



**CTREC
HILTON**
IT ACADEMY

BUILDING TRAINING SOLUTIONS
FOR THE IT WORLD

Securing Networks with Cisco Routers and Switches 1.0 (SECURE)

Course Description:

The Securing Networks with Cisco Routers and Switches (SECURE) 1.0 course is a five-day course that aims at providing network security engineers with the knowledge and skills needed to secure Cisco IOS Software router- and switch-based networks, and provide security services based on Cisco IOS Software. Successful graduates will be able to secure the network environment using existing Cisco IOS Software features, and install and configure components of Cisco IOS Software. Components include the Zone-Based Policy Firewall, Cisco IOS Intrusion Prevention System (IPS), user-based firewall, and secure tunnels using IP Security (IPsec) virtual private network (VPN) technology including public key infrastructure (PKI). Components also include virtual tunnel interface/dynamic virtual tunnel interface (VTI/DVTI), Group Encrypted Transport VPN (GET VPN), Dynamic Multipoint Virtual Private Network (DMVPN), Secure Sockets Layer (SSL)

Days: 5
Format: Instructor-Led
Class Code: SECURE

Recommended Course Sequence

Knowledge of prerequisites noted below.

Course content is subject to change without notice.

VPN, and advanced switch security features. The course focuses on the implementation and troubleshooting aspects of the lifecycle services approach, adding some elements of the design phase as well.

Target Student:

This course is intended for:

- Network Security Engineers (NSEs)
- Anyone that currently has their CCNA Security and/or is working towards CCNP Security certification.

Prerequisites:

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

- Working knowledge of the Microsoft Windows operating system
- Knowledge attained from attending the following prerequisite authorized Cisco courses: ICND 1 & 2 or CCNA Bootcamp; and IINS

At Course Completion:

After completing this course, students will be able to...

- Implement and maintain Cisco IOS Software infrastructure protection controls in a Cisco router- and switch-based network infrastructure
- Implement and maintain Cisco IOS Software threat control and containment technologies in a Cisco router-based perimeter infrastructure
- Implement and maintain Cisco IOS Software VPN technologies in a Cisco router-based WAN
- Implement and maintain Cisco IOS Software remote access VPN technologies in a Cisco router-based remote access solution

Securing Networks with Cisco Routers and Switches 1.0 (SECURE)

Course Outline

Module 1: Deploying Cisco IOS Software Network Foundation Protection

Lesson 1: Deploying Network Foundation Protection Controls
<ul style="list-style-type: none">■ Overview of Network Infrastructure Threats■ Identifying Network Device Planes■ Identifying Network Foundation Protection Deployment Models■ Identifying Network Foundation Protection Feature Availability
Lesson 2: Deploying Advanced Switched Data Plane Security Controls
<ul style="list-style-type: none">■ Overview of Configuration Choices, Basic Procedures, and Required Input Parameters■ Deploying PVLANS and PVLAN Edge■ Deploying DHCP Control■ Deploying ARP Control■ Deploying Source IP Address Control■ Troubleshooting Cisco Catalyst IOS Software Switched Infrastructure Protection Controls
Lesson 3: Implementing Cisco Identity-Based Network Services
<ul style="list-style-type: none">■ Overview of Cisco IBNS and 802.1X■ Identifying Cisco IOS Software 802.1X Features■ Identifying Cisco Secure ACS 802.1X Features■ Identifying Cisco Secure Services Client Features■ Choosing an EAP Type
Lesson 4: Deploying Basic 802.1X Features
<ul style="list-style-type: none">■ Overview of Configuration Choices, Basic Procedures, and Required Input Parameters■ Configuring the Cisco Catalyst IOS Software 802.1X Authenticator■ Configure Cisco Secure ACS for EAP-FAST■ Configure the Cisco Secure Services Client 802.1X Supplicant■ Verify and Troubleshoot Basic 802.1X Features
Lesson 5: Deploying Advanced Routed Data Plane Security Controls
<ul style="list-style-type: none">■ Overview of Configuration Choices, Basic Procedures, and Required Input Parameters■ Deploying Cisco IOS Software Unicast Reverse Path Forwarding■ Deploying Cisco IOS Software Flexible Packet Matching■ Deploying Cisco IOS Software NetFlow

Securing Networks with Cisco Routers and Switches 1.0 (SECURE)

Lesson 6: Deploying Advanced Control Plane Security Controls
<ul style="list-style-type: none">■ Overview of Configuration Choices, Basic Procedures, and Required Input Parameters■ Deploying Infrastructure ACLs■ Deploying Cisco IOS Software Control Plane Policing■ Deploying Cisco IOS Software Control Plane Protection■ Deploying Routing Protocol Authentication■ Deploying Routing Protocol Filtering
Lesson 7: Deploying Advanced Management Plane Security Controls
<ul style="list-style-type: none">■ Overview of Configuration Choices, Basic Procedures, and Required Input Parameters■ Configuring Cisco IOS Software Management Plane Access Control■ Configuring Cisco IOS Software RBAC■ Configuring Security Features of the Cisco IOS Software SNMP Server■ Deploying Digitally Signed Cisco IOS Software Images■ Deploying CPU and Memory Thresholding

