CCNP Security

IMPLEMENTING CISCO EDGE NETWORK SECURITY SOLUTIONS (300-206) SENSS

Describe Threat Defense Concepts

Implementation and verification of firewall (ASA or IOS depending on which supports the implementation)
Implementation and verification of ACLs
Implementation and verification of static/dynamic NAT/PAT
Configuration and Verification of object groups
Describe various threat detection features
Implement botnet traffic filtering
Configuration of application filtering and protocol inspection
Describe various ASA security contexts
Implement and verify Layer 2 Security
Configuration and verification of DHCP snooping
Describe dynamic ARP inspection Works
Describe what is storm control
Configuration of port security methods
Describe various common Layer 2 threats and attacks and mitigation
Describe what is MAC Sec
Configure IP source verification and its implementation
Configure device hardening per best practices on Routers , Switches and Firewalls

Cisco Security Devices GUIs and Secured CLI Management

Implement and configure SSHv2, HTTPS, and SNMPv3 access on the network devices
Implementation and verification of RBAC on the ASA/IOS using CLI and ASDM
Describe how Cisco Prime Infrastructure works
What is the Functions and use cases of Cisco Prime on Device Management

Describe Cisco Security Manager (CSM) and its functions

Implementation of Device Managers
Implement ASA firewall features using ASDM

Management Services on Cisco Devices

Configuration of Net Flow exporter on Cisco Routers, Switches, and ASA
Implement SNMPv3 on cisco devices
Create views, groups, users, authentication, and encryption via SNMPv3
Implementation and verification of logging on Cisco Routers, Switches, and ASA using Cisco best practices
Implementation and verification of NTP with authentication on Cisco Routers, Switches, and ASA

Describe CDP, DNS, SCP, SFTP, and DHCP features
Describe security implications of using CDP on routers and switches

Threat Defense Architectures

Design a Firewall Solution on Threat Defense
What is High-availability
Describe Basic concepts of security zoning
Describe Transparent & Routed Modes
Describe Security Contexts
Describe Layer 2 Security Solutions
Implement defenses against MAC, ARP, VLAN hopping, STP, and DHCP rogue attacks
Describe how PVLANs works to segregate network traffic at Layer 2

Security Components and Considerations

Describe security operations management architectures on Single device manager vs. multi-device manager
Describe Data Center security components and considerations on Virtualization and Cloud security
Describe Collaboration security components and considerations on ASA

CCNP Security

IMPLEMENTING CISCO SECURE ACCESS SOLUTIONS (300-208) SISAS

Identity Management and Secure Access using various methods

Implement and verify device administration
Compare and implement AAA options like TACACS+, RADIUS, Native AD and LDAP
Describe identity management and its features and functionality of authentication and authorization
Describe and learn about identity store op

Implement wired/wireless 802.1X

Describe how RADIUS flows
Define and learn AV pairs
Describe various EAP types
Describe and learn supplicant, authenticator, and server
Define various Supplicant options
Define concepts of 802.1X phasing (monitor mode, low impact, closed mode)
What is AAA server

Implement MAB

Describe the MAB process within an 802.1X framework
Describe how Flexible authentication configuration works
Learn and define ISE authentication/authorization policies
Configuration and implementation of ISE endpoint identity
Verify MAB Operation methods

Implement various network authorization enforcement

Configure and verify ACL
Configure and verify Dynamic VLAN assignment
Describe how SGA Work
Implement and verify Named ACL
Describe how CoA Works

Implement Central Web Authentication (CWA)

Describe the function of CoA to support web authentication
Configure authentication policy to facilitate CWA
Describe various URL redirect policy
Define how Redirect ACL works
Customize the web portal
Verify central web authentication operation

Implement profiling and its Services

What is Network probes
Define how IOS Device Sensor works
Describe Feed service
Describe Profiling policy rules
Describe how to Utilize profile assignment in authorization policies
Verify various profiling operation

Implement and Verify guest services

learn how to Manage sponsor accounts
Describe Sponsor portals
Describe what is Guest portals, Guest Policies, Self, Registration, Guest activation
Differentiate various secure access
Verify guest services operation

Implement and verify posture services

Describe the function of CoA to support posture services
What is Agent options
Define Client provisioning policy and redirect ACL
Describe Posture policy, Quarantine/remediation

Implement and verify BYOD access

Describe various elements of a BYOD policy
Describe Device registration and devices portal

Learn and describe Threat Defense

Describe Trust Sec Architecture in detail
What is SGT Classification – dynamic/static
Describe SGT Transport – inline tagging and SXP
Describe SGT Enforcement – SGACL and SGFW
What is MAC sec

Learn various Threat Defense Architectures

Design highly secure wireless solution with ISE and its implementation
What is Identity Management
Describe 802.1X and its features
Describe MAB and its features
Describe Network authorization enforcement
Define CWA and its features
What is Profiling and its features
What is Guest Services, Posture Services and BYOD Access

Design Identity Management Architectures

Describe how to administrate the Device

What is Identity Management, Profiling, Guest Services
Describe in details about Posturing Services and BYOD Access

