Cisco Certified Network Professional (CCNP) Security

Course Outline

Module 1: Implementing Cisco Edge Network Security Solutions – SENSS

- Cisco Modular Network Security Architectures
- Deploy Cisco Infrastructure Management and Control Plane Security Controls
- Configuring Cisco Layer 2 and Layer 3 Data Plane Security Controls
- Cisco ASA Network Address Translations (NAT)
- Cisco IOS Software Network Address Translations (NAT)
- Cisco Threat Defense Solutions on a Cisco ASA
- Implementing Botnet Traffic Filters
- Deploying Cisco IOS Zone-Based Policy Firewalls (ZBFW)
- Configure and verify Cisco IOS ZBFW Application Inspection Policy

Module 2: Implementing Cisco Secure Mobility Solutions – SIMOS

- VPN Technologies and Deployments
- Implement and Maintain Cisco Site-to-Site VPN Solutions
- Cisco FlexVPN
- Implement and Maintain Cisco Clientless SSL VPNs
- Implement and Maintain Cisco AnyConnect SSL and IPsec VPNs
- Cisco Secure Endpoint and Dynamic Access Policies (DAP)

Module 3: Implementing Cisco Secure Access Solutions – SISAS

- Identity Services Engine Architecture and Access Control Capabilities
- Understand 802.1X Architecture, Implementation, and Operation
- Extensible Authentication Protocols (EAP)
- Public-Key Infrastructure with ISE
- Internal and External Authentication Databases
- MAC Authentication Bypass
- Implement Identity-Based Authorization Policies
- Cisco TrustSec Features
- Web Authentication and Guest Access
- ISE Posture Service
- ISE Profiling
- Understand Bring Your Own Device (BYOD) with ISE
- Troubleshoot ISE

Module 4: Implementing Cisco Threat Control Solutions – SITCS

- Understand Cisco ASA Next-Generation Firewall (NGFW)
- Deploy Cisco Web Security Appliance to Mitigate Malware
- Configure Web Security Appliance for Acceptable Use Controls
- Configure Cisco Cloud Web Security Connectors
- Describe Cisco Email Security Solution
- Configure Cisco Email Appliance Incoming and Outgoing Policies
- IPS Threat Controls
- Cisco IPS Sensor into a Network