COURSE AGENDA:

CCIE Security Certification and Training Syllabus

For Qualifying Exam - Implementing and Operating Cisco Security Core Technologies v1.0 (SCOR 350-701)

Security Concepts – 25%

1.1 Explain common threats against on-premises and cloud environments

1.1.a On-premises: viruses, trojans, DoS/DDoS attacks, phishing, rootkits, man-in-themiddle attacks, SQL injection, cross-site scripting, malware

1.1.b Cloud: data breaches, insecure APIs, DoS/DDoS, compromised credentials

1.2 Compare common security vulnerabilities such as software bugs, weak and/or hardcoded passwords, SQL injection, missing encryption, buffer overflow, path traversal, cross-site scripting/forgery

1.3 Describe functions of the cryptography components such as hashing, encryption, PKI, SSL, IPsec, NAT-T IPv4 for IPsec, pre-shared key and certificate based authorization

1.4 Compare site-to-site VPN and remote access VPN deployment types such as sVTI, IPsec, Cryptomap, DMVPN, FLEXVPN including high availability considerations, and AnyConnect

1.5 Describe security intelligence authoring, sharing, and consumption

1.6 Explain the role of the endpoint in protecting humans from phishing and social engineering attacks

1.7 Explain North Bound and South Bound APIs in the SDN architecture

1.8 Explain DNAC APIs for network provisioning, optimization, monitoring, and troubleshooting

1.9 Interpret basic Python scripts used to call Cisco Security appliances APIs

Network Security – 20%

2.1 Compare network security solutions that provide intrusion prevention and firewall capabilities

2.2 Describe deployment models of network security solutions and architectures that provide intrusion prevention and firewall capabilities

2.3 Describe the components, capabilities, and benefits of NetFlow and Flexible NetFlow records

2.4 Configure and verify network infrastructure security methods (router, switch, wireless)

2.4.a Layer 2 methods (Network segmentation using VLANs and VRF-lite; Layer 2 and port security; DHCP snooping; Dynamic ARP inspection; storm control; PVLANs to segregate network traffic; and defenses against MAC, ARP, VLAN hopping, STP, and DHCP rogue attacks

2.4.b Device hardening of network infrastructure security devices (control plane, data plane, management plane, and routing protocol security)

2.5 Implement segmentation, access control policies, AVC, URL filtering, and malware protection

2.6 Implement management options for network security solutions such as intrusion prevention and perimeter security (Single vs. multidevice manager, in-band vs. out-ofband, CDP, DNS, SCP, SFTP, and DHCP security and risks)

2.7 Configure AAA for device and network access (authentication and authorization, TACACS+, RADIUS and RADIUS flows, accounting, and dACL)

2.8 Configure secure network management of perimeter security and infrastructure devices (secure device management, SNMPv3, views, groups, users, authentication, and

encryption, secure logging, and NTP with authentication)

2.9 Configure and verify site-to-site VPN and remote access VPN

2.9.a Site-to-site VPN utilizing Cisco routers and IOS

2.9.b Remote access VPN using Cisco AnyConnect Secure Mobility client

2.9.c Debug commands to view IPsec tunnel establishment and troubleshooting

Securing the Cloud – 15%

3.1 Identify security solutions for cloud environments

3.1.a Public, private, hybrid, and community clouds

3.1.b Cloud service models: SaaS, PaaS, IaaS (NIST 800-145)

3.2 Compare the customer vs. provider security responsibility for the different cloud service models

3.2.a Patch management in the cloud

3.2.b Security assessment in the cloud

3.2.c Cloud-delivered security solutions such as firewall, management, proxy, security intelligence, and CASB

3.3 Describe the concept of DevSecOps (CI/CD pipeline, container orchestration, and security

3.4 Implement application and data security in cloud environments

3.5 Identify security capabilities, deployment models, and policy management to secure the cloud

3.6 Configure cloud logging and monitoring methodologies

3.7 Describe application and workload security concepts

Content Security – 10%

4.1 Implement traffic redirection and capture methods

4.2 Describe web proxy identity and authentication including transparent user identification

4.3 Compare the components, capabilities, and benefits of local and cloud-based email and web solutions (ESA, CES, WSA)

4.4 Configure and verify web and email security deployment methods to protect onpremises and remote users (inbound and outbound controls and policy management)

