2008年9月CCIE安全认证升级后最新Lab考点Cisco认证考试
 Implement secure networks using Cisco ASA Firewalls Perform basic firewall Initialization Configure device management Configure address translation (nat, global, static) Configure ACLs Configure IP routing Configure object groups Configure VLANs Configure filtering Configure failover Configure Layer 2 Transparent Firewall Configure security contexts (virtual firewall) Configure Modular Policy Framework Configure Application-Aware Inspection Configure high availability solutions Configure QoS policies Implement secure networks using Cisco IOS Firewalls Configure CBAC Configure Zone-Based Firewall Configure Audit Configure Auth Proxy Configure PAM Configure access control Configure performance tuning Configure advanced IOS Firewall features Implement secure networks using Cisco VPN solutions Configure IPsec LAN-to-LAN (IOS/ASA) Configure SSL VPN (IOS/ASA) Configure Dynamic Multipoint VPN (DMVPN) Configure Group Encrypted Transport (GET) VPN Configure Easy VPN (IOS/ASA) Configure CA (PKI) Configure Remote Access VPN Configure Cisco Unity Client Configure Clientless WebVPN Configure AnyConnect VPN Configure XAuth, Split-Tunnel, RRI, NAT-T Configure High Availability Configure QoS for VPN Configure GRE, mGRE Configure L2TP Configure advanced Cisco VPN features Configure Cisco IPS to mitigate network threats Configure IPS 4200 Series Sensor Appliance Initialize the Sensor

Appliance Configure Sensor Appliance management Configure virtual Sensors on the Sensor Appliance Configure security policies Configure promiscuous and inline monitoring on the Sensor Appliance Configure and tune signatures on the Sensor Appliance Configure custom signatures on the Sensor Appliance Configure blocking on the Sensor Appliance Configure TCP resets on the Sensor Appliance Configure rate limiting on the Sensor Appliance Configure signature engines on the Sensor Appliance Use IDM to configure the Sensor Appliance Configure event action on the Sensor Appliance Configure event monitoring on the Sensor Appliance Configure advanced features on the Sensor Appliance Configure and tune Cisco IOS IPS Configure SPAN &amp. RSPAN on Cisco switches Implement Identity Management Configure RADIUS and TACACS security protocols Configure LDAP Configure Cisco Secure ACS Configure certificate-based authentication Configure proxy authentication Configure 802.1x Configure advanced identity management features Configure Cisco NAC Framework Implement Control Plane and Management Plane Security Implement routing plane security features (protocol authentication, route filtering) Configure Control Plane Policing Configure CP protection and management protection Configure broadcast control and switchport security Configure additional CPU protection mechanisms (options 0drop, logging interval) Disable unnecessary services Control device access (Telnet, HTTP, SSH, Privilege levels) Configure SNMP, Syslog, AAA, NTP Configure service authentication (FTP, Telnet, HTTP, other) Configure

RADIUS and TACACS security protocols Configure device management and security Configure Advanced Security Configure mitigation techniques to respond to network attacks Configure packet marking techniques Implement security RFCs (RFC1918/3330, RFC2827/3704) Configure Black Hole and Sink Hole solutions Configure RTBH filtering (Remote Triggered Black Hole) Configure Traffic Filtering using Access-Lists Configure IOS NAT Configure TCP Intercept Configure uRPF Configure CAR Configure NBAR Configure NetFlow Configure Anti-Spoofing solutions Configure Policing Capture and utilize packet captures Configure Transit Traffic Control and Congestion Management Configure Cisco Catalyst advanced security features Identify and Mitigate Network Attacks Identify and protect against fragmentation attacks Identify and protect against malicious IP option usage Identify and protect against network reconnaissance attacks Identify and protect against IP spoofing attacks Identify and protect against MAC spoofing attacks Identify and protect against ARP spoofing attacks Identify and protect against Denial of Service (DoS) attacks Identify and protect against Distributed Denial of Service (DDoS) attacks Identify and protect against Man-in-the-Middle (MiM) attacks Identify and protect against port redirection attacks Identify and protect against DHCP attacks Identify and protect against DNS attacks Identify and protect against Smurf attacks Identify and protect against SYN attacks Identify and protect against MAC Flooding attacks Identify and protect against VLAN hopping attacks Identify and protect against various Layer2 and Layer3 attacks