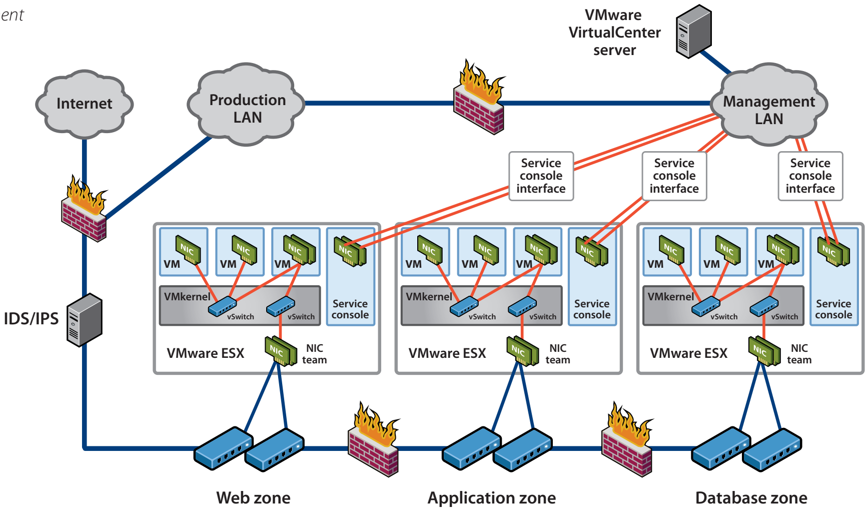

Figure 2 — A typical DMZ in a virtual environment

ogy merely enables you to consolidate servers 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 in a DMZ using virtual technology and continue to rely on your existing security infrastructure.

Three Typical Virtualized DMZ Configurations

A virtualized DMZ 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 DMZ with Separate Physical Trust Zones

Organizations that want to keep DMZ zones physically separated tend to choose this method, shown in Figure 3. In this configuration, each zone uses separate ESX Server clusters. Zone isolation is achieved with physical security devices. The physical network does not require any change. The only difference between this configuration and a purely physical DMZ 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 removes many 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
- Less change to separation of duties; 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 advantages of virtualization