4.5 Configure and verify email security features such as SPAM filtering, antimalware filtering, DLP, block listing, and email encryption

4.6 Configure and verify secure internet gateway and web security features such as block listing, URL filtering, malware scanning, URL categorization, web application filtering, and TLS decryption

4.7 Describe the components, capabilities, and benefits of Cisco Umbrella

4.8 Configure and verify web security controls on Cisco Umbrella (identities, URL content settings, destination lists, and reporting)

Endpoint Protection and Detection – 15%

5.1 Compare Endpoint Protection Platforms (EPP) and Endpoint Detection & Response (EDR) solutions

5.2 Explain antimalware, retrospective security, Indication of Compromise (IOC), antivirus, dynamic file analysis, and endpoint-sourced telemetry

5.3 Configure and verify outbreak control and quarantines to limit infection

5.4 Describe justifications for endpoint-based security

5.5 Describe the value of endpoint device management and asset inventory such as MDM

5.6 Describe the uses and importance of a multifactor authentication (MFA) strategy

5.7 Describe endpoint posture assessment solutions to ensure endpoint security

5.8 Explain the importance of an endpoint patching strategy

Secure Network Access, Visibility, and Enforcement – 15%

6.1 Describe identity management and secure network access concepts such as guest services, profiling, posture assessment and BYOD

6.2 Configure and verify network access device functionality such as 802.1X, MAB, WebAuth

6.3 Describe network access with CoA

6.4 Describe the benefits of device compliance and application control

6.5 Explain exfiltration techniques (DNS tunneling, HTTPS, email, FTP/SSH/SCP/SFTP, ICMP, Messenger, IRC, NTP)

6.6 Describe the benefits of network telemetry

6.7 Describe the components, capabilities, and benefits of these security products and solutions

6.7.a Cisco Stealthwatch

6.7.b Cisco Stealthwatch Cloud

6.7.c Cisco pxGrid

6.7.d Cisco Umbrella Investigate

6.7.e Cisco Cognitive Threat Analytics

6.7.f Cisco Encrypted Traffic Analytics

6.7.g Cisco AnyConnect Network Visibility Module (NVM)

Lab Exam - CCIE Security v6.0

1. Perimeter Security and Intrusion Prevention (20%)

1.1 Deployment modes on Cisco ASA and Cisco FTD

1.1.a Routed

1.1.b Transparent

1.1.c Single

1.1.d Multi-Context

1.1.e Multi-Instance

1.2 Firewall features on Cisco ASA and Cisco FTD

1.2.a NAT

1.2.b Application inspection

1.2.c Traffic zones

1.2.d Policy-based routing

1.2.e Traffic redirection to service modules

1.2.f Identity firewall

1.3 Security features on Cisco IOS/IOS-XE

1.3.a Application awareness

1.3.b Zone-Based Firewall (ZBFW)

