Cisco | Networking Academy®
Mind Wide Open™

Scope and Sequence

CCNP: Implementing Secure Converged Wide-area Networks

Cisco Networking Academy

Version 5.0

Cisco | Networking Academy®
Mind Wide Open™

TABLE OF CONTENTS

Target Audience

Those desiring to continue their post-CCNA preparation for a career as a network administrator, Level 2 support engineer, Level 2 systems engineer, network technician, or deployment engineer. CCNA certified individuals pursuing CCNP, CCIP, CCSP, CCDP, or CCIE certifications.

Prerequisites

Students should have completed CCNA 1 – 4 or equivalent.

CCNA Certification desired but not required.

Work experience beneficial.

Course Description

CCNP: Implementing Secure Converged Wide-area Networks is one of four courses leading to the Cisco Certified Network Professional (CCNP) designation. CCNP: Implementing Secure Converged Wide-area Networks introduces Cisco Networking Academy Program students to providing secure enterprise-class network service for teleworkers and branch sites. Students will

learn how to secure and expand the reach of an enterprise network with focus on VPN configuration and securing network access.

Topics include teleworker configuration and access, frame-mode MPLS, site-to-site IPSEC VPN, Cisco EZVPN, strategies used to mitigate network attacks, Cisco device hardening and IOS firewall features.

Course Objectives

The CCNP certification indicates knowledge of networking for the small-office, home-office (SOHO) market and enterprise markets. Following is a list of claims relevant to the ISCW certification that a CCNP certified individual will be able to do:

- Implement basic teleworker services.
- Implement Frame-Mode MPLS.
- Implement a site-to-site IPSec VPN.
- Describe network security strategies.
- Implement Cisco Device Hardening.
- Implement Cisco IOS firewall.
- Describe and configure Cisco IOS IPS.

CCNP: Implementing Secure Converged Wide-area Networks is an integral step towards achieving CCNP Certification.

Upon completion of this course, students will have performed tasks related to:

- Explaining the Cisco hierarchical network model as it pertains to the WAN
- Describing and implementing teleworker configuration and access
- Implementing and verifying frame mode MPLS
- Describing and configuring a site-to-site IPSEC VPN
- Describing and configuring Cisco EZVPN
- Explaining the strategies used to mitigate network attacks
- Describing and configuring Cisco device hardening
- Describing and configuring IOS firewall and IPS features

Lab Requirements

Please refer to the CCNP Equipment Bundle Spreadsheets on Cisco Academy Connection.

Cisco | Networking Academy®
Mind Wide Open™

Certification Alignment

The curriculum is aligned with Cisco's Career Certifications ISCW course and the 642-825 exam.

Course Overview

The course is designed to be delivered in a 70 contact hour time frame. Approximately 45 hours will be designated to lab activities and 25 hours on curriculum content. A case study on network access and security is required, but format and timing are determined by the Local Academy.

Course Outline

Module 1: Remote Network Connectivity Requirements

Module Overview
1.1 Enterprise Networking
1.1.1 Hierarchical Network Model
1.1.2 Cisco Enterprise Architecture
1.1.3 Remote Connection Requirements in a Converged Network
1.1.4 Remote Connection Considerations
1.1.5 Intelligent Information Network
1.1.6 Cisco SONA Framework

Module Summary
Module Quiz

Module 2: Teleworker Connectivity

Module Overview
2.1 Describing Remote Connection Topologies for Teleworkers
2.1.1 Remote Connection Topologies for the Teleworker
2.1.2 The Teleworker Solution
2.1.3 Options for Connecting the Teleworker
2.1.4 Components of the Teleworker Solution
2.1.5 Traditional Versus Business-Ready Teleworker Requirements

2.2 Describing Cable Technology
2.2.1 What is a Cable System?
2.2.2 Cable Technology Terms
2.2.3 Cable System Components
2.2.4 Cable System Benefits
2.2.5 Sending Digital Signals over Radio Waves

Cisco | Networking Academy®
Mind Wide Open™

2.2.6 The Data-over-Cable Service Interface Specification: DOCSIS

2.3 Deploying Cable System Technology
2.3.1 Hybrid Fiber-Coaxial (HFC) Cable Networks
2.3.2 Sending Data over Cable
2.3.3 Cable Technology: Putting It All Together
2.3.4 Data Cable Network Technology Issues
2.3.5 Provisioning a Cable Modem
2.4 Describing DSL Technology
2.4.1 What is DSL
2.4.2 How Does DSL Work?
2.4.3 DSL Variants
2.4.4 Factors Affecting DSL Performance
2.4.5 DSL Distance Limitations