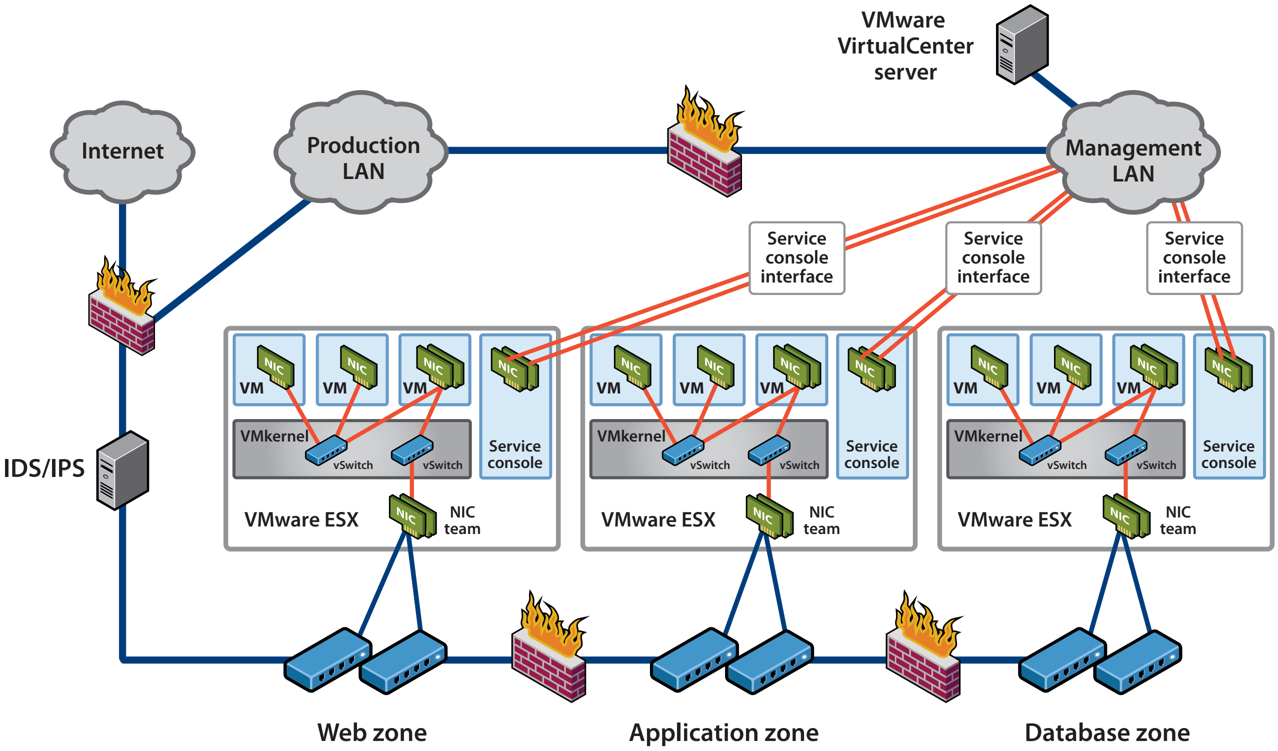

Figure 3 — Partially collapsed DMZ with separate physical trust zones

Partially Collapsed DMZ with Virtual Separation of Trust Zones

In this configuration, shown in Figure 4, you use virtual technology to enforce DMZ trust zone separation. As a result, you can locate virtual servers with different trust levels on the same VMware® ESX host. Although physical security devices are part of the configuration, this approach consolidates all DMZ servers into virtual machines on one ESX host cluster. As a result, you need substantially fewer physical servers. By leveraging the full functionality of the virtual infrastructure, you generate significant cost savings for your IT organization.

Enforcement of the DMZ security zones takes place in both virtual and physical realms. You use virtual switches to enforce which virtual servers are connected to which DMZ 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 DMZ trust zones.

The impact of the potential loss of separation of duties between network switch administrator and server administrator — and the associated risk that an unqualified individual will 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.

Because the trust zones in this configuration are enforced in the virtual infrastructure, 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 4 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 ESX service console. If possible, use two physical NICs for the service console 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

