

CISS – 24hrs

Higher Certificate in Cisco Information Security Specialist

課程簡介

網絡保安已是網絡工程人員不可不認識的一門學問。現今的 Router 及 Switch 其實已內置相當強勁的保安功能。例如，IOS Firewall、AAA、VPN、IDS 等等。但 Cisco 的 CCNA 認證只著重 Routing 及 Switching 的知識，但保安的功能並沒有深入的探討。有見及此，Cisco 便於 2007 年推出全新保安認證 CISS，以補足 CCNA 的不足，從而更能發揮 Router 及 Switch 的全部功能。

課程目標

本課程適合已考取或修畢 CCNA 學員而設，課程將重點教授 Cisco Router 及 Switch 的保安功能，修畢後學員可考取 Cisco 的 CISS 認證。

✧ Exam Code: 642-552 - CCSP/Cisco Firewall Specialist/Cisco IPS Specialist/Cisco VPN Specialist

課程內容

Describe the security threats facing modern network infrastructures

- ✧ Describe and mitigate the common threats to the physical installation
- ✧ Describe and list mitigation methods for common network attacks
- ✧ Describe and list mitigation methods for Worm, Virus, and Trojan Horse attacks
- ✧ Describe the main activities in each phase of a secure network lifecycle
- ✧ Explain how to meet the security needs of a typical enterprise with a comprehensive security policy
- ✧ Describe the Cisco Self Defending Network architecture

Secure Cisco routers

- ✧ Secure Cisco routers using the SDM Security Audit feature
- ✧ Use the One-Step Lockdown feature in SDM to secure a Cisco router
- ✧ Secure administrative access to Cisco routers by setting strong encrypted passwords, exec timeout, login failure rate and using IOS login enhancements
- ✧ Secure administrative access to Cisco routers by configuring multiple privilege levels
- ✧ Secure administrative access to Cisco routers by configuring role based CLI
- ✧ Secure the Cisco IOS image and configuration file

Implement basic AAA using Cisco routers

- ✧ Explain the functions and importance of AAA
- ✧ Describe the features of TACACS+ and RADIUS AAA protocols
- ✧ Describe the methods of authentication that are used to provide access through a router (packet mode) and to provide access to the router (character mode)

Mitigate threats to Cisco routers and networks using ACLs

- ✧ Explain the functionality of standard, extended, and named IP ACLs used by routers to filter packets
- ✧ Configure and verify IP ACLs to mitigate given threats (filter IP traffic destined for Telnet, SNMP, and DDoS attacks) in a network using CLI
- ✧ Configure IP ACLs to prevent IP address spoofing using CLI
- ✧ Discuss the caveats to be considered when building ACLs

Implement secure network management and reporting

- ✧ Describe the factors to be considered when planning for secure management and reporting of network devices
- ✧ Use CLI to configure SSH on Cisco routers to enable secured management access
- ✧ Use CLI to configure Cisco routers to send Syslog messages to a Syslog server
- ✧ Describe SNMPv3 and NTPv3

Mitigate common Layer 2 attacks

- ✧ Describe the common Layer 2 attacks and how to mitigate them (VLAN hopping, STP attacks, ARP spoofing, MAC spoofing, CAM overflow)
- ✧ Describe the function and benefit of the security features in Cisco Catalyst switches (IBNS, PVLAN, SPAN port)
- ✧ Describe common threats to WLANs
- ✧ Describe the security features of the 802.11 protocol

Implement the Cisco IOS firewall feature set using SDM

- ✧ Describe the operational strengths and weaknesses of the different firewall technologies
- ✧ Explain stateful firewall operations and the function of the state table
- ✧ Explain the types of NAT that can be implemented in a firewall
- ✧ Configure and verify basic and advanced firewall on a Cisco router using SDM

Implement the Cisco IOS IPS feature set using SDM

- ✧ Define network based vs. host based intrusion detection and prevention
- ✧ Explain IPS technologies, attack responses, and monitoring options
- ✧ Enable and verify Cisco IOS IPS operations using SDM

Implement IPsec VPN on Cisco routers using SDM

- ✧ Explain IKE protocol functionality and phases
- ✧ Describe the building blocks of IPsec and the security functions it provides
- ✧ Explain hash-based message authentication code (HMAC) operations
- ✧ Explain the different methods of encryption
- ✧ Explain the purpose of the Diffie-Hellman key agreement protocol
- ✧ Describe how IPsec establishes origin authentication
- ✧ Describe the PKI environment at a high level
- ✧ Describe the different types of IPsec VPN implementations
- ✧ Configure and verify an IPsec site-to-site VPN with pre-shared key authentication using SDM
- ✧ Explain Cisco Easy VPN Server and Cisco Easy VPN Remote
- ✧ Configure and verify remote access VPNs using the Cisco Easy VPN Server feature of Cisco SDM