Install and configure a security appliance for basic network connectivity

- Describe the Security Appliance hardware and software architecture
- Determine the Security Appliance hardware and software configuration and verify if it is correct
- Use setup or the CLI to configure basic network settings, including interface configurations
- Use appropriate show commands to verify initial configurations
- Configure NAT and global addressing to meet user requirements
- Configure DHCP client option
- Set default route
- Configure logging options
- Describe the firewall technology
- Explain the information contained in syslog files
- Configure static address translations
- Configure Network Address Translations: PAT
- Configure static port redirection
- Configure a net static
- Set embryonic and connection limits on the security appliance
- Verify network address translation operation

Configure a security appliance to restrict inbound traffic from untrusted sources

- Configure access-lists to filter traffic based on address, time, and protocols
- Configure object-groups to optimize access-list processing
- Configure Network Address Translations: Nat0
- Configure Network Address Translations: Policy NAT
- Configure java/activeX filtering
- Configure URL filtering
- Verify inbound traffic restrictions

Configure a security appliance to provide secure connectivity using site-to-site VPNs

- Explain certificates, certificate authorities and how they are used
- Explain the basic functionality of IPSec
- Configure IKE with preshared keys
- Configure IKE to use certificates
- Differentiate between the types of encryption
- Configure IPSec parameters
- Configure crypto-maps and ACLs

Configure a security appliance to provide secure connectivity using remote access VPNs

- Explain the functions of EasyVPN
- Configure IPSec using EasyVPN Server/Client
- Configure the Cisco Secure VPN client
- Explain the purpose of WebVPN
- Configure WebVPN services: Server/Client
- Verify VPN operations

Configure transparent firewall, virtual firewall, and high availability firewall features on a security appliance

- Explain differences between L2 and L3 operating modes
- Configure security appliance for transparent mode (L2)
- Explain purpose of virtual firewalls
- Configure security appliance to support virtual firewall
- Monitor and maintain virtual firewall
- Explain the types, purpose and operation of fail-over
- Install appropriate topology to support cable-based or LAN-based fail-over
- Explain the hardware, software and licensing requirements for high-availability
- Configure the SA for active/standby fail-over
- Configure the SA for stateful fail-over
- Configure the SA for active-active fail-over
- Verify fail-over operation
- Recover from a fail-over

Configure AAA services for access through a security appliance

- Configure ACS for security appliance support
- Configure security appliance to use AAA feature
- Configure authentication using both local and external databases
- Configure authorization using an external database
- Configure the ACS server for downloadable ACLs
- Configure accounting of connection start/stop
- Verify AAA operation

Configure routing and switching on a security appliance

- Enable DHCP server and relay functionality
- Configure VLANs on a security appliance interface
- Configure routing functionality of security appliance including OSPF, RIP
- Configure security appliance to pass multi-cast traffic
- Configure ICMP on the security appliance

Configure a modular policy on a security appliance

- Configure a class-map
- Configure a policy-map
- Configure a service-policy
- Configure a ftp-map
- Configure a http-map
- Configure an inspection protocol
- Explain the function of protocol inspection
- Explain DNS guard feature
- Describe the AIP-SSM HW and SW
- Load IPS SW on the AIP-SSM
- Verify AIP-SSM
- Configure an IPS modular policy

Monitor and manage an installed security appliance

- Obtain and apply OS updates
- Backup and restore configurations and software
- Explain the security appliance file management system
- Perform password/lockout recovery procedures
- Obtain and upgrade license keys
- Configure passwords for various access methods: Telnet, serial, enable, SSH
- Configure various access methods: Telnet, SSH, PDM
- Configure command authorization and privilege levels
- Configure local username database
- Verify access control methods
- Enable ASDM functionality
- Verify a security appliance configuration via ASDM
- Verify the licensing available on a security appliance