Implementing Cisco Edge Network Security Solutions (300-206)

Exam Description: The Implementing Cisco Edge Network Security (SENSS) (300-206) exam tests the knowledge of a network security engineer to configure and implement security on Cisco network perimeter edge devices such as a Cisco switch, Cisco router, and Cisco ASA firewall. This 90-minute exam consists of 65-75 questions and focuses on the technologies used to strengthen security of a network perimeter such as Network Address Translation (NAT), ASA policy and application inspect, and a zone-based firewall on Cisco routers. Candidates can prepare for this exam by taking the Cisco Edge Network Security (SENSS) course.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. In order to better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

1.0 Threat Defense

- 1.1 Implement firewall (ASA or IOS depending on which supports the implementation)
  - 1.1.a Implement ACLs
- 1.1.b Implement static/dynamic NAT/PAT
  - 1.1.c Implement object groups
  - 1.1.d Describe threat detection features
  - 1.1.e Implement botnet traffic filtering
  - 1.1.f Configure application filtering and protocol inspection
  - 1.1.g Describe ASA security contexts
- 1.2 Implement Layer 2 Security
  - 1.2.a Configure DHCP snooping
  - 1.2.b Describe dynamic ARP inspection
  - 1.2.c Describe storm control
  - 1.2.d Configure port security
  - 1.2.e Describe common Layer 2 threats and attacks and mitigation
  - 1.2.f Describe MACSec
  - 1.2.g Configure IP source verification
- 1.3 Configure device hardening per best practices
  - 1.3.a Routers
  - 1.3.b Switches
  - 1.3.c Firewalls

2.0 Cisco Security Devices GUIs and Secured CLI Management

- 2.1 Implement SSHv2, HTTPS, and SNMPv3 access on the network devices
- 2.2 Implement RBAC on the ASA/IOS using CLI and ASDM
- 2.3 Describe Cisco Prime Infrastructure
- 2.3.a Functions and use cases of Cisco Prime
- 2.3.b Device Management
- 2.4 Describe Cisco Security Manager (CSM)
- 2.4.a Functions and use cases of CSM
- 2.4.b Device Management
- 2.5 Implement Device Managers
- 2.5.a Implement ASA firewall features using ASDM

3.0 Management Services on Cisco Devices

- 3.1 Configure NetFlow exporter on Cisco Routers, Switches, and ASA
- 3.2 Implement SNMPv3
- 3.2.a Create views, groups, users, authentication, and encryption
- 3.3 Implement logging on Cisco Routers, Switches, and ASA using Cisco best practices
- 3.4 Implement NTP with authentication on Cisco Routers, Switches, and ASA
- 3.5 Describe CDP, DNS, SCP, SFTP, and DHCP

3.5.a Describe security implications of using CDP on routers and switches
3.5.b Need for dnssec

4.0 Troubleshooting, Monitoring and Reporting Tools

4.1 Monitor firewall using analysis of packet tracer, packet capture, and syslog
4.1.a Analyze packet tracer on the firewall using CLI/ASDM
4.1.b Configure and analyze packet capture using CLI/ASDM
4.1.c Analyze syslog events generated from ASA

5.0 Threat Defense Architectures

5.1 Design a Firewall Solution
5.1.a High-availability
5.1.b Basic concepts of security zoning
5.1.c Transparent & Routed Modes
5.1.d Security Contexts
5.2 Layer 2 Security Solutions
5.2.a Implement defenses against MAC, ARP, VLAN hopping, STP, and DHCP rogue attacks
5.2.b Describe best practices for implementation
5.2.c Describe how PVLANs can be used to segregate network traffic at Layer 2

6.0 Security Components and Considerations

6.1 Describe security operations management architectures
6.1.a Single device manager vs. multi-device manager
6.2 Describe Data Center security components and considerations
6.2.a Virtualization and Cloud security
6.3 Describe Collaboration security components and considerations
6.3.a Basic ASA UC Inspection features
6.4 Describe common IPv6 security considerations
6.4.a Unified IPv6/IPv4 ACL on the ASA

Implementing Cisco Secure Access Solutions (300-208)

Exam Description: The Implementing Cisco Secure Access Solutions (SISAS) (300-208) exam tests whether a network security engineer knows the components and architecture of secure access, by utilizing 802.1X and Cisco TrustSec. This 90-minute exam consists of 65–75 questions and assesses knowledge of Cisco Identity Services Engine (ISE) architecture, solution, and components as an overall network threat mitigation and endpoint control solutions. It also includes the fundamental concepts of bring your own device (BYOD) using posture and profiling services of ISE. Candidates can prepare for this exam by taking the Implementing Cisco Secure Access Solutions (SISAS) course.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. In order to better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

1.0 Identity Management and Secure Access

1.1 Implement device administration
1.1.a Compare and select AAA options
1.1.b TACACS+
1.1.c RADIUS
1.1.d Describe Native AD and LDAP
1.2 Describe identity management
1.2.a Describe features and functionality of authentication and authorization
1.2.b Describe identity store options (i.e., LDAP, AD, PKI, OTP, Smart Card, local)
1.2.c Implement accounting
1.3 Implement wired/wireless 802.1X
1.3.a Describe RADIUS flows
1.3.b AV pairs
1.3.c EAP types

