Network Topology Overview

1.2.1

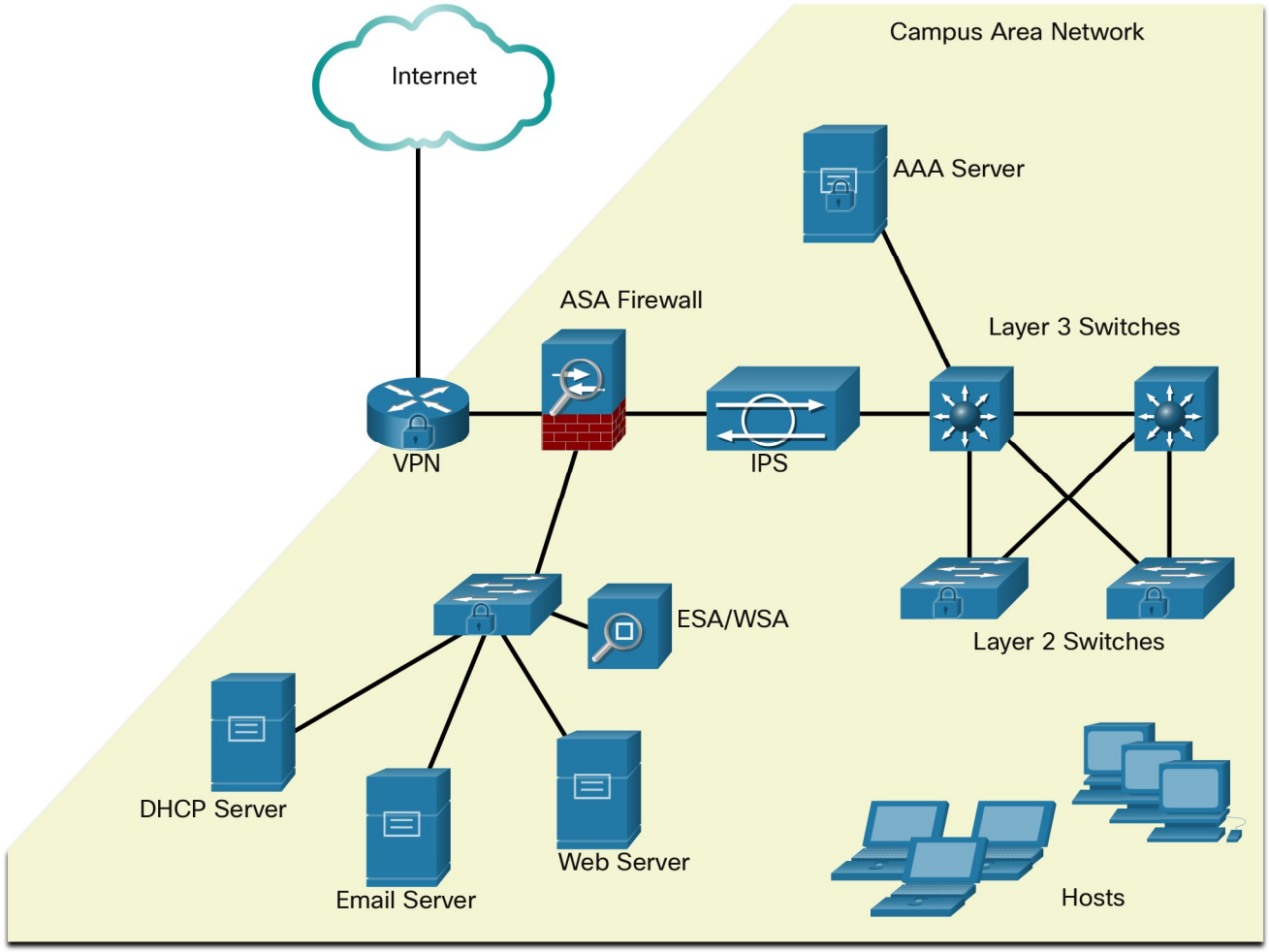
Campus Area Networks

All networks are targets. However, the main focus of this course is on securing Campus Area Networks (CANs). Campus Area Networks consists of interconnected LANs within a limited geographic area.

Network professionals must implement various network security techniques to protect the organization's assets from outside and inside threats. Connections to untrusted networks must be checked in-depth by multiple layers of defense before reaching enterprise resources. This is known as defense-in-depth.

The figure displays a sample CAN with a defense in-depth approach that uses various security features and security devices to secure it. The table provides an Eexplanation of the elements of the defense-in-depth design that are shown in the figure.

Network Security



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.

Term	Definition
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.

