CCNA Security
Contents

1. **Security Concepts**

- Learn the Common security principles like confidentiality, integrity, availability (CIA)
- Describe the Identify common security terms, common network security zones
- Describe the Common security threats concepts like common network attacks,
- Learn the Cryptography concepts like key exchange, key exchange
- Compare the difference between symmetric and asymmetric encryption
- Describe digital signatures, certificates, and PKI
- Classify and define differ net network topologies like Campus area network (CAN), Cloud, wide
- area network (WAN), Data center Network security for a virtual environment

2. **Secure Access**

- Learn how Secure management works
- Learn and Compare in-band and out-of band
- Configure and verify secure network management through SNMP v3 using an ACL
- Describe how to configure and verify NTP Security

3.**AAA concepts**

- Learn how RADIUS and TACACS+ technologies Works
- Configure and verify administrative access on a Cisco router using TACACS+
- Configure and Verify authentication on a Cisco router to a TACACS+ server
- Describe and Explain the integration of Active Directory with AAA
- Describe authentication and authorization using ACS and ISE
- Describe 802.1X authentication and functions of 802.1X components

4. **VPN**

- Detail description of VPN concepts
- Describe how differ net IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode,
- transport mode) Works
- Implement Site-to-site VPN along with IPsec site-to-site VPN with pre-shared key
- authentication on Cisco
- Implement and verify an IPsec site-to-site VPN with pre-shared key authentication on Cisco
- routers and ASA firewalls

5. **Securing Routing and Switching Devices and Protocols**

- Implement and verify Cisco IOS resilient configuration
- Implement routing update authentication on OSPF
- Learn how to Secure the control plane
- Explain control plane policing functions and works
- Explain different Common Layer 2 attacks like STP, ARP, MAC spoofing, CAM table Overflow ,
- VLAN hopping, DHCP Spoofing
- Describe Mitigation procedures for DHCP snooping, Dynamic ARP Inspection,port security
- Describe BPDU guard, root guard, loop guard to Protect L2 Environment
- Describe the security implications of a PVLAN and native VLAN

6. Implementing Cisco Firewall Technologies

- Describe operational strengths and weaknesses of the different firewall technologies
- Describe the different Firewall like Proxy firewalls , Application firewall, Personal firewall
- Compare and contrast stateful vs. stateless firewalls its operation and its state table function
- Implement and verify Static , Dynamic, PAT, Policy NAT, and other NAT operation on Cisco
- ASA 8.x
- Implement zone-based firewall and its component like Zone to Zone and Self Zone features
- Configure Firewall features on the Cisco Adaptive Security Appliance (ASA) 9.x
- Configuration and Verification of ASA access management
- Configuration and Verification of security access policies
- Configuration and Verification of Cisco ASA interface security levels

7.IPS

- Describe IPS deployment considerations
- Define Network-based IPS vs. host-based IPS
- Describe the different Modes of IPS deployment (inline, promiscuous – SPAN, tap)
- Define different IPS Placement (positioning of the IPS within the network)