CCNP Security

The Cisco Certified Internetwork Expert Security (CCIE Security) program recognizes individuals who have the knowledge and skills to implement, maintain and support extensive Cisco Network Security Solutions using the latest industry best practices and technologies.

Prerequisites: There are no formal prerequisites for CCIE certification. Other professional certifications or training courses are not required. Instead, candidates must first pass a written qualification exam and then the corresponding hands-on lab exam.

Recommended Training: SolutionEdge Executive Learning Program for CCIE Security is a complete, blended learning program to accelerate competency and build the skills that are necessary for expert certification.

Exams : CCIE Security Written Exam Version 4.0 (350-018), CCIE Security Lab Exam Version 4.0

Syllabus:

Written Exam Version 4.0 (350-018)

Exam Description: The written exam is a two-hour, multiple choice test with 90-110 questions covering areas such as security protocols, operating systems, application protocols, security technologies, and Cisco security applications. All exam materials are provided and no outside reference materials are allowed.

1.0 Infrastructure, Connectivity, Communications, and Network Security

- 1.1 Network addressing basics
- 1.2 OSI layers
- 1.3 TCP/UDP/IP protocols
- 1.4 LAN switching (for example, VTP, VLANs, spanning tree, and trunking)
- 1.5 Routing protocols (for example, RIP, EIGRP, OSPF, and BGP)
- 1.6 Tunneling protocols
- 1.7 IP multicast
- 1.8 Wireless
- 1.9 Authentication and authorization technologies
- 1.10 VPNs
- 1.11 Mobile IP networks

2.0 Security Protocols

- 2.1 RSA
- 2.2 RC4
- 2.3 MD5
- 2.4 SHA
- 2.5 DES
- 2.6 3DES
- 2.7 AES
- 2.8 IPsec
- 2.9 ISAKMP
- 2.10 IKE and IKEv2
- 2.11 GDOI
- 2.12 AH
- 2.13 ESP
- 2.14 CEP
- 2.15 TLS and DTLS
- 2.16 SSL
- 2.17 SSH
- 2.18 RADIUS
- 2.19 TACACS+
- 2.20 LDAP
- 2.21 EAP methods (for example, EAP-MD5, EAP-TLS, EAP-TTLS, EAP-FAST, PEAP, and LEAP)
- 2.22 PKI, PKIX, and PKCS
- 2.23 IEEE 802.1X
- 2.24 WEP, WPA, and WPA2
- 2.25 WCCP
- 2.26 SXP
- 2.27 MACsec
- 2.27 DNSSEC

3.0 Application and Infrastructure Security

- 3.1 HTTP
- 3.2 HTTPS
- 3.3 SMTP
- 3.4 DHCP
- 3.5 DNS
- 3.6 FTP and SFTP
- 3.7 TFTP
- 3.8 NTP
- 3.9 SNMP
- 3.10 syslog
- 3.11 Netlogon, NetBIOS, and SMB
- 3.12 RPCs
- 3.13 RDP and VNC
- 3.14 PCoIP
- 3.15 OWASP
- 3.16 Manage unnecessary services

4.0 Threats, Vulnerability Analysis, and Mitigation

- 4.1 Recognize and mitigate common attacks
- 4.2 Software and OS exploits
- 4.3 Security and attack tools
- 4.4 Generic network intrusion prevention concepts
- 4.5 Packet filtering
- 4.6 Content filtering and packet inspection
- 4.7 Endpoint and posture assessment
- 4.8 QoS marking attacks

5.0 Cisco Security Products, Features, and Management

- 5.1 Cisco Adaptive Security Appliance (ASA)
- 5.2 Cisco IOS firewalls and NAT
- 5.3 Cisco Intrusion Prevention Systems (IPS)
- 5.4 Cisco IOS IPS
- 5.5 Cisco AAA protocols and application
- 5.6 Cisco Identity Services Engine (ISE)
- 5.7 Cisco Secure ACS Solution Engine
- 5.8 Cisco Network Admission Control (NAC) Appliance Server
- 5.9 Endpoint and client
- 5.10 Secure access gateways (Cisco IOS router or ASA)
- 5.11 Virtual security gateway
- 5.12 Cisco Catalyst 6500 Series ASA Services Modules
- 5.13 ScanSafe functionality and components
- 5.14 Cisco Web Security Appliance and Cisco Email Security Appliance
- 5.15 Cisco Web Security Appliance and Cisco Email Security Appliance
- 5.16 Security management

