

Chapter 1: Modern Network Security Threats

CCNA Security v2.0



Chapter Outline

- 1.0 Introduction
- 1.1 Securing Networks
- 1.2 Network Threats
- 1.3 Mitigating Threats
- 1.4 Summary

Section 1.1: Securing Networks

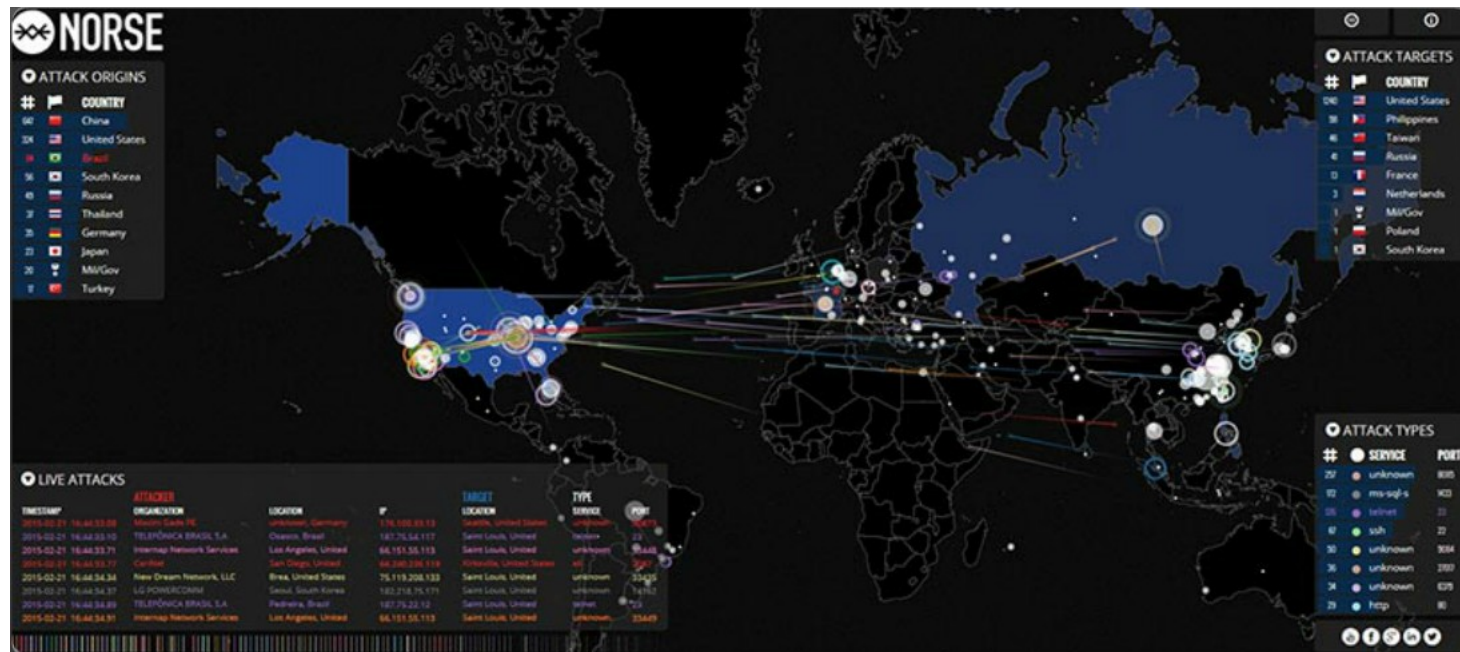
Upon completion of this section, you should be able to:

- Describe the current network security landscape.
- Explain how all types of networks need to be protected.

Topic 1.1.1: Current State of Affairs



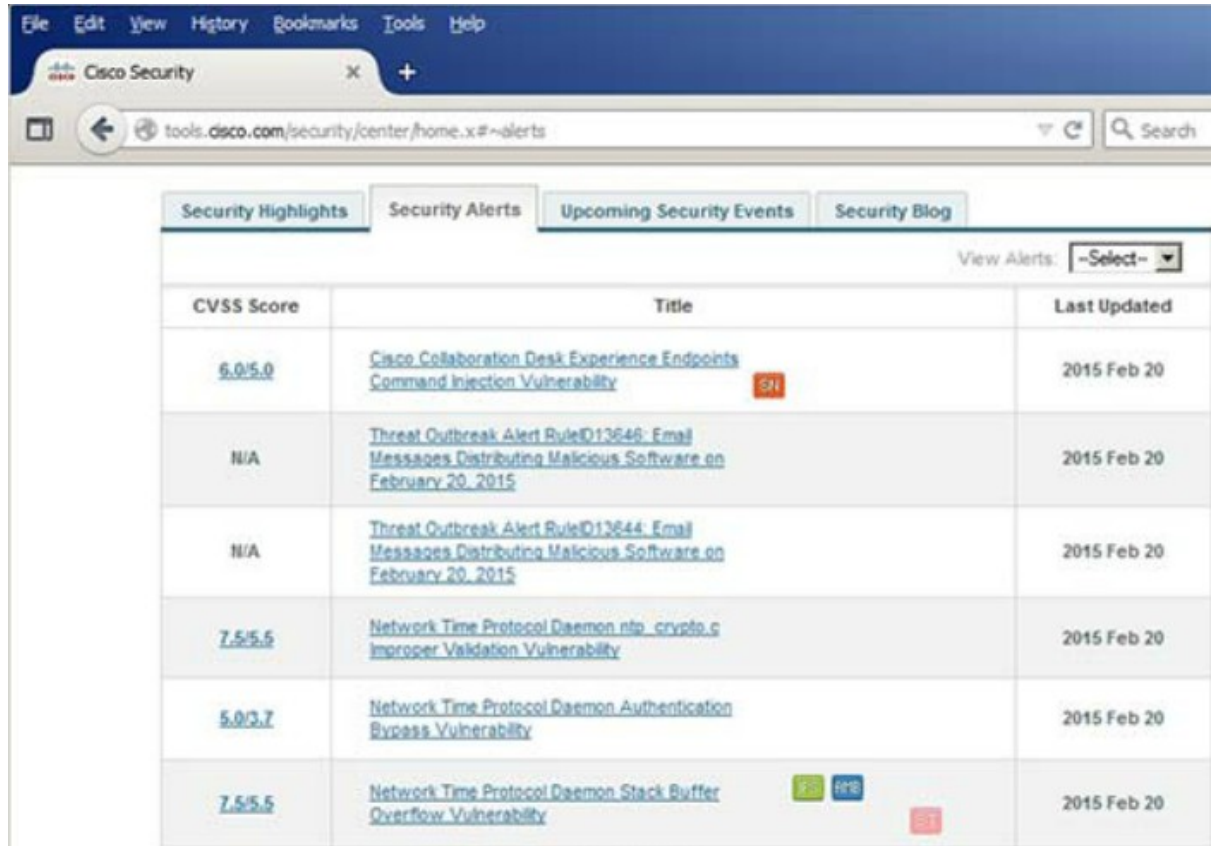
Networks Are Targets



Drivers for Network Security

Common network security terms:

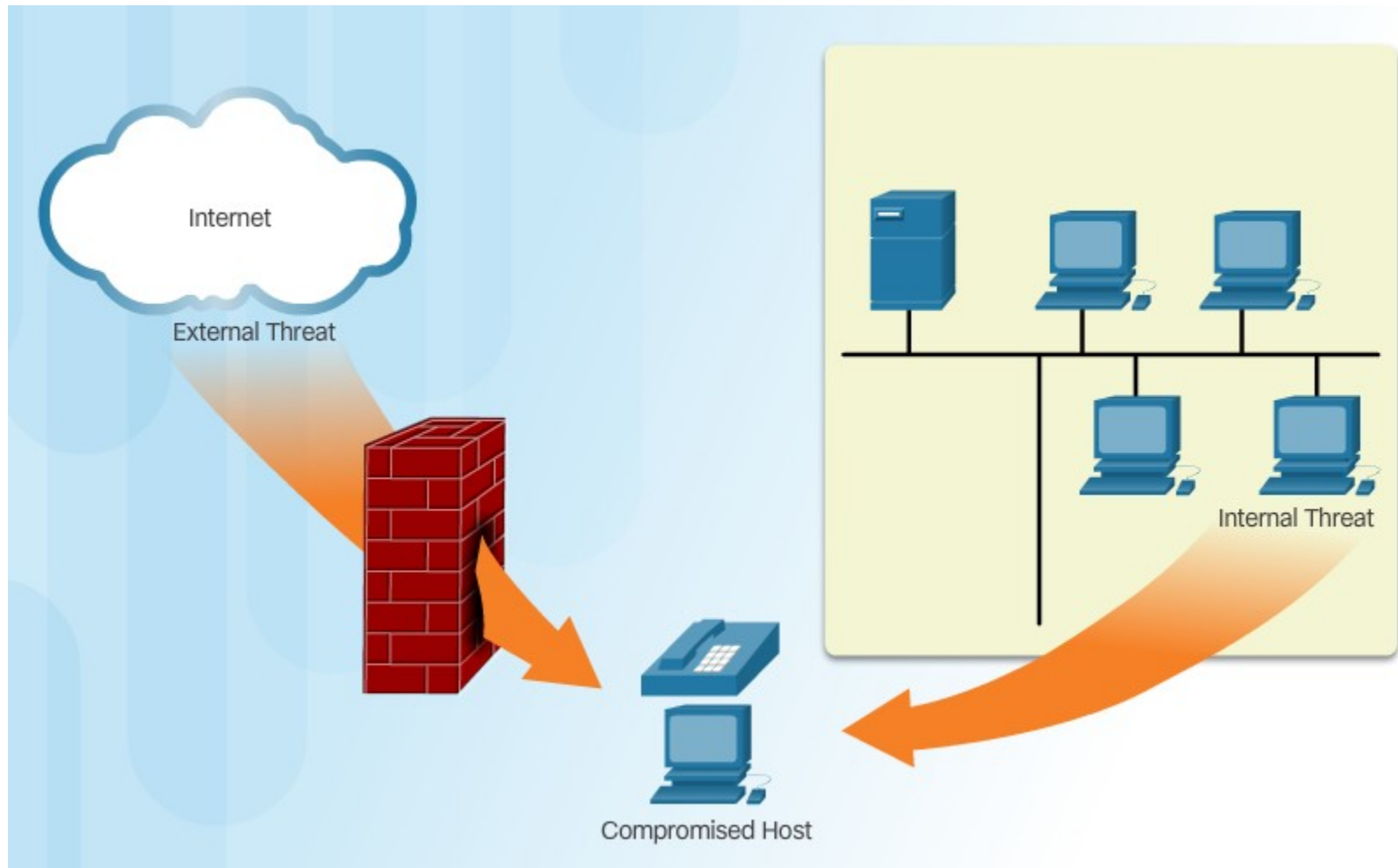
- Threat
- Vulnerability
- Mitigation
- Risk



The screenshot shows the Cisco Security Center web interface. The browser address bar displays `tools.cisco.com/security/center/home.x#~alerts`. The interface includes tabs for 'Security Highlights', 'Security Alerts', 'Upcoming Security Events', and 'Security Blog'. A 'View Alerts' dropdown menu is set to '-Select-'. Below the tabs is a table with three columns: 'CVSS Score', 'Title', and 'Last Updated'. The table lists several security alerts, including vulnerabilities in Cisco Collaboration Desk Experience Endpoints, Threat Outbreak Alert Rules, and Network Time Protocol Daemon.