CCNP Security

IMPLEMENTING CISCO SECURE MOBILITY SOLUTIONS (300-209) SIMOS

Secure Communications Methods

Implement and verify Site-to-site VPNs on routers and firewalls
Implement and verify Describe GETVPN
Implement and verify IPsec (with IKEv1 and IKEv2 for both IPV4 & IPV6)
Implement and verify DMVPN (hub-Spoke and spoke-spoke on both IPV4 & IPV6)
Implement and verify Implement Flex VPN (hub-Spoke on both IPV4 & IPV6) using local AAA
Implement and verify Implement remote access VPNs
Implement and verify AnyConnect IKEv2 VPNs on ASA and routers
Implement and verify AnyConnect SSLVPN on ASA and routers
Implement and verify clientless SSLVPN on ASA and routers
Implement and verify FLEX VPN on routers

Troubleshooting, Monitoring, and Reporting Tools (as implemented above)

Troubleshoot various features of VPN using ASDM & CLI
Troubleshoot various features of IPsec
Troubleshoot various features of DMVPN
Troubleshoot various features of Flex VPN
Troubleshoot various features of AnyConnect IKEv2 and SSL VPNs on ASA and routers
Troubleshoot various features of clientless SSLVPN on ASA and routers

Design and describe various remote access VPN solutions

Identify various functional components of Flex VPN, IPsec, and Clientless SSL
Describe VPN technology considerations based on functional requirements
Identify describe VPN technology based on configuration output
Identify describe AnyConnect client requirements
Define Clientless SSL browser and client considerations/requirements
Identify and describe split tunneling requirements

Describe encryption, hashing, and Next Generation Encryption (NGE)

Compare and describe Symmetric and asymmetric key algorithms
Identify and describe the cryptographic process in VPNs – Diffie-Hellman, IPsec –ESP, AH, IKEv1, IKEv2,
Identify and describe the cryptographic process in VPNs hashing algorithms MD5 and SHA, and authentication methods
Describe and implement PKI components and protection methods
Describe Elliptic Curve Cryptography (ECC)
Compare and contrast SSL, DTLS, and TLS

CCNP Security

IMPLEMENTING CISCO THREAT CONTROL SOLUTIONS (300-207) SITCS

Learn Content Security Concepts

Describe Cisco ASA 5500-X NGFW Security Services like features and functionality
Implement web usage control (URL-filtering, reputation based, file filtering) on ASA
Implementation and verification of AVC and decryption policies on Cisco ASA 5500-X NGFW
Describe and learn traffic redirection and capture methods Cisco ASA 5500-X NGFW
Define Cloud Web Security its features and functionality
Implement Cloud Web Security IOS and ASA connectors
Implementation and verification of AnyConnect web security module
Describe web usage control Works
Implementation of AVC and anti-malware on Cisco Cloud Web Security

Describe Cisco WSA features and functionality

Implementation of data security on Cisco WSA
Implement WSA Identity and Authentication, including Transparent User Identification
Describe web usage control, AVC , anti-malware decryption policies traffic redirection and capture methods on WSA

Describe Cisco ESA features and functionality

Implementation of email encryption, anti-spam policies, virus outbreak filter on Cisco ESA
Implementation of DLP policies, anti-malware Implement inbound and outbound mail policies and authentication on ESA
Describe traffic redirection and various capture methods on Cisco ESA

Learn and implement Threat Defense

What is Network IPS
Configuration and Implementation of traffic redirection and capture methods
Implement various network IPS deployment modes
learn and Describe signatures engines
Implementation and verification of event actions & overrides/filters
Implementation of anomaly detection
Describe various risk ratings
Describe and learn about IOS IPS
Configure device hardening per best practices on IPS
Learn about Content Security appliances

Device GUIs and Secured CLI

learn Content Security
Implementation and verification of HTTPS and SSH access
Describe various configuration elements
Configure and Implement ESA GUI for message tracking

Troubleshooting, Monitoring, and Reporting Tools

Configure and test IME and IP logging for IPS
Describe and implement reporting functionality on Content Security
Configure and Implement the WSA Policy Trace tool
Implementation of the ESA Message Tracking tool
Implement the ESA Trace tool
How web interface is used to verify traffic is being redirected to CWS
Configure and implement CLI on IOS to verify CWS operations
Configure and implement CLI on ASA to verify CWS operations
Configure and implement PRSM Event Viewer to verify ASA NGFW operations
Describe various the PRSM Dashboards and Reports

Threat Defense Architectures

Design and Describe IPS solution
Deploy Inline or Promiscuous
Deploy and implement as IPS appliance, IPS software or hardware module or IOS IPS
Describe various methods of IPS appliance load-balancing
Describe why Traffic Symmetry is needed
Describe the Inline modes comparison – inline interface pair, inline VLAN pair, and inline VLAN group

Content Security Architectures

Design various Web Security solution
Compare ASA NGFW vs. WSA vs. CWS and its functions
Compare Physical WSA vs. Virtual WSA and its functions
List available CWS connectors
Design Email Security solution
Compare Physical ESA vs. Virtual ESA
Describe Hybrid mode
Design Application Security solution
Describe the need for application visibility and control