Securing Networks Summary

1.3.1

What Did I Learn in this Module?

Current State of Affairs
Network security relates directly to an organization's business continuity. Network security breaches can disrupt e-commerce, cause the loss of business data, threaten people's privacy, and compromise the integrity of information. These breaches can result in lost revenue for corporations, theft of intellectual property, lawsuits, and can even threaten public safety. Many tools are available to help network administrators adapt, develop, and implement threat mitigation techniques, including the Cisco Talos Intelligence Group. An attack vector is a path by which a threat actor can gain access to a server, host, or network. Attack vectors originate from inside or outside the corporate network. Data is likely to be an organization's most valuable asset. Various DLP controls must be implemented, that combine strategic, operational, and tactical measures. Common data loss vectors include email and social networking, unencrypted data devices, cloud storage devices, removable media, hard copy, and improper access control.

Network Topology Overview
There are many types of networks. CANs consist of interconnected LANS within a limited geographical area. Elements of the defense-in-depth design include VPN, ASA firewall, IPS, Layer 3 switches, layer 2 switches, ESA/WSA, AAA server, and hosts. SOHO networks are typically protected using consumer grade routers that provide integrated firewall features and secure wireless connections. Wireless hosts connect to the wireless network using WPA2 data encryption technology. WANs span a wide geographical area. Network security professionals must use secure devices on the edge of the network. Data center networks are typically housed in an off-site facility to store sensitive or proprietary data. Data center physical security is divided into two areas: outside perimeter security and inside perimeter security. Security traps require a person to use their badge ID to enter the first area. After the person is inside the security trap, facial recognition, fingerprints, or other biometric verifications are used to open the second door. Cloud computing allows organizations to use services such as data storage or cloud-based applications, to extend their capacity or capabilities without adding infrastructure. The actual cloud network consists of physical

and virtual servers which are commonly housed in data centers. However, data centers are increasingly using VMs to provide server services to their clients. VMs are also prone to specific targeted attacks including hyperjacking, instant on activation, and antivirus storms. The Cisco Secure Data Center solution blocks internal and external threats at the data center edge. The core components of the Cisco Secure Data Center solution provide secure segmentation, threat defense, and visibility. More and more people are using these devices to access enterprise information. This trend is known as BYOD. To accommodate the BYOD trend, Cisco developed the Borderless Network. In a Borderless Network, access to resources can be initiated by users from many locations, on many types of endpoint devices, using various connectivity methods. To support this blurred network edge, Cisco devices support MDM features.

1.3.2

Module 1 - Securing Networks Quiz

1. Which security measure is typically found both inside and outside a data center facility?

- security traps
- biometrics access
- continuous video surveillance
- a gate
- exit sensors

2. Which statement accurately characterizes the evolution of threats to network security?

- Threats have become less sophisticated while the technical knowledge needed by an attacker has grown.
- Internet architects planned for network security from the beginning.
- Early Internet users often engaged in activities that would harm other users.
- Internal threats can cause even greater damage than external threats.

3. Which security technology is commonly used by a teleworker when accessing resources on the main corporate office network?

- IPS
- VPN
- SecureX
- biometric access

4. A security intern is reviewing the corporate network topology diagrams before participating in a security review. Which network topology would commonly have a large number of wired desktop computers?

- CAN
- data center
- SOHO
- cloud

5. In the video that describes the anatomy of an attack, a threat actor was able to gain access through a network device, download data, and destroy it. Which flaw allowed the threat actor to do this?

- improper physical security to gain access to the building
- lack of a strong password policy
- open ports on the firewall
- a flat network with no subnets or VLANs

6. Which type of network commonly makes use of redundant air conditioning and a security trap?

- data center
- CAN
- WAN
- cloud

7. Which technology is used to secure, monitor, and manage mobile devices?

- rootkit
- MDM
- VPN
- ASA firewall

8. When considering network security, what is the most valuable asset of an organization?

- customers
- personnel
- data
- financial resources

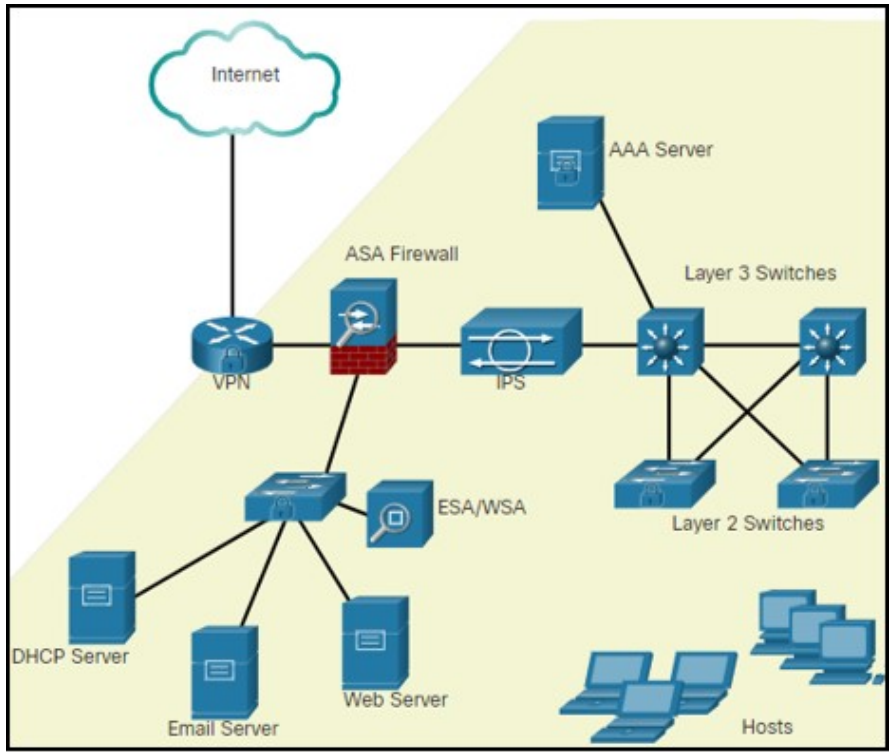
9. What is hyperjacking?

- using processors from multiple computers to increase data processing power
- adding outdated security software to a virtual machine to gain access to a data center server
- overclocking the mesh network which connects the data center servers
- taking over a virtual machine hypervisor as part of a data center attack

10. Which resource is affected due to weak security settings for a device owned by the company, but housed in another location?

- cloud storage device
- social networking
- hard copy
- removable media

11.



Refer to the exhibit. An IT security manager is planning security updates on this particular network. Which type of network is displayed in the exhibit and is being considered for updates?

- SOHO
- data center
- WAN
- CAN

Check
Show Me
Reset

1.2 Network Topology Overview
2.0 Introduction