Cloud Computing Security

Rajendra Kachhwaha
rajendra1983@gmail.com

January 15, 2017

Outline

What is Virtualization?

1. Virtualization is the simulation of the software and/or hardware upon which other software runs. This simulated environment is called a virtual machine (VM).
2. There are many forms of virtualization, distinguished primarily by computing architecture layer. For example, application virtualization provides a virtual implementation of the application programming interface (API) that a running application expects to use, allowing applications developed for one platform to run on another without modifying the application itself.
3. The Java Virtual Machine (JVM) is an example of application virtualization; it acts as an intermediary between the Java application code and the operating system (OS).
4. Another form of virtualization, known as operating system virtualization, provides a virtual implementation of the OS interface that can be used to run applications written for the same OS as the host, with each application in a separate VM container.
5. In full virtualization (a form of virtualization), one or more OSs and the applications they contain are run on top of virtual hardware.

What is Full Virtualization?

6. Each instance of an OS and its applications runs in a separate VM called a guest operating system.
7. The guest OSs on a host are managed by the hypervisor, also called the virtual machine monitor (VMM), which controls the flow of instructions between the guest OSs and the physical hardware, such as CPU, disk storage, memory, and network interface cards.
8. The hypervisor can partition the systems resources and isolate the guest OSs so that each has access to only its own resources, as well as possible access to shared resources such as files on the host OS.
9. Each guest OS can be completely encapsulated, making it portable. Some hypervisors run on top of another OS, which is known as the host operating system.
10. Two forms of full virtualization: In bare metal virtualization, also known as native virtualization, the hypervisor runs directly on the underlying hardware, without a host OS; the hypervisor can even be built into the computers firmware.

Types of Full Virtualization?

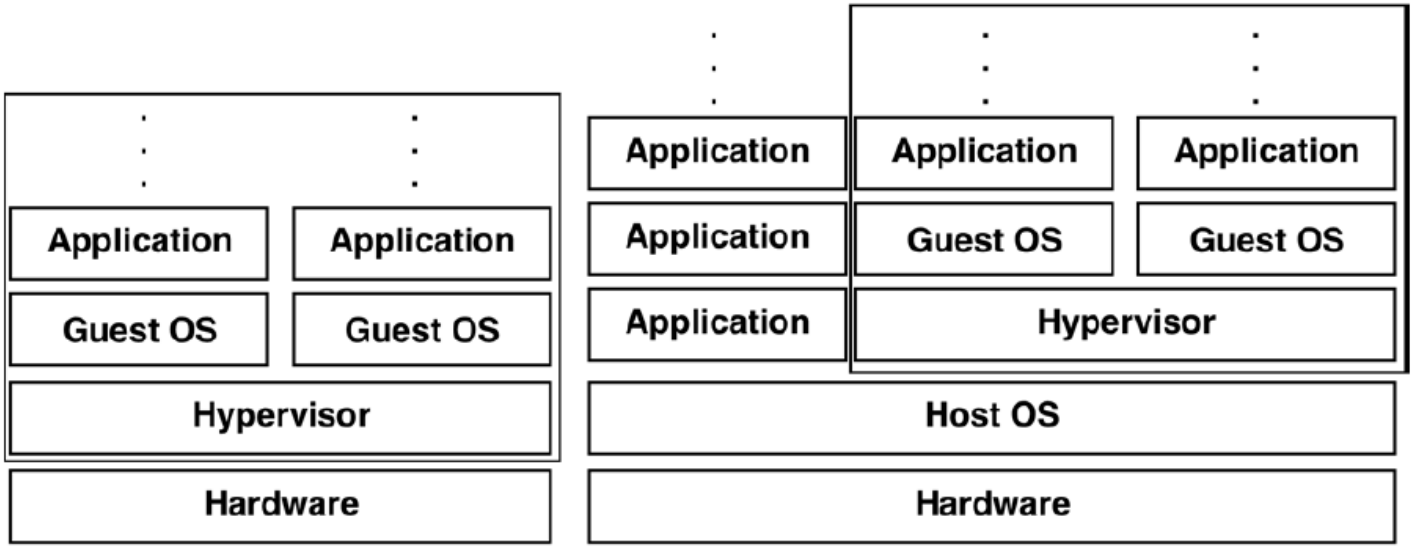
11 In the other form of full virtualization, known as hosted virtualization, the hypervisor runs on top of the host OS; the host OS can be almost any common operating system such as Windows, Linux, or MAC OS.

