CCIE Security Lab Exam version 4.0

Exam Description: The Cisco CCIE® Security Lab Exam version 4.0 is an 8-hour practical hands-on exam that tests the skills and competencies of security professionals in terms of configuring and troubleshooting Cisco security products and solutions.

Candidates may be required to perform implementation, optimization and troubleshooting actions in each of the exam topic sections. Content may include both IPv4 and IPv6 concepts and applications.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. In order to better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

14%	**1.0**	**System Hardening and Availability**
	1.1	Routing plane security features (for example, protocol authentication and route filtering)
	1.2	Control Plane Policing
	1.3	Control plane protection and management plane protection
	1.4	Broadcast control and switch port security
	1.5	Additional CPU protection mechanisms (for example, options drop and logging interval)
	1.6	Disable unnecessary services
	1.7	Control device access (for example, Telnet, HTTP, SSH, and privilege levels)
	1.8	Device services (for example, SNMP, syslog, and NTP)
	1.9	Transit traffic control and congestion management
14%	**2.0**	**Threat Identification and Mitigation**
	2.1	Identify and protect against fragmentation attacks
	2.2	Identify and protect against malicious IP option usage
	2.3	Identify and protect against network reconnaissance attacks
	2.4	Identify and protect against IP spoofing attacks
	2.5	Identify and protect against MAC spoofing attacks
	2.6	Identify and protect against ARP spoofing attacks
	2.7	Identify and protect against DoS attacks
	2.8	Identify and protect against DDoS attacks
	2.9	Identify and protect against man-in-the-middle attacks
	2.10	Identify and protect against port redirection attacks
	2.11	Identify and protect against DHCP attacks
	2.12	Identify and protect against DNS attacks
	2.13	Identify and protect against MAC flooding attacks
	2.14	Identify and protect against VLAN hopping attacks
	2.15	Identify and protect against various Layer 2 and Layer 3 attacks
	2.16	NBAR

2.17 NetFlow
2.18 Capture and utilize packet captures

20% 3.0 Intrusion Prevention and Content Security

3.1 Cisco IPS 4200 Series Sensor appliance and Cisco ASA appliance IPS module
- 3.1.a Initialize the sensor appliance
- 3.1.b Sensor appliance management
- 3.1.c Virtual sensors on the sensor appliance
- 3.1.d Implement security policies
- 3.1.e Promiscuous and inline monitoring on the sensor appliance
- 3.1.f Tune signatures on the sensor appliance
- 3.1.g Custom signatures on the sensor appliance
- 3.1.h Actions on the sensor appliance
- 3.1.i Signature engines on the sensor appliance
- 3.1.j Use Cisco IDM and Cisco IME to manage the sensor appliance
- 3.1.k Event action overrides and filters on the sensor appliance
- 3.1.l Event monitoring on the sensor appliance

3.2 VACL, SPAN and RSPAN on Cisco switches

3.3 Cisco WSA
- 3.3.a Implement WCCP
- 3.3.b Active Directory integration
- 3.3.c Custom categories
- 3.3.d HTTPS configuration
- 3.3.e Services configuration (web reputation)
- 3.3.f Configure proxy bypass lists
- 3.3.g Web proxy modes
- 3.3.h Application visibility and control

16% 4.0 Identity Management

4.1 Identity-based AAA
- 4.1.a Cisco router and appliance AAA
- 4.1.b RADIUS
- 4.1.c TACACS+

4.2 Device administration (Cisco IOS routers, Cisco ASA, and Cisco ACS5.x)

4.3 Network access (TrustSec model)
- 4.3.a Authorization results for network access (ISE)
- 4.3.b IEEE 802.1X (Cisco ISE)
- 4.3.c VSAs (Cisco ASA, Cisco IOS, and Cisco ISE)
- 4.3.d Proxy authentication (Cisco ISE, Cisco ASA, and Cisco IOS)

4.4 Cisco ISE
- 4.4.a Profiling configuration (probes)
- 4.4.b Guest services
- 4.4.c Posture assessment

4.4.d Client provisioning (CPP)
4.4.e Configure Microsoft Active Directory integration and identity sources

20% 5.0 Perimeter Security and Services

5.1 Cisco ASA firewalls
- 5.1.a Basic firewall Initialization
- 5.1.b Device management
- 5.1.c Address translation
- 5.1.d ACLs
- 5.1.e IP routing and route tracking
- 5.1.f Object groups
- 5.1.g VLANs
- 5.1.h Configure EtherChannel
- 5.1.i High availability and redundancy
- 5.1.j Layer 2 transparent firewall
- 5.1.k Security contexts (virtual firewall)
- 5.1.l Cisco Modular Policy Framework
- 5.1.j Identity firewall services
- 5.1.k Configure Cisco ASA with ASDM
- 5.1.l Context-aware services
- 5.1.m IPS capabilities
- 5.1.n QoS capabilities

5.2 Cisco IOS zone-based firewall
- 5.2.a Network, secure group, and user-based policy
- 5.2.b Performance tuning
- 5.2.c Network, protocol, and application inspection

5.3 Perimeter security services
- 5.3.a Cisco IOS QoS and packet-marking techniques
- 5.3.b Traffic filtering using access lists
- 5.3.c Cisco IOS NAT
- 5.3.d uRPF
- 5.3.e Port to Application Mapping (PAM)
- 5.3.f Policy routing and route maps

16% 6.0 Confidentiality and Secure Access

6.1 IKE (v1/v2)

6.2 IPsec LAN-to-LAN (Cisco IOS and Cisco ASA)

6.3 DMVPN

6.4 FlexVPN

6.5 GET VPN

6.6 Remote-access VPN

- 6.6.a Cisco EasyVPN Server (Cisco IOS and Cisco ASA)
- 6.6.b VPN Client 5.X
- 6.6.c Clientless WebVPN
- 6.6.d Cisco AnyConnect VPN
- 6.6.e Cisco EasyVPN Remote
- 6.6.f SSL VPN gateway

6.7 VPN high availability

6.8 QoS for VPN

6.9 VRF-aware VPN

6.10 MACsec

6.11 Digital certificates (enrollment and policy matching)

6.12 Wireless access
- 6.12.a EAP methods
- 6.12.b WPA and WPA2
- 6.12.c wIPS