CCNP Security

Introduction

Software and networking become more and more interconnected every day, creating an ever greater need for robust, scalable security across all platforms—from networks to mobile devices. With intent-based networking, security teams can take advantage of automation to scale their security solutions. To capitalize on these opportunities, today's security professionals need a broader range of skills and a deeper focus in strategic technology areas. The CCNP Security certification program gives you exactly that breadth and depth.

CCNP Security certification helps you prove your skills in the ever-changing landscape of security technologies. The certification covers core technologies and a security focus area of your choice. You choose where you want to focus. You choose where to take your career.

Required Exam

350-701 SCOR: Implementing and Operating Cisco Security Core Technologies

The Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0 course helps you prepare for the Cisco® CCNP® Security and CCIE® Security certifications and for senior-level security roles. In this course, you will master the skills and technologies you need to implement core Cisco security solutions to provide advanced threat protection against cybersecurity attacks. You will learn security for networks, cloud and content, endpoint protection, secure network access, visibility, and enforcement. You will get extensive hands-on experience deploying Cisco Firepower® Next-Generation Firewall and Cisco Adaptive Security Appliance (ASA) Firewall; configuring access control policies, mail policies, and 802.1X Authentication; and more. You will get introductory practice on Cisco Stealthwatch® Enterprise and Cisco Stealthwatch Cloud threat detection features.

This course, including the self-paced material, helps prepare you to take the exam, Implementing and Operating Cisco Security Core Technologies (350-701 SCOR), which leads to the new CCNP Security, CCIE Security, and the Cisco Certified Specialist - Security Core certifications.

Duration

5 Days

Course Objectives

- Describe information security concepts and strategies within the network
- Describe common TCP/IP, network application, and endpoint attacks
- Describe how various network security technologies work together to guard against attacks
- Implement access control on Cisco ASA appliance and Cisco Firepower Next-Generation Firewall
- Describe and implement basic email content security features and functions provided by Cisco Email Security Appliance
- Describe and implement web content security features and functions provided by Cisco Web Security Appliance
- Describe Cisco Umbrella® security capabilities, deployment models, policy management, and Investigate console
- Introduce VPNs and describe cryptography solutions and algorithms
- Describe Cisco secure site-to-site connectivity solutions and explain how to deploy Cisco Internetwork Operating System (Cisco IOS®) Virtual Tunnel Interface (VTI)-based point-to-point IPsec VPNs, and

point-to-point IPsec VPN on the Cisco ASA and Cisco Firepower Next-Generation Firewall (NGFW)
- Describe and deploy Cisco secure remote access connectivity solutions and describe how to configure 802.1X and Extensible Authentication Protocol (EAP) authentication
- Provide a basic understanding of endpoint security and describe Advanced Malware Protection (AMP) for Endpoints architecture and basic features
- Examine various defenses on Cisco devices that protect the control and management plane
- Configure and verify Cisco IOS software Layer 2 and Layer 3 data plane controls
- Describe Cisco Stealthwatch Enterprise and Stealthwatch Cloud solutions
- Describe basics of cloud computing and common cloud attacks and how to secure cloud environment

Prerequisites

- Skills and knowledge equivalent to those learned in Implementing and Administering Cisco Solutions (CCNA®) v1.0 course
- Familiarity with Ethernet and TCP/IP networking
- Working knowledge of the Windows operating system
- Working knowledge of Cisco IOS networking and concepts
- Familiarity with basics of networking security concepts

Target Audience

- Cisco integrators and partners
- Consulting systems engineer
- Network administrator
- Network designer
- Network engineer
- Network manager
- Security engineer
- Systems engineer
- Technical solutions architect

Course Outline

- Describing Information Security Concepts*
    - Information Security Overview
    - Assets, Vulnerabilities, and Countermeasures
    - Managing Risk
- Describing Common TCP/IP Attacks*
    - Legacy TCP/IP Vulnerabilities
    - IP Vulnerabilities
    - Internet Control Message Protocol (ICMP) Vulnerabilities
- Describing Common Network Application Attacks*
    - Password Attacks
    - Domain Name System (DNS)-Based Attacks
    - DNS Tunneling
- Describing Common Endpoint Attacks*
    - Buffer Overflow
    - Malware
    - Reconnaissance Attack
- Describing Network Security Technologies
    - Defense-in-Depth Strategy
    - Defending Across the Attack Continuum
    - Network Segmentation and Virtualization Overview
- Deploying Cisco ASA Firewall

