Cisco Certified Network Professional-Security (300-206)

Threat Defense

- Implement firewall (ASA or IOS depending on which supports the implementation)
- Implement ACLs
- Implement static/dynamic NAT/PAT
- Implement object groups
- Describe threat detection features
- Implement botnet traffic filtering
- Configure application filtering and protocol inspection
- Describe ASA security contexts
- Implement Layer 2 Security
- Configure DHCP snooping
- Describe dynamic ARP inspection
- Describe storm control
- Configure port security
- Describe common Layer 2 threats and attacks and mitigation
- Describe MACSec
- Configure IP source verification
- Configure device hardening per best practices
- Routers
- Switches
- Firewalls

Cisco Security Devices GUIs and Secured CLI Management

- Implement SSHv2, HTTPS, and SNMPv3 access on the network devices
- Implement RBAC on the ASA/IOS using CLI and ASDM
- Describe Cisco Prime Infrastructure
- Functions and use cases of Cisco Prime
- Device Management
- Describe Cisco Security Manager (CSM)
- Functions and use cases of CSM
- Device Management
- Management Services on Cisco Devices
- Configure NetFlow exporter on Cisco Routers, Switches, and ASA
- Implement SNMPv3
- Create views, groups, users, authentication, and encryption
- Implement logging on Cisco Routers, Switches, and ASA using Cisco best practices
- Implement NTP with authentication on Cisco Routers, Switches, and ASA
- Describe CDP, DNS, SCP, SFTP, and DHCP
- Describe security implications of using CDP on routers and switches
- Need for dnssec
- Troubleshooting, Monitoring and Reporting Tools

- Monitor firewall using analysis of packet tracer, packet capture, and syslog
- Analyze packet tracer on the firewall using CLI/ASDM
- Configure and analyze packet capture using CLI/ASDM
- Analyze syslog events generated from ASA
- Threat Defense Architectures
- Design a Firewall Solution
- High-availability
- Basic concepts of security zoning
- Transparent & Routed Modes
- Security Contexts
- Layer 2 Security Solutions
- Implement defenses against MAC, ARP, VLAN hopping, STP, and DHCP rogue attacks
- Describe best practices for implementation
- Describe how PVLANs can be used to segregate network traffic at Layer 2
- Security Components and Considerations
- Describe security operations management architectures
- Single device manager vs. multi-device manager
- Describe Data Center security components and considerations
- Virtualization and Cloud security
- Describe Collaboration security components and considerations
- Basic ASA UC Inspection features
- Describe common IPv6 security considerations
- Unified IPv6/IPv4 ACL on the ASA

cisco certified network professional-security(300-207)

Content Security

- Cisco ASA 5500-X NGFW Security Services
- Describe features and functionality
- Implement web usage control (URL-filtering, reputation based, file filtering)
- Implement AVC
- Implement decryption policies
- Describe traffic redirection and capture methods
- Cisco Cloud Web Security
- Describe features and functionality
- Implement IOS and ASA connectors
- Implement AnyConnect web security module
- Describe web usage control
- Implement AVC
- Implement anti-malware
- Describe decryption policies
- Cisco WSA
- Describe features and functionality
- Implement data security

- Implement WSA Identity and Authentication, including Transparent User Identification
- Describe web usage control
- Implement AVC
- Implement anti-malware
- Describe decryption policies
- Describe traffic redirection and capture methods (Explicit Proxy vs. Transparent Proxy)

Cisco ESA

- Describe features and functionality
- Implement email encryption
- Implement anti-spam policies
- Implement virus outbreak filter
- Implement DLP policies
- Implement anti-malware
- Implement inbound and outbound mail policies and authentication
- Describe traffic redirection and capture methods

Threat Defense

- Network IPS
- Implement traffic redirection and capture methods
- Implement network IPS deployment modes
- Describe signatures engines
- Implement event actions & overrides/filters
- Implement anomaly detection
- Implement risk ratings
- Describe IOS IPS
- Configure device hardening per best practices
- IPS
- Content Security appliances

Device GUIs and Secured CLI

- Content Security
- Implement HTTPS and SSH access
- Describe configuration elements
- Implement ESA GUI for message tracking

Troubleshooting, Monitoring, and Reporting Tools

- Configure IME and IP logging for IPS
- Content Security
- Describe reporting functionality
- Implement the WSA Policy Trace tool
- Implement the ESA Message Tracking tool
- Implement the ESA Trace tool
- Use web interface to verify traffic is being redirected to CWS
- Use CLI on IOS to verify CWS operations
- Use CLI on ASA to verify CWS operations
- Use the PRSM Event Viewer to verify ASA NGFW operations

- Describe the PRSM Dashboards and Reports
- Monitor Cisco Security IntelliShield