2.5 Deploying ADSL
2.5.1 ADSL
2.5.2 ADSL and POTS Coexistence
2.5.3 ADSL Channel Separation
2.5.4 Data over ADSL
2.5.5 PPPoE
2.5.6 DSL and PPPoE Deployment Options
2.5.7 PPPoE Session Establishment
2.5.8 Data over ADSL: PPPoA

2.6 Configuring the CPE as the PPPoE or PPPoA Client
2.6.1 Configuring the CPE as the PPPoE Client
2.6.2 Configuring the CPE as the PPPoE Client over the ATM Interface
2.6.3 Configuring a PPPoE Client
2.6.4 Configuring the PPPoE DSL Dialer Interface
2.6.5 Adjusting MSS and MTU Size
2.6.6 Configuring PAT
2.6.7 Configuring DHCP to Scale DSL
2.6.8 Configuring a Static Default Route
2.6.9 Verifying a PPPoE Configuration
2.6.10 Configuring a PPPoA DSL Connection
2.6.11 Configuring a DSL ATM Interface
2.7 Troubleshooting Broadband ADSL Configurations
2.7.1 Troubleshooting Layers 1, 2, and 3
2.7.2 Determine Whether the Router Is Properly Trained to the DSLAM
2.7.3 Troubleshooting Layer 1 Issues
2.7.4 Determining the Correct DSL Operating Mode
2.7.5 Troubleshooting Layer 2 Issues
2.7.6 Layer 2: Is Data Being Received from the ISP?
2.7.7 Proper PPP Negotiation
2.8 PPPoE Simulation Practice
2.8.1 PPPoE Simulation Practice

Cisco | Networking Academy®
Mind Wide Open™

Module Summary
Module Quiz

Module 3: IPsec VPNs

Module Overview
3.1 Introducing VPN Technology 3.1.1 What Is Needed to Build a VPN?
3.1.2 Overlay and Peer-to-Peer VPN Architecture
3.1.3 VPN Topologies
3.1.4 Characteristics of a Secure VPNs
3.1.5 VPN Security: Encapsulation
3.1.6 VPN Security: IPsec and GRE
3.1.7 VPN Security: Symmetric and Asymmetric Encryption Algorithms
3.1.8 Symmetric Encryption Algorithms
3.1.9 Asymetric Encryption
3.1.10 Diffie-Hellman Key Exchange
3.1.11 Data integrity
3.1.12 VPN Security: Authentication

3.2 Understanding IPsec Components and IPsec VPN Features
3.2.1 IPsec Security Features
3.2.2 IPsec Protocols and Headers
3.2.3 Internet Key Exchange
3.2.4 IKE Phases and Modes
3.2.5 Other IKE Functions
3.2.6 ESP and AH Protocols, Transport, and Tunnel Modes
3.2.7 AH Authentication and Integrity
3.2.8 ESP Protocol
3.2.9 Message Authentication and Integrity Check
3.2.10 PKI Environment

3.3 Implementing Site-to-Site IPsec VPN Operations
3.3.1 Site-to-Site IPsec VPN Operations
3.3.2 Step 2: IKE Phase 1
3.3.3 Step 3: IKE Phase 2
3.3.4 IPsec Tunnel Operation
3.3.5 Configuring a Site-to-Site IPsec VPN

3.4 Configuring IPsec Site-to-Site VPN Using SDM
3.4.1 Cisco SDM Features
3.4.2 Introducing the SDM VPN Wizard Interface
3.4.3 Site-to-Site VPN Components
3.4.4 Launching the Site-to-Site VPN Wizard
3.4.5 Using the Step-by-Step Wizard
3.4.6 Test, Monitor, and Troubleshoot Tunnel Configuration and Operation

3.5 Configuring GRE Tunnels over IPsec

3.5.1 Generic Routing Encapsulation
3.5.2 Secure GRE Tunnels?
3.5.3 Configuring GRE over IPsec Site-to-Site Tunnel Using SDM
3.5.4 Backup GRE Tunnel Information
3.5.5 Configuring VPN Authentication
3.5.6 Configuring IKE Proposals
3.5.7 Configuring the Transform Set
3.5.8 Routing Information
3.5.9 Completing the Configuration
3.5.10 Testing, Monitoring and Troubleshooting GRE Tunnel Configuration

