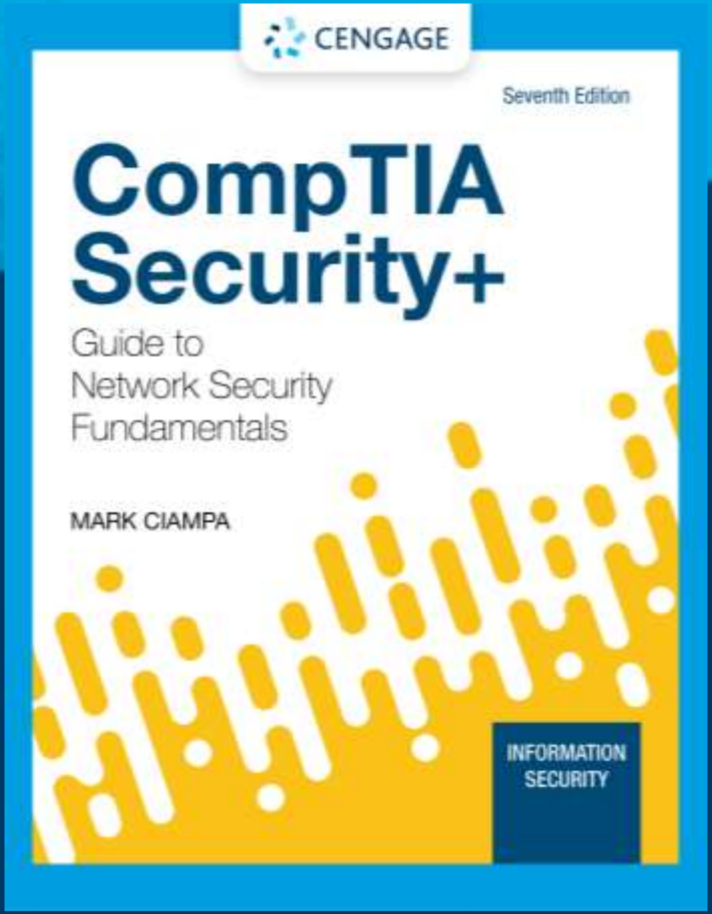


CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition

Module 10: Cloud and Virtualization Security

CENGAGE

Module Objectives

By the end of this module, you should be able to:

1. Define the cloud and explain how it is used and managed
2. Explain virtualization
3. Describe cloud and virtualization security controls
4. List different secure network protocols

Cloud Security

- Understanding cloud security involves an overall introduction to cloud computing
- It also means understanding the steps to take in order to secure the cloud computing environment

Introduction to Cloud Computing (1 of 6)

- In a *hosted services* environment, servers, storage, and the supporting networking infrastructure are shared by multiple enterprises over a remote network connection
- **Cloud computing** is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources
  - Entities that offer cloud computing are called **cloud service providers**
- The savings available through cloud computing are due to the following factors:
  - *Elasticity and scalability*
  - *Pay-per-use*
  - *On demand*
  - *Resiliency*

Introduction to Cloud Computing (2 of 6)

