UNIT III

CYBER SECURITY FOR BUSINESS APPLICATIONS AND NETWORKS

Virtual Servers

- Virtualization refers to a technology that provides an abstraction of the computing resources used by some software, which thus runs in a simulated environment called a virtual machine (VM).
- Benefits arising from using virtualization include better efficiency in the useof the physical system resources than is typically seen using a single operating system instance.
- This is particularly evident in the provision of virtualized server systems.
- Virtualization also provides support for multiple distinct operating systems and associated applications on the one physical system. This is more commonly seen on client systems.

Virtualization Alternatives **:**

- A hypervisor is software that sits between hardware and VMs and acts as a resource broker. It allows multiple VMs to safely coexist on a single physical server host and share that host9s resources.
- The virtualizing software provides abstraction of all physical resources (such as processor, memory, network, and storage resources) and thus enablesmultiple computing stacks, called VMs, to be run on a single physical host.

A hypervisor performs the following functions**:**

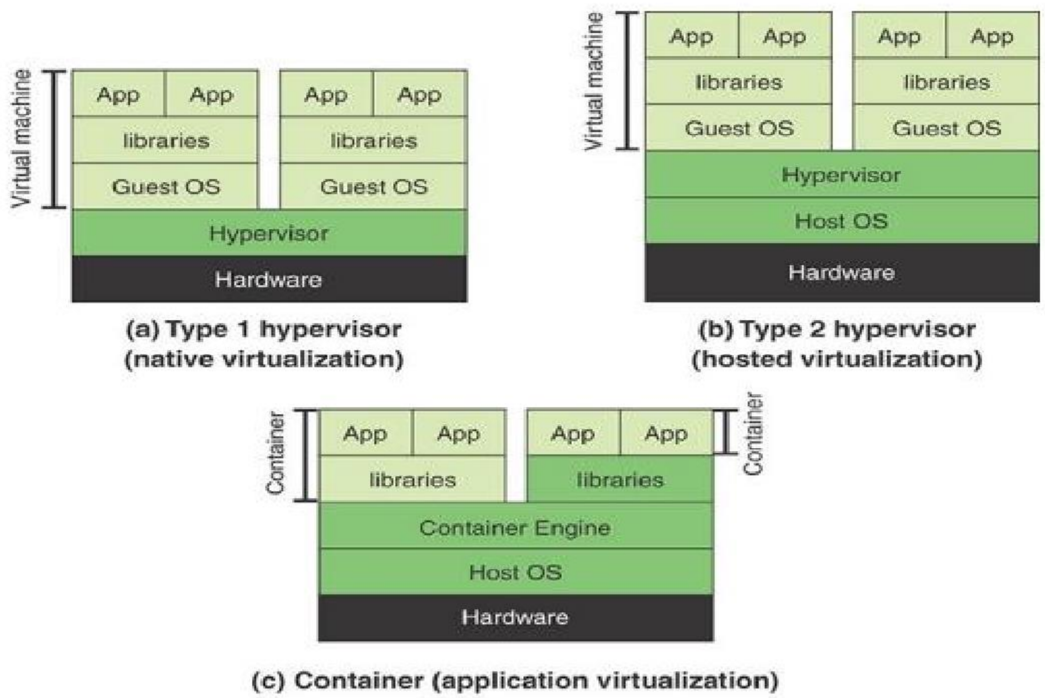
Execution management of VMs: This includes scheduling VMs for execution, virtual memory management to ensure VM isolation from other VMs, and context switching between various processor states. It also includes isolation of VMs to prevent conflicts in resource usage and emulation of timer and interrupt mechanisms.

Devices emulation and access control: A hypervisor emulates all network and storage (block) devices that different native drivers in VMs are expecting, mediating access to physical devices by different VMs.

Execution of privileged operations by hypervisor for guest VMs: Instead of being executed directly by the host hardware, certain operations invoked by guest operating systems, may have to be executed on its behalf by the hypervisor because of their privileged nature.