3.6 Configuring High-Availability VPNs
3.6.1 High Availability for IOS IPsec VPNs
3.6.2 IPsec Backup Peer
3.6.3 Hot Standby Routing Protocol
3.6.4 HSRP for Default Gateway at Remote Site
3.6.5 HSRP for Head-end IPsec Routers
3.6.6 IPsec Stateful Failover
3.6.7 Backing Up a WAN Connection with an IPsec VPN

3.7 Introducing Cisco Easy VPN 3.7.1 Introducing Cisco Easy VPN
3.7.2 Cisco Easy VPN Components
3.7.3 Deployment Models
3.7.4 Requirements and Restrictions for Cisco Easy VPN Remote
3.7.5 Easy VPN Server and Easy VPN Remote Operation

3.8 Configuring Easy VPN Server using Cisco SDM
3.8.1 Required Preparation
3.8.2 Configuring the Prerequisites with VPN Wizards
3.8.3 Start the Easy VPN Server Wizard
3.8.4 Configure IKE Proposals
3.8.5 Configure the Transform Set
3.8.6 Storing Group Policy Configurations on the Local Router
3.8.7 Storing Group Policy Configurations on an External User Database via RADIUS
3.8.8 Local Group Policies
3.8.9 Completing the Configuration

3.9 Implementing the Cisco VPN Client
3.9.1 Cisco VPN Client Configuration Tasks
3.9.2 Task 1: Install Cisco VPN Client
3.9.3 Task 2: Create a New Client Connection Entry
3.9.4 Task 3: Configure Client Authentication Properties
3.9.5 Task 4: Configure Transparent Tunneling
3.9.6 Allowing Local LAN Access
3.9.7 Task 5: Enable and Add Backup Servers
3.9.8 Task 6: Configure Connection to the Internet Through Dialup Networking

3.10 IPsec VPN Lab Exercises
3.10.1 Lab 3.1 Configuring SDM on a Router
3.10.2 Lab 3.2 Configuring a Basic GRE Tunnel
3.10.3 Lab 3.3 Configuring Wireshark and SPAN
3.10.4 Lab 3.4 Configuring Site-to-Site IPsec VPNs with SDM
3.10.5 Lab 3.5 Configuring Site-to-Site IPsec VPNs with the IOS CLI
3.10.6 Lab 3.6 Configuring a Secure GRE Tunnel with SDM
3.10.7 Lab 3.7 Configuring a Secure GRE Tunnel with the IOS CLI
3.10.8 Lab 3.8 Configuring IPsec VTIs
3.10.9 Lab 3.9 Configuring Easy VPN with SDM
3.10.10 Lab 3.10 Configuring Easy VPN with the IOS CLI

Module Summary
Module Quiz

Module 4: Frame Mode MPLS Implementation

Module Overview
4.1 Introducing MPLS Networks 4.1.1 The MPLS Conceptual Model
4.1.2 Router Switching Mechanisms
4.1.3 MPLS Basics
4.1.4 MPLS Architecture
4.1.5 Label Switch Routers
4.1.6 LSR Component Architecture

4.2 Assigning MPLS Labels to Packets
4.2.1 Label Allocation in a Frame Mode MPLS Environment
4.2.2 Label Distribution and Advertisement
4.2.3 Populating the LFIB Table
4.2.4 Packet Propagation Across an MPLS Network
4.2.5 Penultimate Hop Popping

4.3 Implementing Frame Mode MPLS
4.3.1 The Procedure to Configure MPLS
4.3.2 Step 1: Configure CEF
4.3.3 Configuring MPLS on a Frame Mode Interface
4.3.4 Configuring the MTU Size in Label Switching

4.4 Describing MPLS VPN Technology
4.4.1 MPLS VPN Architecture
4.4.2 Benefits and Drawbacks of Each VPN Implementation Model
4.4.3 MPLS VPN Architecture
4.4.4 Propagation of Routing Information Across the P-Network
4.4.5 Using RDs in an MPLS VPN
4.4.6 Using Route Targets in an MPLS VPN
4.4.7 End-to-End Routing Information Flow
4.4.8 MPLS VPNs and Packet Forwarding

