

Implementing Cisco IOS Network Security

Exam Code: 640-554

Duration: 40 Hrs

Course Content:

Common Security Threats

Describe common security threats

Security and Cisco Routers

Implement security on Cisco routers

Describe securing the control, data, and management plane

Describe Cisco Security Manager

Describe IPv4 to IPv6 transition

AAA on Cisco Devices

Implement AAA (authentication, authorization, and accounting)

Describe TACACS+

Describe RADIUS

Describe AAA

Verify AAA functionality

IOS ACLs

Describe standard, extended, and named IP IOS access control lists (ACLs) to filter packets

Describe considerations when building ACLs

Implement IP ACLs to mitigate threats in a network

Secure Network Management and Reporting

Describe secure network management

Implement secure network management

Common Layer 2 Attacks

Describe Layer 2 security using Cisco switches

Describe VLAN security

Implement VLANs and trunking

Implement spanning tree

Cisco Firewall Technologies

Describe operational strengths and weaknesses of the different firewall technologies

Describe stateful firewalls

Describe the types of NAT used in firewall technologies

Implement zone-based policy firewall using CCP

Implement the Cisco Adaptive Security Appliance (ASA)

Implement Network Address Translation (NAT) and Port Address Translation (PAT)

Cisco IPS

Describe Cisco Intrusion Prevention System (IPS) deployment considerations
Describe IPS technologies
Configure Cisco IOS IPS using CCP

VPN Technologies

Describe the different methods used in cryptography
Describe VPN technologies
Describe the building blocks of IPSec
Implement an IOS IPSec site-to-site VPN with pre-shared key authentication
Verify VPN operations
Implement Secure Sockets Layer (SSL) VPN using ASA device manager