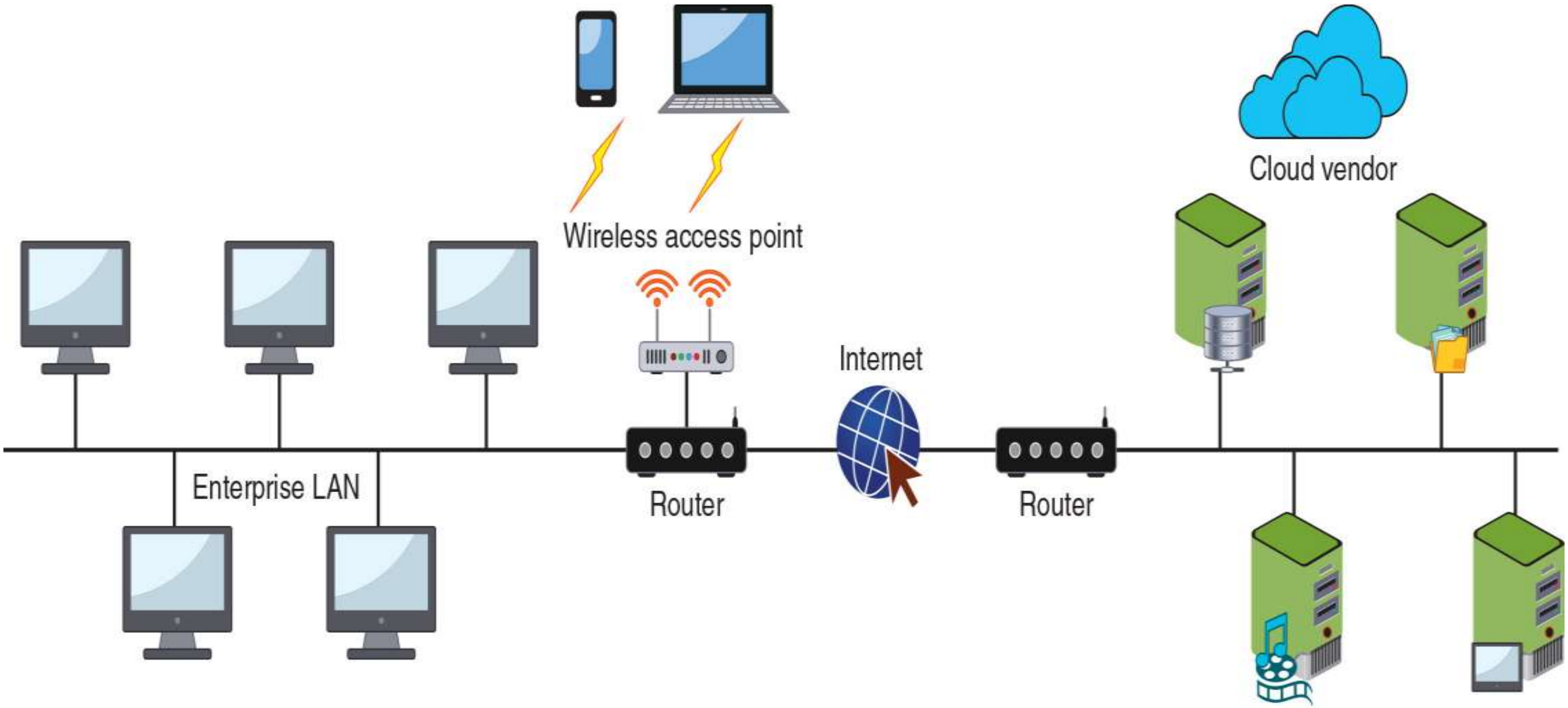


Figure 10-1 Cloud computing

Introduction to Cloud Computing (3 of 6)

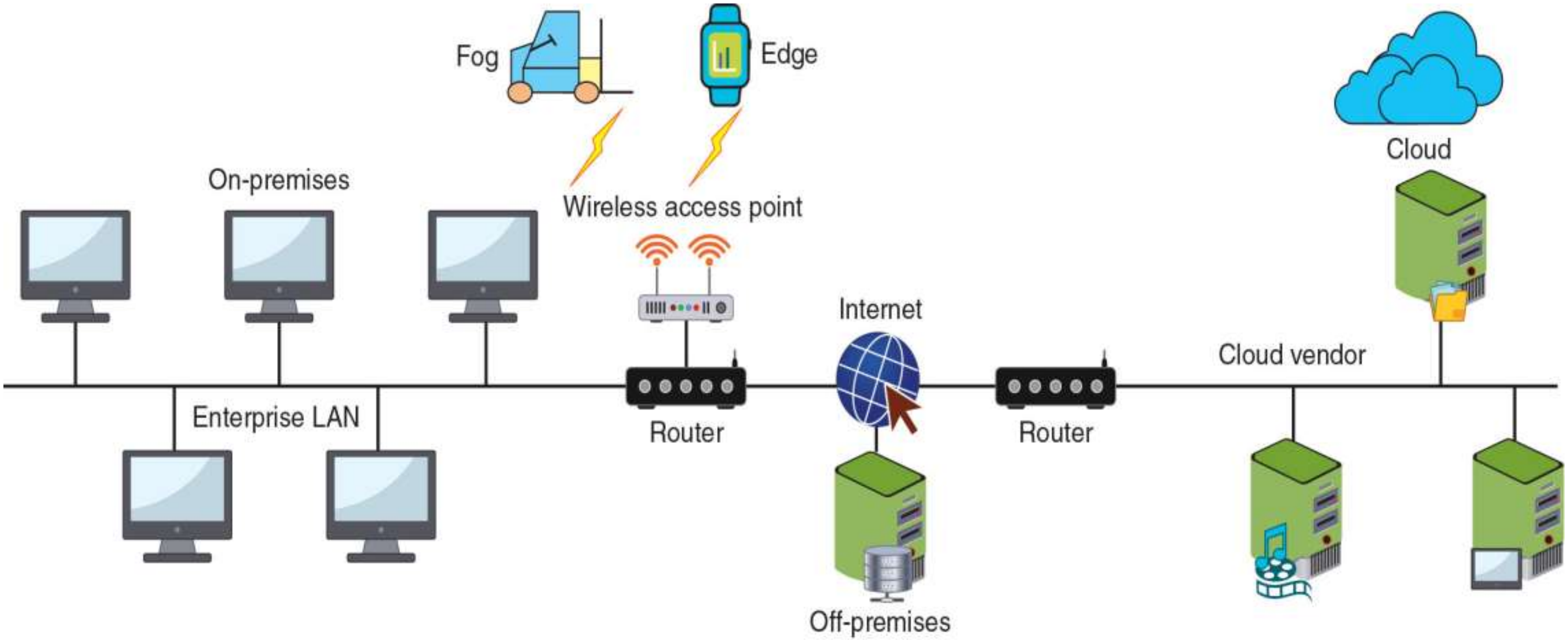


Figure 10-2 Computing locations

Introduction to Cloud Computing (4 of 6)