4.5 MPLS Lab Exercises
4.5.1 Lab 4.1 Configuring Frame Mode MPLS
4.5.2 Lab 4.2 Challenge Lab: Implementing MPLS VPNs (Optional)

Module Summary
Module Quiz

Module 5: Cisco Device Hardening

Module Overview
5.1 Thinking Like a Hacker
5.1.1 Seven Steps to Hacking a Network
5.1.2 Step 1: Footprint Analysis
5.1.3 Step 2: Enumerate Information
5.1.4 Step 3: Manipulate Users to Gain Access
5.1.5 Step 4: Escalate Privileges
5.1.6 Step 5: Gather Additional Passwords and Secrets
5.1.7 Step 6: Install Back Doors and Port Redirectors
5.1.8 Step 7: Leverage the Compromised System
5.1.9 Best Practices to Defeat Hackers

5.2 Mitigating Network Attacks
5.2.1 Types of Network Attacks
5.2.2 Reconnaissance Attacks
5.2.3 Packet Sniffers
5.2.4 Port Scans and Ping Sweeps
5.2.5 Access Attacks and Mitigation
5.2.6 Trust Exploitation
5.2.7 DoS and DDoS Attacks and Mitigation
5.2.8 IP Spoofing in DoS and DDoS

5.3 Network Attacks Using Intelligence
5.3.1 End Station Vulnerabilities: Worm, Virus, and Trojan Horses
5.3.2 Worm Attack, Mitigation and Response
5.3.3 Application Layer Attacks and Mitigation
5.3.4 Management Protocols and Vulnerabilities
5.3.5 Management Protocol Best Practices
5.3.6 Determining Vulnerabilities and Threats

5.4 Disabling Unused Cisco Router Network Services and Interfaces
5.4.1 Vulnerable Router Services and Interfaces
5.4.2 Locking Down Routers with AutoSecure
5.4.3 AutoSecure Process Overview
5.4.4 AutoSecure Processing
5.4.5 Display AutoSecure Configuration
5.4.6 Locking Down Routers with Cisco SDM

5.5 Securing Cisco Router Administrative Access

5.5.1 Cisco Router Passwords
5.5.2 Initial Password Configuration
5.5.3 Protecting Line Access
5.5.4 Additional Password Security
5.5.5 Protecting Your Router by Securing ROMMON
5.5.6 Setting Login Failure Rates and Conditions
5.5.7 Setting Timeouts
5.5.8 Setting Multiple Privilege Levels
5.5.9 Configuring Banner Messages

5.6 Configuring Role-Based CLI
5.6.1 Role-Based CLI Overview
5.6.2 Getting Started with Role-Based CLI
5.6.3 Configuring CLI Views
5.6.4 Configuring Superviews
5.6.5 Role-Based CLI Monitoring
5.6.6 Role-Based CLI Configuration Example
5.6.7 Secure Configuration Files

5.7 Mitigating Threats and Attacks with Access Lists
5.7.1 Overview of Cisco ACL
5.7.2 Applying ACLs to Router Interfaces
5.7.3 Using Traffic Filtering with ACLs
5.7.4 Filtering Network Traffic to Mitigate Threats
5.7.5 Mitigating DDoS with ACLs
5.7.6 Combining Access Functions
5.7.7 Caveats

5.8 Securing Management and Reporting Features
5.8.1 Secure Management and Reporting Planning Considerations
5.8.2 Secure Management and Reporting Architecture
5.8.3 Configuring an SSH Server for Secure Management and Reporting
5.8.4 Using Syslog Logging for Network Security
5.8.5 Configuring Syslog Logging

5.9 Configuring SNMP
5.9.1 SNMP Version 1 and 2
5.9.2 SNMPv3
5.9.3 Configuring an SNMP Managed Node
5.9.4 Task 1: Configuring the SNMP-Server Engine ID
5.9.5 Task 2: Configuring the SNMP-Server Group Names
5.9.6 Task 3: Configuring the SNMP-Server Users
5.9.7 Task 4: Configuring the SNMP-Server Hosts

5.10 Configuring the NTP Client
5.10.1 Understanding NTP
5.10.2 Configuring NTP Authentication

5.10.3 Configuring NTP Associations
5.10.4 Configuring Additional NTP Options
5.10.5 Implementing the NTP Server
5.10.6 Configuring NTP Server