Management of VMs (also called VM life cycle management): A hypervisor configures guest VMs and controls VM states (for example Start, Pause, Stop).

Administration of hypervisor platform and hypervisor software: This involves setting parameters for user interactions with the hypervisor host as well as hypervisor software.



(a) Type 1 hypervisor (native virtualization)

(b) Type 2 hypervisor (hosted virtualization)

(c) Container (application virtualization)

FIGURE 11.2 Comparison of Hypervisors and Containers

There are two types of hypervisors, distinguished by whether there is an operating system between the hypervisor and the host.

A type 1 hypervisor (see Figure 11.2a) is loaded as a software layer directly onto a physical server, much as an operating system is loaded; this is referred to as native virtualization.

The type 1 hypervisor directly controls the physical resources of the host. Once itis installed and configured, the server is then capable of supporting virtual machinesas guests.

A type 2 hypervisor exploits the resources and functions of a host operating system and runs as a software module on top of the operating system (see Figure 11.2b); this is referred to as hosted virtualization, or nested virtualization.

A type 2 hypervisor relies on the operating system to handle all the hardware interactions on the hypervisor's behalf.

Virtualization Security Issues

- A number of security concerns that result from the use of virtualized systems,including the following: **<u>Guest operating system isolation:</u>**

- It is important to ensure that programs executing within a guest operating system can only access and use the resources allocated to it and cannot covertly interact with programs or data in either of the guest operating systems or in the hypervisor.

<u>Guest operating system monitoring by the hypervisor</u>: The hypervisor has privileged access to the programs and data in each guest operating system and mustbe trusted as secure from subversion and compromised use of this access.

<u>Virtualized environment security</u>: It is important to ensure security of the environment, particularly in regard to image and snapshot management, which attackers can attempt to view or modify.

Securing Virtualization Systems

SP 800-125, which provides guidance for appropriate security in virtualized systems, states that organizations using virtualization should do the following:

- ✓ Plan the security of the virtualized system carefully.
- ✓ Secure all elements of a full virtualization solution, including the hypervisor, guest operating systems, and virtualized infrastructure—and also maintain their security
- ✓ Ensure that the hypervisor is properly secured
- ✓ Restrict and protect administrator access to the virtualization solution

Network Storage Systems :

- ➢ Organizations make use of two broad categories of computer storage for files, databases, and other data: local and networked.
- ➢ Local storage, commonly called direct access storage (DAS), is a dedicated digital storage device attached directly to a server or PC via a cable or residing as an internal drive.
- ➢ Most users’ computers and most servers have DAS. DAS creates data islands because data cannot be easily shared with other servers.
- ➢ Networked storage is a term used to describe a storage device (usually many devices paired together) that is available over a network. This kind of storage maintains copies of data across high-speed local area network (LAN) connections and is designed to back up files, databases, and other data to a central location that can be easily accessed via standard network protocols and tools.

Networked storage comes in the following topologies:

<u>Storage area network (SAN):</u>

- A SAN is a dedicated network that provides access to various types of storage devices, including tape libraries, optical jukeboxes, and disk arrays. To servers and other devices in the network, a SAN9s storage devices look like locally attached devices.

- A disk block– based storage technology, SAN is probably the most pervasive form of storage for very large data centers and is a de facto staple for databaseintensive applications. These applications require shareable storage, large bandwidth, and support for the distances from rack to rack within the data center.

Network attached storage (NAS):

- NAS systems are networked appliances that contain one or more hard drives that are shared with multiple, heterogeneous computers. Their specialized role in networks is to store and serve files.

- NAS disk drives typically support built-in data protection mechanisms, including redundant storage containers or redundant arrays of independent disks (RAID). NAS enables file serving responsibilities to be separated from other servers on the network and typically provides faster data access than traditional file servers.

