CETPA INFOTECH PVT. LTD.
CURRICULUM OF CCIE SECURITY

❖ Infrastructure, Connectivity, Communications, and Network Security

1.0 Network addressing basics
1.1 OSI layers
1.2 TCP/UDP/IP protocols
1.3 LAN switching (for example, VTP, VLANs, spanning tree, and trunking)

1.5 Routing protocols (for example, RIP, EIGRP, OSPF, and BGP)
1.5.a Basic functions and characteristics
1.5.b Security features
1.6 Tunneling protocols
1.6.a GRE
1.6.b NHRP
1.6.c IPv6 tunnel types

1.7 IP multicast
1.7.a PIM
1.7.b MSDP
1.7.c IGMP and CGMP
1.7.d Multicast Listener Discovery

1.8 Wireless
1.8.a SSID
1.8.b Authentication and authorization
1.8.c Rogue APs
1.8.d Session establishment

1.9 Authentication and authorization technologies
1.9.a Single sign-on
1.9.b OTPs
1.9.c LDAP and AD
1.9.d RBAC

1.10 VPNs
1.10.a L2 vs L3
1.10.b MPLS, VRFs, and tag switching

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
2.28 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
- 4.1. a. ICMP attacks and PING floods
- 4.1.b MITM
- 4. 1.c Replay
- 4.1.d Spoofing
- 4.1.d Backdoor
- 4.1.e Botnets
- 4.1.f Wireless attacks
- 4.1.g DoS and DDoS attacks
- 4.1.h Virus and worm outbreaks
- 4.1.i Header attacks
- 4.1.j Tunneling 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)
- 5.1.a Firewall functionality
- 5.1.b Routing and multicast capabilities
- 5.1.c Firewall modes
- 5.1.d NAT (before and after version 8.4)
- 5.1.e Object definition and ACLs
- 5.1.f MPF functionality (IPS, QoS, and application awareness)
- 5.1.g Context-aware firewall
- 5.1.h Identity-based services
- 5.1.i Failover options

5.2 Cisco IOS firewalls and NAT
- 5.2.a CBAC
- 5.2.b Zone-based firewall
- 5.2.c Port-to-application mapping
- 5.2.d Identity-based firewalling

5.3 Cisco Intrusion Prevention Systems (IPS)

5.4 Cisco IOS IPS

5.5 Cisco AAA protocols and application
- 5.5.a RADIUS
- 5.5.b TACACS+
- 5.5.c Device administration
- 5.5.d Network access
- 5.5.e IEEE 802.1X
- 5.5.f VSAs

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
- 5.9.a Cisco AnyConnect VPN Client
- 5.9.b Cisco VPN Client
- 5.9.c Cisco Secure Desktop
- 5.9.d Cisco NAC Agent

5.10 Secure access gateways (Cisco IOS router or ASA)
- 5.10.a IPsec
- 5.10.b SSL VPN
- 5.10.c PKI

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 Security management
- 5.15.a Cisco Security Manager
- 5.15.b Cisco Adaptive Security Device Manager (ASDM)
- 5.15.c Cisco IPS Device Manager (IDM)
- 5.15.d Cisco IPS Manager Express (IME)
- 5.15.e Cisco Configuration Professional
- 5.15.f Cisco Prime

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
- 6.5.a VRF-aware technologies
- 6.5.b VXLAN

6.6 VPN solutions
- 6.6.a FlexVPN
- 6.6.b DMVPN
- 6.6.c GET VPN
- 6.6.d Cisco EasyVPN

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

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 Identify and protect against fragmentation attacks
2.2 Identify and protect against malicious IP option usage
2.3 Identify and protect against network reconnaissance attacks
2.4 Identify and protect against IP spoofing 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 attacks
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
- 3.1.a Initialize the sensor appliance
- 3.1.b Sensor appliance management
- 3.1.c Virtual sensors on the sensor appliance
- 3.1.d Implement security policies
- 3.1.e Promiscuous and inline monitoring on the sensor appliance
- 3.1.f Tune signatures on the sensor appliance
- 3.1.g Custom signatures on the sensor appliance
- 3.1.h Actions on the sensor appliance
- 3.1.i Signature engines on the sensor appliance
- 3.1.j Use Cisco IDM and Cisco IME to manage the sensor appliance
- 3.1.k Event action overrides and filters on the sensor appliance
- 3.1.l Event monitoring on the sensor appliance