1.2.2

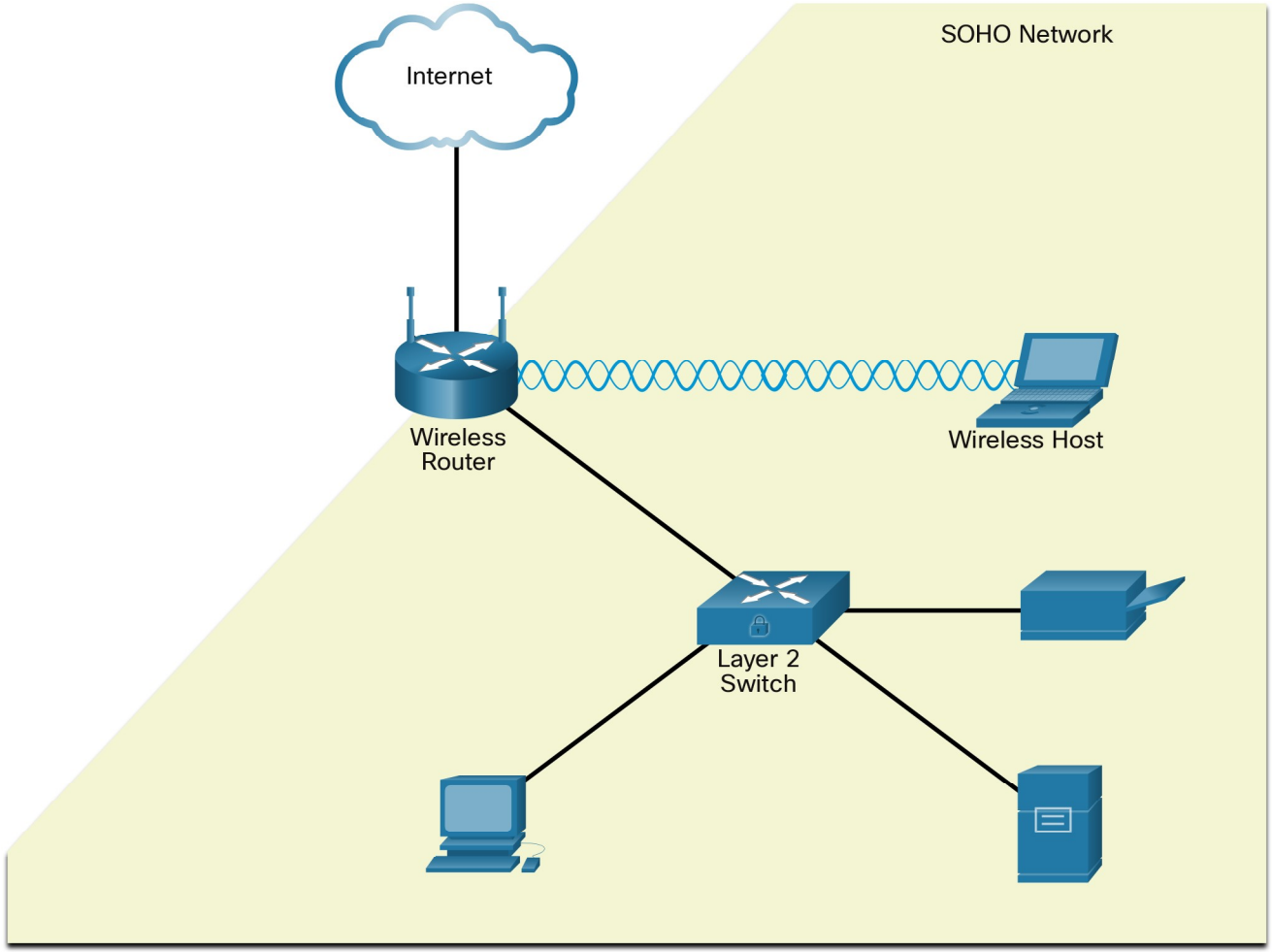
Small Office and Home Office Networks

It is important that all types of networks, regardless of size, are protected. Attackers are also interested in home networks and small office and home office (SOHO) networks. They may want to use someone's internet connection for free, use the internet connection for illegal activity, or view financial transactions, such as online purchases.

Home and SOHO networks are typically protected using a consumer grade router. These routers provide basic security features that adequately protect inside assets from outside attackers.

The figure displays a sample SOHO that uses a consumer-grade wireless router to secure it. A consumer-grade wireless router 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 Wireless Protected Access 2 (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.



