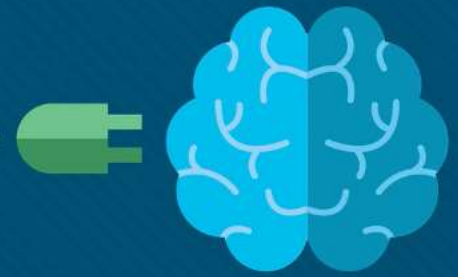


Module 1: Securing Networks

Networking Security v1.0
(NETSEC)

Module Objectives

Module Title: Securing Networks

Module Objective: Explain network security.

Topic Title	Topic Objective
Current State of Affairs	Describe the current network security landscape.
Network Topology Overview	Describe how all types of networks need to be protected.

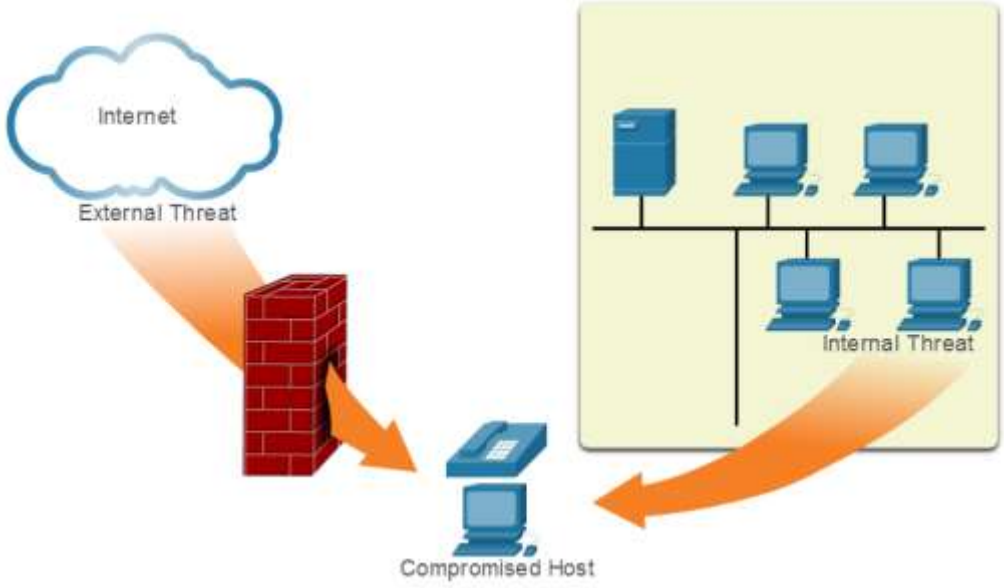
1.1 Current State of Affairs

Networks Are Targets

Networks are routinely under attack. A quick internet search for network attacks will return many articles about them. Kapersky maintains the interactive Cyberthreat Real-Time Map display of current network attacks. The attack data is submitted from Kapersky network security products that are deployed worldwide.

Vectors of Network Attacks

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. Threat actors may target a network through the internet, to disrupt network operations and create a denial of service (DoS) attack.)



Data Loss

Term	Definition
Email/Social Networking	The most common vector for data loss includes instant messaging software and social media sites. For instance, intercepted email or IMs could be captured and confidential information revealed.
Unencrypted Devices	A stolen corporate laptop typically contains confidential organizational data. If the data is not stored using an encryption algorithm, the thief can retrieve valuable confidential data.
Cloud Storage Devices	Saving data to the cloud has many potential benefits. However, sensitive data can be lost if access to the cloud is compromised due to weak security settings.
Removable Media	One risk is that an employee could perform an unauthorized transfer of data to a USB drive. Another risk is that a USB drive containing valuable corporate data could be lost.
Hard Copy	Sensitive data should be disposed of thoroughly. For example, confidential data should be shredded when no longer required. Otherwise, a thief could retrieve discarded reports and gain valuable information.
Improper Access Control	Passwords are the first line of defense. Stolen passwords or weak passwords which have been compromised can provide an attacker easy access to data.