3.2 VACL, SPAN and RSPAN on Cisco switches
3.3 Cisco WSA
- 3.3.a Implement WCCP
- 3.3.b Active Directory integration 3.3.c Custom categories
- 3.3.d HTTPS configuration
- 3.3.e Services configuration (web reputation)
- 3.3.f Configure proxy bypass lists
- 3.3.g Web proxy modes
- 3.3.h Application visibility and control

4.0 Identity Management
4.1 Identity-based AAA
- 4.1.a Cisco router and appliance AAA
- 4.1.b RADIUS
- 4.1.c TACACS+

4.2 Device administration (Cisco IOS routers, Cisco ASA, and Cisco ACS5.x)

4.3 Network access (TrustSec model)
- 4.3.a Authorization results for network access (ISE)
- 4.3.b IEEE 802.1X (Cisco ISE)
- 4.3.c VSAs (Cisco ASA, Cisco IOS, and Cisco ISE)
- 4.3.d Proxy authentication (Cisco ISE, Cisco ASA, and Cisco IOS)

4.4 Cisco ISE
- 4.4.a Profiling configuration (probes)
- 4.4.b Guest services
- 4.4.c Posture assessment
- 4.4 d Client provisioning (CPP)
- 4.4.e Configure Microsoft Active Directory integration and identity sources

5.0 Perimeter Security and Services

5.1 Cisco ASA firewalls

- 5.1.a Basic firewall Initialization
- 5.1.b Device management
- 5.1.c Address translation
- 5.1.d ACLs
- 5.1.e IP routing and route tracking
- 5.1.f Object groups
- 5.1.g VLANs
- 5.1.h Configure EtherChannel
- 5.1.i High availability and redundancy 5.1.j Layer 2 transparent firewall 5.1.k Security contexts (virtual firewall) 5.1.l Cisco Modular Policy Framework
- 5.1.j Identity firewall services
- 5.1.k Configure Cisco ASA with ASDM
- 5.1.l Context-aware services
- 5.1.m IPS capabilities
- 5.1.n QoS capabilities

5.2 Cisco IOS zone-based firewall

- 5.2.a Network, secure group, and user-based policy
- 5.2.b Performance tuning
- 5.2.c Network, protocol, and application inspection

5.3 Perimeter security services

- 5.3.a Cisco IOS QoS and packet-marking techniques
- 5.3.b Traffic filtering using access lists
- 5.3.c Cisco IOS NAT
- 5.3.d uRPF
- 5.3.e Port to Application Mapping (PAM)
- 5.3.f Policy routing and route maps

6.0 Confidentiality and Secure Access

6.1 IKE (v1/v2)
6.2 IPsec LAN-to-LAN (Cisco IOS and Cisco ASA)
6.3 DMVPN
6.4 FlexVPN
6.5 GET VPN
6.6 Remote-access VPN

- 6.6.a Cisco EasyVPN Server (Cisco IOS and Cisco ASA)
- 6.6.b VPN Client 5.X
- 6.6.c Clientless WebVPN
- 6.6.d Cisco AnyConnect VPN
- 6.6.e Cisco EasyVPN Remote
- 6.6.f SSL VPN gateway

6.7 VPN high availability

6.8 QoS for VPN

6.9 VRF-aware VPN

6.10 MAC sec

6.11 Digital certificates (enrollment and policy matching)

6.12 Wireless access

- 6.12.a EAP methods
- 6.12.b WPA and WPA2
- 6.12.c wIPS

HEAD OFFICE: 200 Purwavali , 2nd Floor, (Opp. Railway Ticket Agency), Railway Road, Ganeshpur, Roorkee – 247667, Ph.No.: 09219602769, 01332-270218 Fax - 1332 – 274960

CORPORATE OFFICE: D-58, Sector-2, Near Red FM. Noida -201301, Uttar Pradesh
Contact Us: +91-9212172602 , 0120-4535353

BRANCH OFFICE: 401 A, 4th Floor, Lekhraj Khazana, Faizabad Road, Indira Nagar, Lucknow-220616 (U.P.) Ph. No: +91-522-6590802, +91-9258017974,

BRANCH OFFICE: 105, Mohit Vihar, Near Kamla Palace, GMS Road, Dehradun-248001, UK Contact: +91-9219602771, 0135-6006070

CETPA®
Because Knowledge Matters
ISO 9001 : 2008 Certified

Toll Free- 1800-8333-999 (from any network)