12 Hosted virtualization architectures usually also have an additional layer of software (the virtualization application) running in the guest OS that provides utilities to control the virtualization while in the guest OS, such as the ability to share files with the host OS.

13 Hosted virtualization architectures also allow users to run applications such as web browsers and email clients alongside the hosted virtualization application, unlike bare metal architectures, which can only run applications within virtualized systems.

14 Servers are most often virtualized on computers using bare metal virtualization. Desktops are most often virtualized on computers with hosted virtualization.

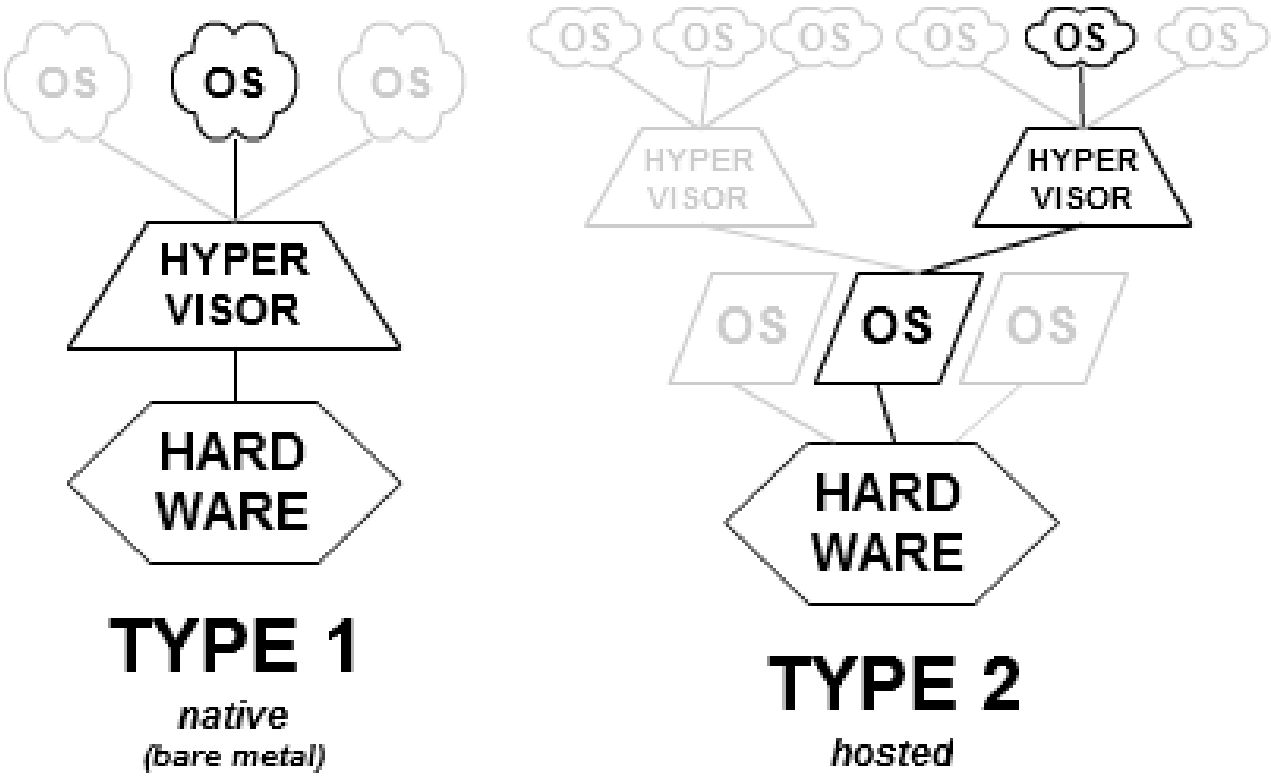
Types of Full Virtualization?