1.3.d Describe supplicant, authenticator, and server
1.3.e Supplicant options
1.3.f 802.1X phasing (monitor mode, low impact, closed mode)
1.3.g AAA server
1.3.h Network access devices

1.4 Implement MAB
1.4.a Describe the MAB process within an 802.1X framework
1.4.b Flexible authentication configuration
1.4.c ISE authentication/authorization policies
1.4.d ISE endpoint identity configuration
1.4.e Verify MAB Operation

1.5 Implement network authorization enforcement
1.5.a dACL
1.5.b Dynamic VLAN assignment
1.5.c Describe SGA
1.5.d Named ACL
1.5.e CoA

1.6 Implement Central Web Authentication (CWA)
1.6.a Describe the function of CoA to support web authentication
1.6.b Configure authentication policy to facilitate CWA
1.6.c URL redirect policy
1.6.d Redirect ACL
1.6.e Customize web portal
1.6.f Verify central web authentication operation

1.7 Implement profiling
1.7.a Enable the profiling services

1.7.b Network probes
1.7.c IOS Device Sensor
1.7.d Feed service
1.7.e Profiling policy rules
1.7.f Utilize profile assignment in authorization policies
1.7.g Verify profiling operation

1.8 Implement guest services
1.8.a Managing sponsor accounts
1.8.b Sponsor portals
1.8.c Guest portals
1.8.d Guest Policies
1.8.e Self registration
1.8.f Guest activation
1.8.g Differentiated secure access
1.8.h Verify guest services operation

1.9 Implement posture services
1.9.a Describe the function of CoA to support posture services
1.9.b Agent options
1.9.c Client provisioning policy and redirect ACL
1.9.d Posture policy
1.9.e Quarantine/remediation
1.9.f Verify posture service operation

1.10 Implement BYOD access
1.10.a Describe elements of a BYOD policy
1.10.b Device registration
1.10.c My devices portal
1.10.d Describe supplicant provisioning

2.0 Threat Defense

2.1 Describe TrustSec Architecture

2.1.a SGT Classification – dynamic/static
2.1.b SGT Transport – inline tagging and SXP
2.1.c SGT Enforcement – SGACL and SGFW
2.1.d MACsec

3.0 Troubleshooting, Monitoring, and Reporting Tools

3.1 Troubleshoot identity management solutions

3.1.a Identify issues using authentication event details in Cisco ISE
3.1.b Troubleshoot using Cisco ISE diagnostic tools
3.1.c Troubleshoot endpoint issues
3.1.d Use debug commands to troubleshoot RADIUS and 802.1X on IOS switches and wireless controllers
3.1.e Troubleshoot backup operations

4.0 Threat Defense Architectures

4.1 Design highly secure wireless solution with ISE

4.1.a Identity Management
4.1.b 802.1X
4.1.c MAB
4.1.d Network authorization enforcement
4.1.e CWA
4.1.f Profiling
4.1.g Guest Services
4.1.h Posture Services
4.1.i BYOD Access

5.0 Design Identity Management Architectures

5.1 Device administration
5.2 Identity Management
5.3 Profiling
5.4 Guest Services
5.5 Posturing Services
5.6 BYOD Access

Implementing Cisco Secure Mobility Solutions (300-209)

Exam Description: The Implementing Cisco Secure Mobility Solutions (SIMOS) (300-209) exam tests a network security engineer on the variety of Virtual Private Network (VPN) solutions that Cisco has available on the Cisco ASA firewall and Cisco IOS software platforms. This 90-minute exam consists of 65–75 questions and assesses the knowledge necessary to properly implement highly secure remote communications through VPN technology, such as remote access SSL VPN and site-to-site VPN (DMVPN, FlexVPN). Candidates can prepare for this exam by taking the Implementing Cisco Secure Mobility Solutions (SIMOS) course.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. In order to better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

1.0 Secure Communications

1.1 Site-to-site VPNs on routers and firewalls

1.1.a Describe GETVPN
1.1.b Implement IPsec (with IKEv1 and IKEv2 for both IPV4 & IPV6)
1.1.c Implement DMVPN (hub-Spoke and spoke-spoke on both IPV4 & IPV6)
1.1.d Implement FlexVPN (hub-Spoke on both IPV4 & IPV6) using local AAA

1.2 Implement remote access VPNs

1.2.a Implement AnyConnect IKEv2 VPNs on ASA and routers
1.2.b Implement AnyConnect SSLVPN on ASA and routers

1.2.c Implement clientless SSLVPN on ASA and routers
1.2.d Implement FLEX VPN on routers

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

2.1 Troubleshoot VPN using ASDM & CLI

2.1.a Troubleshoot IPsec
2.1.b Troubleshoot DMVPN
2.1.c Troubleshoot FlexVPN
2.1.d Troubleshoot AnyConnect IKEv2 and SSL VPNs on ASA and routers
2.1.e Troubleshoot clientless SSLVPN on ASA and routers