    - Cisco ASA Deployment Types
    - Cisco ASA Interface Security Levels
    - Cisco ASA Objects and Object Groups
- Deploying Cisco Firepower Next-Generation Firewall
    - Cisco Firepower NGFW Deployments
    - Cisco Firepower NGFW Packet Processing and Policies
    - Cisco Firepower NGFW Objects
- Deploying Email Content Security
    - Cisco Email Content Security Overview
    - Simple Mail Transfer Protocol (SMTP) Overview
    - Email Pipeline Overview
- Deploying Web Content Security
    - Cisco Web Security Appliance (WSA) Overview
    - Deployment Options
    - Network Users Authentication
- Deploying Cisco Umbrella*
    - Cisco Umbrella Architecture
    - Deploying Cisco Umbrella
    - Cisco Umbrella Roaming Client
- Explaining VPN Technologies and Cryptography
    - VPN Definition
    - VPN Types
    - Secure Communication and Cryptographic Services
- Introducing Cisco Secure Site-to-Site VPN Solutions
    - Site-to-Site VPN Topologies
    - IPsec VPN Overview
    - IPsec Static Crypto Maps
- Deploying Cisco IOS VTI-Based Point-to-Point IPsec VPNs
    - Cisco IOS VTIs
    - Static VTI Point-to-Point IPsec Internet Key Exchange (IKE) v2 VPN Configuration
- Deploying Point-to-Point IPsec VPNs on the Cisco ASA and Cisco Firepower NGFW
    - Point-to-Point VPNs on the Cisco ASA and Cisco Firepower NGFW
    - Cisco ASA Point-to-Point VPN Configuration
    - Cisco Firepower NGFW Point-to-Point VPN Configuration
- Introducing Cisco Secure Remote Access VPN Solutions
    - Remote Access VPN Components
    - Remote Access VPN Technologies
    - Secure Sockets Layer (SSL) Overview
- Deploying Remote Access SSL VPNs on the Cisco ASA and Cisco Firepower NGFW
    - Remote Access Configuration Concepts
    - Connection Profiles
    - Group Policies
- Explaining Cisco Secure Network Access Solutions
    - Cisco Secure Network Access
    - Cisco Secure Network Access Components
    - AAA Role in Cisco Secure Network Access Solution
- Describing 802.1X Authentication
    - 802.1X and Extensible Authentication Protocol (EAP)
    - EAP Methods
    - Role of Remote Authentication Dial-in User Service (RADIUS) in 802.1X Communications
- Configuring 802.1X Authentication
    - Cisco Catalyst® Switch 802.1X Configuration
    - Cisco Wireless LAN Controller (WLC) 802.1X Configuration
    - Cisco Identity Services Engine (ISE) 802.1X Configuration
- Describing Endpoint Security Technologies*
    - Host-Based Personal Firewall
    - Host-Based Anti-Virus
    - Host-Based Intrusion Prevention System

- Deploying Cisco Advanced Malware Protection (AMP) for Endpoints*
    - Cisco AMP for Endpoints Architecture
    - Cisco AMP for Endpoints Engines
    - Retrospective Security with Cisco AMP
- Introducing Network Infrastructure Protection*
    - Identifying Network Device Planes
    - Control Plane Security Controls
    - Management Plane Security Controls
- Deploying Control Plane Security Controls*
    - Infrastructure ACLs
    - Control Plane Policing
    - Control Plane Protection
- Deploying Layer 2 Data Plane Security Controls*
    - Overview of Layer 2 Data Plane Security Controls
    - Virtual LAN (VLAN)-Based Attacks Mitigation
    - Spanning Tree Protocol (STP) Attacks Mitigation
- Deploying Layer 3 Data Plane Security Controls*
    - Infrastructure Antispoofing ACLs
    - Unicast Reverse Path Forwarding
    - IP Source Guard
- Deploying Management Plane Security Controls*
    - Cisco Secure Management Access
    - Simple Network Management Protocol Version 3
    - Secure Access to Cisco Devices
- Deploying Traffic Telemetry Methods*
    - Network Time Protocol
    - Device and Network Events Logging and Export
    - Network Traffic Monitoring Using NetFlow
- Deploying Cisco Stealthwatch Enterprise*
    - Cisco Stealthwatch Offerings Overview
    - Cisco Stealthwatch Enterprise Required Components
    - Flow Stitching and Deduplication
- Describing Cloud and Common Cloud Attacks*
    - Evolution of Cloud Computing
    - Cloud Service Models
    - Security Responsibilities in Cloud
- Securing the Cloud*
    - Cisco Threat-Centric Approach to Network Security
    - Cloud Physical Environment Security
    - Application and Workload Security
- Deploying Cisco Stealthwatch Cloud*
    - Cisco Stealthwatch Cloud for Public Cloud Monitoring
    - Cisco Stealthwatch Cloud for Private Network Monitoring
    - Cisco Stealthwatch Cloud Operations
- Describing Software-Defined Networking (SDN*)
    - Software-Defined Networking Concepts
    - Network Programmability and Automation
    - Cisco Platforms and APIs

Lab Outline

- Configure Network Settings and NAT on Cisco ASA
- Configure Cisco ASA Access Control Policies
- Configure Cisco Firepower NGFW NAT
- Configure Cisco Firepower NGFW Access Control Policy
- Configure Cisco Firepower NGFW Discovery and IPS Policy
- Configure Cisco NGFW Malware and File Policy

- Configure Listener, Host Access Table (HAT), and Recipient Access Table (RAT) on Cisco Email Security Appliance (ESA)
- Configure Mail Policies
- Configure Proxy Services, Authentication, and HTTPS Decryption
- Enforce Acceptable Use Control and Malware Protection
- Examine the Umbrella Dashboard
- Examine Cisco Umbrella Investigate
- Explore DNS Ransomware Protection by Cisco Umbrella
- Configure Static VTI Point-to-Point IPsec IKEv2 Tunnel
- Configure Point-to-Point VPN between the Cisco ASA and Cisco Firepower NGFW
- Configure Remote Access VPN on the Cisco Firepower NGFW
- Explore Cisco AMP for Endpoints
- Perform Endpoint Analysis Using AMP for Endpoints Console
- Explore File Ransomware Protection by Cisco AMP for Endpoints Console
- Explore Cisco Stealthwatch Enterprise v6.9.3
- Explore Cognitive Threat Analytics (CTA) in Stealthwatch Enterprise v7.0
- Explore the Cisco Cloudlock Dashboard and User Security
- Explore Cisco Cloudlock Application and Data Security
- Explore Cisco Stealthwatch Cloud
- Explore Stealthwatch Cloud Alert Settings, Watchlists, and Sensors

Concentration Exams (Choose One)

1. 300-710 SNCF: Securing Networks with Cisco Firepower

A. Securing Networks with Cisco Firepower Next-Generation Firewall (SSNGFW)

The Securing Networks with Cisco Firepower Next-Generation Firewall (SSNGFW) v1.0 course shows you how to deploy and use the Cisco Firepower® Threat Defense system. This hands-on course gives you knowledge and skills to use and configure Cisco® Firepower Threat Defense technology, beginning with initial device setup and configuration and including routing, high availability, Cisco Adaptive Security Appliance (ASA) to Cisco Firepower Threat Defense migration, traffic control, and Network Address Translation (NAT). You will learn how to implement advanced Next-Generation Firewall (NGFW) and Next-Generation Intrusion Prevention System (NGIPS) features, including network intelligence, file type detection, network-based malware detection, and deep packet inspection. You will also learn how to configure site-to-site VPN, remote-access VPN, and SSL decryption before moving on to detailed analysis, system administration, and troubleshooting.

