CCNP Security

Cisco Certified Network Professional Security (CCNP Security) certification program is aligned specifically to the job role of the Cisco Network Security Engineer responsible for Security in Routers, Switches, Networking devices and appliances, as well as choosing, deploying, supporting and troubleshooting Firewalls, VPNS, and IDS/IPS solutions for their networking environments.

Prerequisites: Valid CCNA Security Certification or any CCIE Certification can act as a prerequisite.

Recommended Training: Implementing Cisco Secure Access Solutions (SISAS), Implementing Cisco Edge Network Security Solutions (SENSS), Implementing Cisco Secure Mobility Solutions (SIMOS), Implementing Cisco Threat Control Solutions (SITCS)

Exams : 300-208 SISAS, 300-206 SENSS, 300-209 SIMOS, 300-207 SITCS

Syllabus:

300-208 SISAS

1.0 Identity Management/Secure Access

- 1.1 Implement Device Administration
- 1.2 Describe Identity Management
- 1.3 Implement Wired/Wireless 802.1x
- 1.4 Implement MAB
- 1.5 Implement Network Authorization Enforcement
- 1.6 Implement central web authorization
- 1.7 Implement profiling
- 1.8 Implement guest services
- 1.9 Implement posturing
- 1.10 Implement BYOD access

2.0 Threat Defense

- 2.1 Implement Firewall

3.0 Troubleshooting, Monitoring and Reporting Tools

- 3.1 Troubleshoot identity management solutions

4.0 Threat Defense Architectures

- 4.1 Design secure wireless solution

5.0 Identity Management Architectures

- 5.1 Design AAA security solution
- 5.2 Design Profiling security solution
- 5.3 Design Posturing security solution
- 5.4 Design BYOD security solution
- 5.5 Design Device administration security solution
- 5.6 Design Guest services security solution

300-206 SENSS

1.0 Threat Defense

- 1.1 Implement Firewall
- 1.2 Implement Layer 2 security
- 1.3 Configure device hardening per best practices
- 1.4 Implement Firewalls

2.0 Cisco Security Devices GUIs and Secured CLI Management

- 2.1 Implement SSHv2, SSL, SNMPv3 access on the network devices
- 2.2 Implement RBAC on the ASA/IOS CLI and on ASDM
- 2.3 Describe Cisco Prime Infrastructure
- 2.4 Describe CSM
- 2.5 Implement device managers

3.0 Management Services on Cisco Devices

- 3.1 Implement NetFlow exporter
- 3.2 Implement SNMPv3
- 3.3 Implement logging
- 3.4 Implement NTP with authentication
- 3.5 Describe CDP, DNS, SCP, SFTP, and DHCP

4.0 Troubleshooting, Monitoring and Reporting Tools

- 4.1 Monitor firewall using analysis of packet tracer, packet capture, and syslog

5.0 Threat Defense Architectures

- 5.1 Design a firewall solution
- 5.2 Design Layer 2 security solution

6.0 Security Components and Considerations

- 6.1 Describe security operations management architecture
- 6.2 Describe Data Center Security components and considerations
- 6.3 Describe Collaboration security components and considerations
- 6.4 Describe common IPv6 security considerations

300-209 SIMOS

1.0 Secure Communications

- 1.1 Implement Site to Site VPNs on Routers and Firewalls
- 1.2 Implement remote access VPNs on Routers and Firewalls
- 1.3 Implement Site to Site VPNs on Routers and Firewall
- 1.4 Implement remote access VPNs on Routers and Firewalls

2.0 Troubleshooting, Monitoring and Reporting Tools

- 2.1 Analyze syslog and VPN debug logs via ASDM

3.0 Secure Communications Architectures

- 3.1 Design site-to-site VPN solution
- 3.2 Design remote access VPN solution
- 3.3 Describe encryption, hashing, iNGE

300-207 SITCS

1.0 Content Security

- 1.1 Implement Cisco CX
- 1.2 Implement Cisco Cloud Web Security
- 1.3 Implement Cisco WSA
- 1.4 Implement Cisco ESA

2.0 Threat Defense

- 2.1 Implement network IPS
- 2.2 Configure Device Hardening per Best Practices
- 2.3 Implement anomaly detection

3.0 Devices GUIs and Secured CLI

- 3.1 Implement Content Security

4.0 Troubleshooting, Monitoring and Reporting Tools

- 4.1 Configure IME and IP logging for IPS
- 4.2 Monitor Content Security
- 4.3 Monitor Cisco Security intelliShield

5.0 Threat Defense Architectures

- 5.1 CDesign IPS solution

6.0 Content Security Architectures

- 6.1 Design web security solution
- 6.2 Design email security solution
- 6.3 Design application security solution