Securing Cisco Routers and Switches

Duration: 5 Days Course Code: SECURE

Overview:

This five-day course aims to provide network security engineers with the knowledge and skills needed to secure Cisco Router and Switch based IOS Software networks using security services based on Cisco IOS Software.
Delegates will be able to secure the network environment using existing Cisco IOS Software features, and install and configure components of the 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). Other components 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) 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 Audience:

This course is intended for :Internetwork professionals who want to ensure security of their network using IOS devices Anyone seeking to learn the latest features in IOS 15.0 code to evaluate for their production environments. Internetwork professionals who seek CCNP Security certification.

Objectives:

- **After you complete this course you 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

Prerequisites:

Attendees should meet the following prerequisites:

- CCNA Certification, ICND1 and ICND2 or CCNABC Required
- CCNA Security Certification IINS Required.
- Working knowledge of Microsoft Windows OS is an advantage.

Testing and Certification

Recommended preparation for exam(s):

- 642-637 - Securing Networks with Cisco Routers and Switches

SECURE is one of the four courses required for the Cisco Certified Network Professional for Security Career Certification

Follow-on-Courses:

The following courses are recommended for further study :

- FIREWALL - Deploying Cisco ASA Firewall Solutions
- VPN - Deploying Cisco ASA VPNSolutions
- IPS - Implementing Cisco Intrusion Prevention System

Content:

Deploying Cisco IOS Software Network Foundation Protection

- Deploying Network Foundation Protection Controls
- Deploying Advanced Switched Data Plane Security Controls
- Implementing Cisco Identity-Based Network Services
- Deploying Basic 802.1X Features
- Deploying Advanced Routed Data Plane Security Controls
- Deploying Advanced Control Plane Security Controls
- Deploying Advanced Management Plane Security Controls

Deploying Cisco IOS Software Threat Control and Containment

- Deploying Cisco IOS Software Network Address Translation
- Deploying Basic Zone-Based Policy Firewalls
- Deploying Advanced Zone-Based Policy Firewalls
- Deploying Cisco IOS Software IPS

Deploying Cisco IOS Software Site-to-Site Transmission Security

- Site-to-Site VPN Architectures and Technologies
- Deploying VTI-Based Site-to-Site IPsec VPNs
- Deploying Scalable Authentication in Site-to-Site IPsec VPNs
- Deploying DMVPNs
- Deploying High Availability in Tunnel-Based IPsec VPNs
- Deploying GET VPN

Deploying Secure Remote Access with Cisco IOS Software

- Remote Access VPN Architectures and Technologies
- Deploying Remote Access Solutions Using SSL VPN
- Deploying Remote Access Solutions Using Cisco Easy VPN

Labs

- Lab 1-1: Configuring Advanced Switched Data Plane Security Controls
- Lab 1-2: Configuring Advanced Infrastructure Security Controls
- Lab 2-1: Configuring Basic Zoned-Based Policy Firewall Features
- Lab 2-2: Configuring Advanced Zoned-Based Policy Firewall Features
- Lab 2-3: Configuring Cisco IOS Software IPS
- Lab 3-1: Configuring a PKI-Enabled Site-to-Site IPsec VPN
- Lab 3-2: Configuring Cisco IOS Software DMVPN Spokes
- Lab 3-3: Configuring GET VPN Group Members
- Lab 4-1: Configuring a Cisco IOS Software SSL VPN Gateway
- Lab 4-2: Configuring Cisco Easy VPN

Appendixes

- Appendix A: Case Study - Configuring and Verifying Basic 802.1x Features
- Appendix B: Deploying Advanced 802.1X Features
- Appendix C: Case Study - Configuring and Verifying Advanced 802.1X Features

Additional Information:

Recertification:
Cisco professional level certifications (CCNP, CCNP SP Operations, CCNP Wireless, CCDP, CCNP Security, CCNP Voice, and CCIP) are valid for three years. To recertify, pass any 642 exam that is part of the professional level curriculum or pass any CCIE/CCDE written exam before the certification expiration date.

Achieving or recertifying any of the certifications above automatically extends your active Associate and Professional level certification(s) up to the point of expiration of the last certification achieved. For more information, access the Cisco About Recertification page

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.be