This course helps you prepare to take the exam, Securing Networks with Cisco Firepower (300-710 SNCF), which leads to CCNP Security and Cisco Certified Specialist – Network Security Firepower certifications. The 300-710 SNCF exam has a second preparation course as well, Securing Networks with Cisco Firepower Next-Generation Intrusion Prevention System (SSFIPS).

Duration

5 Days

Course Objectives

- Describe key concepts of NGIPS and NGFW technology and the Cisco Firepower Threat Defense system, and identify deployment scenarios
- Perform initial Cisco Firepower Threat Defense device configuration and setup tasks
- Describe how to manage traffic and implement Quality of Service (QoS) using Cisco Firepower Threat

Defense
- Describe how to implement NAT by using Cisco Firepower Threat Defense
- Perform an initial network discovery, using Cisco Firepower to identify hosts, applications, and services
- Describe the behavior, usage, and implementation procedure for access control policies
- Describe the concepts and procedures for implementing security intelligence features
- Describe Cisco Advanced Malware Protection (AMP) for Networks and the procedures for implementing file control and advanced malware protection
- Implement and manage intrusion policies
- Describe the components and configuration of site-to-site VPN
- Describe and configure a remote-access SSL VPN that uses Cisco AnyConnect®
- Describe SSL decryption capabilities and usage

Prerequisites

To fully benefit from this course, you should have:

- Knowledge of TCP/IP and basic routing protocols
- Familiarity with firewall, VPN, and Intrusion Prevention System (IPS) concepts

Target Audience

- Security administrators
- Security consultants
- Network administrators
- System engineers
- Technical support personnel
- Cisco integrators and partners

Course Outline

- Cisco Firepower Threat Defense Overview
    - Examining Firewall and IPS Technology
    - Firepower Threat Defense Features and Components
    - Examining Firepower Platforms
    - Examining Firepower Threat Defense Licensing
    - Cisco Firepower Implementation Use Cases
- Cisco Firepower NGFW Device Configuration
    - Firepower Threat Defense Device Registration
    - FXOS and Firepower Device Manager
    - Initial Device Setup
    - Managing NGFW Devices
    - Examining Firepower Management Center Policies
    - Examining Objects
    - Examining System Configuration and Health Monitoring
    - Device Management
    - Examining Firepower High Availability
    - Configuring High Availability
    - Cisco ASA to Firepower Migration
    - Migrating from Cisco ASA to Firepower Threat Defense
- Cisco Firepower NGFW Traffic Control
    - Firepower Threat Defense Packet Processing
    - Implementing QoS
    - Bypassing Traffic
- Cisco Firepower NGFW Address Translation

    - NAT Basics
    - Implementing NAT
    - NAT Rule Examples
    - Implementing NAT
- Cisco Firepower Discovery
    - Examining Network Discovery
    - Configuring Network Discovery
- Implementing Access Control Policies
    - Examining Access Control Policies
    - Examining Access Control Policy Rules and Default Action
    - Implementing Further Inspection
    - Examining Connection Events
    - Access Control Policy Advanced Settings
    - Access Control Policy Considerations
    - Implementing an Access Control Policy
- Security Intelligence
    - Examining Security Intelligence
    - Examining Security Intelligence Objects
    - Security Intelligence Deployment and Logging
    - Implementing Security Intelligence
- File Control and Advanced Malware Protection
    - Examining Malware and File Policy
    - Examining Advanced Malware Protection
- Next-Generation Intrusion Prevention Systems
    - Examining Intrusion Prevention and Snort Rules
    - Examining Variables and Variable Sets
    - Examining Intrusion Policies
- Site-to-Site VPN
    - Examining IPsec
    - Site-to-Site VPN Configuration
    - Site-to-Site VPN Troubleshooting
    - Implementing Site-to-Site VPN
- Remote-Access VPN
    - Examining Remote-Access VPN
    - Examining Public-Key Cryptography and Certificates
    - Examining Certificate Enrollment
    - Remote-Access VPN Configuration
    - Implementing Remote-Access VPN
- SSL Decryption
    - Examining SSL Decryption
    - Configuring SSL Policies
    - SSL Decryption Best Practices and Monitoring
- Detailed Analysis Techniques
    - Examining Event Analysis
    - Examining Event Types
    - Examining Contextual Data
    - Examining Analysis Tools
    - Threat Analysis
- System Administration
    - Managing Updates
    - Examining User Account Management Features
    - Configuring User Accounts
    - System Administration
- Cisco Firepower Troubleshooting
    - Examining Common Misconfigurations
    - Examining Troubleshooting Commands
    - Firepower Troubleshooting

Lab Outline

- Initial Device Setup
- Device Management
- Configuring High Availability
- Migrating from Cisco ASA to Cisco Firepower Threat Defense
- Implementing QoS
- Implementing NAT
- Configuring Network Discovery
- Implementing an Access Control Policy
- Implementing Security Intelligence
- Implementing Site-to-Site VPN
- Implementing Remote Access VPN
- Threat Analysis
- System Administration
- Firepower Troubleshooting

B. Securing Networks with Cisco Firepower Next-Generation IPS (SSFIPS)

The Securing Networks with Cisco Firepower Next-Generation IPS (SSFIPS) v4.0 course shows you how to deploy and use Cisco Firepower® Next-Generation Intrusion Prevention System (NGIPS). This hands-on course gives you the knowledge and skills to use the platform features and includes firewall security concepts, platform architecture and key features; in-depth event analysis including detection of network-based malware and file type, NGIPS tuning and configuration including application control, security intelligence, firewall, and network-based malware and file controls; Snort® rules language; file and malware inspection, security intelligence, and network analysis policy configuration designed to detect traffic patterns; configuration and deployment of correlation policies to take action based on events detected; troubleshooting; system and user administration tasks, and more.