Module 2: Deploying Cisco IOS Software Threat Control and Containment

Lesson 1: Deploying Cisco IOS Software Network Address Translation
<ul style="list-style-type: none">■ Overview of Configuration Choices, Basic Procedures, and Required Input Parameters■ Configuring Static NAT and PAT■ Configuring Dynamic NAT and PAT■ Troubleshooting Cisco IOS Software NAT
Lesson 2: Deploying Basic Zone-Based Policy Firewalls
<ul style="list-style-type: none">■ Overview of Configuration Choices, Basic Procedures, and Required Input Parameters■ Configuring Zones and Zone Pairs■ Configuring a Basic OSI Layers 3 and 4 interzone access policy■ Configuring a Basic OSI Layers 3 and 4 intrazone access policy■ Configuring Inspection of Control Plane and Management Plane Traffic■ Tuning Stateful Engine and Connection Settings■ Configuring Support for Transparent Mode, VRF, and NAT■ Troubleshooting the Zone-Based Policy Firewall
Lesson 3: Deploying Advanced Zone-Based Policy Firewalls
<ul style="list-style-type: none">■ Overview of Configuration Choices, Basic Procedures, and Required Input Parameters■ Configure Application-Layer Access Policies

Securing Networks with Cisco Routers and Switches 1.0 (SECURE)

<ul style="list-style-type: none">■ Configure Zone-Based Policy Firewall User-Based Policies■ Configure Zone-Based Policy Firewall URL Filtering
Lesson 4: Deploying Cisco IOS Software IPS
<ul style="list-style-type: none">■ Overview of Configuration Choices, Basic Procedures, and Required Input Parameters■ Configuring Cisco IOS Software IPS Signature Policies■ Tuning Cisco IOS Software IPS Signature Policies■ Deploying Cisco IOS Software IPS Signature Update■ Monitoring Cisco IOS Software IPS Events■ Troubleshooting Cisco IOS Software IPS

Module 3: Deploying Cisco IOS Software Site-to-Site Transmission Security

Lesson 1: Site-to-Site VPN Architectures and Technologies
<ul style="list-style-type: none">■ Choosing a Site-to-Site VPN Topology■ Choosing a Site-to-Site VPN Technology■ IPsec Technology Refresher■ Choosing Cryptographic Controls for a Site-to-Site VPN
Lesson 2: Deploying VTI-Based Site-to-Site IPsec VPNs
<ul style="list-style-type: none">■ Overview of Configuration Choices, Basic Procedures, and Required Input Parameters■ Configuring Basic IKE Peering■ Configuring Static Point-to-Point IPsec VTI Tunnels■ Configuring Dynamic Point-to-Point IPsec VTI Tunnels
Lesson 3: Deploying Scalable Authentication in Site-to-Site IPsec VPNs
<ul style="list-style-type: none">■ Overview of PKI Technology■ Overview of Configuration Choices, Basic Procedures, and Required Input Parameters■ Deploying the Cisco IOS Software Certificate Server■ Configuring PKI Enrollment■ Configuring PKI-Based IKE Authentication in Cisco IOS Software Site-to-Site VPNs■ Deploying Advanced PKI Integration
Lesson 4: Deploying DMVPNs
<ul style="list-style-type: none">■ Overview of Cisco IOS Software DMVPN■ Overview of Configuration Choices, Basic Procedures, and Required Input Parameters■ Deploying Cisco IOS Software GRE Tunnels■ Deploying Cisco IOS Software NHRP■ Deploying a Cisco IOS Software DMVPN Hub■ Deploying a Cisco IOS Software DMVPN Spoke■ Configuring Routing in a Cisco IOS Software DMVPN■ Troubleshooting a Cisco IOS Software DMVPN Network

Securing Networks with Cisco Routers and Switches 1.0 (SECURE)

Lesson 5: Deploying High Availability in Tunnel-Based IPsec VPNs
<ul style="list-style-type: none">■ Overview of Configuration Choices, Basic Procedures, and Required Input Parameters■ Using Routing Protocol-Based Failover■ Managing Failures in a VTI-Based VPN■ Managing Failures in a DMVPN
Lesson 6: Deploying GET VPN
<ul style="list-style-type: none">■ Overview of the Cisco IOS Software GET VPN Architecture■ Overview of Configuration Choices, Basic Procedures, and Required Input Parameters■ Deploying a Cisco IOS Software GET VPN Key Server■ Deploying a Cisco IOS Software GET VPN Group Member■ Deploying GET VPN High Availability

Module 4: Deploying Secure Remote Access with Cisco IOS Software

Lesson 1: Remote Access VPN Architectures and Technologies
<ul style="list-style-type: none">■ Choosing a Remote Access VPN Technology■ Choosing Cryptographic Controls for a Remote Access VPN
Lesson 2: Deploying Remote Access Solutions Using SSL VPN
<ul style="list-style-type: none">■ Overview of Configuration Choices, Basic Procedures, and Required Input Parameters■ Configuring Common Cisco IOS Software SSL VPN Gateway Parameters■ Configuring Client Authentication and Policies■ Configuring Full-Tunneling Connectivity on a Cisco IOS Software SSL VPN Gateway Installing and Configuring the Cisco AnyConnect Client■ Configuring Clientless Access on a Cisco IOS Software SSL VPN Gateway■ Troubleshooting Basic SSL VPN Operation
Lesson 3: Deploying Remote Access Solutions Using Cisco Easy VPN
<ul style="list-style-type: none">■ Overview of Configuration Choices, Basic Procedures, and Required Input Parameters■ Configuring Basic VTI-Based Cisco Easy VPN Server Features■ Configuring the Cisco VPN Client■ Deploying a Cisco Easy VPN Remote Device■ Deploying a PKI-Enabled Cisco Easy VPN■ Troubleshooting Basic Cisco Easy VPN Operation