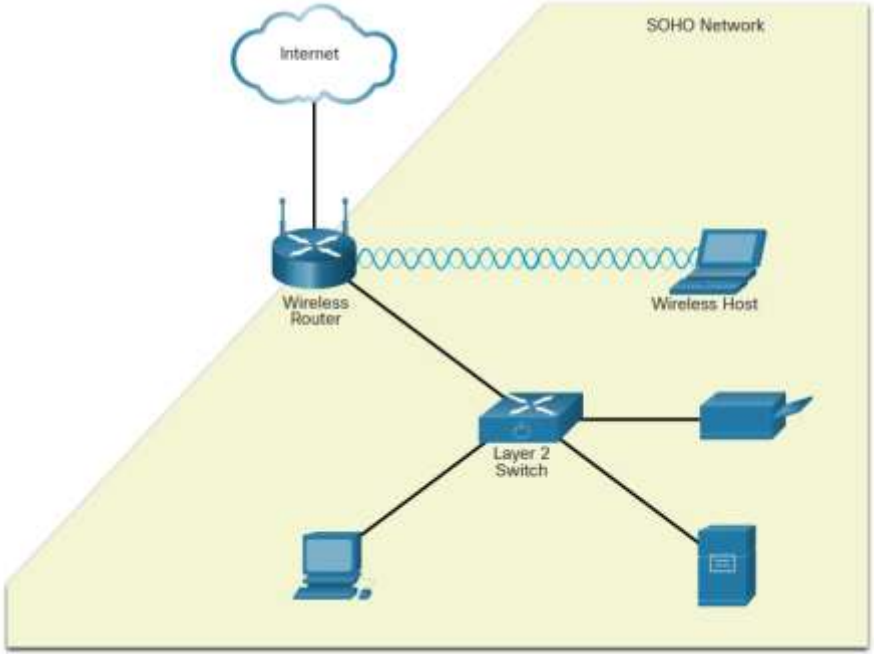
1.2 Network Topology Overview

Campus Area Networks

Term	Definition
VPN	The Cisco ISR is secured. It protects data in motion that is flowing from the CAN to the outside world by establishing Virtual Private Networks (VPNs). VPNs ensure data confidentiality and integrity from authenticated sources.
ASA Firewall	A Cisco Adaptive Security Appliance (ASA) firewall performs stateful packet filtering to filter return traffic from the outside network into the campus network.
IPS	A Cisco Intrusion Prevention System (IPS) device continuously monitors incoming and outgoing network traffic for malicious activity. It logs information about the activity and attempts to block and report it.
Layer 3 Switches	These distribution layer switches are secured and provide secure redundant trunk connections to the Layer 2 switches. Several different security features can be implemented, such as ACLs, DHCP snooping, Dynamic ARP Inspection (DAI), and IP source guard.
Layer 2 Switches	These access layer switches are secured and connect user-facing ports to the network. Several different security features can be implemented, such as port security, DHCP snooping, and 802.1X user authentication.
ESA/WSA	A Cisco Email Security Appliance (ESA) and Web Security Appliance (WSA) provide advanced threat defense, application visibility and control, reporting, and secure mobility to secure and control email and web traffic.
AAA Server	An authentication, authorization, and accounting (AAA) server authenticates users, authorizes what they are allowed to do, and tracks what they are doing.
Hosts	End points are secured using various features including antivirus and antimalware software, Host Intrusion Protection System features, and 802.1X authentication features.