1.3.c NAT

1.4 Cisco Firepower Management Center (FMC) features

1.4.a Alerting

1.4.b Logging

1.4.c Reporting

1.5 NGIPS deployment modes

1.5.a In-Line

1.5.b Passive

1.5.c TAP

1.6 Next Generation Firewall (NGFW) features

1.6.a SSL inspection

1.6.b user identity

1.6.c geolocation

1.6.d AVC

1.7 Detect, and mitigate common types of attacks

1.7.a DoS/DDoS

1.7.b Evasion Techniques

1.7.c Spoofing

1.7.d Man-In-The-Middle

1.7.e Botnet

1.8 Clustering/HA features on Cisco ASA and Cisco FTD

1.9 Policies and rules for traffic control on Cisco ASA and Cisco FTD

1.10 Routing protocols security on Cisco IOS, Cisco ASA and Cisco FTD

1.11 Network connectivity through Cisco ASA and Cisco FTD

1.12 Correlation and remediation rules on Cisco FMC

2. Secure Connectivity and Segmentation (20%)

2.1 AnyConnect client-based remote access VPN technologies on Cisco ASA, Cisco FTD, and Cisco Routers.

2.2 Cisco IOS CA for VPN authentication

2.3 FlexVPN, DMVPN, and IPsec L2L Tunnels

2.4 Uplink and downlink MACsec (802.1AE)

2.5 VPN high availability using

2.5.a Cisco ASA VPN clustering

2.5.b Dual-Hub DMVPN deployments

2.6 Infrastructure segmentation methods

2.6.a VLAN

2.6.b PVLAN

2.6.c GRE

2.6.d VRF-Lite

2.7 Micro-segmentation with Cisco TrustSec using SGT and SXP

3. Infrastructure Security (15%)

3.1 Device hardening techniques and control plane protection methods

3.1.a CoPP

3.1.b IP Source routing

3.1.c iACLs

3.2 Management plane protection techniques

3.2.a CPU

3.2.b Memory thresholding

3.2.c Securing device access

3.3 Data plane protection techniques

3.3.a uRPF

3.3.b QoS

3.3.c RTBH

3.4 Layer 2 security techniques

3.4.a DAI

3.4.b IPDT

3.4.c STP security

3.4.d Port security

3.4.e DHCP snooping

3.4.f RA Guard

3.4.g VACL

3.5 Wireless security technologies

3.5.a WPA

3.5.b WPA2

3.5.c WPA3

3.5.d TKIP

3.5.e AES

3.6 Monitoring protocols

3.6.a NetFlow/IPFIX/NSEL

3.6.b SNMP

3.6.c SYSLOG

3.6.d RMON

3.6.e eStreamer

3.7 Security features to comply with organizational security policies, procedures, and standards BCP 38

3.7.a ISO 27001

3.7.b RFC 2827

3.7.c PCI-DSS

3.8 Cisco SAFE model to validate network security design and to identify threats to different Places in the Network (PINs)

3.9 Interaction with network devices through APIs using basic Python scripts

3.9.a REST API requests and responses

3.9.a i HTTP action verbs, error codes, cookies, headers

3.9.a ii JSON or XML payload

3.9.a iii Authentication

3.9.b Data encoding formats

3.9.b I JSON

3.9.b ii XML

3.9.b iii YAML

3.10 Cisco DNAC Northbound APIs use cases

3.10.a. Authentication/Authorization

3.10.b. Network Discovery

3.10.c. Network Device

3.10.d. Network Host

4. Identity Management, Information Exchange, and Access Control (25%)

4.1 ISE scalability using multiple nodes and personas.

4.2 Cisco switches and Cisco Wireless LAN Controllers for network access AAA with ISE.

4.3 Cisco devices for administrative access with ISE

4.4 AAA for network access with 802.1X and MAB using ISE.

4.5 Guest lifecycle management using ISE and Cisco Wireless LAN controllers

4.6 BYOD on-boarding and network access flows

4.7 ISE integration with external identity sources

4.7.a LDAP

4.7.b AD

4.7.c External RADIUS

4.8 Provisioning of AnyConnect with ISE and ASA

4.9 Posture assessment with ISE

4.10 Endpoint profiling using ISE and Cisco network infrastructure including device sensor

4.11 Integration of MDM with ISE

4.12 Certificate-based authentication using ISE

4.13 Authentication methods

4.13.a EAP Chaining

4.13.b Machine Access Restriction (MAR)

4.14 Identity mapping on ASA, ISE, WSA, and FTD

4.15 pxGrid integration between security devices WSA, ISE, and Cisco FMC

4.16 Integration of ISE with multi-factor authentication

4.17 Access control and single sign-on using Cisco DUO security technology

5. Advanced Threat Protection and Content Security (20%)

5.1 AMP for networks, AMP for endpoints, and AMP for content security (ESA, and WSA)

5.2 Detect, analyze, and mitigate malware incidents

5.3 Perform packet capture and analysis using Wireshark, tcpdump, SPAN, ERSPAN, and RSPAN

5.4 DNS layer security, intelligent proxy, and user identification using Cisco Umbrella

5.5 Web filtering, user identification, and Application Visibility and Control (AVC) on Cisco FTD and WSA.

5.6 WCCP redirection on Cisco devices

5.7 Email security features

5.7.a Mail policies

5.7.b DLP

5.7.c Quarantine

5.7.d Authentication

5.7.e Encryption

5.8 HTTPS decryption and inspection on Cisco FTD, WSA and Umbrella

5.9 SMA for centralized content security management

5.10 Cisco advanced threat solutions and their integration: Stealthwatch, FMC,

AMP, Cognitive Threat Analytics (CTA), Threat Grid, Encrypted Traffic Analytics (ETA), WSA, SMA, CTR, and Umbrella