**CCIE Security v.4 Course Content:**

## 1.System Hardening and Availability

- Routing plane security features
- Control Plane Policing
- Control Plane Protection & Management Plane Protection
- Broadcast control and switchport security
- Additional CPU protection mechanisms
- Disable unnecessary services
- Control device access (e.g. Telnet, HTTP, SSH, Privileges )
- Device services (e.g. SNMP, Syslog, NTP)
- Transit Traffic Control and Congestion Management

## 2.Threat Identification and Mitigation

- 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 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 MAC Flooding attacks
- Identify and protect against VLAN hopping attacks
- Identify and protect against various Layer2 & Layer3 attacks
- NetFlow
- Capture and utilize packet captures

## 3.Intrusion Prevention and Content Security

- IPS 4200 Series Sensor Appliance
- Initialize the Sensor Appliance
- Sensor Appliance management
- Virtual Sensors on the Sensor Appliance

- Implementing security policies
- Promiscuous and inline monitoring on the Sensor Appliance
- Tune signatures on the Sensor Appliance
- Custom signatures on the Sensor Appliance
- Actions on the Sensor Appliance
- Signature engines on the Sensor Appliance
- Use IDM/IME to the Sensor Appliance
- Event action overrides/filters on the Sensor Appliance
- Event monitoring on the Sensor Appliance
- VACL/SPAN & RSPAN on Cisco switches

**4.Ironport/WSA**

- Implementing WCCP
- Active Dir Integration
- Custom Categories
- HTTPS Config
- Services Configuration (Web Reputation)
- Configuring Proxy By-pass Lists
- Web proxy modes
- App visibility and control
- Identity Management
- Identity Based Authentication/Authorization/Accounting
- Cisco Router/Appliance AAA
- RADIUS
- (c)TACACS+
- Device Admin (Cisco IOS Routers, ASA, ACS5.x)

**5.Network Access (TrustSec Model)**

- Authorization Results for Network Access (ISE)
- 1X (ISE)(c)VSAs (ASA / Cisco IOS / ISE)
- Proxy-Authentication (ISE/ASA/Cisco IOS)
- Cisco Identity Services Engine (ISE)
- Profiling Configuration (Probes)
- Guest Services
- Posture Assessment
- Client Provisioning (CPP)
- Config AD Integration/Identity Sources

## 6.Perimeter Security and Services

- Cisco ASA Firewall
- Basic firewall Initialization
- Device management
- Address translation (nat, global, static)
- Access Control Lists
- IP routing/Route Tracking
- Object groups
- VLANs
- Configuring Ether channel
- High Availability and Redundancy
- Layer 2 Transparent Firewall
- Security contexts (virtual firewall)
- Modular Policy Framework
- Identity Firewall Services
- Configuring ASA with ASDM
- Context-aware services
- IPS capabilities
- QoS capabilities

## 7.Cisco IOS Zone Based Firewall

- Network, Secure Group
- Performance Tuning
- Network, Protocol & App Inspection
- Perimeter Security Services
- Cisco IOS QoS and Packet marking
- Traffic Filtering using Access-Lists
- (c)Cisco IOS NAT
- PAM – Port to Application Mapping
- Policy Routing and Route Maps

## 8.Confidentiality and Secure Access

- IKE (V1/V2)
- IPsec LAN-to-LAN (Cisco IOS/ASA)
- Dynamic Multipoint VPN (DMVPN)
- Group Encrypted Transport (GET) VPN

- Remote Access VPN
- Easy VPN Server (Cisco IOS/ASA)
- VPN Client 5.X
- Clientless WebVPN
- AnyConnect VPN
- EasyVPN Remote
- SSL VPN Gateway
- VPN High Availability
- QoS for VPN
- VRF-aware VPN
- MacSec
- Digital Certificates (Enrolment & Policy)