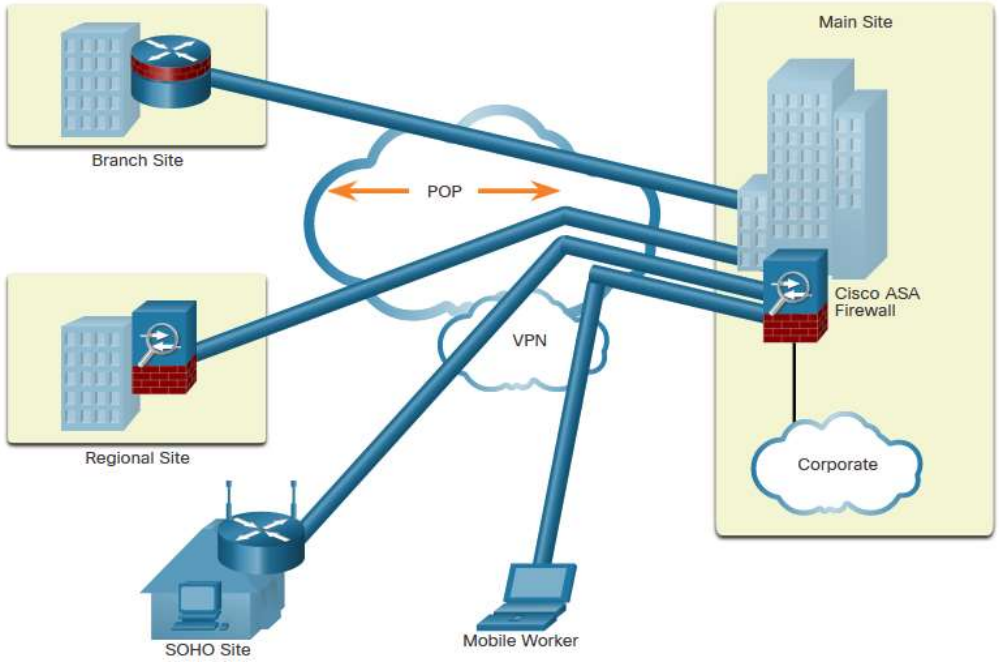
Small Office and Home Office Networks

The figure displays a sample SOHO secured with a consumer-grade wireless router which provides integrated firewall features and secure wireless connections. The Layer 2 Switch is an access layer switch that is hardened with various security measures. It connects user-facing ports that use port security to the SOHO network. Wireless hosts connect to the wireless network using WPA2 data encryption technology. Hosts typically have antivirus and antimalware software installed. Combined, these security measures provide comprehensive defense at different layers of the network.



Wide Area Networks

Wide Area Networks (WANs) span a wide geographical area, often over the public internet. Organizations must ensure secure transport for the data in motion as it travels between sites over the public network. Network security professionals must use secure devices on the edge of the network. In the figure, the main site is protected by an Adaptive Security Appliance (ASA), which provides stateful firewall features and establishes secure Virtual Private Network (VPN) tunnels to various destinations.



Data Center Networks

Data center networks are typically housed in an off-site facility to store sensitive or proprietary data. These sites are connected to corporate sites using VPN technology with ASA devices and integrated data center switches. Because they store such vast quantities of sensitive, business-critical information, physical security is critical to their operation. Physical security not only protects access to the facility but also protects people and equipment. For example, fire alarms, sprinklers, seismically-braced server racks, redundant heating, ventilation, and air conditioning (HVAC), and UPS systems are in place to protect people, equipment, and data.

Data center physical security can be divided into two areas:

- **Outside perimeter security** - This can include on-premise security officers, fences, gates, continuous video surveillance, and security breach alarms.
- **Inside perimeter security** - This can include continuous video surveillance, electronic motion detectors, security traps, and biometric access and exit sensors.