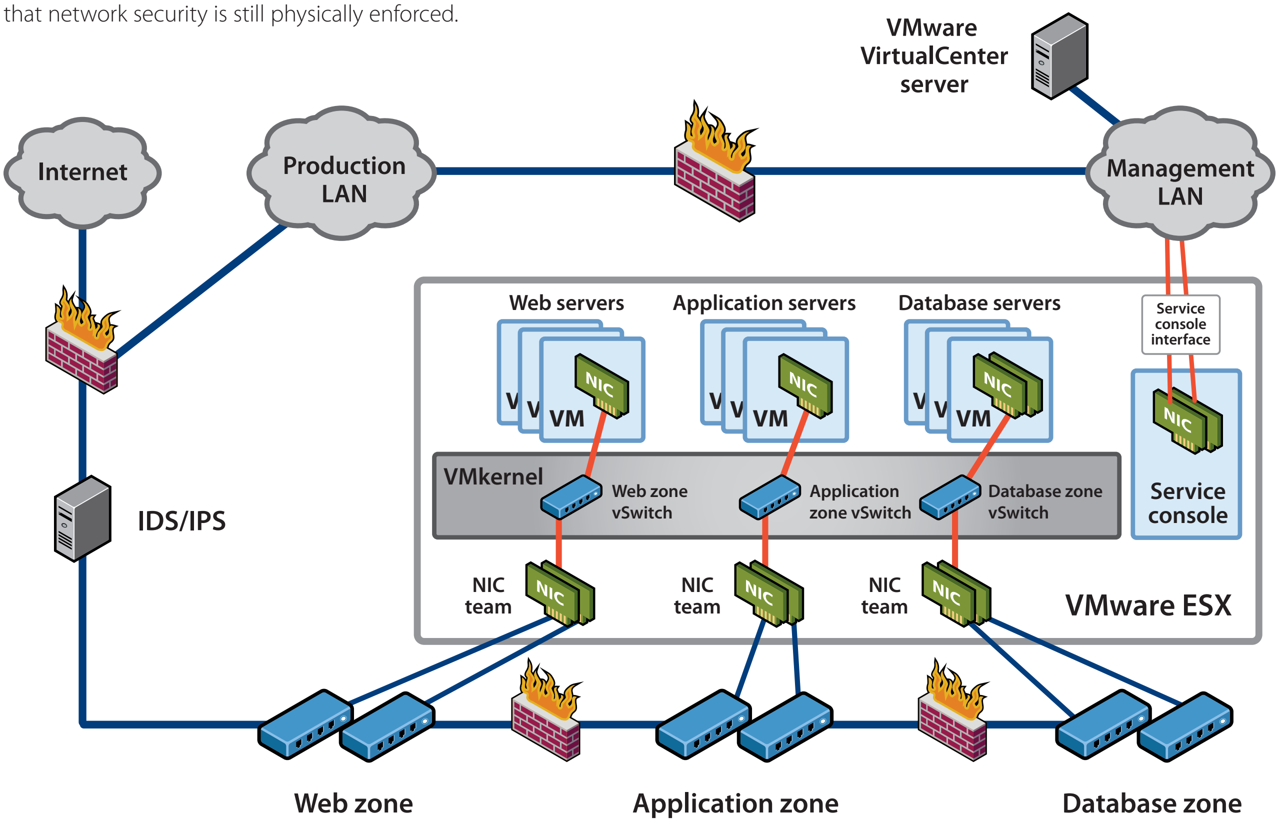

Figure 4 — Partially collapsed DMZ with virtual separation of trust zones

Fully Collapsed DMZ

Taking full advantage of VMware technology, this approach, shown in Figure 5, virtualizes the entire DMZ — including all network and security devices. 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. On the other hand, security appliances in this configuration can also interfere with such VMware Infrastructure capabilities as VMware VMotion and VMware Distributed Resource Scheduler because of limitations in current virtual security devices. The introduction of the VMsafe security-specific APIs will remove these limitations in future releases of VMware Infrastructure.

This completely virtual infrastructure can fully enforce isolation and security between the DMZ zones. You can locate virtual servers of different security levels on the same physical ESX host and bring network security devices into the virtual infrastructure.

You must consider the same potential risks you would in a completely physical infrastructure, but with proper configuration and application of best practices, you can mitigate those risks. Compared to the two other approaches discussed in this paper, this is the most complex configuration. Therefore, risks associated with misconfiguration are higher and you need to take great care when planning this configuration. You should enforce separation of duties by using roles and permissions within VirtualCenter. You should also plan and deploy virtual networks very carefully to make sure that the isolation of those networks is enforced and that any communications between virtual machines in separate networks are properly routed through the virtual firewalls as well as any other inline security devices you are using.

It is especially important in this configuration that you 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 might see such issues as dropped connections when a virtual machine is moved using VMotion.

You can use 802.1q VLANs in this configuration, but VLANs are not required as they are in the partially collapsed DMZ with virtual separation of trust zones. With a fully collapsed DMZ, you need a minimum of three NICs per ESX host — one to connect to the Internet, a second to connect to the internal network, and a third for the ESX service console or management network. VMware strongly encourages NIC teaming for redundancy, so