Full Virtualization Architectures

Types of Full Virtualization?

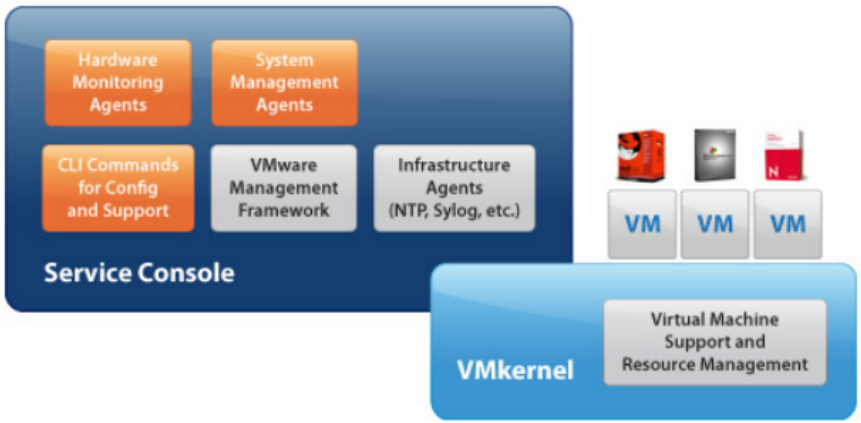
15 In both bare metal and hosted virtualization, each guest OS appears to have its own hardware, like a regular computer. This includes:CPU, Memory, Storage (hard disk, and possibly floppy and CD-ROM drives), Storage controllers, Ethernet controllers, Display and sound devices, Keyboard and mouse.



What is VMWare ESX and ESXi?

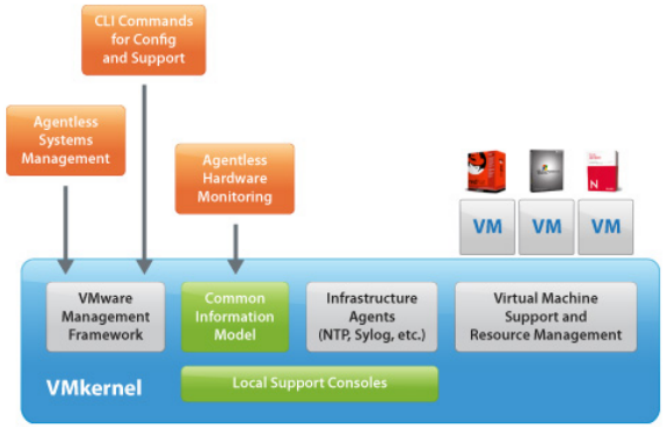
1. VMware ESXi (formerly ESX) is an enterprise-class, type-1 hypervisor developed by VMware for deploying and serving virtual computers.
2. As a type-1 hypervisor, ESXi is not a software application that one installs in an operating system (OS); instead, it includes and integrates vital OS components, such as a kernel.
3. The name ESX originated as an abbreviation of Elastic Sky X.

- ESX (Elastic Sky X) is the VMwares enterprise server virtualization platform. In ESX, VMkernel is the virtualization kernel which is managed by a console operating system which is also called as Service console. Which is linux based and its main purpose is it to provide a Management interface for the host and lot of management agents and other third party software agents are installed on the service console to provide the functionalists like hardware management and monitoring of ESX hypervisor.