Cloud Networks and Virtualization

The terms “cloud computing” and “virtualization” are often used interchangeably; however, they mean different things. Virtualization is the foundation of cloud computing. Without it, cloud computing, as it is most-widely implemented, would not be possible. Cloud computing separates the application from the hardware. Virtualization separates the operating system from the hardware. The cloud network consists of physical and virtual servers usually found in data centers. Data centers are increasingly using virtual machines (VM) to provide server services to their clients. This allows for multiple operating systems to exist on a single hardware platform. VMs are prone to specific targeted attacks:

- **Hyperjacking** -An attacker could hijack a VM hypervisor (VM controlling software) and then use it as a launch point to attack other devices on the data center network.
- **Instant On Activation** - When a VM that has not been used for a period of time is brought online, it may have outdated security policies that deviate from the baseline security and can introduce security vulnerabilities.
- **Antivirus Storms** - This happens when all VMs attempt to download antivirus data files at the same time.

The Evolving Network Border

Smartphones, tablets, etc., are becoming substitutes for the office PC that is behind a firewall. This trend is known as Bring Your Own Device (BYOD). To accommodate this, Cisco developed the Borderless Network. In a Borderless Network, access to resources can be initiated by users from many locations, on many types of end devices, using various connectivity methods. Cisco devices support Mobile Device Management (MDM) features:

- **Data Encryption** - MDM features can ensure that only devices that support data encryption and have it enabled can access the network and content.
- **PIN Enforcement** - Enforcing a PIN lock is the first and most effective step in preventing unauthorized access to a device.
- **Data Wipe** - Lost or stolen devices can be remotely fully- or partially-wiped, either by the user or by an administrator via the MDM.
- **Data Loss Prevention (DLP)** - DLP prevents authorized users from doing careless or malicious things with critical data.
- **Jailbreak/Root Detection** - Jailbreaking (on Apple iOS devices) and rooting (on Android devices) are a means to bypass the management of a device. MDM features can detect such bypasses and immediately restrict a device's access to the network or assets.

1.3 Module 1: Securing Networks Summary

What Did I Learn in this Module?

- Network security breaches can disrupt e-commerce, cause the loss of business data, threaten people's privacy, and compromise the integrity of information.
- Many tools are available to help network administrators adapt, develop, and implement threat mitigation techniques, including the Cisco Talos Intelligence Group.
- Various DLP controls must be implemented, that combine strategic, operational, and tactical measures.
- Elements of the defense-in-depth design include VPN, ASA firewall, IPS, Layer 3 switches, layer 2 switches, ESA/WSA, AAA server, and hosts.
- Network security professionals must use secure devices on the edge of the network.
- Data center physical security is divided into two areas: outside perimeter security and inside perimeter security.
- VMs are also prone to specific targeted attacks including hyperjacking, instant on activation, and antivirus storms.
- 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.

New Terms and Commands

- Cisco Talos Intelligence Group
- Cisco Product Security Incident Response Team (PSIRT)
- Attack vector
- Denial of service (DoS) attack
- Data Loss Prevention (DLP)
- Email/Social Networking
- Unencrypted Devices
- Cloud Storage Devices
- Removable Media
- Hard Copy
- Improper Access Control
- Campus Area Network (CAN)
- Defense in-depth
- VPN
- ASA Firewall
- IPS

- Layer 3 Switches
- Layer 2 Switches
- ESA/WSA
- AAA Server
- Hosts
- Small office and home office (SOHO) network
- Wireless Protected Access 2 (WPA2)
- Wide Area Network (WAN)
- Cisco AnyConnect VPN client
- Data center network
- Heating, ventilation, and air conditioning (HVAC)
- Outside perimeter security
- Inside perimeter security
- Security trap
- Cloud computing
- Virtualization
- Cloud network

New Terms and Commands (Cont.)

- Virtual machine (VM)
- Hyperjacking
- Instant On Activation
- VM hypervisor
- Instant On Activation
- Antivirus Storms
- Cisco Secure Data Center solution
- Secure Segmentation
- Threat Defense
- Visibility
- Bring Your Own Device (BYOD)
- Borderless Network
- Mobile Device Management (MDM)
- Data encryption
- PIN enforcement
- Data wipe
- Data Loss Prevention (DLP)

- Jailbreak/Root detection


CISCO