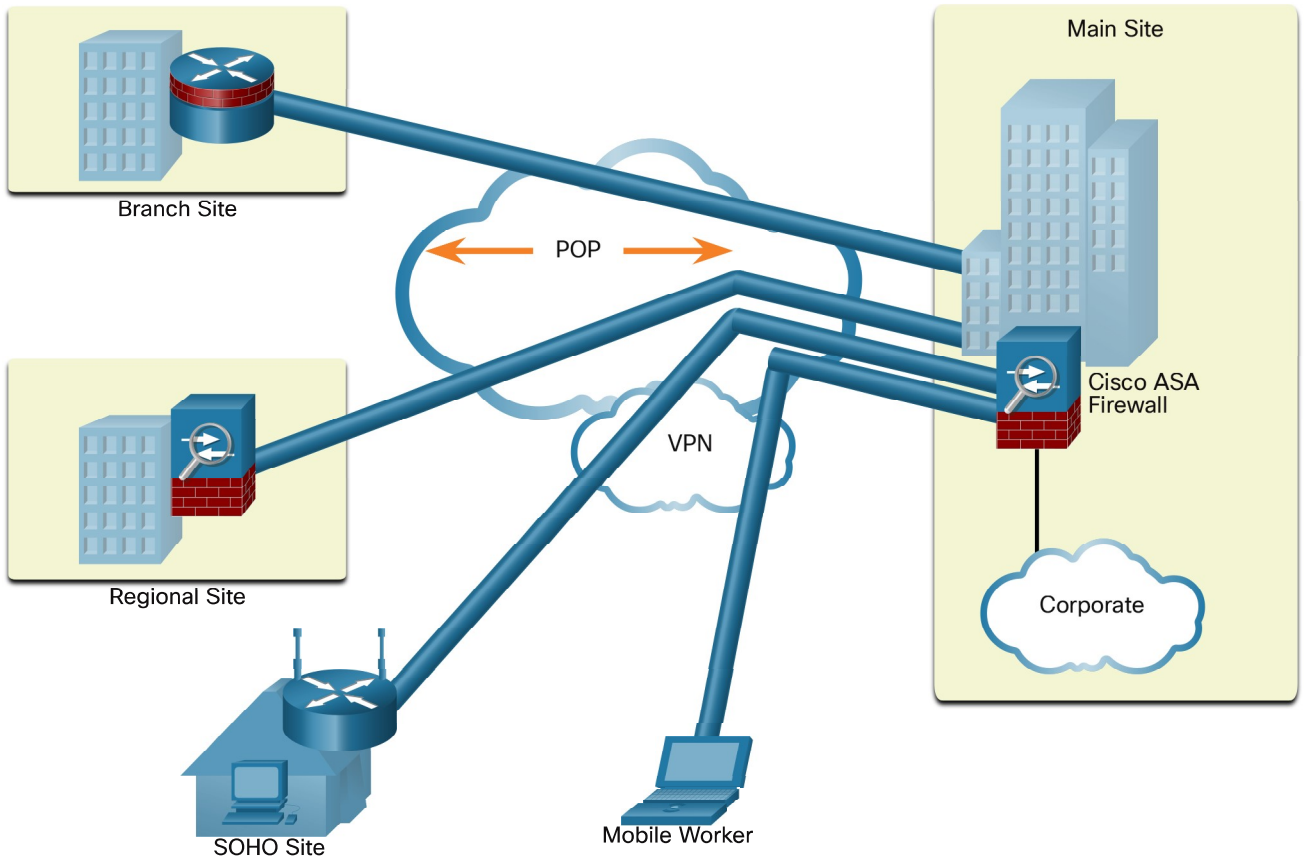
1.2.3

Wide Area Networks

Wide Area Networks (WANs), as shown in the figure, 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 networks. In the figure, the main site is protected by an ASA, which provides stateful firewall features and establishes secure VPN tunnels to various destinations.

Network Security



The figure shows a branch site, a regional site, a SOHO site, and a mobile worker. A branch site connects to the corporate main site using a hardened ISR. The ISR can establish a permanent always-on VPN connection to the main site ASA firewall. A regional site is larger than a branch site and connects to the corporate main site using an ASA. The ASA can establish a permanent always-on VPN connection to the main site ASA. A SOHO site is a small branch site that connects to the corporate main site using a Cisco wireless router. The wireless router can establish a permanent always-on VPN connection to the main site ASA. Alternatively, the internal SOHO users could use the Cisco AnyConnect VPN client to establish a secure VPN connection to the main site ASA. A mobile worker is a teleworker who may use the Cisco AnyConnect VPN client to establish a secure VPN connection to the main site ASA from any location.

