CCIE Security Lab Exam Exam Topics *(blueprint)*v3.0

This lab exam blueprint v3.0 is a detailed outline of the topics likely to appear on the lab exam effective mid-April 2009. Knowledge of troubleshooting is an important skill and candidates are expected to diagnose and solve issues as part of the CCIE lab exam. The topics listed are guidelines and other relevant or related topics may also appear. Candidates for lab exams scheduled in mid April'09 or later should prepare using the v3.0 blueprints below.

In general, new product features become eligible for testing on CCIE lab exams six months after general release.

1. **Implement secure networks using Cisco ASA Firewalls**

1. Perform basic firewall Initialization
2. Configure device management
3. Configure address translation (nat, global, static)
4. Configure ACLs
5. Configure IP routing
6. Configure object groups
7. Configure VLANs
8. Configure filtering
9. Configure failover
10. Configure Layer 2 Transparent Firewall
11. Configure security contexts (virtual firewall)
12. Configure Modular Policy Framework
13. Configure Application-Aware Inspection
14. Configure high availability solutions
15. Configure QoS policies

2. **Implement secure networks using Cisco IOS Firewalls**

1. Configure CBAC
2. Configure Zone-Based Firewall
3. Configure Audit
4. Configure Auth Proxy
5. Configure PAM
6. Configure access control
7. Configure performance tuning
8. Configure advanced IOS Firewall features

3. **Implement secure networks using Cisco VPN solutions**

1. Configure IPsec LAN-to-LAN (IOS/ASA)
2. Configure SSL VPN (IOS/ASA)
3. Configure Dynamic Multipoint VPN (DMVPN)

4. Configure Group Encrypted Transport (GET) VPN
5. Configure Easy VPN (IOS/ASA)
6. Configure CA (PKI)
7. Configure Remote Access VPN
8. Configure Cisco Unity Client
9. Configure Clientless WebVPN
10. Configure AnyConnect VPN
11. Configure XAuth, Split-Tunnel, RRI, NAT-T
12. Configure High Availability
13. Configure QoS for VPN
14. Configure GRE, mGRE
15. Configure L2TP
16. Configure advanced Cisco VPN features

4. **Configure Cisco IPS to mitigate network threats**

1. Configure IPS 4200 Series Sensor Appliance
2. Initialize the Sensor Appliance
3. Configure Sensor Appliance management
4. Configure virtual Sensors on the Sensor Appliance
5. Configure security policies
6. Configure promiscuous and inline monitoring on the Sensor Appliance
7. Configure and tune signatures on the Sensor Appliance
8. Configure custom signatures on the Sensor Appliance
9. Configure blocking on the Sensor Appliance
10. Configure TCP resets on the Sensor Appliance
11. Configure rate limiting on the Sensor Appliance
12. Configure signature engines on the Sensor Appliance
13. Use IDM to configure the Sensor Appliance
14. Configure event action on the Sensor Appliance
15. Configure event monitoring on the Sensor Appliance
16. Configure advanced features on the Sensor Appliance
17. Configure and tune Cisco IOS IPS
18. Configure SPAN & RSPAN on Cisco switches

5. **Implement Identity Management**

1. Configure RADIUS and TACACS+ security protocols
2. Configure LDAP
3. Configure Cisco Secure ACS
4. Configure certificate-based authentication
5. Configure proxy authentication
6. Configure 802.1x
7. Configure advanced identity management features

8. Configure Cisco NAC Framework

6. **Implement Control Plane and Management Plane Security**

1. Implement routing plane security features (protocol authentication, route filtering)
2. Configure Control Plane Policing
3. Configure CP protection and management protection
4. Configure broadcast control and switchport security
5. Configure additional CPU protection mechanisms (options drop, logging interval)
6. Disable unnecessary services
7. Control device access (Telnet, HTTP, SSH, Privilege levels)
8. Configure SNMP, Syslog, AAA, NTP
9. Configure service authentication (FTP, Telnet, HTTP, other)
10. Configure RADIUS and TACACS+ security protocols
11. Configure device management and security

7. **Configure Advanced Security**

1. Configure mitigation techniques to respond to network attacks
2. Configure packet marking techniques
3. Implement security RFCs (RFC1918/3330, RFC2827/3704)
4. Configure Black Hole and Sink Hole solutions
5. Configure RTBH filtering (Remote Triggered Black Hole)
6. Configure Traffic Filtering using Access-Lists
7. Configure IOS NAT
8. Configure TCP Intercept
9. Configure uRPF
10. Configure CAR
11. Configure NBAR
12. Configure NetFlow
13. Configure Anti-Spoofing solutions
14. Configure Policing
15. Capture and utilize packet captures
16. Configure Transit Traffic Control and Congestion Management
17. Configure Cisco Catalyst advanced security features

8. **Identify and Mitigate Network Attacks**

1. Identify and protect against fragmentation attacks
2. Identify and protect against malicious IP option usage
3. Identify and protect against network reconnaissance attacks
4. Identify and protect against IP spoofing attacks
5. Identify and protect against MAC spoofing attacks
6. Identify and protect against ARP spoofing attacks
7. Identify and protect against Denial of Service (DoS) attacks

8. Identify and protect against Distributed Denial of Service (DDoS) attacks
9. Identify and protect against Man-in-the-Middle (MiM) attacks
10. Identify and protect against port redirection attacks
11. Identify and protect against DHCP attacks
12. Identify and protect against DNS attacks
13. Identify and protect against Smurf attacks
14. Identify and protect against SYN attacks
15. Identify and protect against MAC Flooding attacks
16. Identify and protect against VLAN hopping attacks
17. Identify and protect against various Layer2 and Layer3 attacks