- Cloud Architecture
  - *Thin client* is a computer that runs from resources stored on a central cloud server
  - *Transit gateway* is an Amazon Web Services (AWS) technology that allows organizations to connect all existing virtual private clouds (VPCs), physical data centers, remote offices, and remote gateways into a single managed source
  - *Serverless infrastructure* is one in which the capacity planning, installation, setup, and management are all invisible to the user because they are handled by the cloud provider

Introduction to Cloud Computing (5 of 6)

- There are four service models in cloud computing:
  - **Software as a Service (SaaS)**
    - Vendor provides access to the vendor’s software applications running on a cloud infrastructure
  - **Platform as a Service (PaaS)**
    - Consumers install and run their own specialized applications on the cloud computing network
  - **Infrastructure as a Service (IaaS)**
    - Vendor allows customers to deploy and run their own software, including OSs and applications
  - **Anything as a Service (XaaS)**
    - A broad category of subscription services related to cloud computing

Introduction to Cloud Computing (6 of 6)

- Management
  - Cloud management can be conducted by the local organization performing the work itself or by contracting with a third-party management service provider
- **Services integration** attempts to achieve a “boundary-less” approach
  - Involves integrating all users across the enterprise who are using cloud computing
- When locally managing cloud computing, an enterprise should have written **resource policies** in place
  - They must outline who is responsible for cloud computing, what are their duties and responsibilities, how cloud computing can be used (and not used), and the processes for acquiring these resources
- A **managed service provider** (**MSP**) delivers services through ongoing and regular support as well as active administration of those resources
  - An MSP assumes the role of a traditional on-prem IT organization

Securing Cloud Computing (1 of 6)

Security issue	Description
Unauthorized access to data	Improper cloud security configurations can result in data being left exposed.
Lack of visibility	Organizations have limited or no visibility into the security mechanisms of the cloud provider and thus cannot verify the effectiveness of security controls.
Insecure application program interfaces (APIs)	While APIs help cloud customers customize their PaaS by providing data recognition, access, and effective encryption, a vulnerable API can be exploited by threat actors.
Compliance regulations	Maintaining compliance requires that an organization know where its data is, who can access it, and how it is protected, but this can be difficult in an opaque cloud system, which lacks transparency.
System vulnerabilities	A cloud infrastructure is prone to system vulnerabilities due to complex networks and multiple third-party platforms.

Securing Cloud Computing (2 of 6)

- Cloud Security Controls
  - Securing cloud computing involves using controls such as the following:
    - **Conducting audits** – a **cloud security audit** is an independent examination of cloud service controls
    - **Use Regions and Zones** – reliability and resiliency are achieved through duplicating processes across one or more geographical areas (called **high availability across zones**)
    - **Secrets management** – enables strong security and improved management of a microservices-based architecture, allowing the entire cloud infrastructure to remain flexible and scalable without sacrificing security
    - **Enforce Functional Area Mitigations** – See Table 10-6

CENGAGE

Securing Cloud Computing (3 of 6)

Feature	Description
Limited and automated replication	While secret data and secret names are “project-global” resources, the secret data is stored in regions, which the user can specify or the cloud provider can designate.
Secret-specific versioning	A secret can be pinned to a specific version of the code (like “v3.2”).
Audit logging	Every interaction generates an audit entry in a log file that can be used to find abnormal access patterns that may indicate possible security breaches.
Default encryption	Data is encrypted in transit and at rest with AES-256-bit encryption keys.
Extensibility	One system is able to extend and integrate into other existing secrets management systems.

Securing Cloud Computing (4 of 6)

- Application Security
  - One of an organization’s security protections for cloud computing application security is to use a **cloud access security broker** (**CSAB**)
  - CASB is a set of software tools or services that resides between the enterprises’ on-premises infrastructure and the cloud provider’s infrastructure
  - CASB acts as a “gatekeeper”, ensuring that the security policies of the enterprise extend to its data in the cloud
- Security Virtual Device Solutions
  - A **next generation secure web gateway** (**SWG**) examines both incoming and outgoing traffic and performs basic URL and monitoring in web applications
  - A **cloud firewall** is virtual software that functions in a similar manner to a physical security appliance by examining traffic into and out of the cloud

Securing Cloud Computing (5 of 6)