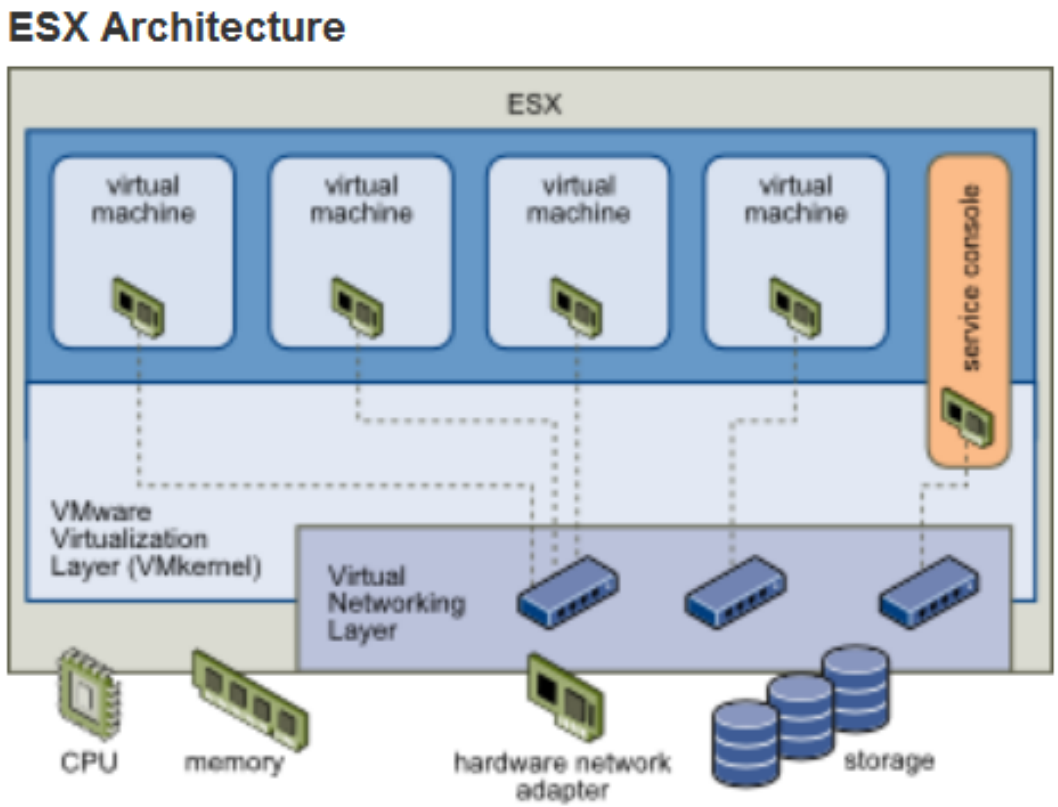
What is VMWare ESXi?

4. ESXi (Elastic sky X Integrated) is also the VMwares enterprise server virtualization platform.
5. In ESXi, Service console is removed. All the VMware related agents and third party agents such as management and monitoring agents can also run directly on the VMkernel.
6. ESXi is ultra-thin architecture which is highly reliable and its small codebase allows it to be more secure with less codes to patch. ESXi uses Direct Console User Interface (DCUI) instead of a service console to perform management of ESXi server. ESXi installation will happen very quickly as compared to ESX installation.



ESX Architecture and Security Features?

1. The components and the overall architecture of ESX are designed to ensure security of the ESX system as a whole.
2. From a security perspective, ESX consists of four major components: the virtualization layer, the virtual machines, the service console, and the virtual networking layer.



Security and the Virtualization Layer?

1. The virtualization layer, or VMkernel, is a kernel designed by VMware to run virtual machines. It controls the hardware that hosts use and schedules the allocation of hardware resources among the virtual machines.
2. Because the VMkernel is fully dedicated to supporting virtual machines and is not used for other purposes, the interface to the VMkernel is strictly limited to the API required to manage virtual machines.
3. ESX provides additional VMkernel protection with the following features:
   - Memory Hardening:
     The ESX kernel, user-mode applications, and executable components such as drivers and libraries are located at random, non-predictable memory addresses. Combined with the non-executable memory protections made available by microprocessors, this provides protection that makes it difficult for malicious code to use memory exploits to take advantage of vulnerabilities.
   - Kernel Module Integrity:
     Digital signing ensures the integrity and authenticity of modules, drivers and applications as they are loaded by the VMkernel. Module signing allows ESX to identify the providers of modules, drivers, or applications and whether they are VMware-certified.