CVSS Score	Title	Last Updated
6.0/5.0	Cisco Collaboration Desk Experience Endpoints Command Injection Vulnerability 	2015 Feb 20
N/A	Threat Outbreak Alert RuleID13646: Email Messages Distributing Malicious Software on February 20, 2015	2015 Feb 20
N/A	Threat Outbreak Alert RuleID13644: Email Messages Distributing Malicious Software on February 20, 2015	2015 Feb 20
7.5/5.5	Network Time Protocol Daemon ntp_crypto.c Improper Validation Vulnerability	2015 Feb 20
5.0/3.7	Network Time Protocol Daemon Authentication Bypass Vulnerability	2015 Feb 20
7.5/5.5	Network Time Protocol Daemon Stack Buffer Overflow Vulnerability   	2015 Feb 20

Vectors of Network Attacks



Data Loss

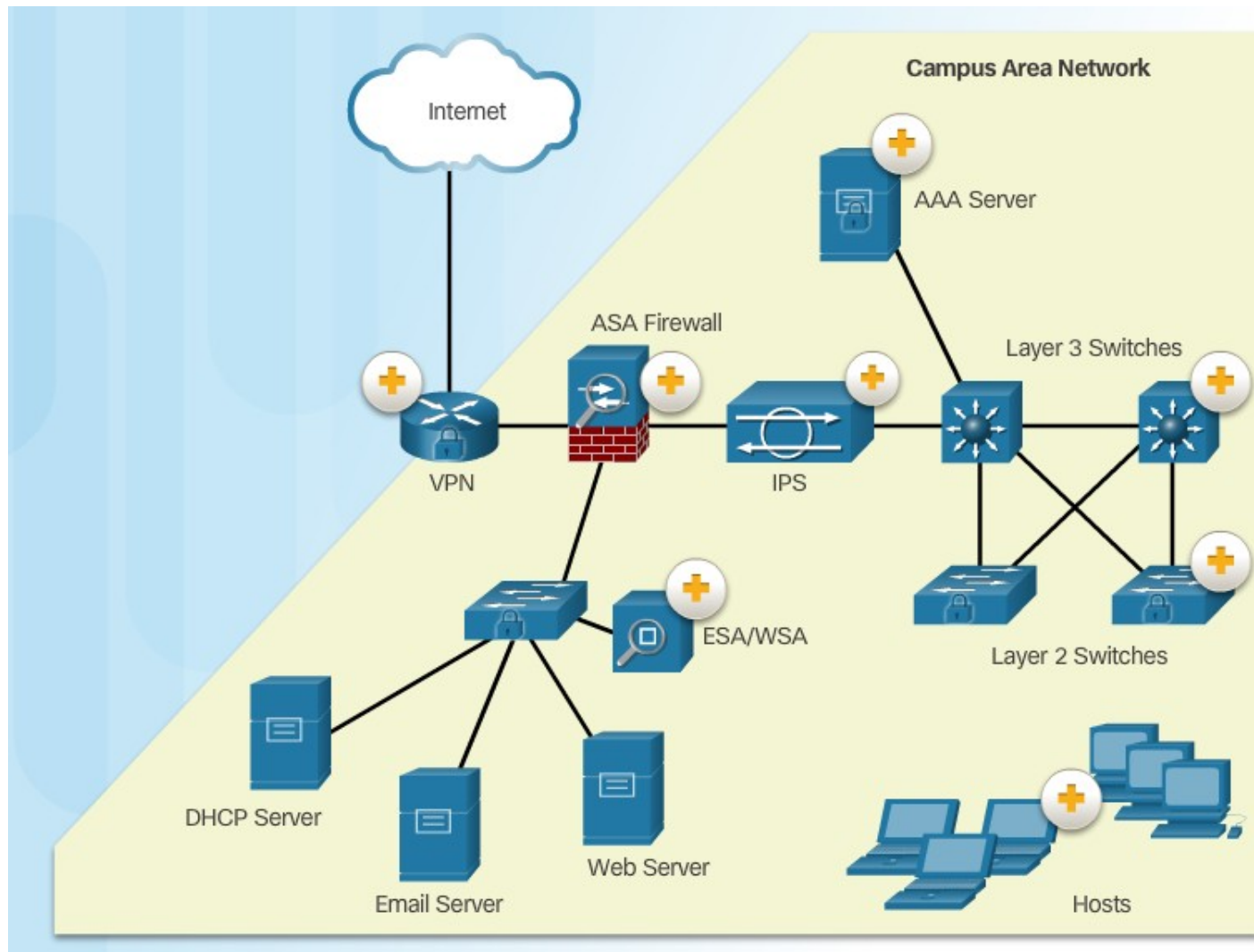
Vectors of data loss:

- Email/Webmail
- Unencrypted Devices
- Cloud Storage Devices
- Removable Media
- Hard Copy
- Improper Access Control

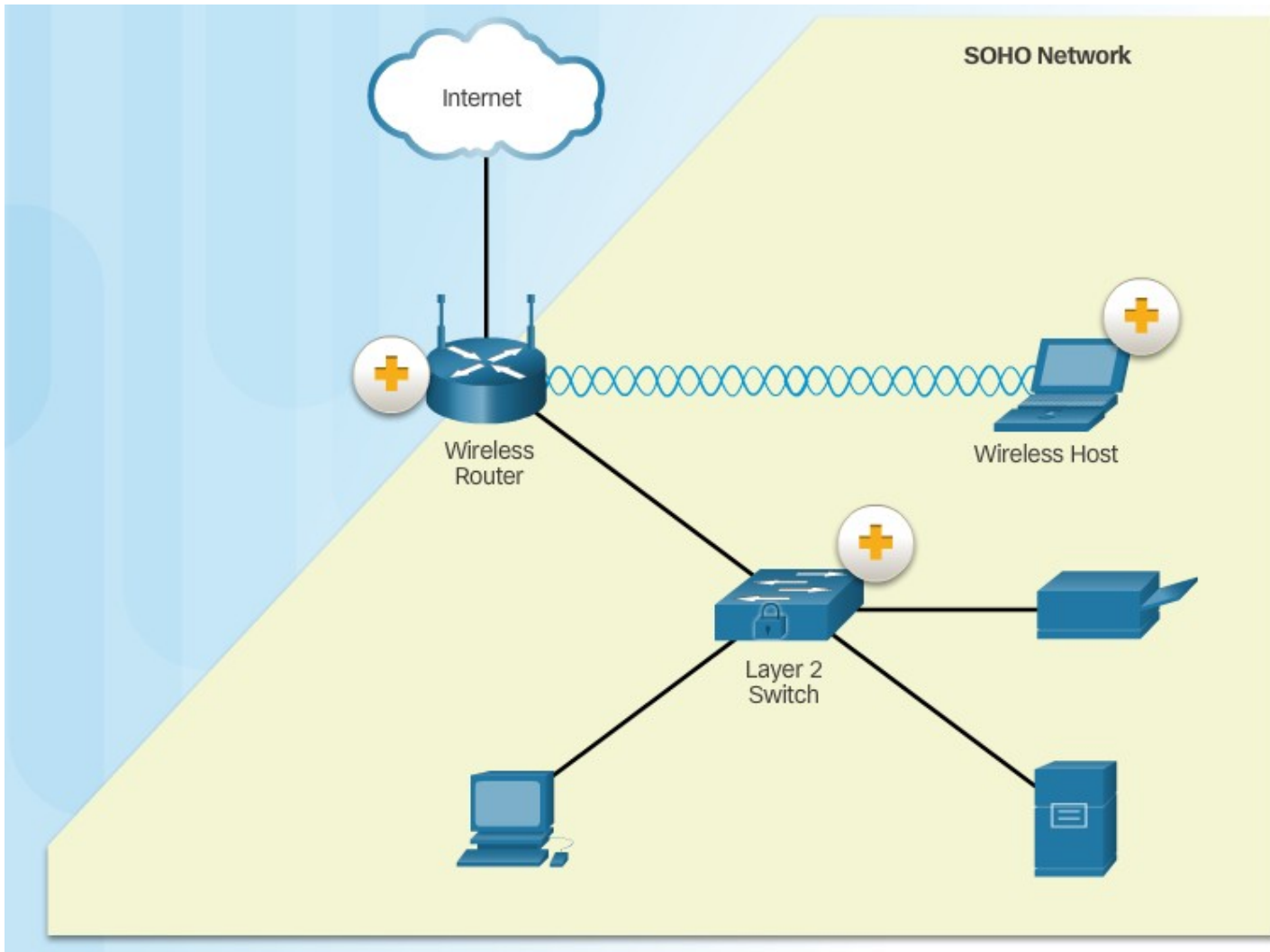
Topic 1.1.2: Network Topology Overview



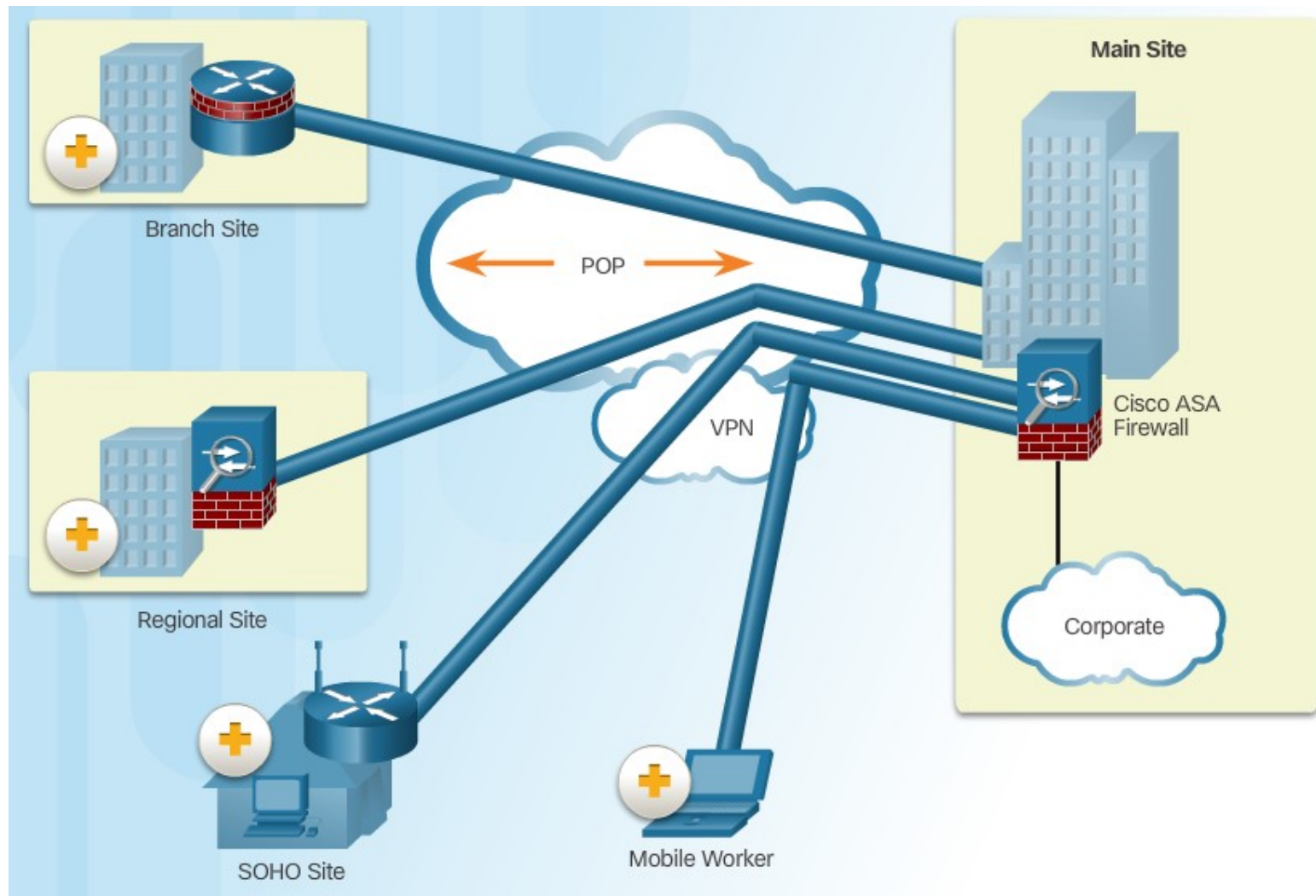
Campus Area Networks



Small Office and Home Office Networks



Wide Area Networks



Data Center Networks

Outside perimeter security:

- On-premise security officers
- Fences and gates
- Continuous video surveillance
- Security breach alarms

Inside perimeter security:

- Electronic motion detectors
- Security traps
- Continuous video surveillance
- Biometric access and exit sensors

Cloud and Virtual Networks

VM-specific threats:

- Hyperjacking
- Instant On activation
- Antivirus storm

Components of a secure data center:

- Secure segmentation
- Threat defense
- Visibility

The Evolving Network Border

Critical MDM functions for BYOD network:

- Data encryption
- PIN enforcement
- Data wipe
- Data loss prevention
- Jailbreak/root detection

Section 1.2: Network Threats

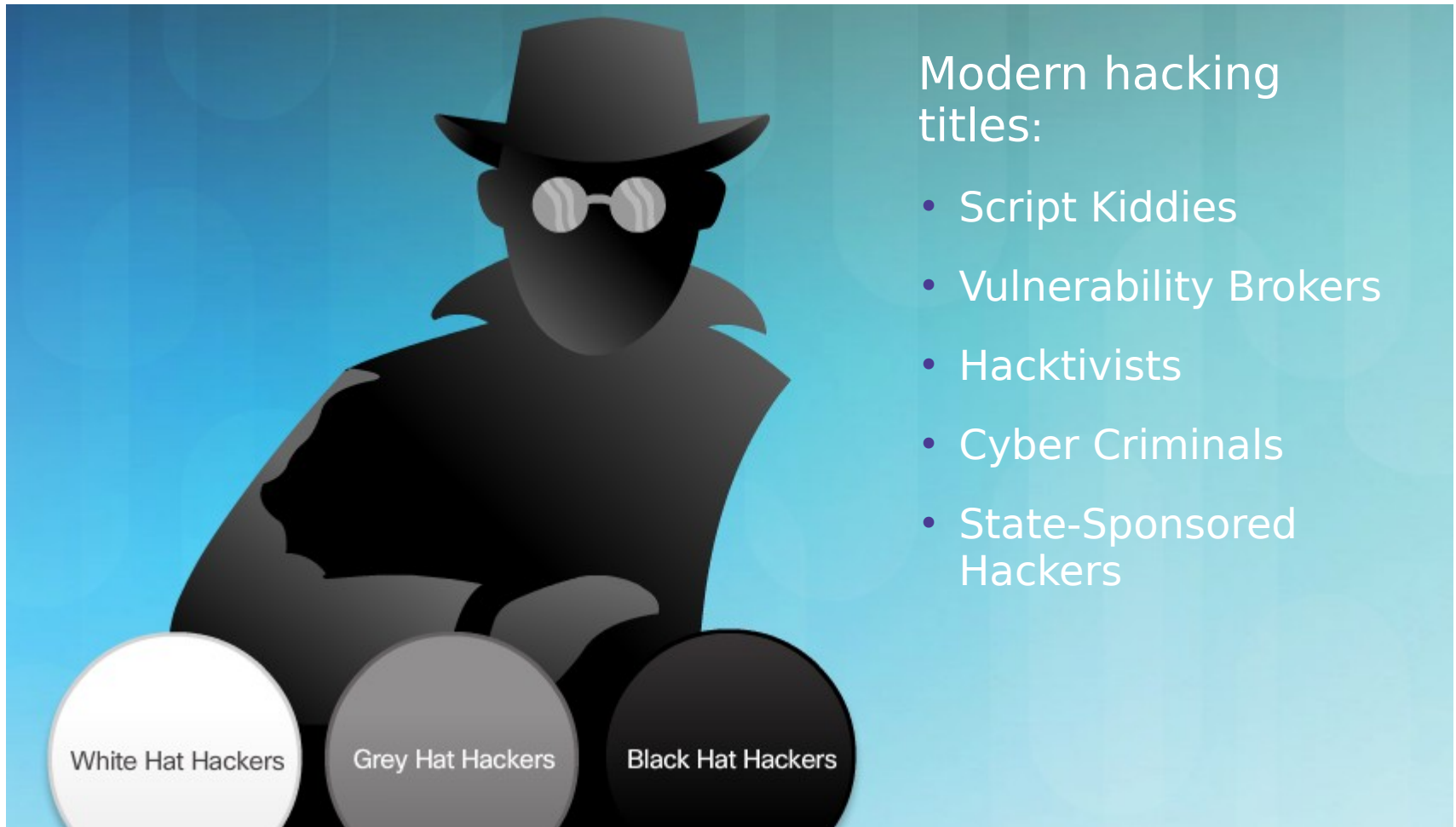
Upon completion of the section, you should be able to:

- Describe the evolution of network security.
- Describe the various types of attack tools used by hackers.
- Describe malware.
- Explain common network attacks.

Topic 1.2.1: Who is Hacking Our Networks?



The Hacker & The Evolution of Hackers



Modern hacking titles:

- Script Kiddies
- Vulnerability Brokers
- Hacktivists
- Cyber Criminals
- State-Sponsored Hackers

White Hat Hackers

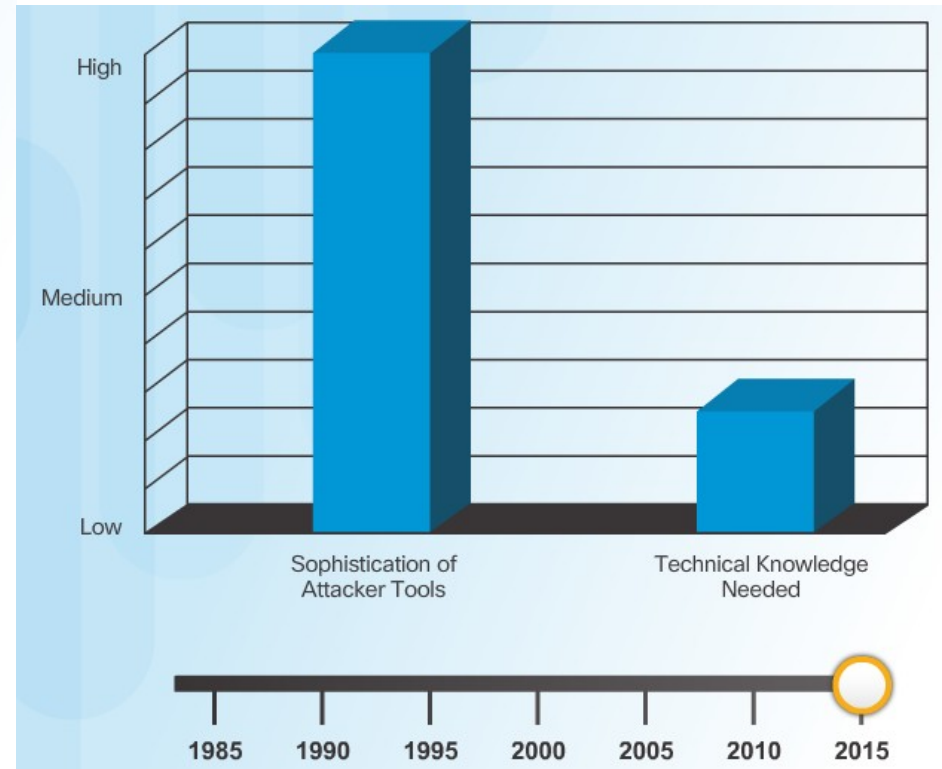
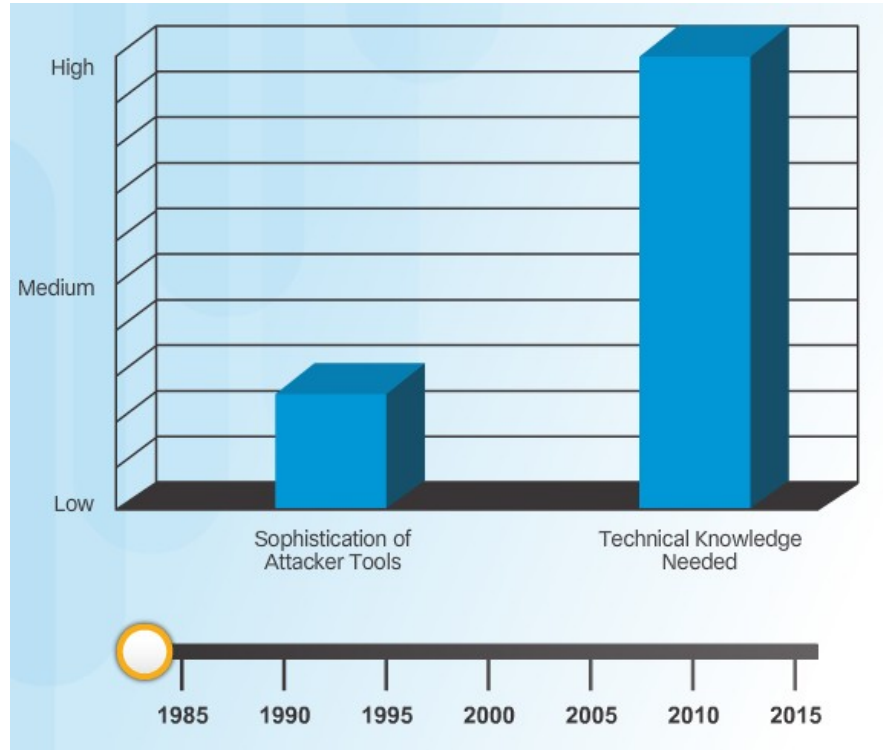
Grey Hat Hackers

Black Hat Hackers

Topic 1.2.2: Hacker Tools



Introduction of Attack Tools



Evolution of Security Tools

Penetration testing tools:

- Password crackers
- Wireless hacking
- Network scanning and hacking
- Packet crafting
- Packet sniffers
- Rootkit detectors
- Fuzzers to search vulnerabilities
- Forensic
- Debuggers
- Hacking operating systems
- Encryption
- Vulnerability exploitation
- Vulnerability Scanners