3.0 Secure Communications Architectures

3.1 Design site-to-site VPN solutions

3.1.a Identify functional components of GETVPN, FlexVPN, DMVPN, and IPsec
3.1.b VPN technology considerations based on functional requirements
3.1.c High availability considerations
3.1.d Identify VPN technology based on configuration output

3.2 Design remote access VPN solutions

3.2.a Identify functional components of FlexVPN, IPsec, and Clientless SSL
3.2.b VPN technology considerations based on functional requirements
3.2.c High availability considerations
3.2.d Identify VPN technology based on configuration output
3.2.e Identify AnyConnect client requirements
3.2.f Clientless SSL browser and client considerations/requirements
3.2.g Identify split tunneling requirements

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

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

Implementing Cisco Threat Control Solutions (300-210)

1.0 Content Security

1.1 Cisco Cloud Web Security (CWS)

- 1.1.a Describe the features and functionality
- 1.1.b Implement the IOS and ASA connectors
- 1.1.c Implement the Cisco AnyConnect web security module
- 1.1.d Implement web usage control
- 1.1.e Implement AVC
- 1.1.f Implement antimalware
- 1.1.g Implement decryption policies

1.2 Cisco Web Security Appliance (WSA)

- 1.2.a Describe the features and functionality
- 1.2.b Implement data security
- 1.2.c Implement WSA identity and authentication, including transparent user identification
- 1.2.d Implement web usage control
- 1.2.e Implement AVC
- 1.2.f Implement antimalware and AMP
- 1.2.g Implement decryption policies
- 1.2.h Implement traffic redirection and capture methods (explicit proxy vs. transparent proxy)

1.3 Cisco Email Security Appliance

- 1.3.a Describe the features and functionality
- 1.3.b Implement email encryption
- 1.3.c Implement antispam policies
- 1.3.d Implement virus outbreak filter
- 1.3.e Implement DLP policies
- 1.3.f Implement antimalware and AMP
- 1.3.g Implement inbound and outbound mail policies and authentication
- 1.3.h Implement traffic redirection and capture methods
- 1.3.i Implement ESA GUI for message tracking

2.0 Network Threat Defense

2.1 Cisco Next-Generation Firewall (NGFW) Security Services

- 2.1.a Implement application awareness
- 2.1.b Implement access control policies (URL-filtering, reputation based, file filtering)
- 2.1.c Configure and verify traffic redirection
- 2.1.d Implement Cisco AMP for Networks

2.2 Cisco Advanced Malware Protection (AMP)

- 2.2.a Describe cloud detection technologies
- 2.2.b Compare and contrast AMP architectures (public cloud, private cloud)
- 2.2.c Configure AMP endpoint deployments
- 2.2.d Describe analysis tools
- 2.2.e Describe incident response functionality
- 2.2.f Describe sandbox analysis
- 2.2.g Describe AMP integration

3.0 Cisco FirePOWER Next-Generation IPS (NGIPS)

3.1 Configurations

3.2 Describe traffic redirection and capture methods

- 3.2.a Describe preprocessors and detection engines
- 3.2.b Implement event actions and suppression thresholds
- 3.2.c Implement correlation policies
- 3.2.d Describe SNORT rules
- 3.2.e Implement SSL decryption policies

3.3 Deployments

- 3.3.a Deploy inline or passive modes
- 3.3.b Deploy NGIPS as appliance, virtual appliance, or module within an ASA
- 3.3.c Describe the need for traffic symmetry
- 3.3.d Compare inline modes: inline interface pair and inline tap mode

4.0 Security Architectures

4.1 Design a web security solution

- 4.1.a Compare and contrast Cisco FirePOWER NGFW, WSA, and CWS
- 4.1.b Compare and contrast physical WSA and virtual WSA
- 4.1.c Describe the available CWS connectors

4.2 Design an email security solution

- 4.2.a Compare and contrast physical ESA and virtual ESA
- 4.2.b Describe hybrid mode

4.3 Design Cisco FirePOWER solutions

- 4.3.a Configure the virtual routed, switched, and hybrid interfaces
- 4.3.b Configure the physical routed interfaces

5.0 Troubleshooting, Monitoring, and Reporting Tools

5.1 Design a web security solution

- 5.1.a Compare and contrast FirePOWER NGFW, WSA, and CWS
- 5.1.b Compare and contrast physical WSA and virtual WSA
- 5.1.c Describe the available CWS connectors

5.2 Cisco Web Security Appliance (WSA)

- 5.2.a Implement the WSA Policy Trace tool
- 5.2.b Describe WSA reporting functionality
- 5.2.c Troubleshoot using CLI tools

5.3 Cisco Email Security Appliance (ESA)

- 5.3.a Implement the ESA Policy Trace tool
- 5.3.b Describe ESA reporting functionality
- 5.3.c Troubleshoot using CLI tools

5.4 Cisco FirePOWER

- 5.4.a Describe the Cisco FirePOWER Management Center dashboards and reports
- 5.4.b Implement health policy
- 5.4.c Configure email, SNMP, and syslog alerts
- 5.4.d Troubleshoot NGIPS using CLI tools