- Lack of a Cloud Conceptual Model
  - Physical networks use the Open Source Interconnection (OSI) seven-layer model to illustrate network functionality
  - With cloud computing, the OSI model is no longer as useful
  - The lack of a conceptual model like the OSI model makes selecting and managing security virtual devices more challenging
  - Different cloud-based conceptual models are starting to be proposed
    - However, no single model has been widely adapted
    - One model is shown in Table 10-7

Securing Cloud Computing (6 of 6)

Layer and name	Description	Party responsible
5—Application Experience	End-user facing interface	Customer
4—Native Service	Create, store, process	Customer
3—Software-Defined Datacenter	Create infrastructure	SaaS—Cloud computing provider PaaS and IaaS—Customer
2—Virtualization Software	Software that virtualizes the hardware	Cloud computing provider
1—Physical Infrastructure	Buildings, power, cables, hardware, utilities	Cloud computing provider

Knowledge Check Activity 1

Which cloud security control provides reliability and resiliency through the duplication of processes across geographical areas?

a. Conducting audits

b. Implementing secrets management

c. Using regions and zones

d. Enforcing functional area mitigations

Knowledge Check Activity 1: Answer

Which cloud security control provides reliability and resiliency through the duplication of processes across geographical areas?

Answer: c. Using regions and zones

In a cloud computing environment, reliability and resiliency are achieved through duplicating processes across one or more geographical areas. This is called using regions and zones or high availability across zones.

Virtualization Security

- Virtualization security involves an understanding of the topic along with specific examples
- It includes specific steps to be taken to secure a virtualized environment

Defining Virtualization (1 of 5)

- What is Virtualization?
  - **Virtualization** is a means of managing and presenting computer resources without regard to physical layout or location
  - *Host virtualization* is a type of virtualization in which an entire operating system environment is simulated
  - A *virtual machine* (*VM*) is a simulated software-based emulation of a computer
  - The *host system* runs a hypervisor that manages the virtual operating systems and supports one or more guest systems
  - Virtualization is used to consolidate multiple physical servers into VMs that can run on a single physical computer

Defining Virtualization (2 of 5)

- The VM monitor program is called a *hypervisor*, which manages the VM operating systems
- Two types of hypervisor:
  - *Type I* – run directly on the computer’s hardware instead of the underlying OS
  - *Type II* – run on the host OS, much like an application
- A **container** holds only the necessary OS components that are needed for that specific application to run
  - Reduces the necessary hard drive storage space and RAM needed
  - Allows for containers to start more quickly because the OS does not have to be started

Defining Virtualization (3 of 5)