6.0 Cisco Security Technologies and Solutions

- 6.1 Router hardening features (for example, CoPP, MPP, uRPF, and PBR)
- 6.2 Switch security features (for example, anti-spoofing, port, STP, MACSEC, NDAC, and NEAT)
- 6.3 NetFlow
- 6.4 Wireless security
- 6.5 Network segregation
- 6.6 VPN solutions
- 6.7 Content and packet filtering
- 6.8 QoS application for security
- 6.9 Load balancing and failover

7.0 Security Policies and Procedures, Best Practices, and Standards

- 7.1 Security policy elements
- 7.2 Information security standards (for example, ISO/IEC 27001 and ISO/IEC 27002)
- 7.3 Standards bodies (for example, ISO, IEC, ITU, ISOC, IETF, IAB, IANA, and ICANN)
- 7.4 Industry best practices (for example, SOX and PCI DSS)

- 7.5 Common RFC and BCP (for example, RFC2827/BCP38, RFC3704/BCP84, and RFC5735)
- 7.6 Security audit and validation
- 7.7 Risk assessment
- 7.8 Change management process
- 7.9 Incident response framework
- 7.10 Computer security forensics
- 7.11 Desktop security risk assessment and desktop security risk management

Lab Exam Version 4.0

Exam Description: The Cisco CCIE Security Lab Exam version 4.0 is an 8-hour practical hands-on exam that tests the skills and competencies of security professionals in terms of configuring and troubleshooting Cisco security products and solutions. Candidates may be required to perform implementation, optimization and troubleshooting actions in each of the exam topic sections. Content may include both IPv4 and IPv6 concepts and applications

1.0 System Hardening and Availability

- 1.1 Routing plane security features (for example, protocol authentication and route filtering)
- 1.2 Control Plane Policing
- 1.3 Control plane protection and management plane protection
- 1.4 Broadcast control and switch port security
- 1.5 Additional CPU protection mechanisms (for example, options drop and logging interval)
- 1.6 Disable unnecessary services
- 1.7 Control device access (for example, Telnet, HTTP, SSH, and privilege levels)
- 1.8 Device services (for example, SNMP, syslog, and NTP)
- 1.9 Transit traffic control and congestion management

2.0 Threat Identification and Mitigation

- 2.1 RSA
- 2.2 Identify and protect against fragmentation attacks
- 2.3 Identify and protect against malicious IP option usage
- 2.4 Identify and protect against network reconnaissance attacks
- 2.5 Identify and protect against MAC spoofing attacks
- 2.6 Identify and protect against ARP spoofing attacks
- 2.7 Identify and protect against DoS attacks
- 2.8 Identify and protect against DDoS attacks
- 2.9 Identify and protect against man-in-the-middle attacks
- 2.10 Identify and protect against port redirection attacks
- 2.11 Identify and protect against DHCP attacks
- 2.12 Identify and protect against DNS attacks
- 2.13 Identify and protect against MAC flooding attacks
- 2.14 Identify and protect against VLAN hopping attacks
- 2.15 Identify and protect against various Layer 2 and Layer 3 attacksS
- 2.16 NBAR
- 2.17 NetFlow
- 2.18 Capture and utilize packet captures

3.0 Intrusion Prevention and Content Security

- 3.1 Cisco IPS 4200 Series Sensor appliance and Cisco ASA appliance IPS module
- 3.2 VACL, SPAN and RSPAN on Cisco switches
- 3.3 Cisco WSA

4.0 Identity Management

- 4.1 Identity-based AAA
- 4.2 Device administration (Cisco IOS routers, Cisco ASA, and Cisco ACS5.x)
- 4.3 Network access (TrustSec model)
- 4.4 Cisco ISE

5.0 Perimeter Security and Services

- 5.1 Cisco ASA firewalls
- 5.2 Cisco IOS zone-based firewall
- 5.3 Perimeter security services

6.0 Confidentiality and Secure Access

- 6.1 IKE (v1/v2)
- 6.2 DMVPN
- 6.3 FlexVPN
- 6.4 GET VPN
- 6.5 Remote-access VPN
- 6.6 VPN high availability
- 6.7 QoS for VPN
- 6.8 VRF-aware VPN
- 6.9 MACsec
- 6.10 Digital certificates (enrollment and policy matching)
- 6.11 Wireless access