1.2.4

Data Center Networks

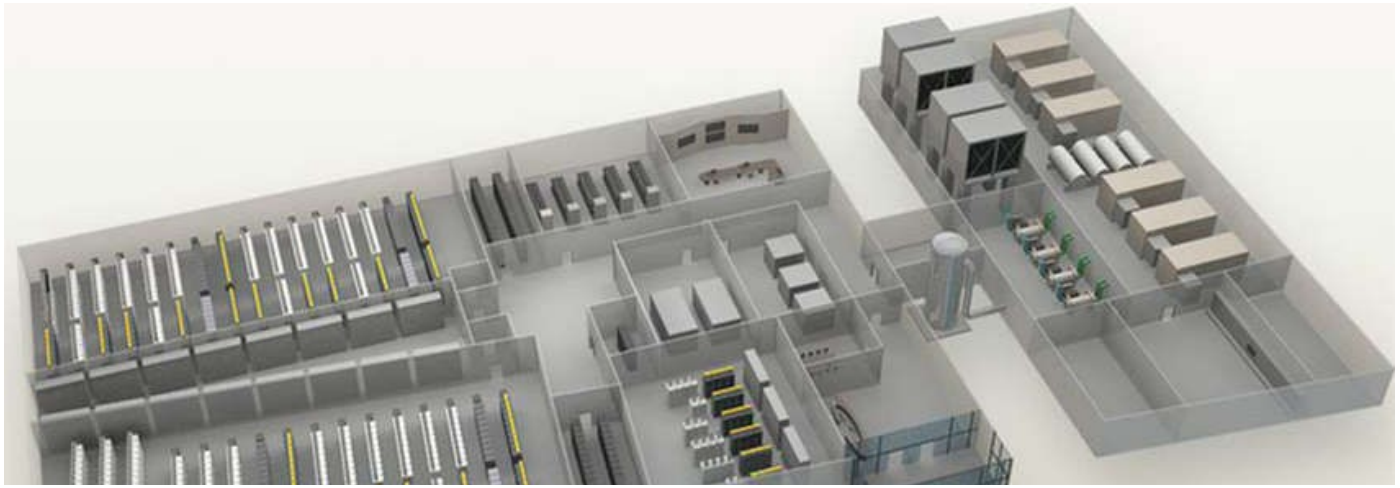
Data center networks are typically housed in an off-site facility to store sensitive or proprietary data. These sites are connected to corporate sites using VPN technology with ASA devices and integrated data center switches, such as a high-speed Cisco Nexus switches.

Today's data centers store vast quantities of sensitive, business-critical information. Therefore, 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.

As highlighted in the figure, data center physical security can be divided into two areas:

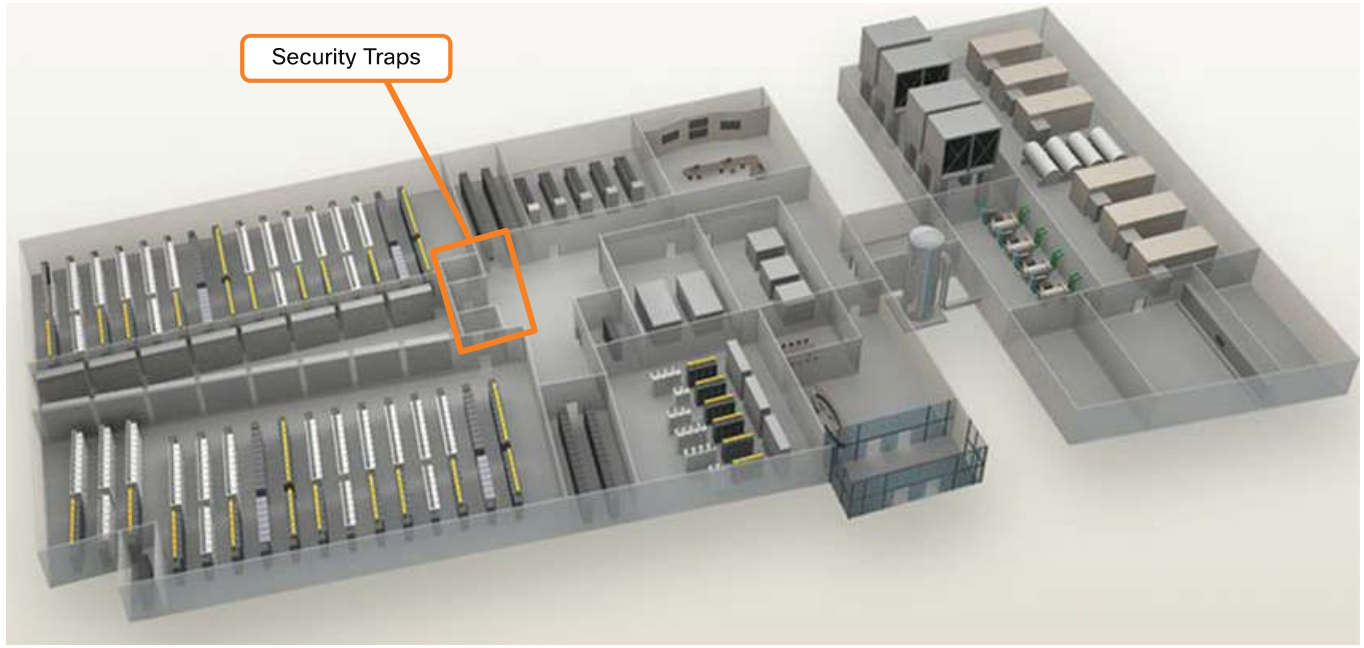
- **Outside perimeter security** - This can include on-premise security officers, fences, gates, continuous video surveillance, and security breach alarms.
- **Inside perimeter security** - This can include continuous video surveillance, electronic motion detectors, security traps, and biometric access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