This course helps you prepare to take the exam, Securing Networks with Cisco Firepower (300-710 SNCF), which leads to CCNP Security and Cisco Certified Specialist – Network Security Firepower certifications. The 300-710 SNCF exam has a second preparation course as well, Securing Networks with Cisco Firepower Next Generation Firewall (SSNGFW).

Duration

5 Days

Course Objectives

- Describe the components of Cisco Firepower Threat Defense and the managed device registration process
- Detail Next-Generation Firewalls (NGFW) traffic control and configure the Cisco Firepower system for network discovery
- Implement access control policies and describe access control policy advanced features
- Configure security intelligences features and the Advanced Malware Protection (AMP) for Networks implementation procedure for file control and advanced malware protection
- Implement and manage intrusion and network analysis policies for NGIPS inspection
- Describe and demonstrate the detailed analysis techniques and reporting features provided by the Cisco Firepower Management Center
- Integrate the Cisco Firepower Management Center with an external logging destination
- Describe and demonstrate the external alerting options available to Cisco Firepower Management Center and configure a correlation policy
- Describe key Cisco Firepower Management Center software update and user account management

features
- Identify commonly misconfigured settings within the Cisco Firepower Management Center and use basic commands to troubleshoot a Cisco Firepower Threat Defense device

Prerequisites

To fully benefit from this course, you should have the following knowledge and skills:

- Technical understanding of TCP/IP networking and network architecture
- Basic familiarity with the concepts of Intrusion Detection Systems (IDS) and IPS

Target Audience

This course is designed for technical professionals who need to know how to deploy and manage a Cisco Firepower NGIPS in their network environment.

- Security administrators
- Security consultants
- Network administrators
- System engineers
- Technical support personnel
- Channel partners and resellers

Course Outline

- Cisco Firepower Threat Defense Overview
- Cisco Firepower NGFW Device Configuration
- Cisco Firepower NGFW Traffic Control
- Cisco Firepower Discovery
- Implementing Access Control Policies
- Security Intelligence
- File Control and Advanced Malware Protection
- Next-Generation Intrusion Prevention Systems
- Network Analysis Policies
- Detailed Analysis Techniques
- Cisco Firepower Platform Integration
- Alerting and Correlation Policies
- Performing System Administration
- Firepower Troubleshooting

2. 300-735 SAUTO: Automating and Programming Cisco Security Solutions

The Implementing Automation for Cisco Security Solutions (SAUI) v1.0 course teaches you how to design advanced automated security solutions for your network. Through a combination of lessons and hands-on labs, you will master the use of modern programming concepts, RESTful Application Program Interfaces (APIs), data models, protocols, firewalls, web, Domain Name System (DNS), cloud, email security, and Cisco® Identity Services Engine (ISE) to strengthen cybersecurity for your web services, network, and devices. You will learn to work within the following platforms: Cisco Firepower® Management Center, Cisco Firepower Threat Defense, Cisco ISE, Cisco pxGrid, Cisco Stealthwatch® Enterprise, Cisco Stealthwatch Cloud, Cisco Umbrella®, Cisco Advanced Malware Protection (AMP), Cisco Threat Grid, and Cisco Security Management Appliances. This course will teach you when to use the API for each Cisco security solution to drive network efficiency and reduce complexity.

Duration

3 Days

Course Objectives

- Describe the overall architecture of the Cisco security solutions and how APIs help enable security
- Know how to use Cisco Firepower APIs
- Explain how pxGrid APIs function and their benefits
- Demonstrate what capabilities the Cisco Stealthwatch APIs offer and construct API requests to them for configuration changes and auditing purposes
- Describe the features and benefits of using Cisco Stealthwatch Cloud APIs
- Learn how to use the Cisco Umbrella Investigate API
- Explain the functionality provided by Cisco AMP and its APIs
- Describe how to use Cisco Threat Grid APIs to analyze, search, and dispose of threats

Prerequisites

Before taking this course, you should have:

- Basic programming language concepts
- Basic understanding of virtualization
- Ability to use Linux and Command Line Interface (CLI) tools, such as Secure Shell (SSH) and bash
- CCNP level core networking knowledge
- CCNP level security networking knowledge

Target Audience

This course is designed primarily for professionals in job roles such as:

- Network engineer
- Systems engineer
- Wireless engineer
- Consulting systems engineer
- Technical solutions architect
- Network administrator
- Wireless design engineer
- Network manager
- Sales engineer
- Account manager

Course Outline

- Introducing Cisco Security APIs
- Consuming Cisco Advanced Malware Protection APIs
- Using Cisco ISE
- Using Cisco pxGrid APIs
- Using Cisco Threat Grid APIs
- Investigating Cisco Umbrella Security Data Programmatically
- Exploring Cisco Umbrella Reporting and Enforcement APIs
- Automating Security with Cisco Firepower APIs
- Operationalizing Cisco Stealthwatch and the API Capabilities
- Using Cisco Stealthwatch Cloud APIs

- Describing Cisco Security Management Appliance APIs

Lab Outline

- Query Cisco AMP Endpoint APIs for Verifying Compliance
- Use the REST API and Cisco pxGrid with Cisco Identity Services Engine
- Construct a Python Script Using the Cisco Threat Grid API
- Generate Reports Using the Cisco Umbrella Reporting API
- Explore the Cisco Firepower Management Center API
- Use Ansible to Automate Cisco Firepower Threat Defense Configuration
- Automate Firewall Policies Using the Cisco Firepower Device Manager API
- Automate Alarm Policies and Create Reports Using the Cisco Stealthwatch APIs
- Construct Reports Using Cisco Security Management Appliance (SMA) APIs

3. 300-730 SVPN: Implementing Secure Solutions with Virtual Private Networks

The Implementing Secure Solutions with Virtual Private Networks (SVPN) v1.0 course teaches you how to implement, configure, monitor, and support enterprise Virtual Private Network (VPN) solutions. Through a combination of lessons and hands-on experiences you will acquire the knowledge and skills to deploy and troubleshoot traditional Internet Protocol Security (IPsec), Dynamic Multipoint Virtual Private Network (DMVPN), FlexVPN, and remote access VPN to create secure and encrypted data, remote accessibility, and increased privacy.

