Network Security Scope and Sequence

Last updated March 22, 2021

Introduction

Today's organizations are challenged with responding rapidly to emerging network security threats. Security personnel configure and monitor various network security threat mitigation measures, such as device hardening, intrusion prevention systems, and firewalls, to protect data assets and network systems from attack. The purpose of this course is to provide skills and knowledge in the field of network security.

Target Audience

The Network Security course is designed for Cisco Networking Academy® students who are seeking career-oriented, entry-level network security skills. Target students include individuals enrolled in technology degree programs at institutions of higher education and IT professionals who want to pursue a career in the network security field. Learners in this course are exposed to the foundational knowledge required to respond to network security threats through various threat mitigation measures.

Inclusive Language

We are proud to join the technology community in evolving the language we use. Rethinking the words we use is just one of the ways to reduce barriers of equity and respect. As a matter of policy, Cisco Networking Academy content should be free of offensive or suggestive language, graphics, and scenarios. You may still see industry terms such as “black hat” in the course curriculum. Our team is working to modify these terms as well.

Prerequisites

While there are no set prerequisites for the Network Security course, it is RECOMMENDED that students have the following skills and knowledge:

- PC and internet navigation skills
- Familiarity with Cisco Packet Tracer
- Basic understanding of computer networks (CCNA ITN and SRWE level)

Course Description

The course has many features to help students understand these concepts:

- The course is comprised of twenty-two (22) modules. Each module is comprised of topics.
- Modules emphasize critical thinking, problem solving, collaboration, and the practical application of skills.
- Many modules contain some way to practice and assess understanding, such as a lab or a Packet Tracer activity. These module-level activities provide feedback and are designed to indicate the learner’s mastery of the skills needed for the course. Learners can ensure their level of understanding well before taking a graded quiz or exam.
- Some topics may contain a Check Your Understanding interactive quiz. These topic-level assessments are designed to tell learners if they have a good grasp of the topic content, or if they need to review before continuing. Learners can ensure their level of understanding well before taking a graded quiz or exam. Check Your Understanding quizzes do not affect the learner’s overall grade.
- Rich multimedia content, including activities, videos, and quizzes, addresses a variety of learning styles, helps stimulate learning, and increases knowledge retention.

- Hands-on labs help students develop critical thinking and complex problem-solving skills.
- Innovative assessments provide immediate feedback to support the evaluation of knowledge and acquired skills.
- Technical concepts are explained using language that works well for learners at all levels and embedded interactive activities break up reading of the content and help reinforce understanding.
- The curriculum encourages students to consider additional IT education, but also emphasizes applied skills and hands-on experience.
- Cisco Packet Tracer activities are designed for use with Packet Tracer v8.0 or later.

Course Objectives

Network Security helps students develop the skills needed for entry-level network security career opportunities. It provides a theoretically rich, hands-on introduction to network security, in a logical sequence driven by technologies.

The goals of the Network Security course are as follows:

- Provide an in-depth, theoretical understanding of network security.
- Provide students with the knowledge and skills necessary to design and support network security.
- Provide an experience-oriented course that employs industry-relevant instructional approaches to prepare students for entry-level jobs in the industry.
- Enable students to have significant hands-on interaction with IT equipment to prepare them for exams and career opportunities.

Upon completion of the Network Security course, students will be able to perform the following tasks:

- Explain the various types of threats and attacks.
- Explain the tools and procedures to mitigate the effects of malware and common network attacks.
- Configure command authorization using privilege levels and role-based CLI.
- Implement the secure management and monitoring of network devices.
- Configure AAA to secure a network.
- Implement ACLs to filter traffic and mitigate network attacks on a network.
- Implement Zone-Based Policy Firewall using the CLI.
- Explain how network-based Intrusion Prevention Systems are used to help secure a network.
- Explain endpoint vulnerabilities and protection methods.
- Implement security measures to mitigate Layer 2 attacks.
- Explain how the types of encryption, hashes, and digital signatures work together to provide confidentiality, integrity, and authentication.
- Explain how a public key infrastructure is used to ensure data confidentiality and provide authentication.
- Configure a site-to-site IPsec VPN, with pre-shared key authentication, using the CLI.
- Explain how the ASA operates as an advanced stateful firewall.
- Implement an ASA firewall configuration.
- Implement an ASA firewall configuration using ASDM (optional).
- Test network security.