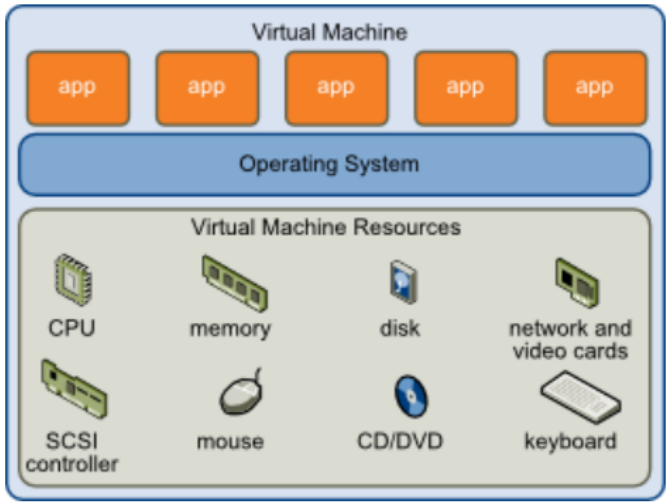
Security and Virtual Machines?

1. Virtual machines are the containers in which applications and guest operating systems run.
2. By design, all VMware virtual machines are isolated from one another. This isolation enables multiple virtual machines to run securely while sharing hardware and ensures both their ability to access hardware and their uninterrupted performance.
3. Even a user with system administrator privileges on a virtual machines guest operating system cannot breach this layer of isolation to access another virtual machine without privileges explicitly granted by the ESX system administrator.
4. As a result of virtual machine isolation, if a guest operating system running in a virtual machine fails, other virtual machines on the same host continue to run.
5. The guest operating system failure has no effect on:
   - The ability of users to access the other virtual machines.
   - The ability of the operational virtual machines to access the resources they need
   - The performance of the other virtual machines

Virtual Machines Isolation?

6. Each virtual machine is isolated from other virtual machines running on the same hardware.
7. Although virtual machines share physical resources such as CPU, memory, and I/O devices, a guest operating system on an individual virtual machine cannot detect any device other than the virtual devices made available to it, as shown in Virtual Machine Isolation.
8. Because the VMkernel mediates the physical resources and all physical hardware access takes place through the VMkernel, virtual machines cannot circumvent this level of isolation.

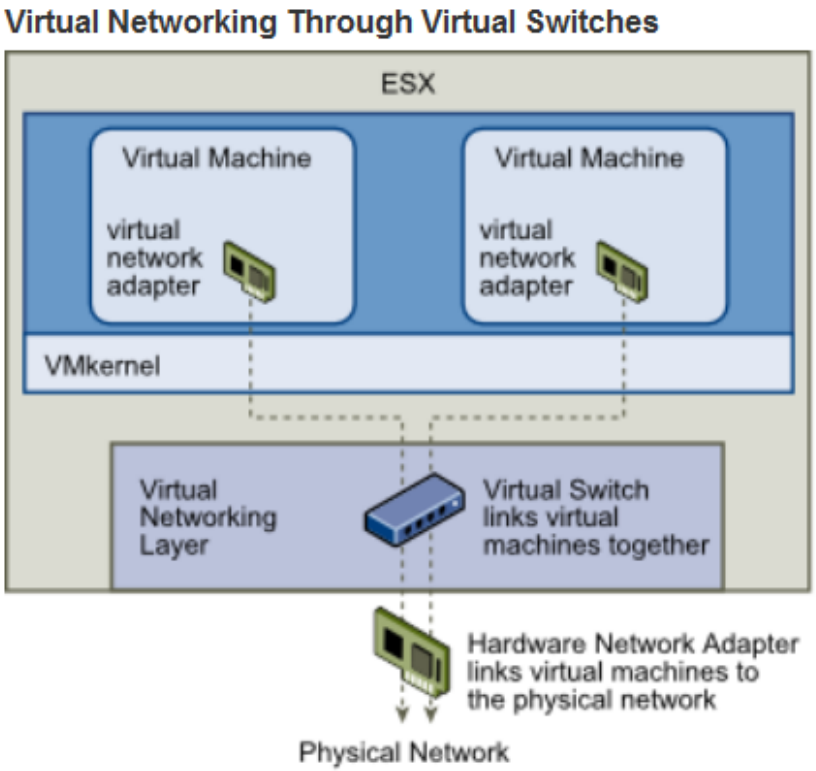
Virtual Machine Isolation



Virtual Networking Through Virtual Switches?