Data Center Physical Security



Security traps provide access to the data halls where data center data is stored. As shown in the figure below, a security trap is similar to an air lock. A person must first enter the security trap using their badge ID proximity card. After the person is inside the security trap, facial recognition, fingerprints, or other biometric verifications are used to open the second door. The user must repeat the process to exit the data hall.

Security Traps



The figure below displays the biometric finger print scanner that is used to secure access to the Cisco Allen Data Center, in Allen, Texas.

Biometric Access

1.2.5

Cloud Networks and Virtualization

The cloud is playing an increasing role in enterprise networks. Cloud computing allows organizations to use services such as data storage or cloud-based applications, to extend their capacity or capabilities without adding infrastructure. By its very nature, the cloud is outside of the traditional network perimeter, allowing an organization to have a data center that may or may not reside behind the traditional firewall.

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 which are commonly housed in data centers. However, data centers are increasingly using virtual machines (VM) to provide server services to their clients. Server virtualization takes advantage of idle computing resources and consolidates the number of required servers. This also allows for multiple operating systems to exist on a single hardware platform. However, VMs are also prone to specific targeted attacks as listed below.

- **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.

For security teams, an easy to implement yet comprehensive strategy that addresses business demands and defends the data center is a necessity. Cisco developed the Secure Data Center solution to operate in this unpredictable threat landscape. 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 the following services:

- **Secure Segmentation** - ASA devices and a Virtual Security Gateway integrated into the Cisco Nexus Series switches are deployed in a data center network to provide secure segmentation. This provides granular inter-virtual-machine security.
- **Threat Defense** - ASAs and IPS devices in data center networks use threat intelligence, passive OS fingerprinting, and reputation and contextual analysis to provide threat defense.
- **Visibility** - Visibility solutions are provided using software such as the Cisco Security Manager which help simplify operations and compliance reporting.

1.2.6

The Evolving Network Border

In the past, employees and data resources remained within a predefined perimeter that was protected by firewall technology. Employees typically used company-issued computers connected to a corporate LAN that were continuously monitored and updated to meet security requirements.

Today, consumer endpoints, such as iPhones, smartphones, tablets, and thousands of other devices, are becoming powerful substitutes for, or complements to, the traditional PC. More and more people are using these devices to access enterprise information. This trend is known as Bring Your Own Device (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 Mobile Device Management (MDM) features. MDM features secure, monitor, and manage mobile devices, including corporate-owned devices and employee-owned devices. MDM-supported and managed devices include not only handheld devices, such as smartphones and tablets, but also laptop and desktop computing devices.

Click each button below to learn about the critical functions performed by MDM.

Data Encryption | PIN Enforcement | Data Wipe | Data Loss Prevention (DLP) | Jailbreak/Root Detection

Most devices have built-in encryption capabilities, both at the device and file level. MDM features can ensure that only devices that support data encryption and have it enabled can access the network and corporate content.

1.2.7

Check Your Understanding - Network Topology Protection Overview

Network Security

Check your understanding of Network Topologies by choosing the best answer to the following questions.

1. Which network type includes a consumer grade router with basic security features to protect inside assets from outside attackers?

- SOHO
- CAN
- WAN
- Cloud

2. Which network type uses high-speed Nexus switches to connect an off-site facility to the corporate site?

- SOHO
- CAN
- Data Center
- Cloud

Check

Show Me

Reset

1.1 Current State of Affairs

1.3 Securing Networks Summary