Lab Equipment Requirements

This course requires no physical equipment other than the student's lab PC. Practice activities for the technical and critical skills needed in this course are delivered using Cisco Packet Tracer.

Baseline Equipment Bundle:

- PCs - minimum system requirements
  - CPU: Intel Pentium 4, 2.53 GHz or equivalent.
  - OS: Microsoft Windows, Linux, or macOS
  - RAM: 8 GB
  - Storage: 20GB of free disk space
  - Display resolution: 1024 x 768
  - Language fonts supporting Unicode encoding (if viewing in languages other than English)
  - Latest video card drivers and operating system updates
- Internet connection for lab and study PCs

Student PC Software:

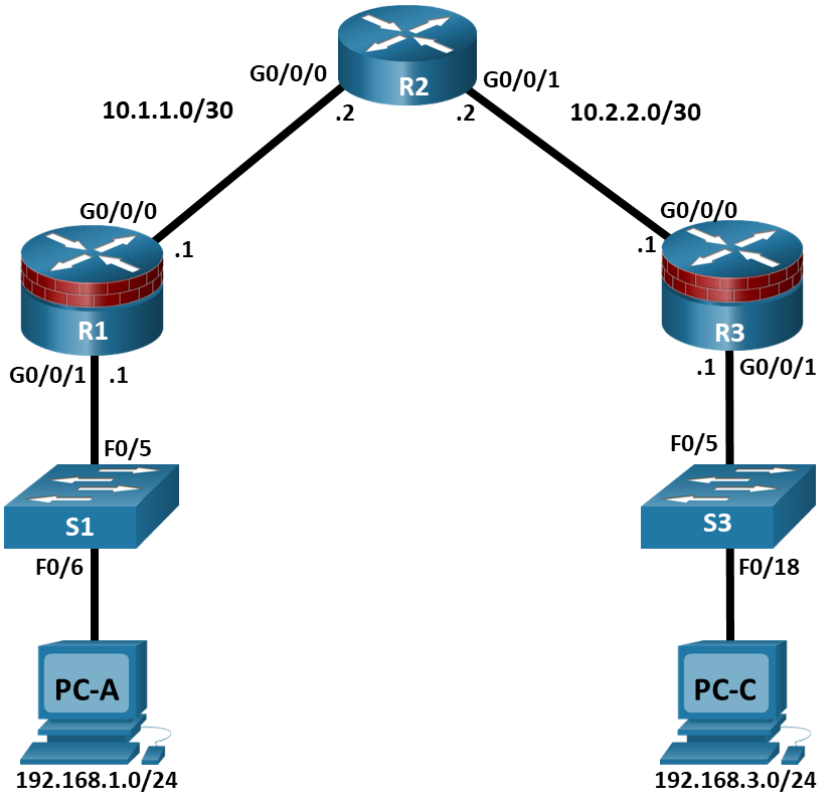
- Cisco Packet Tracer v 8.0 or higher
- Latest stable version of Wireshark
- SSH client software, such as PuTTy or Tera Term, for lab PCs.
- Oracle VirtualBox
- Security Workstation VM
  - Download from the course
  - Requires 1 GB RAM, 15 GB disk space

Lab bundle requirements:

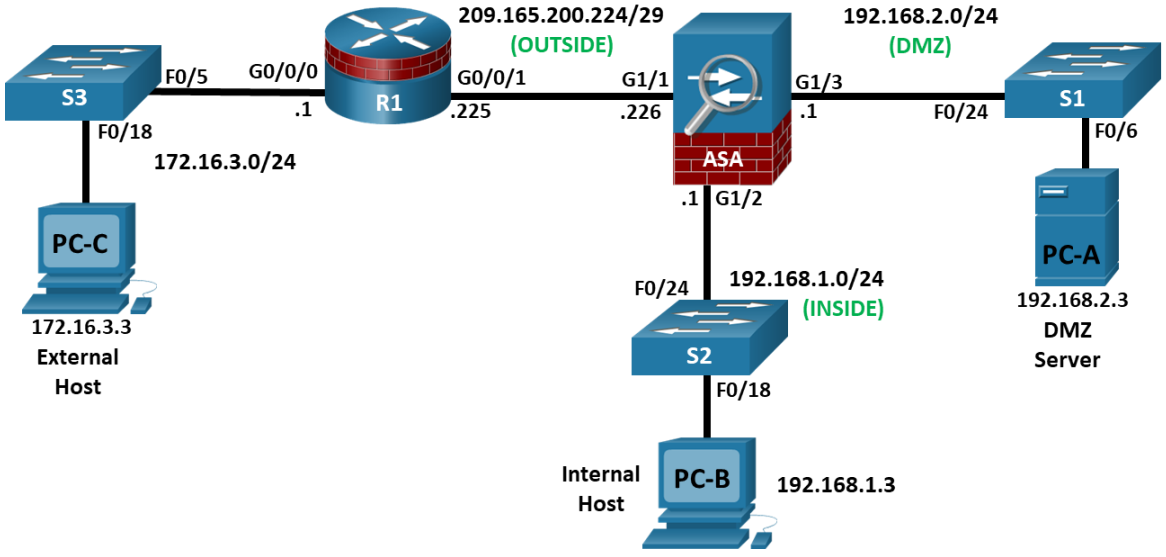
Detailed equipment information, including descriptions and part numbers, is available on Cisco netacad.com on the Equipment Information page. Please refer to that document for the latest information, which includes specifications for the following minimum equipment required:

- 3 Cisco ISR 4221 SEC Bundle with Security License
- 2 Cisco Catalyst 2960 Plus 24 10/100 + 2T/SFP LAN Base
- (Optional) 1 Cisco ASA 5506-X with FirePOWER services, 8GE, AC, 3DES/AES)
- Console cables
- Assorted ethernet cables

Topology



Optional ASA Topology



Network Security Outline

Listed below are the current set of modules and their associated competencies outlined for this course. Each module is an integrated unit of learning that consists of content, activities, and assessments that target a specific set of competencies. The size of the module will depend on the depth of knowledge and skill needed

to master the competency. Some modules are considered foundational, in that the artifacts presented, while not assessed, enable learning of concepts covered on the exam.

Table 1. Network Security Course Outline

Module/Topics	Goals/Objectives
Module 1. Securing Networks	**Explain Network Security.**
1.0 Introduction	A brief introduction to the course and the first module.
1.1 Current State of Affairs	Describe the current network security landscape.
1.2 Network Topology Overview	Describe how all types of networks need to be protected.
1.3 Securing Networks Summary	A brief summary and the module quiz.
Module 2. Network Threats	**Explain the various types of threats and attacks**
2.0 Introduction	An introduction to the module.
2.1 Who is Attacking Our Network?	Explain how network threats have evolved.
2.2 Threat Actor Tools	Describe the various types of attack tools used by Threat Actors.
2.3 Malware	Describe types of malware.
2.4 Common Network Attacks - Reconnaissance, Access, and Social Engineering	Explain reconnaissance, access, and social engineering network attacks.
2.5 Network Attacks - Denial of Service, Buffer Overflows, and Evasion	Explain Denial of Service, buffer overflow, and evasion attacks.
2.6 Network Threats Summary	A brief summary and the module quiz.
Module 3. Mitigating Threats	**Explain tools and procedures to mitigate the effects of malware and common network attacks.**
3.0 Introduction	An introduction to the module.
3.1 Defending the Network	Describe methods and resources to protect the network.
3.2 Network Security Policies	Explain several types of network security policies
3.3 Security Tools, Platforms, and Services	Explain the purpose of security platforms.
3.4 Mitigating Common Network Attacks	Describe the techniques used to mitigate common network attacks.
3.5 Cisco Network Foundation Protection Framework	Explain how to secure the three functional areas of Cisco routers and switches.
3.6 Mitigating Threats Summary	A brief summary and the module quiz.
Module 4. Secure Device Access	**Configure secure administrative access.**
4.0 Introduction	An introduction to the module.
4.1 Secure the Edge Router	Explain how to secure a network perimeter.
4.2 Configure Secure Administrative Access	Use the correct commands to configure passwords on a Cisco IOS device.
4.3 Configure Enhanced Security for Virtual Logins	Use the correct commands to configure enhanced security for virtual logins.
4.4 Configure SSH	Configure an SSH daemon for secure remote management.