9 Just as a physical machine communicates with other machines in a network through a network card, a virtual machine communicates with other virtual machines running in the same host through a virtual switch.

10 Further, a virtual machine communicates with the physical network, including virtual machines on other ESX hosts, through a physical network adapter, as shown in Virtual Networking Through Virtual Switches.



Protect Virtual Machines?

11 These characteristics apply to virtual machine isolation in a network context:

- If a virtual machine does not share a virtual switch with any other virtual machine, it is completely isolated from virtual networks within the host.
- If no physical network adapter is configured for a virtual machine, the virtual machine is completely isolated from any physical networks.
- If you use the same safeguards (firewalls, antivirus software, and so forth) to protect a virtual machine from the network as you would for a physical machine, the virtual machine is as secure as the physical machine.

12 You can further protect virtual machines by setting up resource reservations and limits on the host. For example, through the detailed resource controls available in ESX, you can configure a virtual machine so that it always receives at least 10 percent of the hosts CPU resources, but never more than 20 percent.

13 Resource reservations and limits protect virtual machines from performance degradation that would result if another virtual machine consumed excessive shared hardware resources. For example, if one of the virtual machines on a host is incapacitated by a denial-of-service (DoS) attack.....????

Protect Virtual Machines?

14 For example, if one of the virtual machines on a host is incapacitated by a denial-of-service (DoS) attack, a resource limit on that machine prevents the attack from taking up so much of the hardware resources that the other virtual machines are also affected.

15 Similarly, a resource reservation on each of the virtual machines ensures that, in the event of high resource demands by the virtual machine targeted by the DoS attack, all the other virtual machines still have enough resources to operate.

16 By default, ESX imposes a form of resource reservation by applying a distribution algorithm that divides the available host resources equally among the virtual machines while keeping a certain percentage of resources for use by other system components.

17 This default behavior provides a degree of natural protection from DoS and distributed denial-of-service (DDoS) attacks.

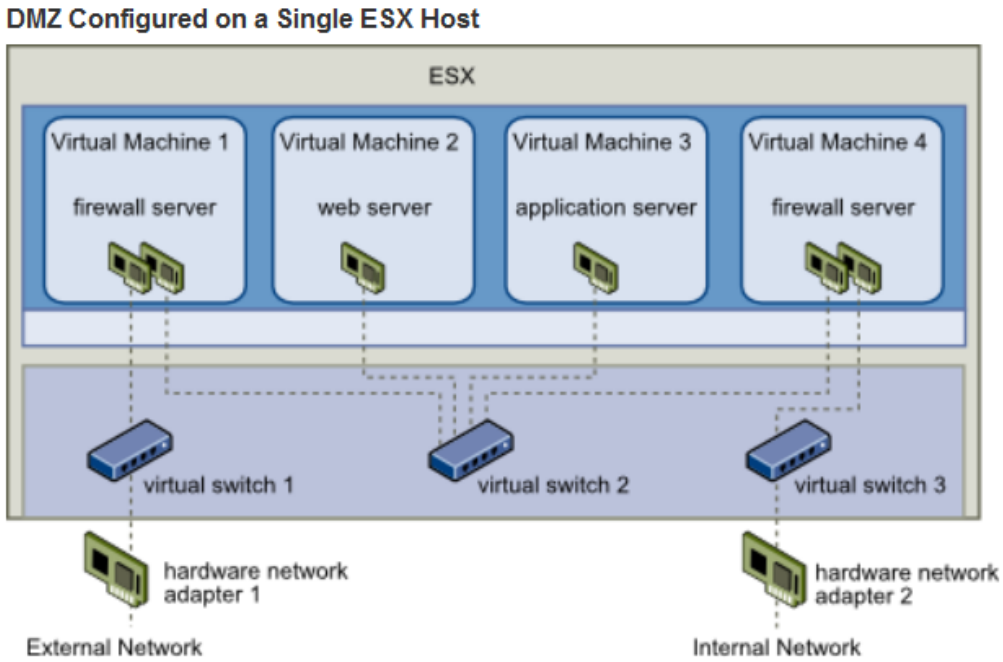
18 You set specific resource reservations and limits on an individual basis to customize the default behavior so that the distribution is not equal across the virtual machine configuration.