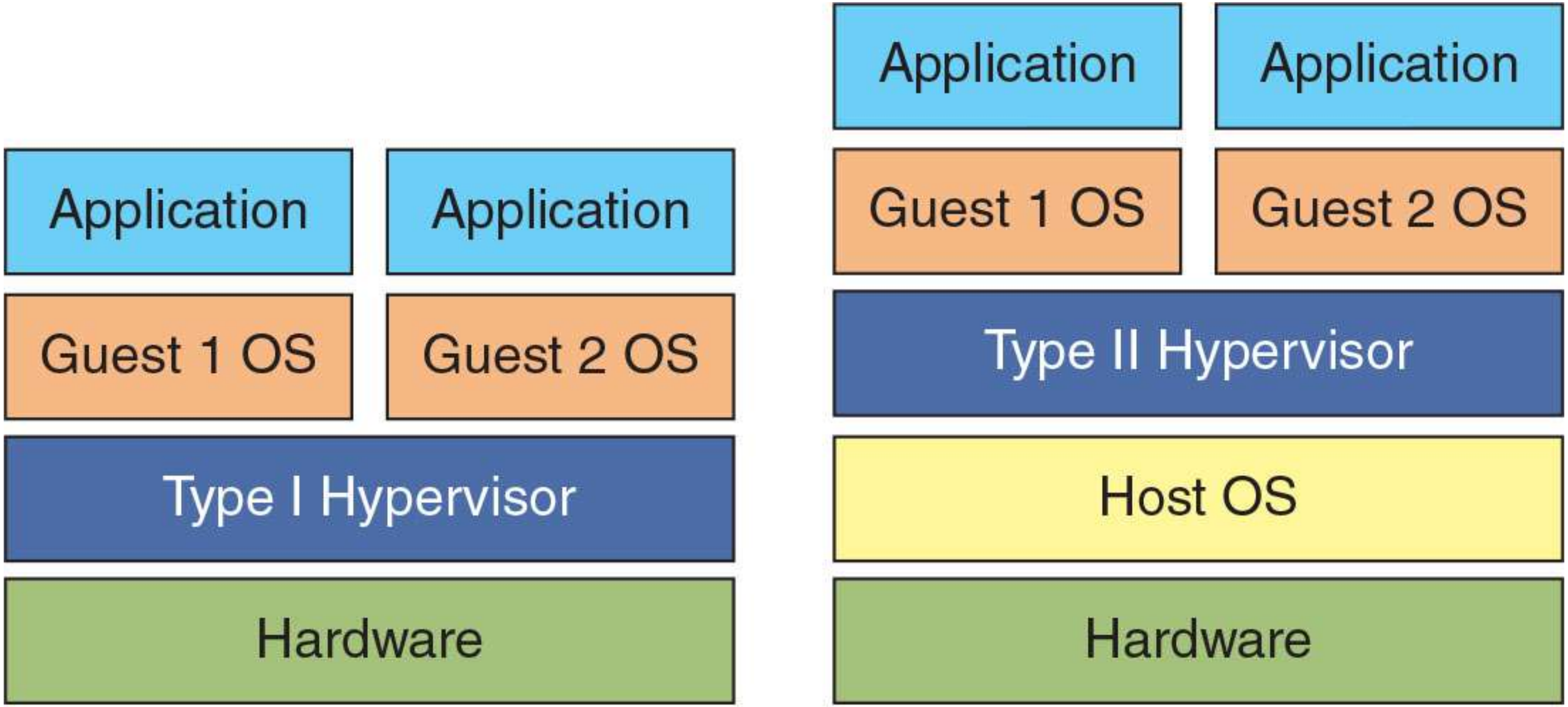


Figure 10-7 Type I and Type II hypervisors

Defining Virtualization (4 of 5)

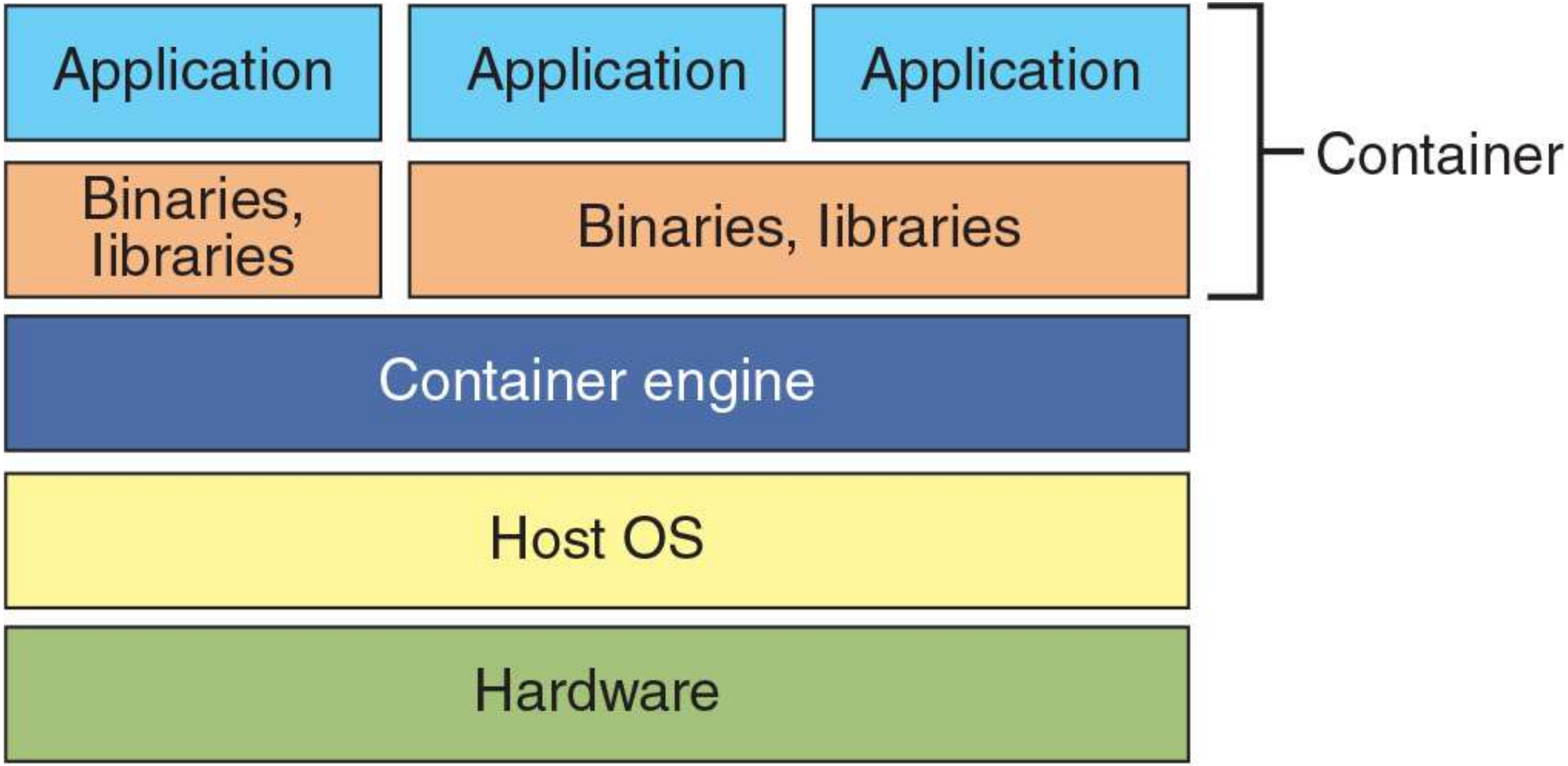


Figure 10-8 Container

Defining Virtualization (5 of 5)