Module/Topics	Goals/Objectives
4.5 Secure Device Access Summary	A brief summary and the module quiz.
Module 5. Assign Administrative Roles	**Configure command authorization using privilege levels and role-based CLI.**
5.0 Introduction	An introduction to the module.
5.1 Configure Privilege Levels	Use the correct commands to configure administrative privilege levels to control command availability.
5.2 Configure Role-Based CLI	Use the correct commands to configure role-based CLI access to control command availability.
5.3 Assign Administrative Roles Summary	A brief summary and the module quiz.
Module 6. Device Monitoring and Management	**Implement the secure management and monitoring of network devices.**
6.0 Introduction	An introduction to the module.
6.1 Secure Cisco IOS Image and Configuration Files	Explain how the Cisco IOS resilient configuration feature and Secure Copy are used to secure the Cisco IOS image and configuration files.
6.2 Lock Down a Router Using AutoSecure	Use the correct commands for AutoSecure to enable security on IOS-based routers.
6.3 Routing Protocol Authentication	Use the correct commands to configure routing protocol authentication.
6.4 Secure Management and Reporting	Compare in-band and out-of-band management access.
6.5 Network Security Using Syslog	Explain how to configure syslog to log system events.
6.6 NTP Configuration	Configure NTP to enable accurate timestamping between all devices.
6.7 SNMP Configuration	Configure SNMP to monitor system status.
6.8 Device Monitoring and Management Summary	A brief summary and the module quiz.
Module 7. Authentication, Authorization and Accounting (AAA)	**Configure AAA to secure a network.**
7.0 Introduction	An introduction to the module.
7.1 AAA Characteristics	Describe AAA.
7.2 Configure Local AAA Authentication	Configure AAA authentication to validate users against a local database.
7.3 Server-Based AAA Characteristics and Protocols	Describe the server-based AAA protocols.
7.4 Configure Server-Based Authentication	Configure server-based AAA authentication on Cisco routers.
7.5 Configure Server-Based Authorization and Accounting	Use the correct commands to configure server-based AAA authorization and accounting.
7.6 Authentication, Authorization and Accounting (AAA) Summary	A brief summary and the module quiz.
Module 8. Access Control Lists	**Implement access control lists (ACLs) to filter traffic and mitigate network attacks on a network.**
8.0 Introduction	An introduction to the module.

