Cisco 300-206

Exam Name	Implementing Cisco Edge Network Security Solutions
Exam Number	300-206 SENSS
Practice Exam	**Cisco Certified Network Professional Security**

1 Implement firewall (ASA or IOS depending on which supports the implementation)

Threat Defense

a) Implement ACLs
b) Implement static/dynamic
NAT/PAT
c) Implement object groups
d) Describe threat detection features
e) Implement botnet traffic filtering
f) Configure application filtering and protocol inspection
g) Describe ASA security contexts

2 Implement Layer 2 Security
a) Configure DHCP snooping
b) Describe dynamic ARP inspection
c) Describe storm control
d) Configure port security
e) Describe common Layer 2 threats and attacks and mitigation
f) Describe MACSec
g) Configure IP source verification

3 Configure device hardening per best practices
a) Routers
b) Switches

c) Firewalls

Cisco Security Devices GUIs and Secured CLI Management

1 Implement SSHv2, HTTPS, and SNMPv3 access on the network devices
2 Implement RBAC on the ASA/IOS using CLI and ASDM

3 Describe Cisco Prime Infrastructure
a) Functions and use cases of Cisco Prime
b) Device Management

4 Describe Cisco Security Manager (CSM)
a) Functions and use cases of CSM
b) Device Management

5 Implement Device Managers

a) Implement ASA firewall features using ASDM

Management Services on Cisco Devices

1 Configure NetFlow exporter on Cisco Routers, Switches, and ASA

2 Implement SNMPv3
a) Create views, groups, users, authentication, and encryption

3 Implement logging on Cisco Routers, Switches, and ASA using Cisco best practices

4 Implement NTP with authentication on Cisco Routers, Switches, and ASA

5 Describe CDP, DNS, SCP, SFTP, and DHCP
a) Describe security implications of using CDP on routers and switches

b) Need for dnssec

Troubleshooting, Monitoring and Reporting Tools

1 Monitor firewall using analysis of packet tracer, packet capture, and syslog
a) Analyze packet tracer on the firewall using CLI/ASDM
b) Configure and analyze packet capture using CLI/ASDM

c) Analyze syslog events generated from ASA

Threat Defense Architectures

1 Design a Firewall Solution
a) High-availability
b) Basic concepts of security zoning
c) Transparent & Routed Modes
d) Security Contexts

2 Layer 2 Security Solutions
a) Implement defenses against MAC, ARP, VLAN hopping, STP, and DHCP rogue attacks
b) Describe best practices for implementation

c) Describe how PVLANs can be used to segregate network traffic at Layer 2

Security Components and Considerations

1 Describe security operations management architectures
a) Single device manager vs. multi-device manager

2 Describe Data Center security components and considerations
a) Virtualization and Cloud security

3 Describe Collaboration security components and considerations
a) Basic ASA UC Inspection features

4 Describe common IPv6 security considerations

a) Unified IPv6/IPv4 ACL on the ASA