

Cisco Networks

Implementing Secure Converged Wide Area Networks (ISCW)

Course:ET913

Course Description

Learn to secure the network environment using existing Cisco IOS security features and configure the three primary components of the Cisco IOS Firewall Feature set (Firewall, Intrusion Prevention System [IPS], and Authentication, Authorization, and Accounting [AAA]). In this task-oriented course, you'll get the knowledge and skills needed to secure Cisco IOS router networks. Expand the reach of your enterprise network to teleworkers and remote sites, and explore implementing a highly available network with connectivity options such as VPN and wireless.

Who should attend?

IT professionals, network administrators, and technicians who need to design, configure, or support a Cisco WAN that utilizes Cisco's remote access technologies. This course is highly recommended for people pursuing CCNP, CCDP, and CCIE certifications.

Pre-requisites

- Cisco Certified Network Associate (CCNA)

Course Objectives

- Cisco hierarchical network model as it pertains to the WAN
- Implement teleworker configuration and access
- Implement and verify frame-mode MPLS
- Configure a site-to-site IPSEC VPN
- Configure Cisco EZVPN
- Strategies used to mitigate network attacks
- Configure Cisco device hardening
- Configure IOS firewall features

Lab Equipments

Course Outline

1. Network Requirements
 - The In and the SONA framework
 - Cisco conceptual network models, such as Cisco Enterprise Architecture and Cisco hierarchical network model
 - Requirements for establishing secure remote connections in a converged network
2. Connect Teleworkers
 - Topologies for Facilitating Remote Connections
 - Cable Technology
 - DSL Technology
 - Configuring the CPE as the PPPoE and PPPoA Client
 - Verifying Broadband ADSL Configurations

Hands-On Labs

Configuring DSL

3. Implement Frame-Mode MPLS
 - Introducing MPLS Networks
 - Assigning MPLS Labels to Packets
 - Implementing Frame-Mode MPLS
 - MPLS VPN Technology

Hands-On Labs

Configuring Frame-Mode MPLS

4. IPsec VPNs
 - IPsec Components and IPsec VPN Features
 - Site-to-Site IPsec VPN Operations
 - Configuring IPsec Site-to-Site VPN Using SDM
 - Configuring GRE Tunnels over IPsec
 - High Availability Options
 - Configuring Cisco Easy VPN and Easy VPN Server Using SDM
 - Implementing the Cisco VPN Client

Hands-On Labs

Configuring Site-to-Site IPsec VPNs
Configuring GRE Tunnels over IPsec Using SDM
Configuring IPsec VPN to Back Up a WAN Connection
Configuring Cisco Easy VPN Server Using SDM

5. Cisco Device Hardening
 - Mitigating Network Attacks
 - Disabling Unused Cisco Router Network Services and Interfaces
 - Securing Cisco Router Installations and Administrative Access
 - Mitigating Threats and Attacks with Access Lists
 - Securing Management and Reporting Features

- Configuring AAA on Cisco Routers

Hands-On Labs

Securing Cisco Routers
Securing Cisco Router Management
Configuring AAA Login Authentication and Exec Authorization on Cisco Routers

6. Cisco IOS Threat Defense Features
 - Introducing the Cisco IOS Firewall
 - Implementing Cisco IOS Firewalls
 - Introducing Cisco IOS IPS
 - Configuring Cisco IOS IPS

Hands-On Labs

Configuring a Cisco IOS Firewall
Configuring Cisco IOS IPS
Troubleshooting Security

Register Now 02-260-3233
<http://www.ctt-center.com>

Certifeid Technical Training Center Co.,Ltd