Security and the Virtual Networking Layer?

1. The virtual networking layer includes virtual network adapters and virtual switches.
2. ESX relies on the virtual networking layer to support communications between virtual machines and their users. In addition, hosts use the virtual networking layer to communicate with iSCSI SANs, NAS storage, and so forth.
3. The methods you use to secure a virtual machine network depend on which guest operating system is installed, whether the virtual machines operate in a trusted environment, and a variety of other factors.
4. Virtual switches provide a substantial degree of protection when used with other common security practices, such as installing firewalls.
5. ESX also supports IEEE 802.1q VLANs, which you can use to further protect the virtual machine network, service console, or storage configuration. VLANs let you segment a physical network so that two machines on the same physical network cannot send packets to or receive packets from each other unless they are on the same VLAN.
6. One example of how to use ESX isolation and virtual networking features to configure a secure environment is the creation of a network demilitarized zone (DMZ) on a single host.

Security and the Virtual Networking Layer?

7 In this example, four virtual machines are configured to create a virtual DMZ on Virtual Switch 2:



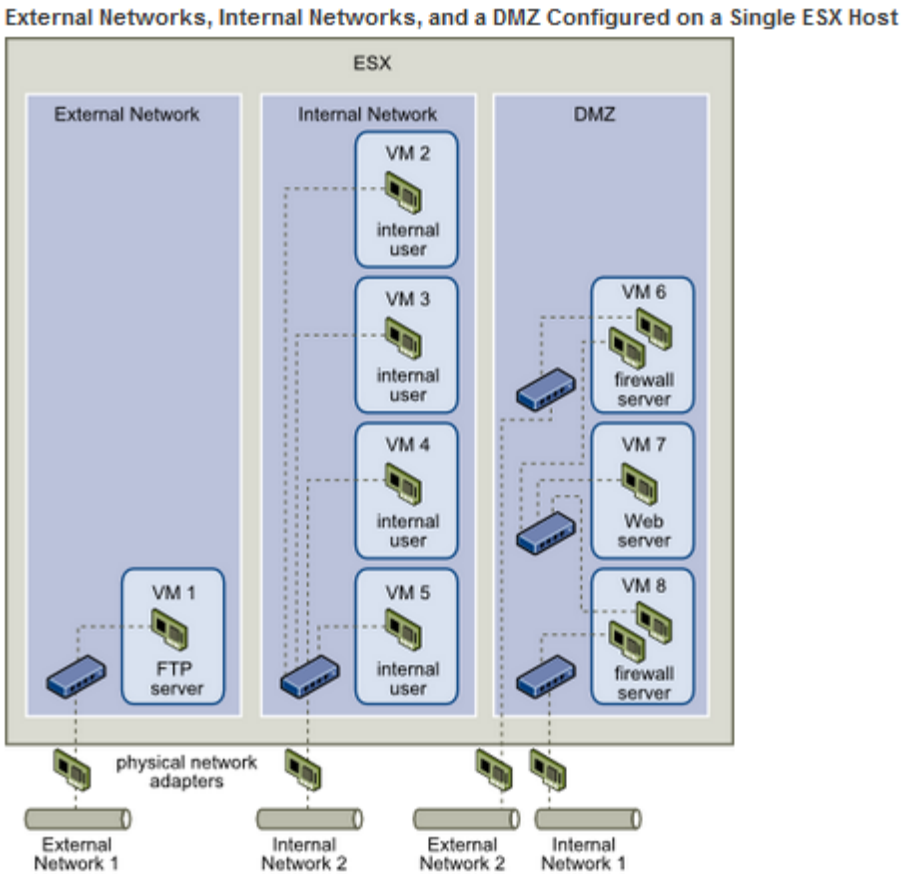
- Virtual Machine 1 and Virtual Machine 4 run firewalls and are connected to virtual adapters through virtual switches. Both of these virtual machines are multi homed.
- Virtual Machine 2 runs a Web server, and Virtual Machine 3 runs as an application server. Both of these virtual machines are single-homed.