- Advantages of Virtualization
  - New virtual server machines can be made available (*host availability*) and resources can easily be expanded or contracted as needed (*host elasticity*)
  - Can reduce costs
    - Fewer physical computers must be purchased and maintained
  - Can provide uninterrupted server access to users
    - Supports *live migration* which allows a virtual machine to be moved to a different physical computer with no impact to users

Infrastructure as Code (1 of 2)

- **Software defined network (SDN)**
  - An SDN virtualizes parts of the physical network so that it can be more quickly and easily reconfigured
  - This is accomplished by separating the *control plane* from the *data plane*
  - If traffic needs to flow through the network:
    - It receives permission from the SDN controller, which verifies the communication is permitted by the network policy of the enterprise
    - Once approved, the SDN controller computes a route for the flow to take and adds an entry for that flow in each of the switches along the path

Infrastructure as Code (2 of 2)

- Software-Defined Visibility (SDV)
  - **Software-defined visibility (SDV)** is a framework that allows users to create programs in which critical security functions can be automated
  - SDV allows network administrators to automate multiple functions in a network infrastructure including:
    - Dynamic response to detected threat patterns
    - Adjustments to traffic mode configurations for in-line security tools
    - Additional IT operations-management functions and capabilities

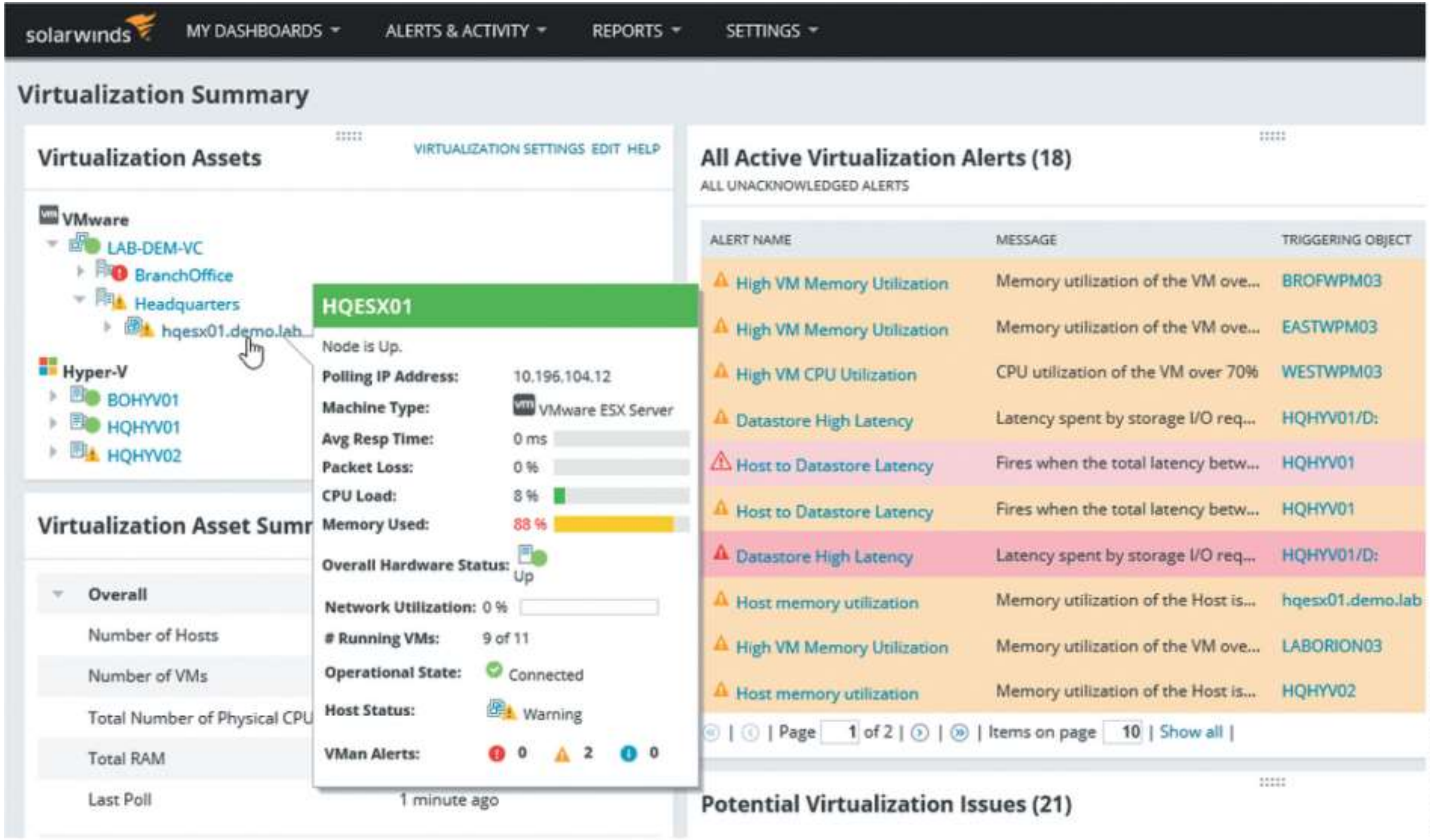
Security Concerns for Virtual Environments (1 of 3)