This course will prepare you for the 300-730 Implementing Secure Solutions with Virtual Private Networks (SVPN) exam.

Duration

5 Days

Course Objectives

After taking this course, you should be able to:

- Introduce site-to-site VPN options available on Cisco router and firewalls
- Introduce remote access VPN options available on Cisco router and firewalls
- Review site-to-site and remote access VPN design options
- Review troubleshooting processes for various VPN options available on Cisco router and firewalls

Prerequisites

Before taking this course, you should have the following knowledge and skills:

- Familiarity with the various Cisco router and firewall command modes
- Experience navigating and managing Cisco routers and firewalls
- Clear understanding of the benefits of site-to-site and Remote Access VPN options

Target Audience

This course is designed for professionals in the following job roles:

- Network security engineer
- CCNP Security candidate
- Channel Partner

Course Outline

- Introducing VPN Technology Fundamentals
- Implementing Site-to-Site VPN Solutions
- Implementing Cisco Internetwork Operating System (Cisco IOS®) Site-to-Site FlexVPN Solutions
- Implement Cisco IOS Group Encrypted Transport (GET) VPN Solutions
- Implementing Cisco AnyConnect VPNs
- Implementing Clientless VPNs

Lab Outline

- Explore IPsec Technologies
- Implement and Verify Cisco IOS Point-to-Point VPN
- Implement and Verify Cisco Adaptive Security Appliance (ASA) Point-to-Point VPN
- Implement and Verify Cisco IOS Virtual Tunnel Interface (VTI) VPN
- Implement and Verify Dynamic Multipoint VPN (DMVPN)
- Troubleshoot DMVPN
- Implement and Verify FlexVPN with Smart Defaults
- Implement and Verify Point-to-Point FlexVPN
- Implement and Verify Hub and Spoke FlexVPN
- Implement and Verify Spoke-to-Spoke FlexVPN
- Troubleshoot Cisco IOS FlexVPN
- Implement and Verify AnyConnect Transport Layer Security (TLS) VPN on ASA
- Implement and Verify Advanced Authentication, Authorization, and Accounting (AAA) on Cisco AnyConnect VPN
- Implement and Verify Clientless VPN on ASA

4. 300-725 SWSA: Securing the Web with Cisco Web Security Appliance

The Securing the Web with Cisco Web Security Appliance (SWSA) v3.0 course shows you how to implement, use, and maintain Cisco® Web Security Appliance (WSA), powered by Cisco Talos, to provide advanced protection for business email and control against web security threats. Through a combination of expert instruction and hands-on practice, you'll learn how to deploy proxy services, use authentication, implement policies to control HTTPS traffic and access, implement use control settings and policies, use the solution's anti-malware features, implement data security and data loss prevention, perform administration of Cisco WSA solution, and more.

This course helps you prepare to take the exam, Securing the Web with Cisco Web Security Appliance (300-725 SWSA), which leads to CCNP® Security and the Cisco Certified Specialist - Web Content Security.

Duration

2 Days

Course Objectives

After taking this course, you should be able to:

- Describe Cisco WSA
- Deploy proxy services
- Utilize authentication
- Describe decryption policies to control HTTPS traffic
- Understand differentiated traffic access policies and identification profiles
- Enforce acceptable use control settings
- Defend against malware
- Describe data security and data loss prevention
- Perform administration and troubleshooting

Prerequisites

To fully benefit from this course, you should have knowledge of these topics:

- TCP/IP services, including Domain Name System (DNS), Secure Shell (SSH), FTP, Simple Network Management Protocol (SNMP), HTTP, and HTTPS
- IP routing

You are expected to have one or more of the following basic technical competencies or equivalent knowledge:

- Cisco certification (CCENT certification or higher)
- Relevant industry certification [International Information System Security Certification Consortium ((ISC)2), Computing Technology Industry Association (CompTIA) Security+, International Council of Electronic Commerce Consultants (EC-Council), Global Information Assurance Certification (GIAC), ISACA]
- Cisco Networking Academy letter of completion (CCNA 1 and CCNA 2)
- Windows expertise: Microsoft [Microsoft Specialist, Microsoft Certified Solutions Associate (MCSA), Microsoft Certified Solutions Expert (MCSE)], CompTIA (A+, Network+, Server+)

Target Audience

- Security architects
- System designers
- Network administrators
- Operations engineers
- Network managers, network or security technicians, and security engineers and managers responsible for web security
- Cisco integrators and partners

Course Outline

- Describing Cisco WSA
    - Technology Use Case
    - Cisco WSA Solution
    - Cisco WSA Features
    - Cisco WSA Architecture
    - Proxy Service
    - Integrated Layer 4 Traffic Monitor
    - Data Loss Prevention
    - Cisco Cognitive Intelligence