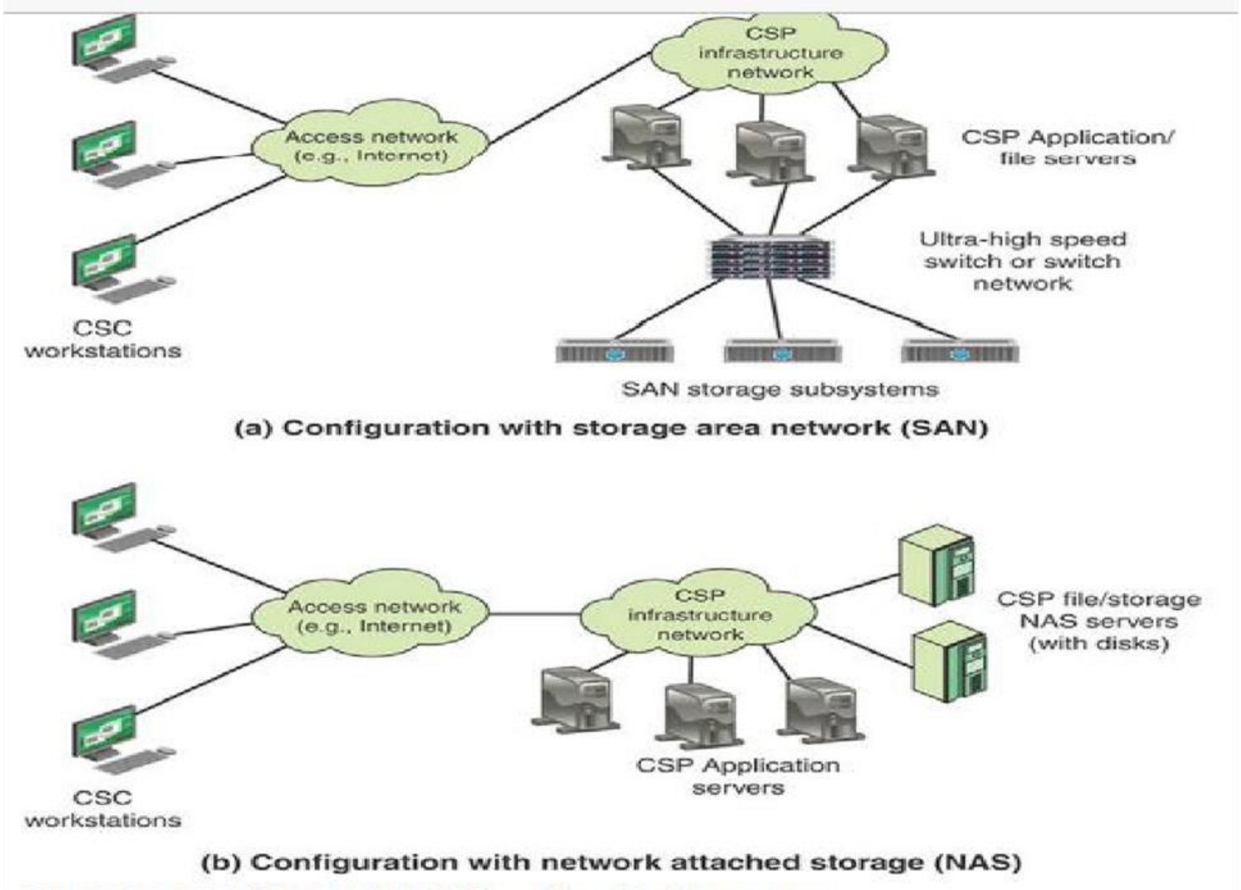

CSP infrastructure network
Access network (e.g., Internet)
CSP Application/ file servers
Ultra-high speed switch or switch network
CSC workstations
SAN storage subsystems
(a) Configuration with storage area network (SAN)
Access network (e.g., Internet)
CSP infrastructure network
CSP file/storage NAS servers (with disks)
CSP Application servers
CSC workstations
(b) Configuration with network attached storage (NAS)

FIGURE 11.3 SAN and NAS in a Cloud Infrastructure

The SGP recommends the following security measures:

- ✓ Follow the system development and configuration security policies for design and configuration of network storage systems.