Module/Topics	Goals/Objectives
8.1 Introduction to Access Control Lists	Describe standard and extended IPv4 ACLs.
8.2 Wildcard Masking	Explain how ACLs use wildcard masks
8.3 Configure ACLs	Explain how to configure ACLs.
8.4 Modify ACLs	Use sequence numbers to edit existing standard IPv4 ACLs
8.5 Implement ACLs	Implement ACLs.
8.6 Mitigate Attacks with ACLs	Use ACLs to mitigate common network attacks.
8.7 IPv6 ACLs	Configure IPv6 ACLs using CLI.
8.8 Access Control Lists Summary	A brief summary and the module quiz.
Module 9: Firewall Technologies	**Explain how firewalls are implemented to provide network security.**
9.0 Introduction	An introduction to the module.
9.1 Secure Networks with Firewalls	Explain how firewalls are used to help secure networks.
9.2 Firewalls in Network Design	Explain design considerations for implementing firewall technologies
9.3 Firewall Technologies Summary	A brief summary and the module quiz.
Module 10: Zone-Based Policy Firewalls	**Implement Zone-Based Policy Firewall using CLI.**
10.0 Introduction	An introduction to the module.
10.1 ZPF Overview	Explain how Zone-Based Policy Firewalls are used to help secure a network.
10.2 ZPF Operation	Explain the operation of a Zone-Based Policy Firewall.
10.3 Configure a ZPF	Configure a Zone-Based Policy Firewall with CLI.
10.4 Zone-Based Policy Firewalls Summary	A brief summary and the module quiz.
Module 11: IPS Technologies	**Explain how network-based Intrusion Prevention Systems are used to help secure a network.**
11.0 Introduction	An introduction to the module.
11.1 IDS and IPS Characteristics	Explain the functions and operations of IDS and IPS systems.
11.2 IPS Implementations	Explain how network-based IPS are implemented.
11.3 IPS on Cisco ISRs	Describe the IPS technologies that are available on Cisco ISR routers.
11.4 Cisco Switched Port Analyzer	Configure Cisco SPAN.
11.5 IPS Technologies Summary	A brief summary and the module quiz.
Module 12: IPS Operation and Implementation	**Explain how signatures are used to detect malicious network traffic.**
12.0 Introduction	An introduction to the module.
12.1 IPS Signatures	Describe IPS signatures.
12.2 Cisco Snort IPS	Explain how the Cisco Snort IPS provides network security services.
12.3 Configure Snort IPS	Explain how to configure Snort IPS on a Cisco ISR G2.

Module/Topics	Goals/Objectives
12.4 IPS Operation and Implementation Summary	A brief summary and the module quiz.
Module 13: Endpoint Security	**Explain endpoint vulnerabilities and protection methods.**
13.0 Introduction	An introduction to the module.
13.1 Endpoint Security Overview	Describe endpoint security and the enabling technologies.
13.2 802.1X Authentication	Explain the functions of 802.1x components.
13.3 Endpoint Security Summary	A brief summary and the module quiz.
Module 14: Layer 2 Security Considerations	**Implement security measures to mitigate Layer 2 attacks.**
14.0 Introduction	An introduction to the module.
14.1 Layer 2 Security Threats	Describe Layer 2 vulnerabilities.
14.2 MAC Table Attacks	Describe MAC address spoofing attacks.
14.3 Mitigate MAC Table Attacks	Configure port security.
14.4 Mitigate VLAN Attacks	Explain how to mitigate VLAN attacks.
14.5 Mitigate DHCP Attacks	Use the correct command to implement DHCP Snooping for attack mitigation.
14.6 Mitigate ARP Attacks	Use the correct command to mitigate ARP attacks.
14.7 Mitigate Address Spoofing Attacks	Use the correct command to mitigate address spoofing attacks.
14.8 Spanning Tree Protocol	Explain the operation of Spanning Tree Protocol.
14.9 Mitigate STP Attacks	Configure security measures to mitigate STP attacks.
14.10 Layer 2 Security Considerations Summary	A brief summary and the module quiz.
15 Cryptographic Services	**Explain how the types of encryption, hashes, and digital signatures work together to provide confidentiality, integrity, and authentication.**
15.0 Introduction	An introduction to the module.
15.1 Secure Communications	Explain the requirements of secure communications including integrity, authentication, and confidentiality.
15.2 Cryptography	Describe cryptography.
15.3 Cryptanalysis	Describe cryptanalysis.
15.4 Cryptology	Describe cryptology.
15.5 Cryptographic Services Summary	A brief summary and the module quiz.
Module 16: Basic Integrity and Authenticity	**Explain how cryptography is used to ensure data integrity and authentication.**
16.0 Introduction	An introduction to the module.
16.1 Integrity and Authenticity	Explain the role of cryptography in ensuring the integrity and authenticity of data.
16.2 Key Management	Describe the components of key management.