- Security-related advantages of virtualization:
  - Test latest security updates by downloading on a virtual machine before installing on production computers
  - A *snapshot* of a particular state of a virtual machine can be saved for later use
  - Testing the existing security configuration *(security control testing)* can be performed using a simulated network environment
  - VMs can promote security segregation and isolation
  - A suspicious program can be loaded into an isolated virtual machine and executed *(sandboxing)*
    - If the program is malware, only the virtual machine will be impacted

Security Concerns for Virtual Environments (2 of 3)

- Security concerns for virtualized environments:
  - Not all hypervisors have the necessary security controls to keep out attackers
  - Existing security tools were designed for single physical servers
  - VMs must be protected from both outside networks and other VMs on the same physical computer
  - VMs may be able to “escape” from the contained environment and directly interact with the host OS
    - Important to have **virtual machine escape protection**
- *Virtual machine sprawl* is the widespread proliferation of VMs without proper oversight or management
- Combating VM sprawl is called **virtual machine sprawl avoidance**
  - Installing a virtual machine manager can help

Security Concerns for Virtual Environments (3 of 3)



Virtualization Summary

Virtualization Assets

VMware
- LAB-DEM-VC
  - BranchOffice
  - Headquarters
    - hqesx01.demo.lab

Hyper-V
- BOHYV01
- HQHYV01
- HQHYV02

Virtualization Asset Summ

Overall	
Number of Hosts	
Number of VMs	
Total Number of Physical CPU	
Total RAM	
Last Poll	1 minute ago

HQESX01

Node is Up.

Polling IP Address: 10.196.104.12
Machine Type: VMware ESX Server
Avg Resp Time: 0 ms
Packet Loss: 0 %
CPU Load: 8 %
Memory Used: 88 %
Overall Hardware Status: Up
Network Utilization: 0 %
Running VMs: 9 of 11
Operational State: Connected
Host Status: Warning
VMan Alerts: 0 2 0

All Active Virtualization Alerts (18)

ALL UNACKNOWLEDGED ALERTS

ALERT NAME	MESSAGE	TRIGGERING OBJECT
High VM Memory Utilization	Memory utilization of the VM ove...	BROFWPM03
High VM Memory Utilization	Memory utilization of the VM ove...	EASTWPM03
High VM CPU Utilization	CPU utilization of the VM over 70%	WESTWPM03
Datastore High Latency	Latency spent by storage I/O req...	HQHYV01/D:
Host to Datastore Latency	Fires when the total latency betw...	HQHYV01
Host to Datastore Latency	Fires when the total latency betw...	HQHYV01
Datastore High Latency	Latency spent by storage I/O req...	HQHYV01/D:
Host memory utilization	Memory utilization of the Host is...	hqesx01.demo.lab
High VM Memory Utilization	Memory utilization of the VM ove...	LABORION03
Host memory utilization	Memory utilization of the Host is...	HQHYV02

| Page 1 of 2 | | Items on page 10 | Show all |

Potential Virtualization Issues (21)

Source: SolarWinds

Figure 10-10 Virtual machine manager

Knowledge Check Activity 2

What virtualization technology separates the control plane from the data plane on networking devices such as switches and routers?

a. SDV

b. Hypervisor

c. Containers

d. SDN

Knowledge Check Activity 2: Answer

What virtualization technology separates the control plane from the data plane on networking devices such as switches and routers?

Answer: d. SDN

A software-defined network (SDN) virtualizes parts of the physical network by separating the control plane from the data plane.