5.11 Configuring AAA on Cisco Routers
5.11.1 Introduction to AAA
5.11.2 Router Access Modes
5.11.3 AAA Protocols: RADIUS and TACACS+
5.11.4 Configure AAA Login Authentication on Cisco Routers Using CLI
5.11.5 Configure AAA Login Authentication on Cisco Routers Using SDM
5.11.6 Troubleshoot AAA Login Authentication on Cisco Routers
5.11.7 AAA Authorization Commands
5.11.8 AAA Accounting Commands
5.11.9 Troubleshooting Accounting

5.12 Cisco Device Hardening Lab Exercises
5.12.1 Lab 5.1 Using SDM One-Step Lockdown
5.12.2 Lab 5.2 Securing a Router with Cisco AutoSecure
5.12.3 Lab 5.3 Disabling Unneeded Services
5.12.4 Lab 5.4 Enhancing Router Security
5.12.5 Lab 5.5 Configuring Logging
5.12.6 Lab 5.6 Configuring AAA Authentication
5.12.7 Lab 5.7 Configuring Role-Based CLI Views
5.12.8 Lab 5.8 Configuring NTP

Module Summary
Module Quiz

Module 6: Cisco IOS Threat Defense Features

Module Overview
6.1 Introducing the Cisco IOS Firewall
6.1.1 Layered Defense Strategy
6.1.2 Private VLAN
6.1.3 Firewall Technologies
6.1.4 Stateful Firewall Operation
6.1.5 Introducing the Cisco IOS Firewall Feature Set
6.1.6 Cisco IOS Firewall Functions
6.1.7 Cisco IOS Firewall Process/font>
6.1.8 Stateful Inspection Enhancements
6.1.9 Alerts and Audit Trails

6.2 Configuring Cisco IOS Firewall from the CLI
6.2.1 Configuration Tasks
6.2.2 Pick an Interface: Internal or External
6.2.3 Configure IP ACLs at the Interface
6.2.4 Set Audit Trails and Alerts

Cisco | Networking Academy®
Mind Wide Open™

6.2.5 Inspection Rules for Application Protocols
6.2.6 Apply an Inspection Rule to an Interface
6.2.7 Verifying Cisco IOS Firewall
6.2.8 Troubleshooting Cisco IOS Firewall

6.3 Basic and Advanced Firewall Wizards
6.3.1 Basic and Advanced Firewall Wizards
6.3.2 Configuring a Basic Firewall
6.3.3 Configuring Interfaces on an Advanced Firewall
6.3.4 Configuring a DMZ on an Advanced Firewall
6.3.5 Advanced Firewall Security Configuration
6.3.6 Complete the Configuration
6.3.7 Viewing Firewall Activity

6.4 Introducing Cisco IOS IPS
6.4.1 Introducing Cisco IOS IDS and IPS
6.4.2 Types of IDS and IPS Systems
6.4.3 Network-Based and Host-Based IPS
6.4.4 NIPS Features
6.4.5 Signature-Based IDS and IPS
6.4.6 Policy-Based IDS and IPS
6.4.7 Anomaly-Based IDS and IPS
6.4.8 Honeypot-Based IDS and IPS
6.4.9 IDS and IPS Signatures

6.5 Configuring Cisco IOS IPS
6.5.1 Cisco IOS IPS Signature Definition Files (SDF)
6.5.2 Cisco IOS IPS Alarms
6.5.3 Configuring Cisco IOS IPS
6.5.4 Cisco IOS IPS SDM Tasks
6.5.5 Selecting Interfaces and Configuring SDF Locations
6.5.6 Viewing the IPS Policy Summary and Delivering the Configuration to the Router
6.5.7 Configuring IPS Policies and Global Settings
6.5.8 Viewing SDEE Messages
6.5.9 Tuning Signatures

6.6 Threat Defense Lab Exercises
6.6.1 Lab 6.1 Configuring a Cisco IOS Firewall Using SDM
6.6.2 Lab 6.2 Configuring CBAC
6.6.3 Lab 6.3 Configuring IPS with SDM
6.6.4 Lab 6.4 Configuring IPS with CLI

Module Summary
Module Quiz

Case Studies

Case Study 1: CLI IPsec and Frame-Mode MPLS

Cisco | Networking Academy®
Mind Wide Open™

Case Study 2: SDM