    - Management Tools
    - Cisco Advanced Web Security Reporting (AWSR) and Third-Party Integration
    - Cisco Content Security Management Appliance (SMA)
- Deploying Proxy Services
    - Explicit Forward Mode vs. Transparent Mode
    - Transparent Mode Traffic Redirection
    - Web Cache Control Protocol
    - Web Cache Communication Protocol (WCCP) Upstream and Downstream Flow
    - Proxy Bypass
    - Proxy Caching
    - Proxy Auto-Config (PAC) Files
    - FTP Proxy
    - Socket Secure (SOCKS) Proxy
    - Proxy Access Log and HTTP Headers
    - Customizing Error Notifications with End User Notification (EUN) Pages
- Utilizing Authentication
    - Authentication Protocols
    - Authentication Realms
    - Tracking User Credentials
    - Explicit (Forward) and Transparent Proxy Mode
    - Bypassing Authentication with Problematic Agents
    - Reporting and Authentication
    - Re-Authentication
    - FTP Proxy Authentication
    - Troubleshooting Joining Domains and Test Authentication
    - Integration with Cisco Identity Services Engine (ISE)
- Creating Decryption Policies to Control HTTPS Traffic
    - Transport Layer Security (TLS)/Secure Sockets Layer (SSL) Inspection Overview
    - Certificate Overview
    - Overview of HTTPS Decryption Policies
    - Activating HTTPS Proxy Function
    - Access Control List (ACL) Tags for HTTPS Inspection
    - Access Log Examples
- Understanding Differentiated Traffic Access Policies and Identification Profiles
    - Overview of Access Policies
    - Access Policy Groups
    - Overview of Identification Profiles
    - Identification Profiles and Authentication
    - Access Policy and Identification Profiles Processing Order
    - Other Policy Types
    - Access Log Examples
    - ACL Decision Tags and Policy Groups
    - Enforcing Time-Based and Traffic Volume Acceptable Use Policies, and End User Notifications
- Defending Against Malware
    - Web Reputation Filters
    - Anti-Malware Scanning
    - Scanning Outbound Traffic
    - Anti-Malware and Reputation in Policies
    - File Reputation Filtering and File Analysis
    - Cisco Advanced Malware Protection
    - File Reputation and Analysis Features
    - Integration with Cisco Cognitive Intelligence
- Enforcing Acceptable Use Control Settings
    - Controlling Web Usage
    - URL Filtering
    - URL Category Solutions
    - Dynamic Content Analysis Engine
    - Web Application Visibility and Control

    - Enforcing Media Bandwidth Limits
    - Software as a Service (SaaS) Access Control
    - Filtering Adult Content
- Data Security and Data Loss Prevention
    - Data Security
    - Cisco Data Security Solution
    - Data Security Policy Definitions
    - Data Security Logs
- Performing Administration and Troubleshooting
    - Monitor the Cisco Web Security Appliance
    - Cisco WSA Reports
    - Monitoring System Activity Through Logs
    - System Administration Tasks
    - Troubleshooting
    - Command Line Interface
- References
    - Comparing Cisco WSA Models
    - Comparing Cisco SMA Models
    - Overview of Connect, Install, and Configure
    - Deploying the Cisco Web Security Appliance Open Virtualization Format (OVF) Template
    - Mapping Cisco Web Security Appliance Virtual Machine (VM) Ports to Correct Networks
    - Connecting to the Cisco Web Security Virtual Appliance
    - Enabling Layer 4 Traffic Monitor (L4TM)
    - Accessing and Running the System Setup Wizard
    - Reconnecting to the Cisco Web Security Appliance
    - High Availability Overview
    - Hardware Redundancy
    - Introducing Common Address Redundancy Protocol (CARP)
    - Configuring Failover Groups for High Availability
    - Feature Comparison Across Traffic Redirection Options
    - Architecture Scenarios When Deploying Cisco AnyConnect® Secure Mobility

Lab Outline

- Configure the Cisco Web Security Appliance
- Deploy Proxy Services
- Configure Proxy Authentication
- Configure HTTPS Inspection
- Create and Enforce a Time/Date-Based Acceptable Use Policy
- Configure Advanced Malware Protection
- Configure Referrer Header Exceptions
- Utilize Third-Party Security Feeds and MS Office 365 External Feed
- Validate an Intermediate Certificate
- View Reporting Services and Web Tracking
- Perform Centralized Cisco AsyncOS Software Upgrade Using Cisco SMA

5. 300-720 SESA: Securing Email with Cisco Email Security Appliance

The Securing Email with Cisco Email Security Appliance (SESA) v3.1 course shows you how to deploy and use Cisco® Email Security Appliance to establish protection for your email systems against phishing, business email compromise, and ransomware, and to help streamline email security policy management. This hands-on course provides you with the knowledge and skills to implement, troubleshoot, and administer Cisco Email Security Appliance, including key capabilities such as advanced malware protection, spam blocking, anti-virus protection, outbreak filtering, encryption, quarantines, and data loss prevention.

This course helps you prepare to take the exam, Securing Email with Cisco Email Security Appliance (300-720 SESA), which leads to CCNP® Security and the Certified Specialist - Email Content Security certifications.

Duration

4 Days

Course Objectives

- Describe and administer the Cisco Email Security Appliance (ESA)
- Control sender and recipient domains
- Control spam with Talos SenderBase and anti-spam
- Use anti-virus and outbreak filters
- Use mail policies
- Use content filters
- Use message filters to enforce email policies
- Prevent data loss
- Perform LDAP queries
- Authenticate Simple Mail Transfer Protocol (SMTP) sessions
- Authenticate email
- Encrypt email
- Use system quarantines and delivery methods
- Perform centralized management using clusters
- Test and troubleshoot

Prerequisites

To fully benefit from this course, you should have one or more of the following basic technical competencies:

- Cisco certification (Cisco CCENT® certification or higher)
- Relevant industry certification, such as (ISC)2, CompTIA Security+, EC-Council, Global Information Assurance Certification (GIAC), and ISACA
- Cisco Networking Academy letter of completion (CCNA® 1 and CCNA 2)
- Windows expertise: Microsoft [Microsoft Specialist, Microsoft Certified Solutions Associate (MCSA), Microsoft Certified Systems Engineer (MCSE)], CompTIA (A+, Network+, Server+)