Module/Topics	Goals/Objectives
16.3 Confidentiality	Explain how cryptographic approaches enhance data confidentiality.
16.4 Basic Integrity and Authenticity Summary	A brief summary and the module quiz.
Module 17: Public Key Cryptography	**Explain how a public key infrastructure is used to ensure data confidentiality and provide authentication.**
17.0 Introduction	An introduction to the module.
17.1 Public Key Cryptography with Digital Signatures	Explain public key cryptography.
17.2 Authorities and the PKI Trust System	Explain how the public key infrastructure functions.
17.3 Applications and Impacts of Cryptography	Explain how the use of cryptography affects cybersecurity operations.
17.4 Public Key Cryptography Summary	A brief summary and the module quiz.
Module 18: VPNs	**Explain the purpose of VPNs.**
18.0 Introduction	An introduction to the module.
18.1 VPN Overview	Describe VPNs and their benefits.
18.2 VPN Topologies	Compare remote-access and site-to-site VPNs.
18.3 IPsec Overview	Describe the IPsec protocol and its basic functions.
18.4 IPsec Protocols	Compare AH and ESP protocols.
18.5 Internet Key Exchange	Describe the IKE protocol.
18.6 VPNs Summary	A brief summary and the module quiz.
Module 19: Implement Site-to-Site IPsec VPNs with CLI	**Configure a site-to-site IPsec VPN, with pre-shared key authentication, using CLI.**
19.0 Introduction	An introduction to the module.
19.1 Configure a Site-to-Site IPsec VPN	Describe IPsec negotiation and the five steps of IPsec configuration.
19.2 ISAKMP Policy	Use the correct commands to configure an ISAKMP policy.
19.3 IPsec Policy	Use the correct commands to configure the IPsec policy.
19.4 Crypto Map	Use the correct command to configure and apply a Cryptomap.
19.5 IPsec VPN	Configure the IPsec VPN.
19.6 Implement Site-to-Site IPsec VPNs with CLI Summary	A brief summary and the module quiz.
Module 20: Introduction to the ASA	**Explain how the ASA operates as an advanced stateful firewall.**
20.0 Introduction	An introduction to the module.
20.1 ASA Solutions	Compare ASA solutions to other routing firewall technologies.
20.2 The ASA 5506-X with FirePOWER Services	Describe three ASA deployment scenarios.
20.3 Introduction to the ASA Summary	A brief summary and the module quiz.

Module/Topics	Goals/Objectives
Module 21: ASA Firewall Configuration	**Implement an ASA firewall configuration.**
21.0 Introduction	An introduction to the module.
21.1 Basic ASA Firewall Configuration	Explain how to configure an ASA-5506-X with FirePOWER Services.
21.2 Configure Management Settings and Services	Configure management settings and services on a ASA5506-X firewall.
21.3 Object Groups	Explain how to configure object groups on an ASA.
21.4 ASA ACLs	Use the correct commands to configure access lists with object groups on an ASA.
21.5 NAT Services on an ASA	Use the correct commands to configure an ASA to provide NAT services.
21.6 AAA	Use correct command to configure access control using the local database and AAA server.
21.7 Service Policies on an ASA	Configure service policies on an ASA
21.8 ASA Firewall Configuration Summary	A brief summary and the module quiz.
21.9 Introduction to ASDM (Optional)	
Module 22: Network Security Testing	**Describe the various techniques and tools used for network security testing.**
22.0 Introduction	An introduction to the module.
22.1 Network Security Testing Techniques	Describe the techniques used in network security testing.
22.2 Network Security Testing Tools	Describe the tools used in network security testing
22.3 Network Security Testing Summary	A brief summary and a module quiz.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**