Security and the Virtual Networking Layer?

8. The Web server and application server occupy the DMZ between the two firewalls.
9. The conduit between these elements is Virtual Switch 2, which connects the firewalls with the servers. This switch has no direct connection with any elements outside the DMZ and is isolated from external traffic by the two firewalls.
10. From an operational viewpoint, external traffic from the Internet enters Virtual Machine 1 through Hardware Network Adapter 1 (routed by Virtual Switch 1) and is verified by the firewall installed on this machine.
11. If the firewall authorizes the traffic, it is routed to the virtual switch in the DMZ, Virtual Switch 2. Because the Web server and application server are also connected to this switch, they can serve external requests.
12. Virtual Switch 2 is also connected to Virtual Machine 4. This virtual machine provides a firewall between the DMZ and the internal corporate network. This firewall filters packets from the Web server and application server.
13. If a packet is verified, it is routed to Hardware Network Adapter 2 through Virtual Switch 3. Hardware Network Adapter 2 is connected to the internal corporate network.

Security and the Virtual Networking Layer?

15 Creating Multiple Networks Within a Single ESX Host:



16 In this, the system administrator configured a host into three distinct virtual machine zones: FTP server, internal virtual machines, and DMZ. Each zone serves a unique function.

Security and the Virtual Networking Layer?

1. FTP server:
   Virtual Machine 1 is configured with FTP software and acts as a holding area for data sent to and from outside resources such as forms and collateral localized by a vendor.
   This virtual machine is associated with an external network only. It has its own virtual switch and physical network adapter that connect it to External Network 1. This network is dedicated to servers that the company uses to receive data from outside sources. For example, the company uses External Network 1 to receive FTP traffic from vendors and allow vendors access to data stored on externally available servers though FTP. In addition to servicing Virtual Machine 1, External Network 1 services FTP servers configured on different ESX hosts throughout the site.
   Because Virtual Machine 1 does not share a virtual switch or physical network adapter with any virtual machines in the host, the other resident virtual machines cannot transmit packets to or receive packets from the Virtual Machine 1 network. This restriction prevents sniffing attacks, which require sending network traffic to the victim. More importantly, an attacker cannot use the natural vulnerability of FTP to access any of the hosts other virtual machines.

Security and the Virtual Networking Layer?

2. Internal virtual machines:
   Virtual Machines 2 through 5 are reserved for internal use. These virtual machines process and store company-private data such as medical records, legal settlements, and fraud investigations. As a result, the system administrators must ensure the highest level of protection for these virtual machines.
   These virtual machines connect to Internal Network 2 through their own virtual switch and network adapter. Internal Network 2 is reserved for internal use by personnel such as claims processors, in-house lawyers, or adjustors.
   Virtual Machines 2 through 5 can communicate with one another through the virtual switch and with internal virtual machines elsewhere on Internal Network 2 through the physical network adapter. They cannot communicate with externally facing machines. As with the FTP server, these virtual machines cannot send packets to or receive packets from the other virtual machines networks. Similarly, the hosts other virtual machines cannot send packets to or receive packets from Virtual Machines 2 through 5.

Security and the Virtual Networking Layer?

3. DMZ:
   Virtual Machines 6 through 8 are configured as a DMZ that the marketing group uses to publish the companys external Web site.
   This group of virtual machines is associated with External Network 2 and Internal Network 1. The company uses External Network 2 to support the Web servers that use the marketing and financial department to host the corporate Web site and other Web facilities that it hosts to outside users. Internal Network 1 is the conduit that the marketing department uses to publish content to the corporate Web site, post downloads, and maintain services like user forums.
   Because these networks are separate from External Network 1 and Internal Network 2, and the virtual machines have no shared points of contact (switches or adapters), there is no risk of attack to or from the FTP server or the internal virtual machine group.