Target Audience

- Security engineers
- Security administrators
- Security architects
- Operations engineers
- Network engineers
- Network administrators
- Network or security technicians
- Network managers
- System designers
- Cisco integrators and partners

Course Outline

- Describing the Cisco Email Security Appliance
    - Cisco Email Security Appliance Overview
    - Technology Use Case
    - Cisco Email Security Appliance Data Sheet
    - SMTP Overview
    - Email Pipeline Overview
    - Installation Scenarios
    - Initial Cisco Email Security Appliance Configuration
    - Centralizing Services on a Cisco Content Security Management Appliance (SMA)
    - Release Notes for AsyncOS 11.x
- Administering the Cisco Email Security Appliance
    - Distributing Administrative Tasks
    - System Administration
    - Managing and Monitoring Using the Command Line Interface (CLI)
    - Other Tasks in the GUI
    - Advanced Network Configuration
    - Using Email Security Monitor
    - Tracking Messages
    - Logging
- Controlling Sender and Recipient Domains
    - Public and Private Listeners
    - Configuring the Gateway to Receive Email
    - Host Access Table Overview
    - Recipient Access Table Overview
    - Configuring Routing and Delivery Features
- Controlling Spam with Talos SenderBase and Anti-Spam
    - SenderBase Overview
    - Anti-Spam
    - Managing Graymail
    - Protecting Against Malicious or Undesirable URLs
    - File Reputation Filtering and File Analysis
    - Bounce Verification
- Using Anti-Virus and Outbreak Filters
    - Anti-Virus Scanning Overview
    - Sophos Anti-Virus Filtering
    - McAfee Anti-Virus Filtering
    - Configuring the Appliance to Scan for Viruses
    - Outbreak Filters
    - How the Outbreak Filters Feature Works
    - Managing Outbreak Filters
- Using Mail Policies
    - Email Security Manager Overview
    - Mail Policies Overview
    - Handling Incoming and Outgoing Messages Differently
    - Matching Users to a Mail Policy
    - Message Splintering
    - Configuring Mail Policies
- Using Content Filters
    - Content Filters Overview
    - Content Filter Conditions
    - Content Filter Actions
    - Filter Messages Based on Content
    - Text Resources Overview
    - Using and Testing the Content Dictionaries Filter Rules
    - Understanding Text Resources
    - Text Resource Management

    - Using Text Resources
- Using Message Filters to Enforce Email Policies
    - Message Filters Overview
    - Components of a Message Filter
    - Message Filter Processing
    - Message Filter Rules
    - Message Filter Actions
    - Attachment Scanning
    - Examples of Attachment Scanning Message Filters
    - Using the CLI to Manage Message Filters
    - Message Filter Examples
    - Configuring Scan Behavior
- Preventing Data Loss
    - Overview of the Data Loss Prevention (DLP) Scanning Process
    - Setting Up Data Loss Prevention
    - Policies for Data Loss Prevention
    - Message Actions
    - Updating the DLP Engine and Content Matching Classifiers
- Using LDAP
    - Overview of LDAP
    - Working with LDAP
    - Using LDAP Queries
    - Authenticating End-Users of the Spam Quarantine
    - Configuring External LDAP Authentication for Users
    - Testing Servers and Queries
    - Using LDAP for Directory Harvest Attack Prevention
    - Spam Quarantine Alias Consolidation Queries
    - Validating Recipients Using an SMTP Server
- SMTP Session Authentication
    - Configuring AsyncOS for SMTP Authentication
    - Authenticating SMTP Sessions Using Client Certificates
    - Checking the Validity of a Client Certificate
    - Authenticating User Using LDAP Directory
    - Authenticating SMTP Connection Over Transport Layer Security (TLS) Using a Client Certificate
    - Establishing a TLS Connection from the Appliance
    - Updating a List of Revoked Certificates
- Email Authentication
    - Email Authentication Overview
    - Configuring DomainKeys and DomainKeys Identified Mail (DKIM) Signing
    - Verifying Incoming Messages Using DKIM
    - Overview of Sender Policy Framework (SPF) and SIDF Verification
    - Domain-based Message Authentication Reporting and Conformance (DMARC) Verification
    - Forged Email Detection
- Email Encryption
    - Overview of Cisco Email Encryption
    - Encrypting Messages
    - Determining Which Messages to Encrypt
    - Inserting Encryption Headers into Messages
    - Encrypting Communication with Other Message Transfer Agents (MTAs)
    - Working with Certificates
    - Managing Lists of Certificate Authorities
    - Enabling TLS on a Listener's Host Access Table (HAT)
    - Enabling TLS and Certificate Verification on Delivery
    - Secure/Multipurpose Internet Mail Extensions (S/MIME) Security Services
- Using System Quarantines and Delivery Methods
    - Describing Quarantines
    - Spam Quarantine

    - Setting Up the Centralized Spam Quarantine
    - Using Safelists and Blocklists to Control Email Delivery Based on Sender
    - Configuring Spam Management Features for End Users
    - Managing Messages in the Spam Quarantine
    - Policy, Virus, and Outbreak Quarantines
    - Managing Policy, Virus, and Outbreak Quarantines
    - Working with Messages in Policy, Virus, or Outbreak Quarantines
    - Delivery Methods
- Centralized Management Using Clusters
    - Overview of Centralized Management Using Clusters
    - Cluster Organization
    - Creating and Joining a Cluster
    - Managing Clusters
    - Cluster Communication
    - Loading a Configuration in Clustered Appliances
    - Best Practices
- Testing and Troubleshooting
    - Debugging Mail Flow Using Test Messages: Trace
    - Using the Listener to Test the Appliance
    - Troubleshooting the Network
    - Troubleshooting the Listener
    - Troubleshooting Email Delivery
    - Troubleshooting Performance
    - Web Interface Appearance and Rendering Issues
    - Responding to Alerts
    - Troubleshooting Hardware Issues
    - Working with Technical Support
- References
    - Model Specifications for Large Enterprises
    - Model Specifications for Midsize Enterprises and Small-to-Midsize Enterprises or Branch Offices
    - Cisco Email Security Appliance Model Specifications for Virtual Appliances
    - Packages and Licenses