Categories of Attack Tools

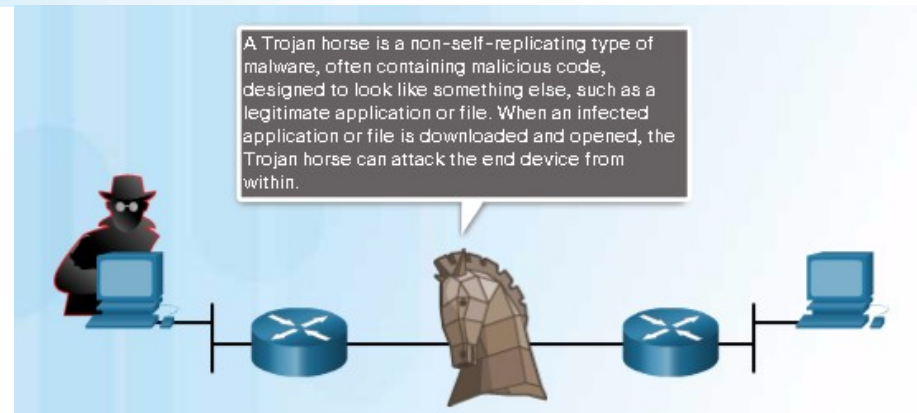
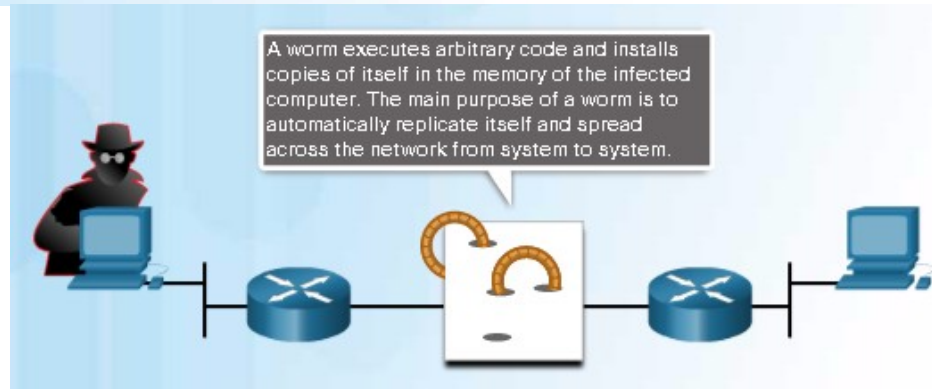
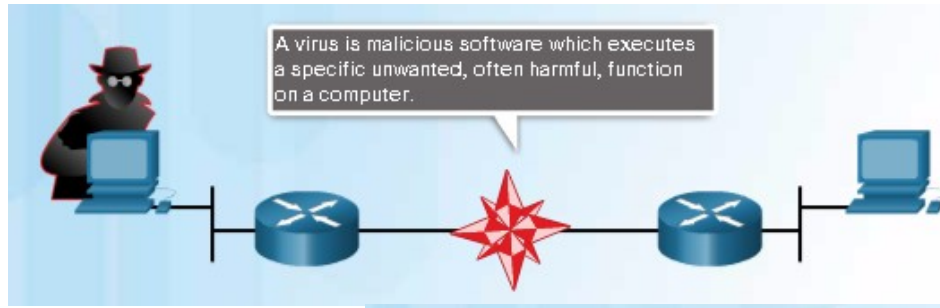
Network hacking attacks:

- Eavesdropping
- Data modification
- IP address spoofing
- Password-based
- Denial-of-service
- Man-in-the-middle
- Compromised-key
- Sniffer

Topic 1.2.3: Malware



Various Types of Malware



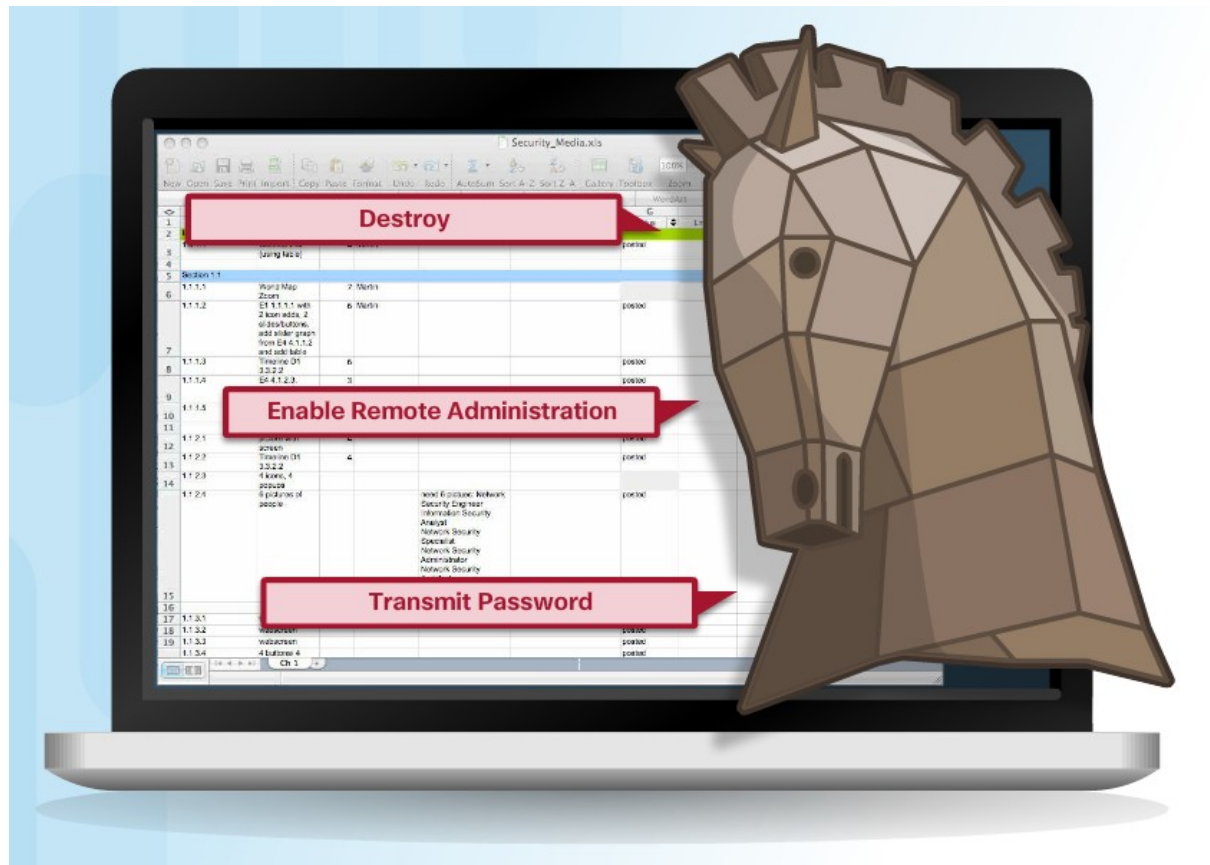
Viruses



Trojan Horse Classification

Classifications:

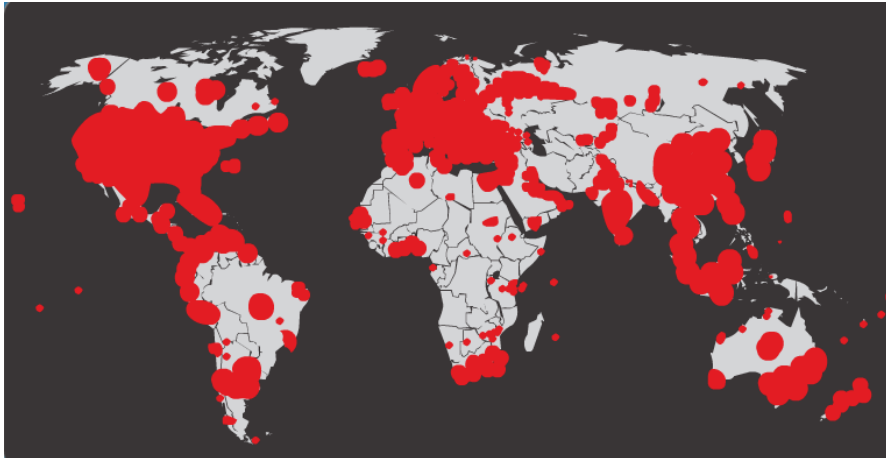
- Security software disabler
- Remote-access
- Data-sending
- Destructive
- Proxy
- FTP
- DoS



Worms



Initial Code Red Worm
Infection

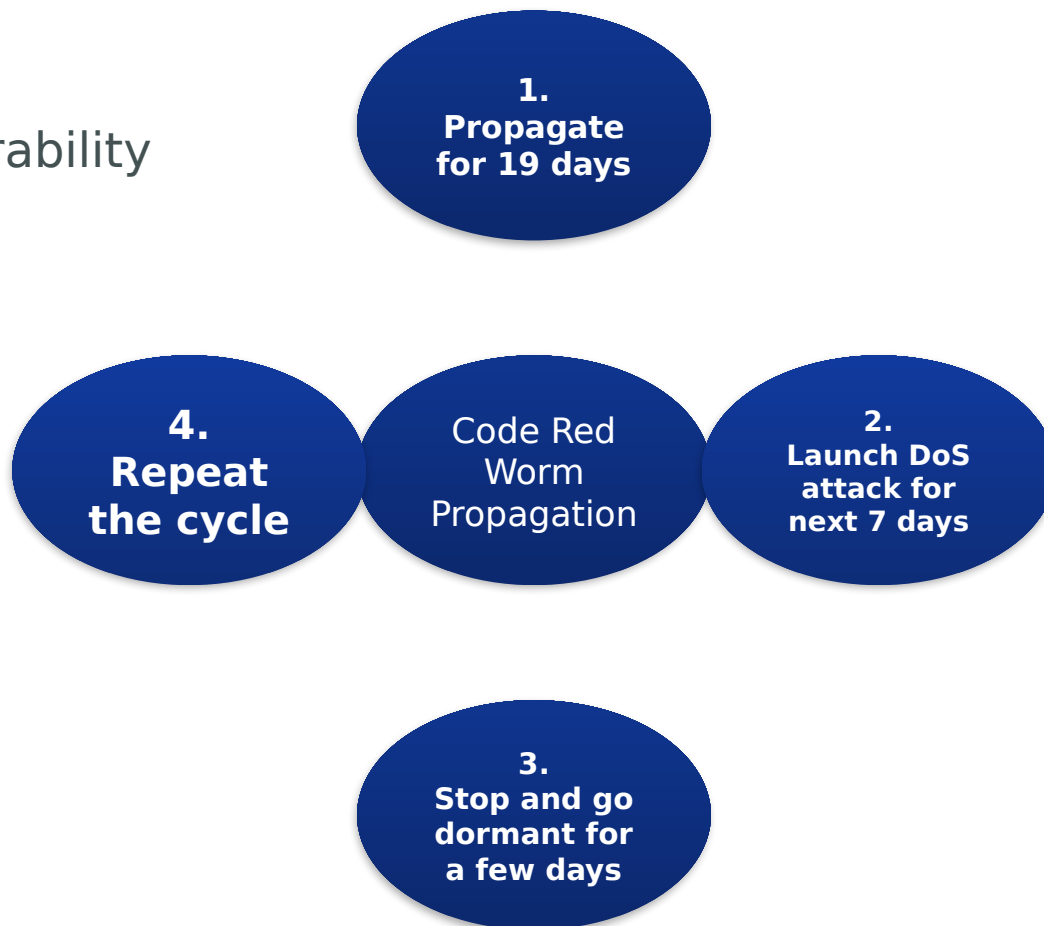


Code Red Worm Infection 19 Hours
Later

Worm Components

Components:

- Enabling vulnerability
- Propagation mechanism
- Payload



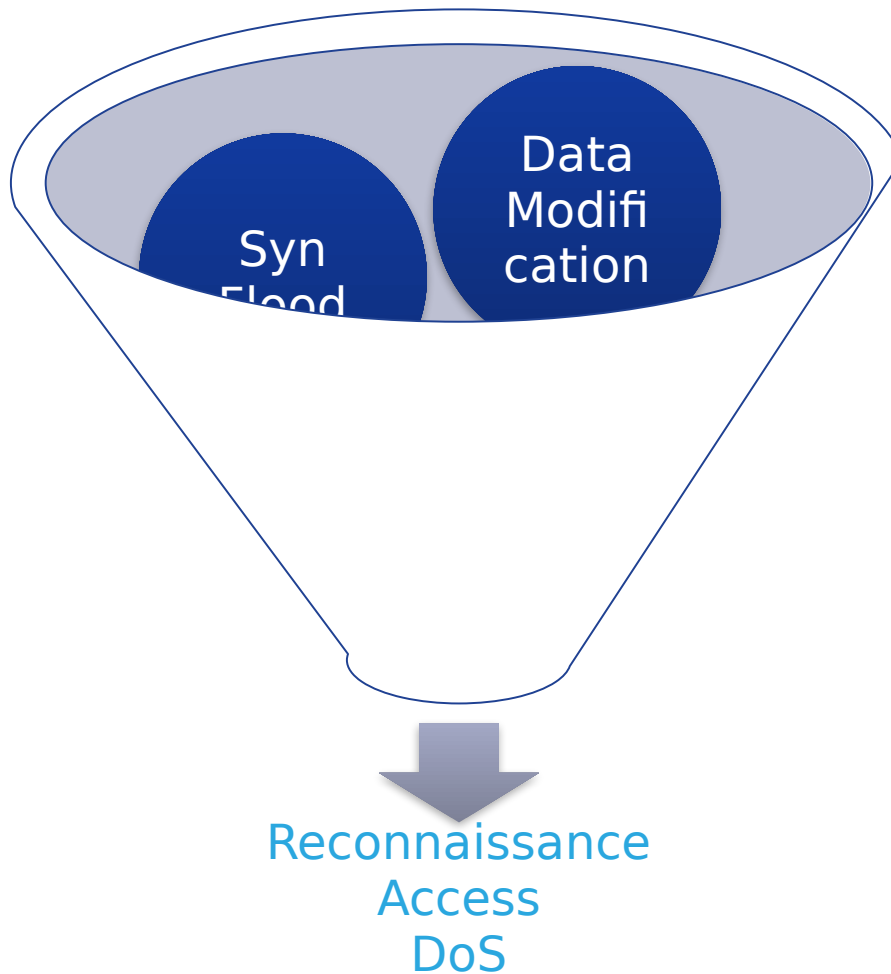
Other Malware



Topic 1.2.4: Common Network Attacks



Types of Network Attacks



Reconnaissance Attacks

- Initial query of a target
- Ping sweep of the target network
- Port scan of active IP addresses
- Vulnerability scanners
- Exploitation tools



Access Attacks

A few reasons why hackers use access attacks:

- To retrieve data
- To gain access
- To escalate access privileges

A few types of access attacks include:

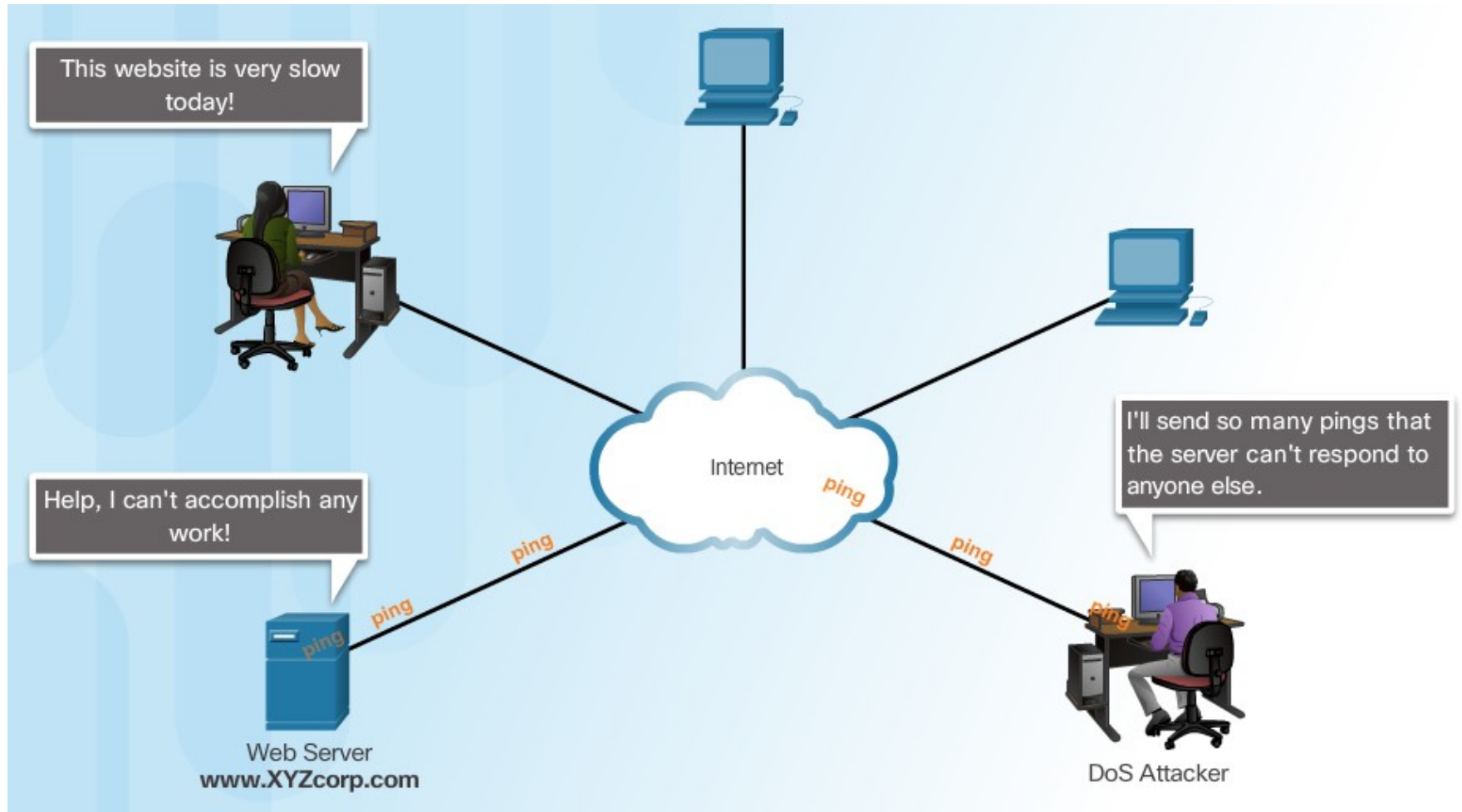
- Password
- Trust exploitation
- Port redirection
- Man-in-the-middle
- Buffer overflow
- IP, MAC, DHCP spoofing

Social Engineering Attacks

- Pretexting
- Phishing
- Spearphishing
- Spam
- Tailgating
- Something for Something
- Baiting



Denial of Service Attacks



DDoS Attacks

1. Hacker builds a network of infected machines
 - A network of infected hosts is called a botnet.
 - The compromised computers are called zombies.
 - Zombies are controlled by handler systems.
2. Zombie computers continue to scan and infect more targets
3. Hacker instructs handler system to make the botnet of zombies carry out the DDoS attack

1.3 Mitigating Threats

Upon completion of this section, you should be able to::

- Describe methods and resources to protect the networks.
- Describe a collection of domains for network security.
- Explain the purpose of the Cisco SecureX Architecture.
- Describe the techniques used to mitigate common network attacks.
- Explain how to secure the three functional areas of Cisco routers and switches.

Topic 1.3.1: Defending the Network



Network Security Professionals



Chief Information Officer (CIO)



Chief Information Security Officer
(CISO)



Security Operations (SecOps)
Manager



Chief Security Officer (CSO)



