Implementing Cisco Edge Network Security Solution (SENSS) (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 Defence

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 Firewall

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 Analyse packet tracer on the firewall using CLI/ASDM
- 4.1.b Configure and analyse packet capture using CLI/ASDM
- 4.1.c Analyse syslog events generated from ASA

5.0 Threat Defence 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 defences 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 Centre security components and considerations

6.2.a Virtualisation 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