

I. Implement secure networks using Cisco ASA Firewalls

- A. Perform basic firewall Initialization
- B. Configure device management
- C. Configure address translation (nat, global, static)
- D. Configure ACLs
- E. Configure IP routing
- F. Configure object groups
- G. Configure VLANs
- H. Configure filtering
- I. Configure failover
- J. Configure Layer 2 Transparent Firewall
- K. Configure security contexts (virtual firewall)
- L. Configure Modular Policy Framework
- M. Configure Application-Aware Inspection
- N. Configure high availability solutions
- O. Configure QoS policies

II. Implement secure networks using Cisco IOS Firewalls

- A. Configure CBAC
- B. Configure Zone-Based Firewall
- C. Configure Audit
- D. Configure Auth Proxy
- E. Configure PAM
- F. Configure access control
- G. Configure performance tuning
- H. Configure advanced IOS Firewall features

III. Implement secure networks using Cisco VPN solutions

- A. Configure IPsec LAN-to-LAN (IOS/ASA)
- B. Configure SSL VPN (IOS/ASA)
- C. Configure Dynamic Multipoint VPN (DMVPN)
- D. Configure Group Encrypted Transport (GET) VPN
- E. Configure Easy VPN (IOS/ASA)
- F. Configure CA (PKI)
- G. Configure Remote Access VPN
- H. Configure Cisco Unity Client
- I. Configure Clientless WebVPN
- J. Configure AnyConnect VPN
- K. Configure XAuth, Split-Tunnel, RRI, NAT-T
- L. Configure High Availability
- M. Configure QoS for VPN
- N. Configure GRE, mGRE
- O. Configure L2TP
- P. Configure advanced Cisco VPN features

IV. Configure Cisco IPS to mitigate network threats

- A. Configure IPS 4200 Series Sensor Appliance
- B. Initialize the Sensor Appliance
- C. Configure Sensor Appliance management
- D. Configure virtual Sensors on the Sensor Appliance
- E. Configure security policies
- F. Configure promiscuous and inline monitoring on the Sensor Appliance
- G. Configure and tune signatures on the Sensor Appliance
- H. Configure custom signatures on the Sensor Appliance
- I. Configure blocking on the Sensor Appliance
- J. Configure TCP resets on the Sensor Appliance
- K. Configure rate limiting on the Sensor Appliance
- L. Configure signature engines on the Sensor Appliance
- M. Use IDM to configure the Sensor Appliance
- N. Configure event action on the Sensor Appliance
- O. Configure event monitoring on the Sensor Appliance
- P. Configure advanced features on the Sensor Appliance
- Q. Configure and tune Cisco IOS IPS
- R. Configure SPAN & RSPAN on Cisco switches

V. Implement Identity Management

- A. Configure RADIUS and TACACS+ security protocols
- B. Configure LDAP
- C. Configure Cisco Secure ACS
- D. Configure certificate-based authentication
- E. Configure proxy authentication
- F. Configure 802.1x
- G. Configure advanced identity management features
- H. Configure Cisco NAC Framework

VI. Implement Control Plane and Management Plane Security

- A. Implement routing plane security features (protocol authentication, route filtering)
- B. Configure Control Plane Policing
- C. Configure CP protection and management protection
- D. Configure broadcast control and switchport security
- E. Configure additional CPU protection mechanisms (options drop, logging interval)
- F. Disable unnecessary services
- G. Control device access (Telnet, HTTP, SSH, Privilege levels)
- H. Configure SNMP, Syslog, AAA, NTP
- I. Configure service authentication (FTP, Telnet, HTTP, other)
- J. Configure RADIUS and TACACS+ security protocols
- K. Configure device management and security

VII. **Configure Advanced Security**

- A. Configure mitigation techniques to respond to network attacks
- B. Configure packet marking techniques
- C. Implement security RFCs (RFC1918/3330, RFC2827/3704)
- D. Configure Black Hole and Sink Hole solutions
- E. Configure RTBH filtering (Remote Triggered Black Hole)
- F. Configure Traffic Filtering using Access-Lists
- G. Configure IOS NAT
- H. Configure TCP Intercept
- I. Configure uRPF
- J. Configure CAR
- K. Configure NBAR
- L. Configure NetFlow
- M. Configure Anti-Spoofing solutions
- N. Configure Policing
- O. Capture and utilize packet captures
- P. Configure Transit Traffic Control and Congestion Management
- Q. Configure Cisco Catalyst advanced security features

VIII. **Identify and Mitigate Network Attacks**

- A. Identify and protect against fragmentation attacks
- B. Identify and protect against malicious IP option usage
- C. Identify and protect against network reconnaissance attacks
- D. Identify and protect against IP spoofing attacks
- E. Identify and protect against MAC spoofing attacks
- F. Identify and protect against ARP spoofing attacks
- G. Identify and protect against Denial of Service (DoS) attacks
- H. Identify and protect against Distributed Denial of Service (DDoS) attacks
- I. Identify and protect against Man-in-the-Middle (MiM) attacks
- J. Identify and protect against port redirection attacks
- K. Identify and protect against DHCP attacks
- L. Identify and protect against DNS attacks
- M. Identify and protect against Smurf attacks
- N. Identify and protect against SYN attacks
- O. Identify and protect against MAC Flooding attacks
- P. Identify and protect against VLAN hopping attacks
- Q. Identify and protect against various Layer2 and Layer3 attacks