Security Manager

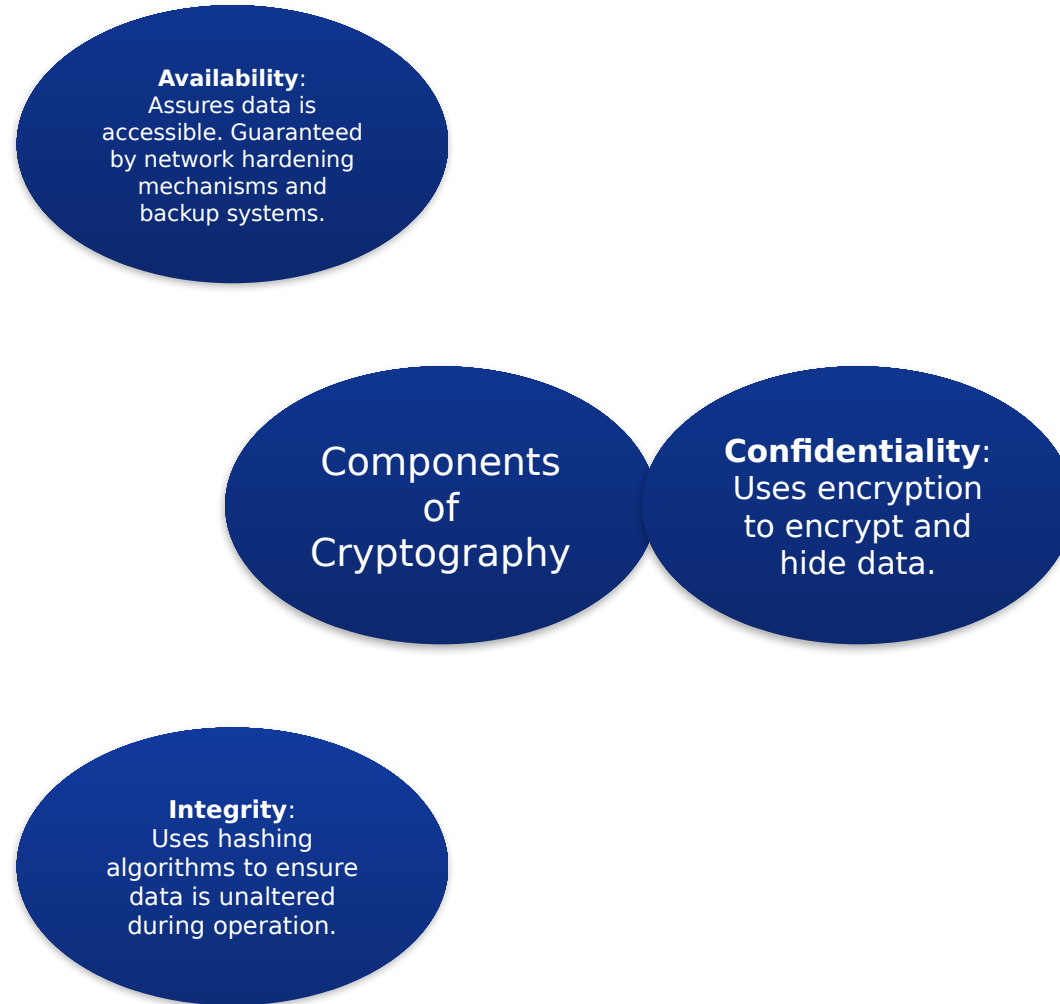


Network Security Engineer

Network Security Organizations



Confidentiality, Integrity, Availability



Topic 1.3.2: Domains of Network Security



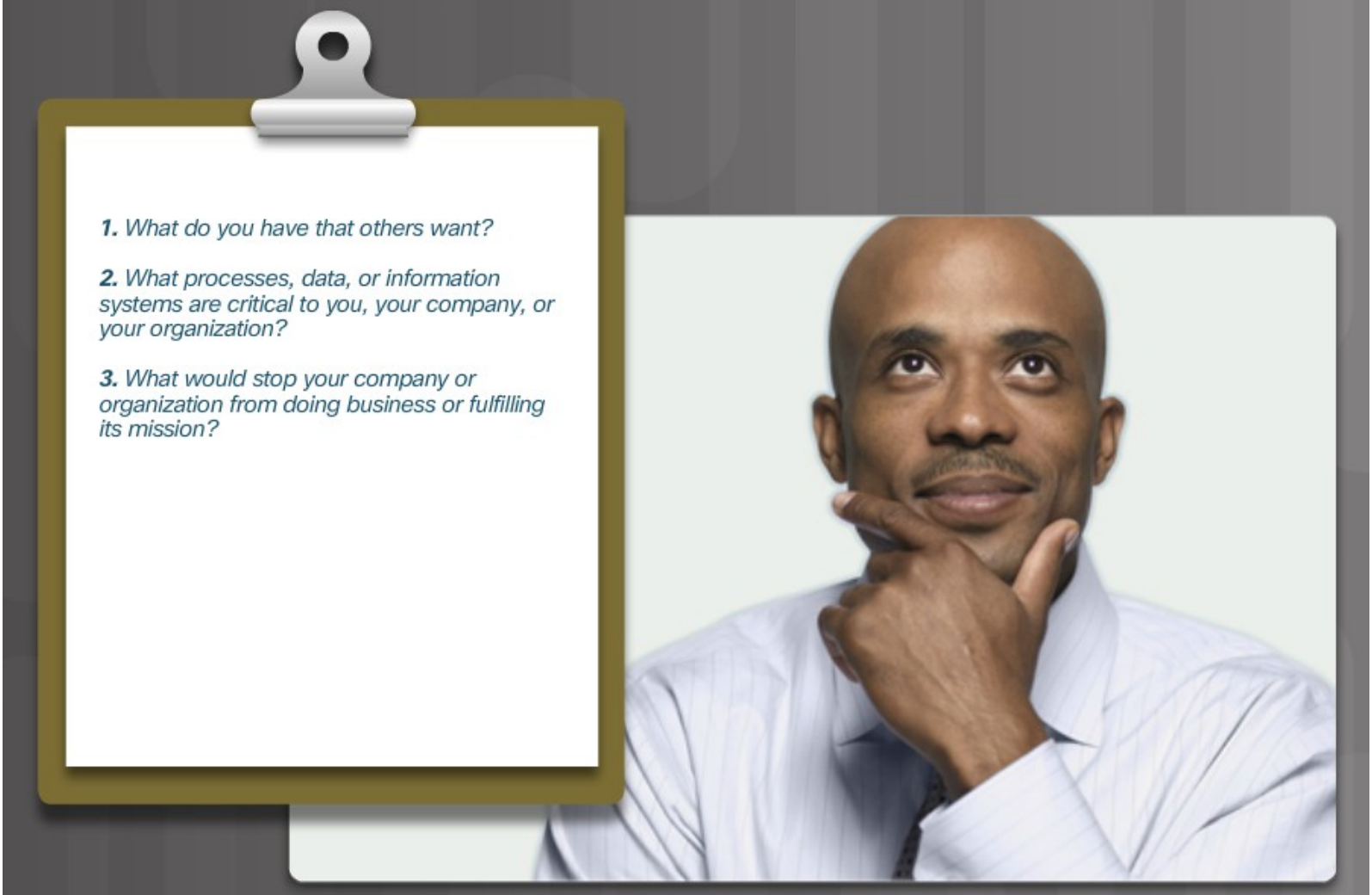
Network Security Domains

- Risk assessment
- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Information systems acquisition, development, and maintenance
- Access control
- Information security incident management
- Business continuity management
- Compliance

Network Security Policy



Network Security Policy Objectives

- 
- 1. What do you have that others want?*
- 2. What processes, data, or information systems are critical to you, your company, or your organization?*
- 3. What would stop your company or organization from doing business or fulfilling its mission?*

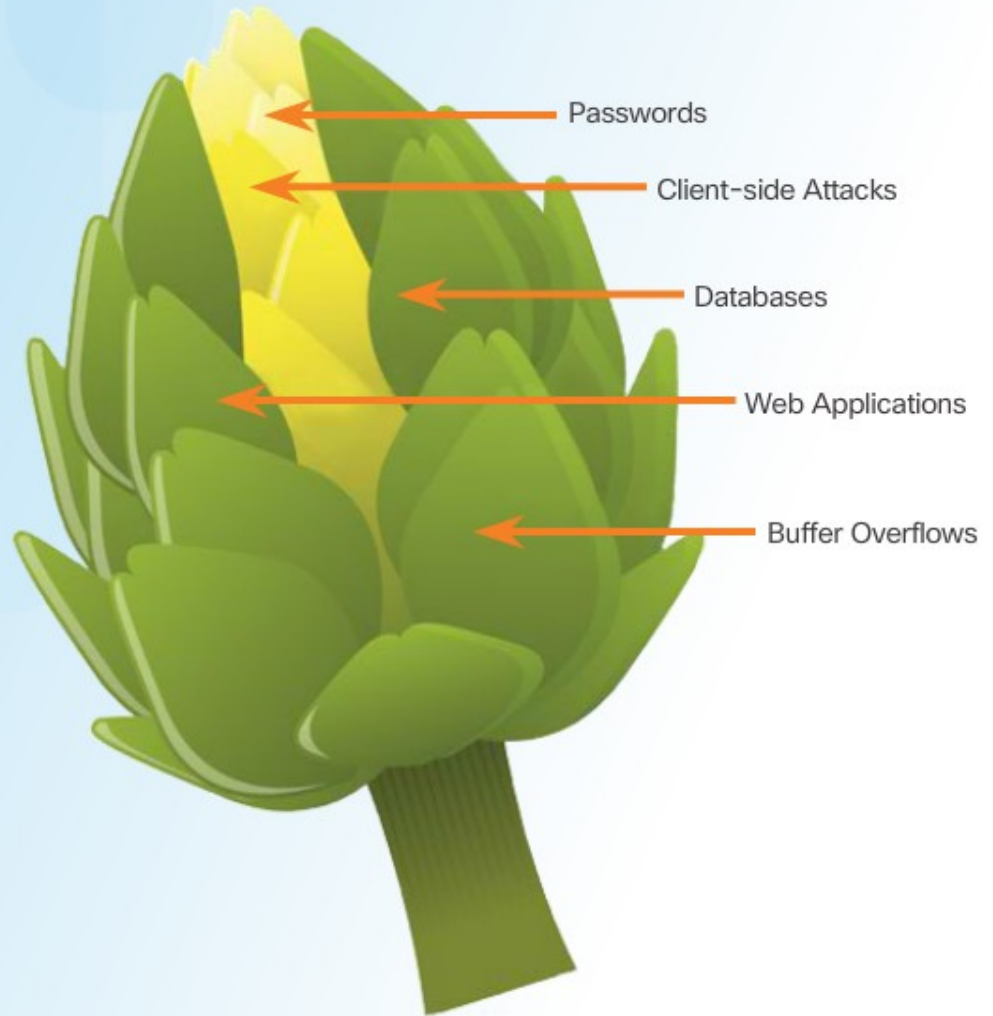
Topic 1.3.3: Introducing the Cisco SecureX Architecture