- ✓ Be sure that SANs and NASs are subject to standard security practices (for example, configuration, malware protection, change management, patch management).

✓ Ensure that the IT facility provides protection of network storage management consoles and administration interfaces.

✓ Store encryption information on network storage systems.

✓ Allow for additional security arrangements specific to NAS and SAN. Security arrangements specific to NAS and SAN depend on the type of server configuration, whether virtualization is used, and network configuration.

Network Management Concepts: Firewall -IP Security

- This section provides an overview of network management. Let9s begin by looking at the requirements for network management.
- This will provide an idea of the scope of the task to be accomplished. To manage a network, it is fundamental to know something about the current status and behavior of that network.
- Effective management requires a network management system that includesa comprehensive set of data gathering and control tools and that is integrated with the network hardware and software.

Let’s look at the general architecture of a network management system.

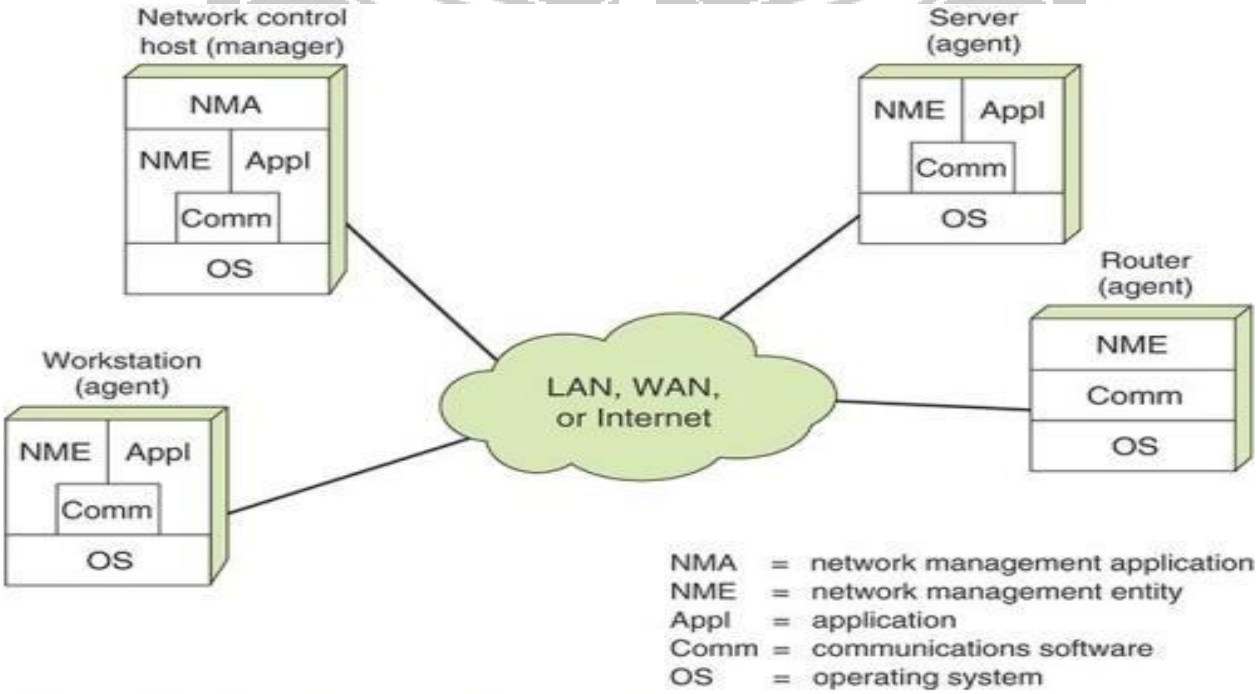


FIGURE 12.1 Components of a Network Management System

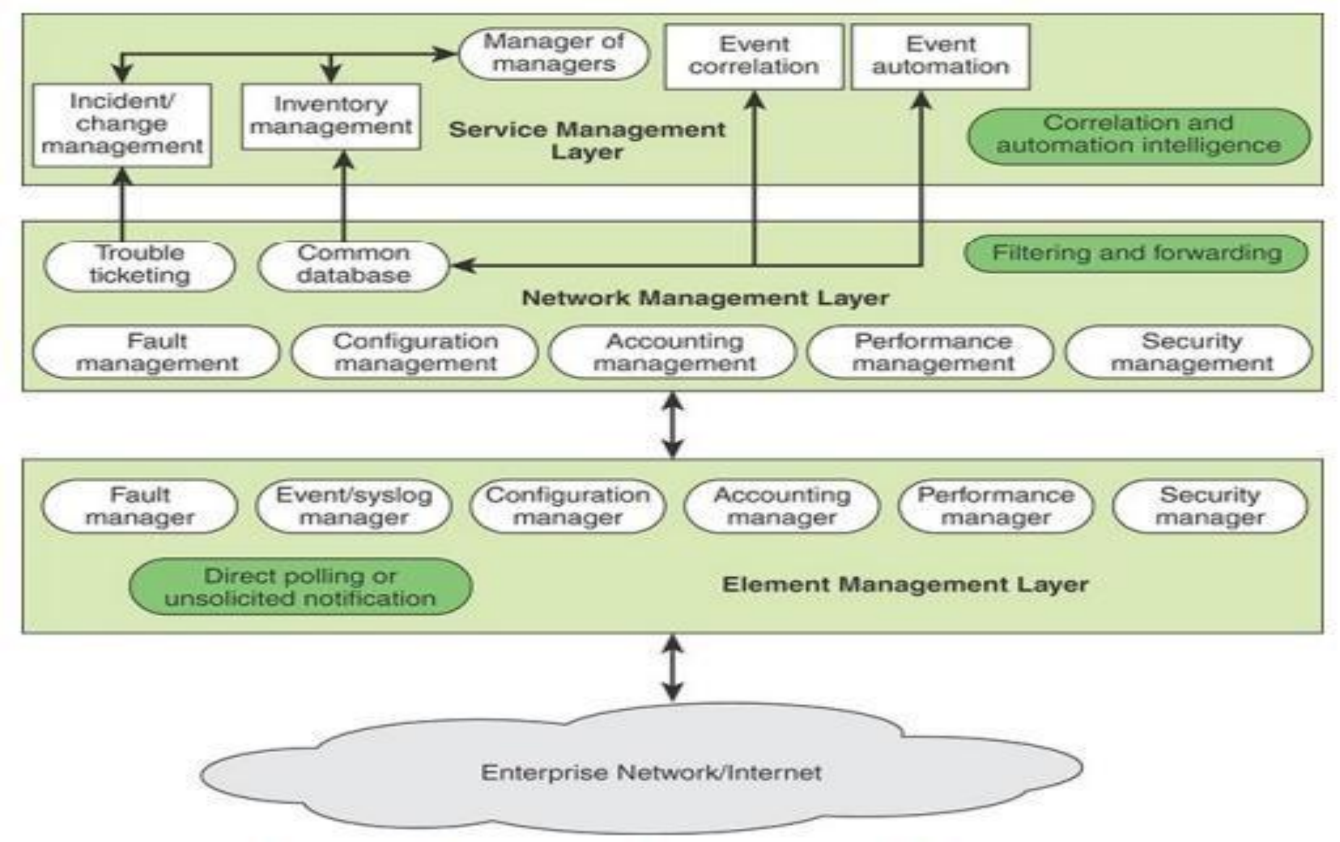


FIGURE 12.3 Network Management System Logical Architecture