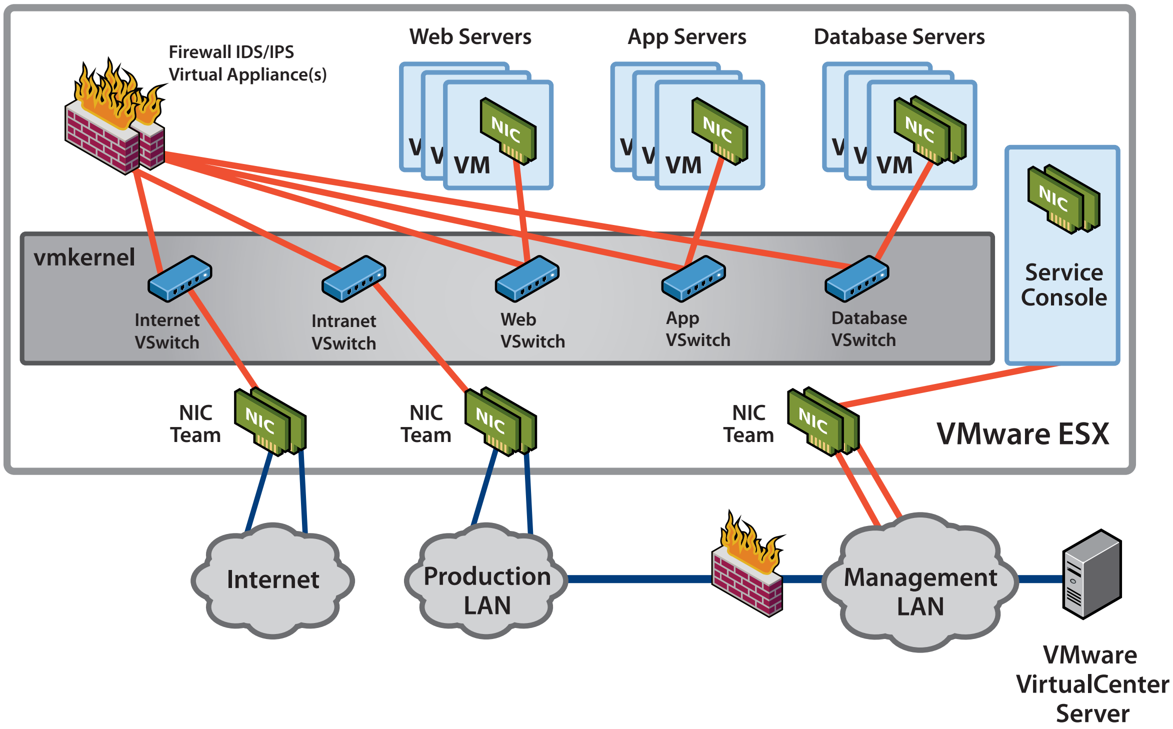

Figure 5 — Fully collapsed DMZ

you should consider using a minimum of six physical NICs per host in this configuration.

Advantages

- Full utilization of resources, replacing physical security devices with virtual
- Lowest-cost option
- Management of entire DMZ and 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 DMZ 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 configuring a DMZ in a virtualized environment 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 types 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 virtualize a DMZ, your first step should be to map out which virtual servers will reside on which physical ESX hosts and to establish the level of trust that is required for each system. Afterwards, you should follow the guidelines in this section

Virtualized DMZ Security Checklist

- Harden and isolate the service console
- Clearly label networks for each zone within the DMZ
- Set Layer 2 security options on virtual switches
- Enforce separation of duties
- Use ESX resource management capabilities
- Regularly audit virtualized DMZ configuration

Harden and Isolate the Service Console

This step is especially important in a DMZ because access to the service console of an ESX host allows for 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 following the hardening guidelines in "VMware Infrastructure 3 Security Hardening" (see References for a link).

In addition, you should physically 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. Also, although VMware ESXi does not have a service console and much of the hardening is not necessary if you are using ESXi, you should nonetheless isolate the management interface, which provides access to the ESXi APIs.

You should also isolate SAN connections and the VMotion networks from this management network.

Clearly Label Networks for each Zone within the DMZ

Clearly labeling networks for each zone within the DMZ 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.

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, with VMware Infrastructure 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 VirtualCenter to define roles and responsibilities for each administrator of the VMware Infrastructure 3 environment. 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.

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 VirtualCenter.

Regularly Audit Virtualized DMZ Configuration

Regular audit of configurations is essential in both physical and virtual environments. When virtualizing a DMZ or any part of your infrastructure, it is important to audit the configurations of all of the components — including VirtualCenter, virtual switches, 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 a DMZ just as you do elsewhere in your organization's networks, and you can do so securely, maintaining compliance with your organization's policies. There are a number of configurations you can use to achieve a secure virtualized DMZ.

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 the service console and VirtualCenter and to ensure the overall security of your VMware Infrastructure 3 environment. 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).

References

- "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: 20080508 Item: BP-059-INF-01-01

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