Lab Outline

- Verify and Test Cisco ESA Configuration
- Perform Basic Administration
- Advanced Malware in Attachments (Macro Detection)
- Protect Against Malicious or Undesirable URLs Beneath Shortened URLs
- Protect Against Malicious or Undesirable URLs Inside Attachments
- Intelligently Handle Unscannable Messages
- Leverage AMP Cloud Intelligence Via Pre-Classification Enhancement
- Integrate Cisco ESA with AMP Console
- Prevent Threats with Anti-Virus Protection
- Applying Content and Outbreak Filters
- Configure Attachment Scanning
- Configure Outbound Data Loss Prevention
- Integrate Cisco ESA with LDAP and Enable the LDAP Accept Query
- Domain Keys Identified Mail (DKIM)
- Sender Policy Framework (SPF)
- Forged Email Detection
- Configure the Cisco SMA for Tracking and Reporting

6. 300-715 SISE: Implementing and Configuring Cisco Identity Services Engine

The Implementing and Configuring Cisco Identity Services Engine (SISE) v3.0 course shows you how to deploy and use Cisco® Identity Services Engine (ISE) v2.4, an identity and access control policy platform that simplifies the delivery of consistent, highly secure access control across wired, wireless, and VPN connections. This hands-on course provides you with the knowledge and skills to implement and use Cisco ISE, including policy enforcement, profiling services, web authentication and guest access services, BYOD, endpoint compliance services, and TACACS+ device administration. Through expert instruction and hands-on practice, you will learn how to use Cisco ISE to gain visibility into what is happening in your network, streamline security policy management, and contribute to operational efficiency.

This course helps you prepare to take the exam, Implementing and Configuring Cisco Identity Services Engine (300-715 SISE), which leads to CCNP® Security and the Cisco Certified Specialist - Security Identity Management Implementation certifications.

Duration

5 Days

Course Objectives

- Describe Cisco ISE deployments, including core deployment components and how they interact to create a cohesive security architecture. Describe the advantages of such a deployment and how each Cisco ISE capability contributes to these advantages
- Describe concepts and configure components related to 802.1X and MAC Authentication Bypass (MAB) authentication, identity management, and certificate services
- Describe how Cisco ISE policy sets are used to implement authentication and authorization, and how to leverage this capability to meet the needs of your organization
- Describe third-party Network Access Devices (NADs), Cisco TrustSec®, and Easy Connect
- Describe and configure web authentication, processes, operation, and guest services, including guest access components and various guest access scenarios
- Describe and configure Cisco ISE profiling services, and understand how to monitor these services to enhance your situational awareness about network-connected endpoints. Describe best practices for deploying this profiler service in your specific environment
- Describe BYOD challenges, solutions, processes, and portals. Configure a BYOD solution, and describe the relationship between BYOD processes and their related configuration components. Describe and configure various certificates related to a BYOD solution
- Describe the value of the My Devices portal and how to configure this portal
- Describe endpoint compliance, compliance components, posture agents, posture deployment and licensing, and the posture service in Cisco ISE
- Describe and configure TACACS+ device administration using Cisco ISE, including command sets, profiles, and policy sets. Understand the role of TACACS+ within the Authentication, Authentication, and Accounting (AAA) framework and the differences between the RADIUS and TACACS+ protocols
- Migrate TACACS+ functionality from Cisco Secure Access Control System (ACS) to Cisco ISE, using a migration tool

Prerequisites

To fully benefit from this course, you should have the following knowledge:

- Familiarity with the Cisco IOS® Software Command-Line Interface (CLI)
- Familiarity with Cisco AnyConnect® Secure Mobility Client
- Familiarity with Microsoft Windows operating systems

- Familiarity with 802.1X

Target Audience

- Network security engineers
- ISE administrators
- Wireless network security engineers
- Cisco integrators and partners

Course Outline

- Introducing Cisco ISE Architecture and Deployment
    - Using Cisco ISE as a Network Access Policy Engine
    - Cisco ISE Use Cases
    - Describing Cisco ISE Functions
    - Cisco ISE Deployment Models
    - Context Visibility
- Cisco ISE Policy Enforcement
    - Using 802.1X for Wired and Wireless Access
    - Using MAC Authentication Bypass for Wired and Wireless Access
    - Introducing Identity Management
    - Configuring Certificate Services
    - Introducing Cisco ISE Policy
    - Implementing Third-Party Network Access Device Support
    - Introducing Cisco TrustSec
    - Cisco TrustSec Configuration
    - Easy Connect
- Web Authentication and Guest Services
    - Introducing Web Access with Cisco ISE
    - Introducing Guest Access Components
    - Configuring Guest Access Settings
    - Configuring Sponsor and Guest Portals
- Cisco ISE Profiler
    - Introducing Cisco ISE Profiler
    - Profiling Deployment and Best Practices
- Cisco ISE BYOD
    - Introducing the Cisco ISE BYOD Process
    - Describing BYOD Flow
    - Configuring the My Devices Portal
    - Configuring Certificates in BYOD Scenarios
- Cisco ISE Endpoint Compliance Services
    - Introducing Endpoint Compliance Services
    - Configuring Client Posture Services and Provisioning in Cisco ISE
- Working with Network Access Devices
    - Review TACACS+
    - Cisco ISE TACACS+ Device Administration
    - Configure TACACS+ Device Administration
    - TACACS+ Device Administration Guidelines and Best Practices
    - Migrating from Cisco ACS to Cisco ISE