Secure Network Protocols

- Common secure network protocols include:
  - Simple Network Management Protocol (SNMP)
  - Domain Name System (DNS) Security Extensions
  - File Transfer Protocol
  - Secure email protocols
  - Lightweight Directory Access Protocol (LDAP)
  - Internet Protocol version 6 (IPv6)

Simple Network Management Protocol (SNMP)

- SNMP is used to manage network equipment and is supported by most network equipment manufacturers
- It allows administrators to remotely monitor, manage, and configure network devices
- SNMP functions by exchanging management information between network devices
- Each SNMP-managed device has an agent or a service
  - Listens for and executes commands
- Agents are password protected
  - Password is known as a *community string*
- Security vulnerabilities were present in SMNP versions 1 and 2
  - Version 3 uses usernames and passwords along with encryption to address vulnerabilities

Domain Name System Security Extensions (DNSSEC)

- DNS is often the focus of attacks
  - DNS poisoning and DNS hijacking are examples
- These attacks can be thwarted by using **Domain Name System Security Extensions** (**DNSSEC**)
  - DNSSEC adds additional resource records and message header information which can be used to verify the requested data has not been altered in transmission
- Using asymmetric cryptography, a private key that is specific to a zone is used in encrypting a hash of a set of resource records
  - Which is then used to create the digital signature to be stored in the resource record

File Transfer Protocol (1 of 2)

- File transfer protocol (FTP) is an unsecure protocol used to connect to an FTP server in order to transfer files
- Methods for using FTP on local host computer
  - *Using an FTP client*
  - *From a command prompt*
  - *Using a web browser*
- FTP vulnerabilities include:
  - FTP does not use encryption
  - Files transferred using FTP are vulnerable to man-in-the-middle attacks

File Transfer Protocol (2 of 2)

- There are two options for secure transmissions over FTP
  - FTP Secure (FTPS) uses SSL or TLS to encrypt commands sent over the control port (port 21)
    - The data port (port 20) may not be encrypted
  - Secure FTP (SFTP)
    - Uses only a single TCP port instead of two ports
    - All data and commands are encrypted

Secure Email Protocols

- Earlier email systems use two TCP/IP protocols to send and receive messages:
  - Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP)
- IMAP (Internet Mail Access Protocol) is a more recent and advanced email system
- As a means of security, a *mail gateway* monitors emails for unwanted content and prevents these messages from being delivered
- A mail gateway can automatically and transparently encrypt outbound email messages

Lightweight Directory Access Protocol (LDAP)

- A **directory service** is a database stored on the network that contains information about users and network devices
  - The directory service also keeps track of all the resources on the network and a user’s privileges to those resources and grants or denies access based on the directory service information
- **Lightweight Directory Access Protocol** (**LDAP**) makes it possible for almost any application running on any computer platform to obtain directory information
- A weakness of LDAP is that it can be subject to **LDAP injection attacks**
  - This may allow an attacker to construct LDAP statements based on user input statements
- The defense against LDAP injection attacks is to examine all user input before processing

Internet Protocol Version 6 (IPv6)

- IPv6 addresses weaknesses of IPv4 and also provides other significant improvements
  - IPv6 increases the number of available addresses
- IPv6 has enhanced security features:
  - IPv6 can implement end-to-end encryption
    - This makes man-in-the-middle attacks significantly more difficult
  - IPv6 supports more secure name resolution
    - The Secure Neighbor Discovery (SEND) protocol can send cryptographic confirmation that an endpoint is who it claims to be
    - This makes ARP poisoning more difficult

Knowledge Check Activity 3

Which type of networking service is potentially susceptible to LDAP injection attacks?

a. Directory service

b. Domain name service

c. Web service

d. Mail service

CENGAGE

Knowledge Check Activity 3: Answer

Which type of networking service is potentially susceptible to LDAP injection attacks?

Answer: a. Directory service

Lightweight Directory Access Protocol (LDAP) is a protocol for using and maintaining directory services which is a database stored on a network that contains information about users and other network services.

Self-Assessment

Rate your competence of the following module objectives on a scale of 1 to 5 where 5 indicates you have full confidence in your competence of that objective and 1 indicates you have very little to no confidence in your competence of that objective. After you self-score, consider why some topics were easier for you to digest than others and review any objective you are not confident about.

1. Define the cloud and explain how it is used and managed
2. Explain virtualization
3. Describe cloud and virtualization security controls
4. List different secure network protocols

Summary (1 of 2)

- Cloud computing is a popular and flexible approach to computing resources
- A public cloud is one in which the services and infrastructure are offered to all users with access provided remotely through the Internet
- On-premises is computing resources located on the campus of the organization while off-premises is a computing resource hosted and supported by a third party
- There are many elements that make up a cloud architecture: a thin client, a transit gateway, and a serverless infrastructure
- Cloud computing service models include: Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Anything as a Service (XaaS)
- Cloud computing has several potential security issues

Summary (2 of 2)

- While securing the functional areas of the cloud is important, an area often overlooked is application security or protecting applications
- Virtualization is a means of managing and presenting computer resources by function without regard to their physical layout or location
- Instances of virtualization are sometimes referred to as infrastructure as code
- There are several secure network protocols that are used today: SNMP, DNSSEC, FTPS, and SFTP
- Electronic email systems that are in use today: SMTP/POP3 and IMAP