Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

CCNP Security - Cisco Certified Network Professional-Security

SecureNinja's fifteen (15) day CCNP Security Boot Camp will prepare you to take the required 4 certification exams for the CCNP Security Certification. The 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.

Course Completion

Upon completing this course, you will be able to meet these overall objectives:

- Understand Cisco Identity Services Engine architecture and access control capabilities
- Understand 802.1X architecture, implementation, and operation
- Understand commonly implemented Extensible Authentication Protocols (EAP)
- Implement Public-Key Infrastructure with ISE
- Understand the implement Internal and External authentication databases
- Implement MAC Authentication Bypass
- Implement identity-based authorization policies
- Understand Cisco TrustSec features
- Implement Web Authentication and Guest Access
- Implement ISE Posture service
- Implement ISE Profiling
- Understand Bring Your Own Device (BYOD) with ISE
- Troubleshoot ISE
- Understand the current security threat landscape
- Understanding and implementing Cisco modular Network Security Architectures such as SecureX and TrustSec
- Deploy Cisco Infrastructure management and control plane security controls
- Configuring Cisco layer 2 and layer 3 data plane security controls
- Implement and maintain Cisco ASA Network Address Translations (NAT)
- Implement and maintain Cisco IOS Software Network Address Translations (NAT)
- Designing and deploying Cisco Threat Defense solutions on a Cisco ASA utilizing access policy and application and identity-based inspection
- Implementing Botnet Traffic Filters
- Deploying Cisco IOS Zone-Based Policy Firewalls (ZBFW)
- Configure and verify Cisco IOS ZBFW Application Inspection Policy
- Describe the various VPN technologies and deployments as well as the cryptographic algorithms and protocols that provide VPN security.
- Implement and maintain Cisco site-to-site VPN solutions.
- Implement and maintain Cisco FlexVPN in point-to-point, hub-and-spoke, and spoke-to-spoke IPsec VPNs.
- Implement and maintain Cisco clientless SSL VPNs.
- Implement and maintain Cisco AnyConnect SSL and IPsec VPNs.

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

- Implement and maintain endpoint security and dynamic access policies (DAP)
- 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
- Describe IPS Threat Controls
- Configure and Implement Cisco IPS Sensor into a Network

Prerequisites

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

Required Exams

- 300-208 SISAS Implementing Cisco Secure Access Solutions (SISAS)
- 300-206 SENSS Implementing Cisco Edge Network Security Solutions (SENSS)
- 300-209 SIMOS Implementing Cisco Secure Mobility Solutions (SIMOS)
- 300-207 SITCS Implementing Cisco Threat Control Solutions (SITCS)

Course Length

120 Hours