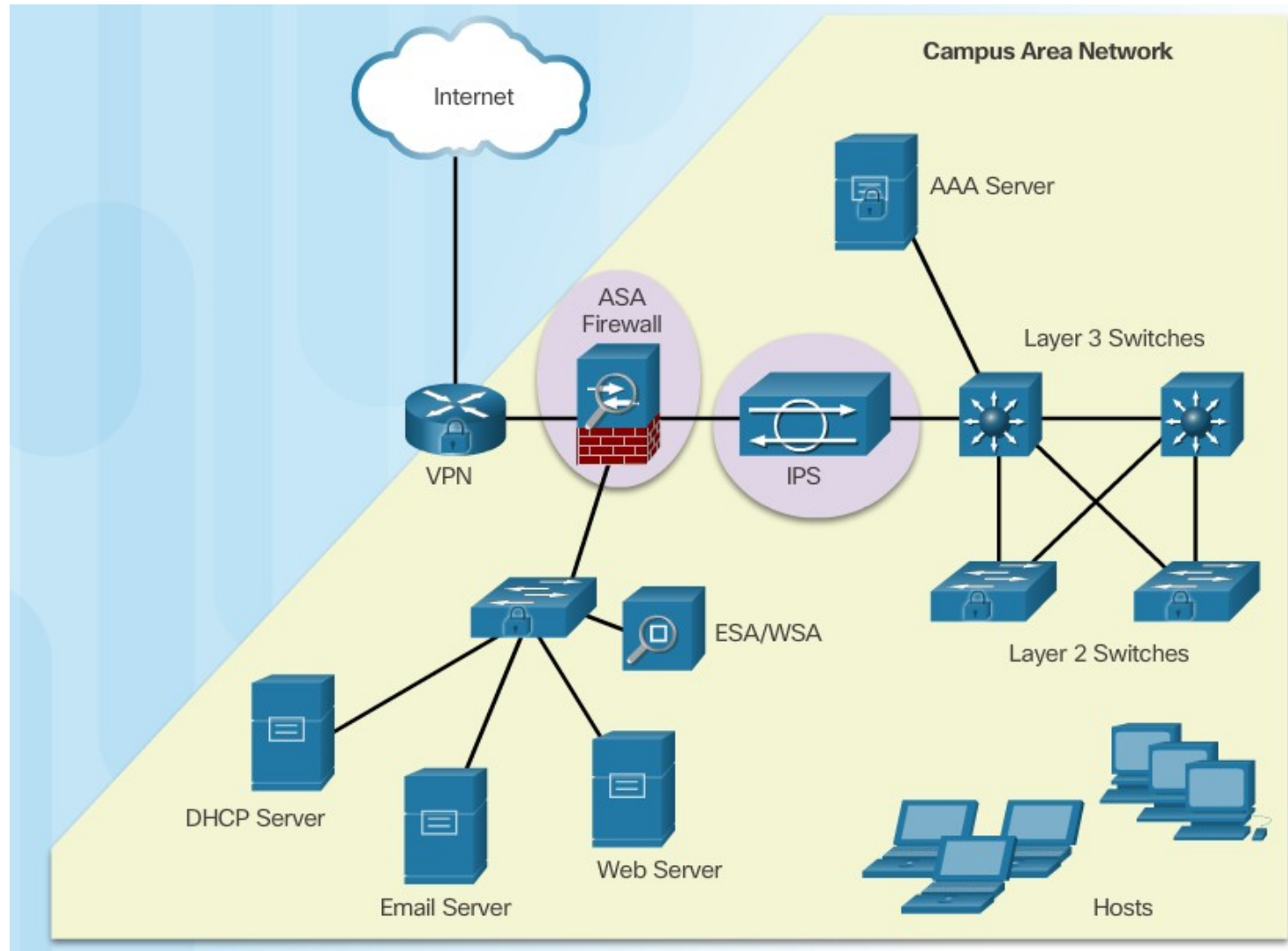
The Security Artichoke

The Artichoke of Attack

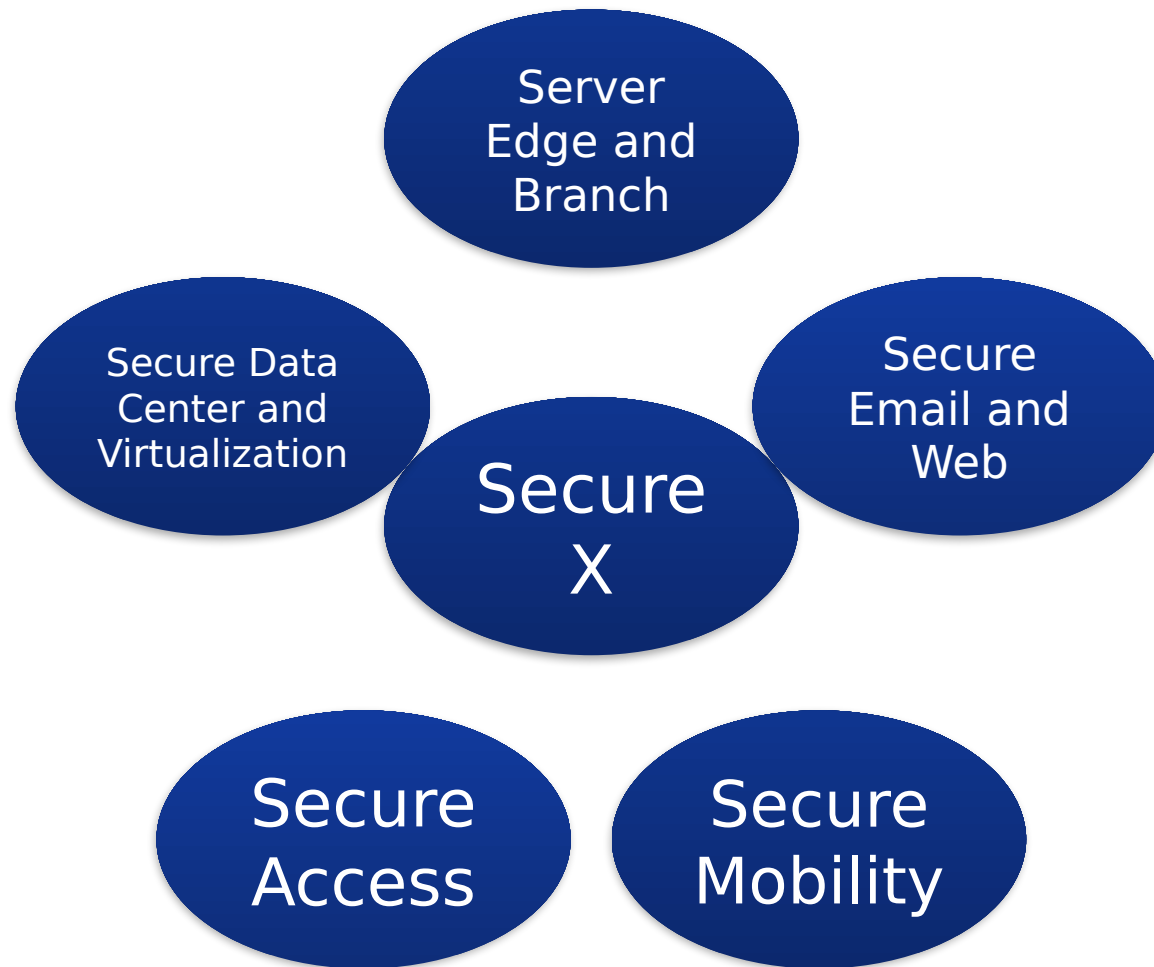
Modern hackers chip away at the hard-core exterior along the perimeter of the network to get to the heart of the enterprise. They remove certain "leaves" to reveal sensitive data that is either unprotected, or secured by weak defenses, such as easy-to-crack passwords and IDs.



Evolution of Network Security Tools



SecureX Product Families



SecureX Security Technology

Cisco SecureX Architecture:

- Scanning engines
- Delivery mechanisms
- Security intelligence operations (SIO)
- Policy management consoles
- Next-generation endpoint

Centralized Context-Aware Network Scanning Element

Defines security policies based on five parameters:

- Type of device being used for access
- Person's identity
- Application in use
- Location
- Time of access



Cisco Security Intelligence Operations



Cisco Security Intelligence Operations (cont.)



Topic 1.3.4: Mitigating Common Network Threats



Defending the Network

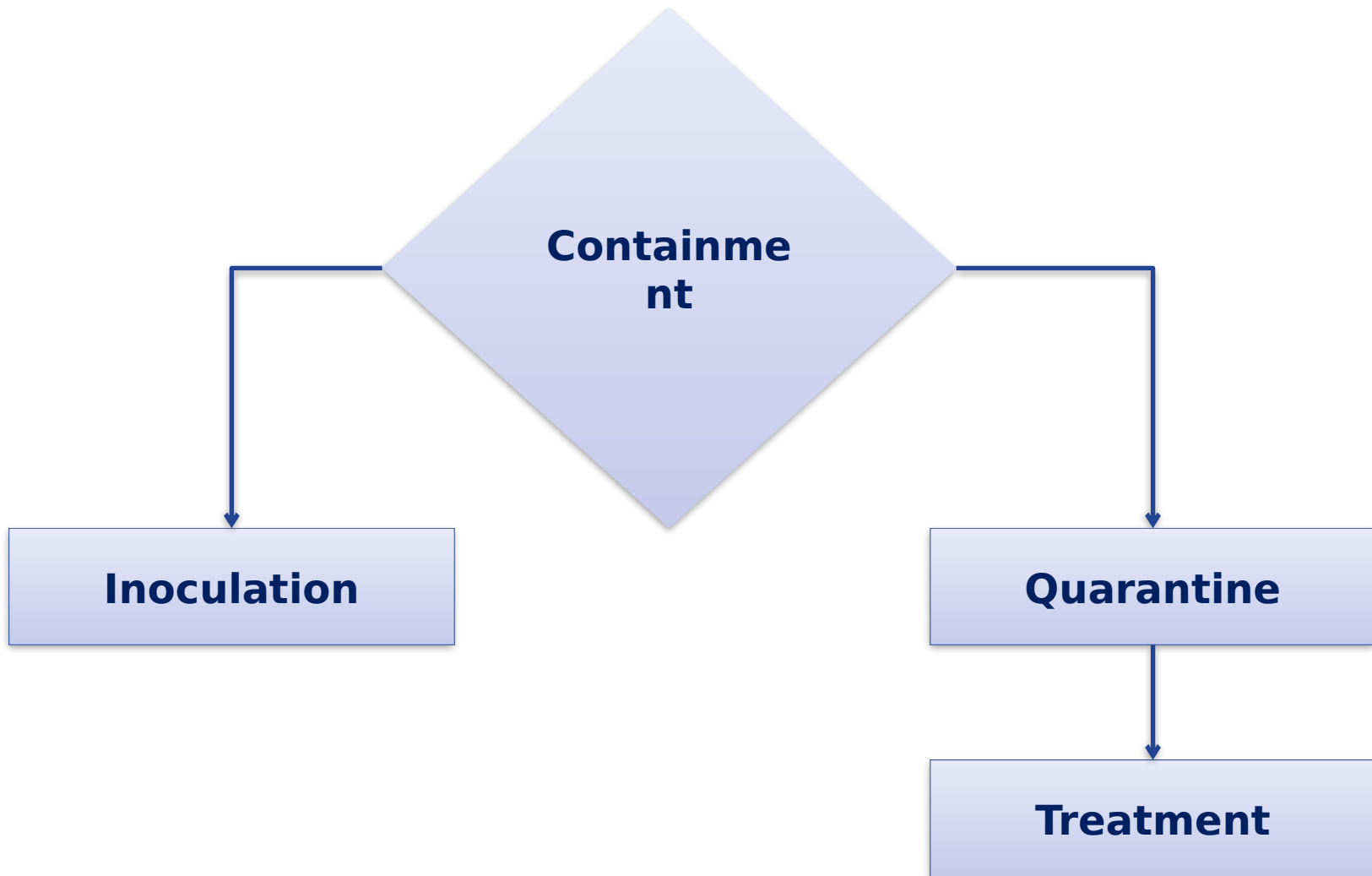
Best practices:

- Develop a written security policy.
- Educate employees about the risks of social engineering, and develop strategies to validate identities over the phone, via email, or in person.
- Control physical access to systems.
- Use strong passwords and change them often.
- Encrypt and password-protect sensitive data.
- Implement security hardware and software.
- Perform backups and test the backed up files on a regular basis.
- Shut down unnecessary services and ports.
- Keep patches up-to-date by installing them weekly or daily to prevent buffer overflow and privilege escalation attacks.
- Perform security audits to test the network.