Threat Defense Architectures

- Design IPS solution
- Deploy Inline or Promiscuous
- Deploy as IPS appliance, IPS software or hardware module or IOS IPS
- Describe methods of IPS appliance load-balancing
- Describe the need for Traffic Symmetry
- Inline modes comparison – inline interface pair, inline VLAN pair, and inline VLAN group
- Management options

Content Security Architectures

- Design Web Security solution
- Compare ASA NGFW vs. WSA vs. CWS
- Compare Physical WSA vs. Virtual WSA
- List available CWS connectors
- Design Email Security solution
- Compare Physical ESA vs. Virtual ESA
- Describe Hybrid mode
- Design Application Security solution
- Describe the need for application visibility and control

cisco certified network professional - security(300-208)

Identity Management and Secure Access

- Implement device administration
- Compare and select AAA options
- TACACS+
- RADIUS
- Describe Native AD and LDAP
- Describe identity management
- Describe features and functionality of authentication and authorization
- Describe identity store options (i.e., LDAP, AD, PKI, OTP, Smart Card, local)
- Implement accounting
- Implement wired/wireless 802.1X
- Describe RADIUS flows
- AV pairs
- EAP types
- Describe supplicant, authenticator, and server
- Supplicant options
- 802.1X phasing (monitor mode, low impact, closed mode)
- AAA server
- Network access devices
- Implement MAB
- Describe the MAB process within an 802.1X framework
- Flexible authentication configuration

- ISE authentication/authorization policies
- ISE endpoint identity configuration
- Verify MAB Operation
- Describe identity management
- Describe features and functionality of authentication and authorization Describe identity store options (i.e., LDAP, AD, PKI, OTP, Smart Card, local) Implement accounting
- Implement wired/wireless 802.1X
- Describe RADIUS flows
- AV pairs
- EAP types
- Describe supplicant, authenticator, and server
- Supplicant options
- 802.1X phasing (monitor mode, low impact, closed mode)
- AAA server
- Network access devices
- Implement MAB
- Describe the MAB process within an 802.1X framework
- Flexible authentication configuration
- ISE authentication/authorization policies
- ISE endpoint identity configuration
- Verify MAB Operation

Threat Defense

- Describe TrustSec Architecture
- SGT Classification – dynamic/static
- SGT Transport – inline tagging and SXP
- SGT Enforcement – SGACL and SGFW
- MACsec

Troubleshooting, Monitoring, and Reporting Tools

- Troubleshoot identity management solutions
- Identify issues using authentication event details in Cisco ISE
- Troubleshoot using Cisco ISE diagnostic tools
- Troubleshoot endpoint issues
- Use debug commands to troubleshoot RADIUS and 802.1X on IOS switches and wireless controllers
- Troubleshoot backup operations

Threat Defense Architectures

- Design highly secure wireless solution with ISE
- Identity Management
- 802.1X
- MAB
- Network authorization enforcement
- CWA
- Profiling
- Guest Services

- Posture Services
- BYOD Access
- Design Identity Management Architectures
- Device administration
- Identity Management
- Profiling
- Guest Services
- Posturing Services
- BYOD Access

cisco certified network professional-security(300-209)

Secure Communications

- Site-to-site VPNs on routers and firewalls
- Describe GETVPN
- Implement IPsec (with IKEv1 and IKEv2 for both IPV4 & IPV6)
- Implement DMVPN (hub-Spoke and spoke-spoke on both IPV4 & IPV6)
- Implement FlexVPN (hub-Spoke on both IPV4 & IPV6) using local AAA
- Implement remote access VPNs
- Implement AnyConnect IKEv2 VPNs on ASA and routers
- Implement AnyConnect SSLVPN on ASA and routers
- Implement clientless SSLVPN on ASA and routers
- Implement FLEX VPN on routers

Troubleshooting, Monitoring, and Reporting Tools

- Troubleshoot VPN using ASDM & CLI
- Troubleshoot IPsec
- Troubleshoot DMVPN
- Troubleshoot FlexVPN
- Troubleshoot AnyConnect IKEv2 and SSL VPNs on ASA and routers
- Troubleshoot clientless SSLVPN on ASA and routers

Secure Communications Architectures

- Design site-to-site VPN solutions
- Identify functional components of GETVPN, FlexVPN, DMVPN, and IPsec
- VPN technology considerations based on functional requirements
- High availability considerations
- Identify VPN technology based on configuration output

Batch Timing : 7 - 9 am/9 - 11am/11 – 1pm/ 2 – 4pm /4– 6pm / 6 – 8pm / Sat & Sun Only / Sunday Only.

IndiaOptionsSoftwares Pvt Ltd

ISO 9001:2008 Certified

India's No.1 Training Centre

Kochi : Deshabimani Junction,Kaloor,Cochin-17 Ph: 0484-2 53 63 03/04

E-Mail : **info@indiaoptions.in** facebook.com/indiaoption