Course Name: CCIE Security

Version: v4.0

Course Time: 100 Hrs.

Course Prerequisites: CCNA and CNNP Security

Course Outline:

- **Infrastructure, Connectivity, Communications, Network Security**
  - Network Addressing Basics
  - OSI Layers
  - TCP/UDP/IP Protocols
  - LAN Switching (e.g. VTP, VLANs, Spanning Tree, Trunking)
  - Routing Protocols (RIP, EIGRP, OSPF, and BGP)
    - Basic Functions/Characteristics
    - Security Features
  - Tunneling Protocols
    - GRE
    - NHRP
    - v6 Tunnel Types
  - IP Multicast
    - PIM
    - Multi Src Disc Protocol
    - IGMP/CGMP
    - Multi Listener Discovery
  - Wireless
    - SSID
    - Authentication/Authorization
    - Rogue Aps
    - Session Establishment
  - Authentication/Authorization Technologies
    - Single Sign-on
    - OTPs
    - LDAP/AD
    - Role Based Access Control
  - VPNs
    - L2 vs L3
    - MPLS/VRFs/Tag switching
  - MobileIP Networks
- **Security Protocols**
  - Rivest, Shamir and Adleman (RSA)
  - Rivest Cipher 4 (RC4)
  - Message Digest 5 (MD5)
  - Secure Hash Algorithm (SHA)
  - Data Encryption Standard (DES)
  - Triple DES (3DES)
  - Advanced Encryption Standard (AES)
  - IP Security (IPsec)
  - Internet Security Association and Key Management Protocol (ISAKMP)
  - Internet Key Exchange IKE/IKEv2
  - Group Domain of Interpretation (GDOI)
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)
  - Certificate Enrollment Protocol (CEP)
  - Transport Layer Security TLS/DTLS

    - Secure Socket Layer (SSL)
    - Secure Shell (SSH)
    - Remote Authentication Dial In User Service (RADIUS)
    - Terminal Access Controller Access-Control System Plus (TACACS+)
    - Lightweight Directory Access Protocol (LDAP)
    - EAP Methods (e.g. EAP-MD5, EAP-TLS, EAP-TTLS, EAP-FAST, PEAP, LEAP)
    - Public Key Infrastructure (PKI)/PKIX/PKCS
    - 802.1X
    - WEP/WPA/WPA2
    - Web Cache Communication Protocol (WCCP)
    - Secure Group Tagging Exchange Protocol (SXP)
    - MacSec
    - DNSSec
- **Application and Infrastructure Security**
    - Hypertext Transfer Protocol (HTTP)
    - Hypertext Transfer Protocol Secure (HTTPS)
    - Simple Mail Transfer Protocol (SMTP)
    - Dynamic Host Configuration Protocol (DHCP)
    - Domain Name System (DNS)
    - File Transfer Protocol (FTP/SFTP)
    - Trivial File Transfer Protocol (TFTP)
    - Network Time Protocol (NTP)
    - Simple Network Management Protocol (SNMP)
    - Syslog
    - Netlogon,Netbios,SMB
    - RPCs
    - RDP/VNC
    - PCoIP
    - OWASP
    - Basic unnecessary services
- **Threats, Vulnerability Analysis and Mitigation**
    - Recognizing and mitigating common attacks
        - ICMP attacks, PING floods
        - MITM
        - Replay
        - Spoofing
        - Backdoor
        - Botnets
        - Wireless attacks
        - DoS/DDoS Attacks
        - Virus and Worms Outbreaks
        - Header Attacks
        - Tunneling attacks
    - Software/OS Exploits
    - Security/Attack Tools
    - Generic Network Intrusion Prevention Concepts
    - Packet Filtering
    - Content Filtering/Packet Inspection
    - Endpoint/Posture Assessment
    - QoS marking attacks

- **Cisco Security Products, Features and Management**
  - Cisco Adaptive Security Appliance (ASA)
    - Firewall Functionality
    - Routing/Multicast Cababilities
    - Firewall modes
    - NAT - Pre 8.4/Post 8.4
    - Object Definition/ACLs
    - MPF functionality (IPS/QoS/Application Awareness)
    - Context Aware Firewall
    - Identity Based Services
    - Failover Options
  - Cisco IOS Firewalls and NAT
    - CBAC
    - Zone-Based Firewall
    - Port-to-Application Mapping
    - Identity Based Firewalling
  - Cisco Intrusion Prevention Systems (IPS)
  - Cisco IOS IPS
  - Cisco AAA Protocols and Application
    - RADIUS
    - TACACS+
    - Device Admin
    - Network Access
    - 802.1X
    - VSAs
  - Cisco Identity Services Engine
  - Cisco Secure ACS Solution Engine
  - Cisco Network Admission Control (NAC) Appliance Server
  - Endpoint/Client
    - Cisco AnyConnect VPN Client
    - Cisco VPN Client
    - Cisco Secure Desktop (CSD)
    - NAC Agent
  - Secure Access Gateways (Cisco IOS Router/ASA)
    - IPsec
    - SSL VPN
    - PKI
  - Virtual Security Gateway
  - Cisco Catalyst 6500 Series Security Services Modules
  - Scansafe Functionality&Components
  - IronPort ProductsSecurity Management
    - Cisco Security Manager (CSM)
    - Cisco Adaptive Security Device Manager (ASDM)
    - Cisco IPS Device Manager (IDM)
    - Cisco IPS Manager Express (IME)
    - Cisco Configuration Professional (CCP)
    - Cisco Prime

- **Cisco Security Technologies and Solutions**
  - Router Hardening Features (e.g. CoPP, MPP. uRPF, PBR)
  - Switch Security Features (e.g. anti-spoofing, port, STP, MacSec,NDAC,NEAT)
  - NetFlow
  - Wireless Security
  - Network Segregation
    - VRF-aware technologies
    - VXLAN
  - VPN Solutions
    - FlexVPN
    - Dynamic Multipoint VPN (DMVPN)
    - Group Encrypted Transport VPN (GETVPN)
    - EasyVPN
  - Content and Packet Filtering
  - QoS application for security
  - Load Balancing & Failover
- **Security Policies and Procedures, Best Practices, Standards**
  - Security Policy Elements
  - Information Security Standards (e.g. ISO/IEC 27001, ISO/IEC 27002)
  - Standards Bodies (e.g. ISO, IEC, ITU, ISOC, IETF, IAB, IANA, ICANN)
  - Industry Best Practices (e.g. SOX, PCI DSS)
  - Common RFC/BCP (e.g. RFC2827/BCP38, RFC3704/BCP84,RFC5735)
  - Security Audit & Validation
  - Risk Assessment
  - Change Management Process
  - Incident Response Framework
  - Computer Security Forensics
  - Desktop Security Risk Assessment/Desktop Security Risk Management