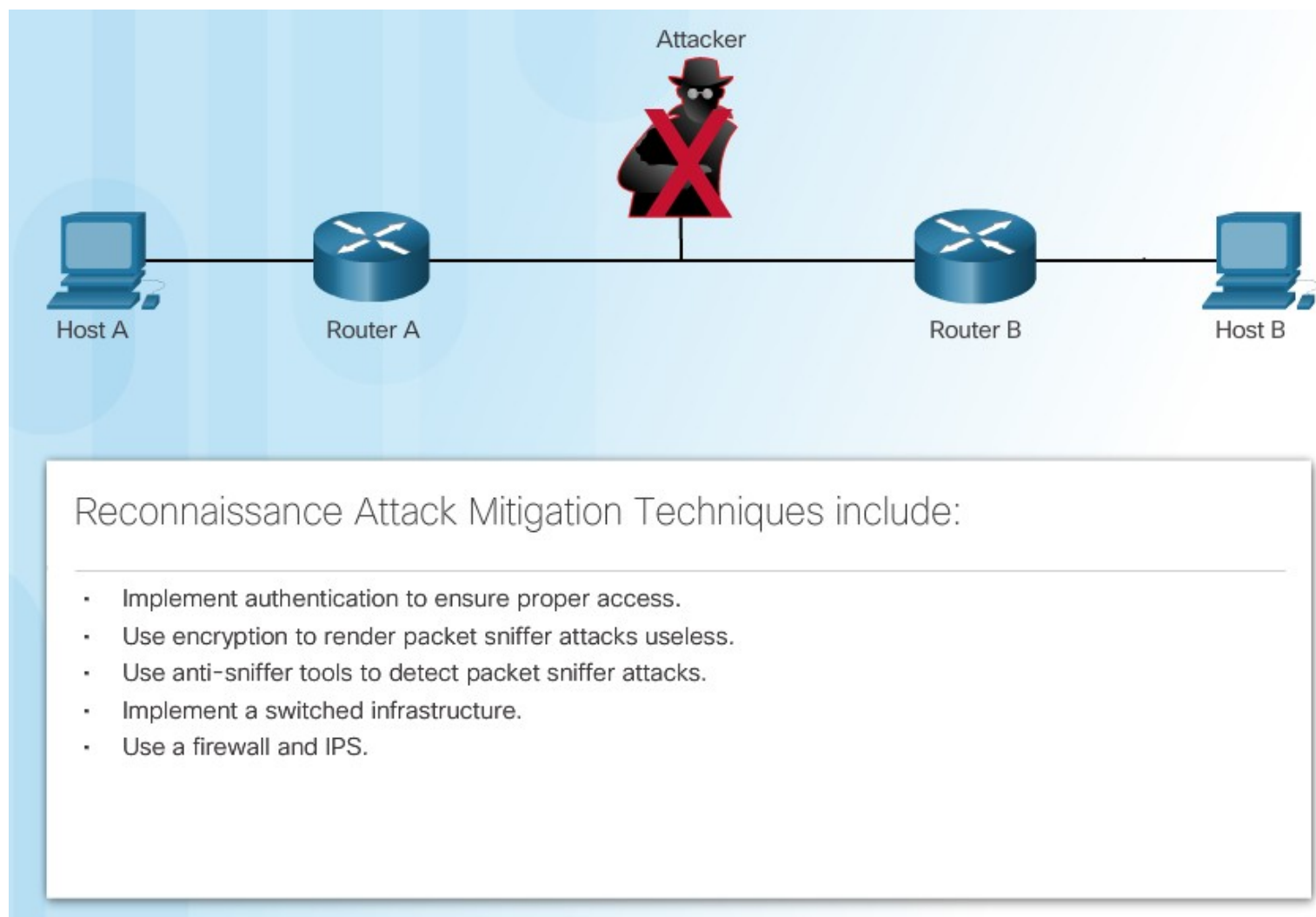
Mitigating Malware



Mitigating Worms



Mitigating Reconnaissance Attacks



Mitigating Access Attacks



THINK

Using a password based on a dictionary word may result in someone abusing your account and misusing our server.

- Strong password security
- Principle of minimum trust
- Cryptography
- Applying operating system and application patches

Mitigating DoS Attacks

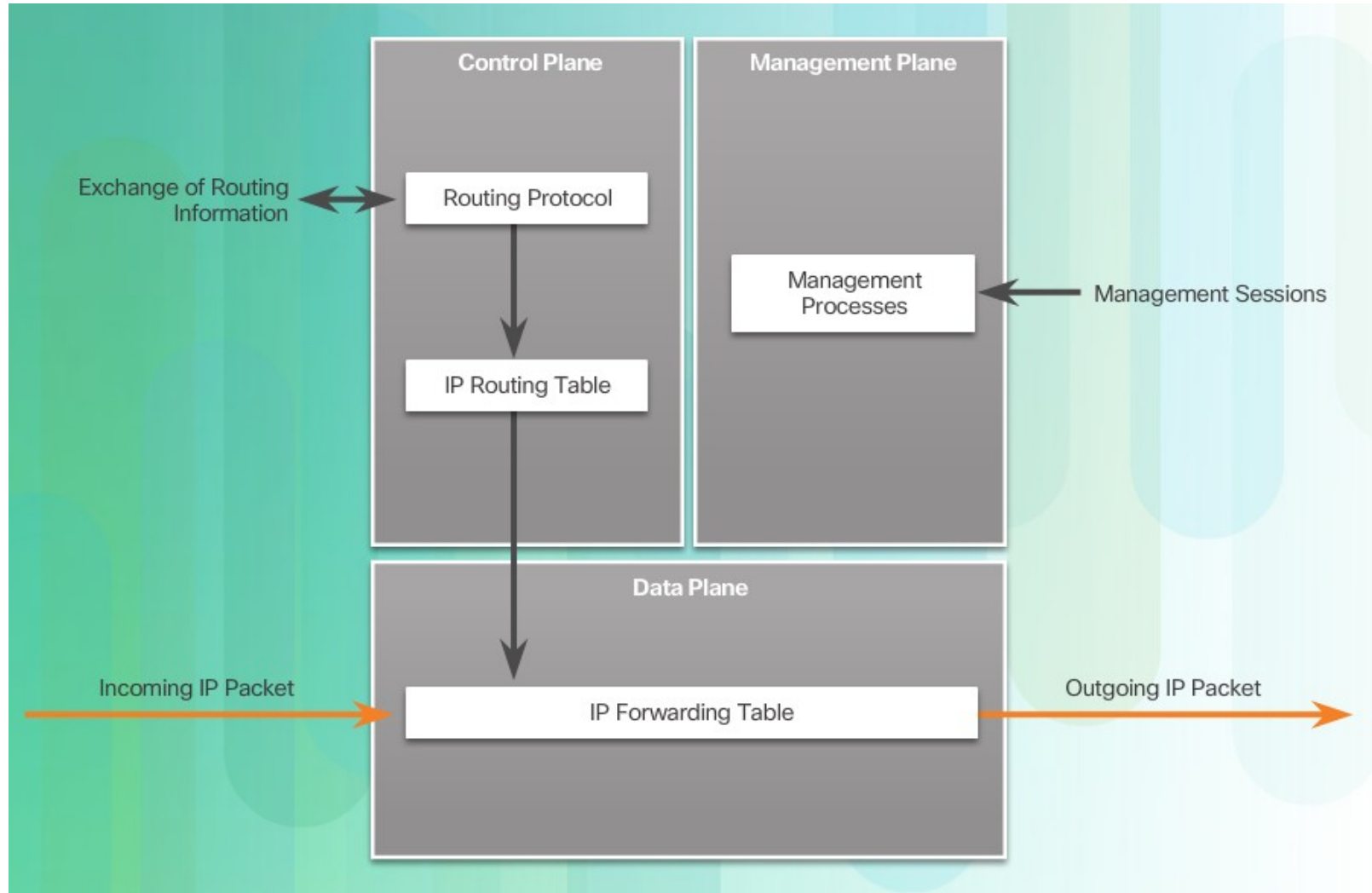


- IPS and firewalls (Cisco ASAs and ISRs)
- Antispoofing technologies
- Quality of Service-traffic policing

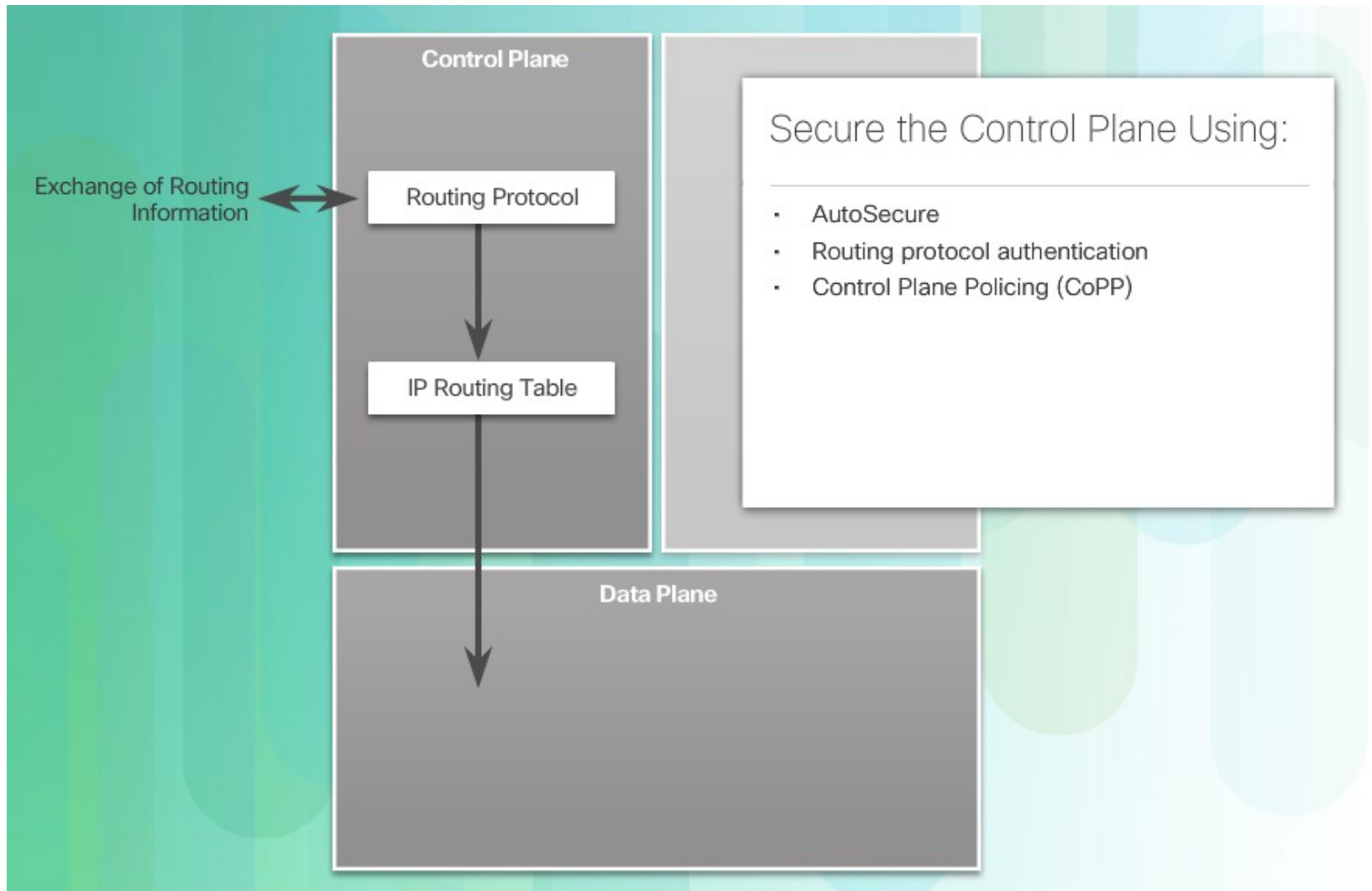
Topic 1.3.5: Cisco Network Foundation Protection Framework



NFP Framework



Securing the Control Plane



Securing the Management Plane

Secure the Management Plane By:

- Enabling login and password policy
- Presenting legal notification
- Ensuring the confidentiality of data using SSH and HTTPS
- Enabling role-based access control
- Authorizing actions
- Enabling management access reporting

Management Plane

Management
Processes

Management Sessions

Securing the Data Plane



Section 1.4: Summary

Chapter Objectives:

- Explain network security.
- Describe various types of threats and attacks.
- Explain tools and procedures to mitigate the effects of malware and common network attacks.

Thank you.



Cisco Networking Academy
Mind Wide Open

Instructor Resources

- **Remember**, there are helpful tutorials and user guides available via your NetSpace home page. (<https://www.netacad.com>)
- These resources cover a variety of topics including navigation, assessments, and assignments.
- A screenshot has been provided here highlighting the tutorials related to activating exams, managing assessments, and creating quizzes.

