CCNA Security Certification

Learning@Cisco

Exam Content Updates

Introduction

The CCNA Security IINS exam topics have been refreshed from version 2.0 to version 3.0. This document will highlight exam topic changes between the current 640-554 IINS exam and the new 210-260 IINS exam.

The IINS acronym to this exam will remain but the title will change slightly, removing "IOS" from the title, making the new title **Implementing Cisco Network Security**.

The new exam topics combine and adjust the current domains. The overall number of domains has been reduced from nine to seven. Although there are fewer domains, the exam remains the same length. The same number of questions has been spread across the seven domain topics. The domains better reflect current job roles and job tasks required in the jobs typically held by CCNA Security Certified individuals.

Exam Topic Update Summary

- The current exam topics specify Cisco Configuration Pro (CCP) for nearly all router configuration elements. The new exam topics focus on CLI-based configuration for IOS router and switch configuration.
- The new exam topics include updates to the Intrusion Prevention Systems (IPS) sections, specifying legacy Cisco IPS and Cisco Next Generation IPS terminology side by side. Content now includes descriptions of NGIPS technologies such as FirePOWER Services, FireSIGHT Management Center, and Cisco Advanced Malware Protection.
- Focus on Access Control Lists (ACL's) has been reduced in the new IINS exam topics, since ACL's are covered in the ICND1 prerequisite.
- Many newer technologies are now expressly included in the course materials:
  - 802.1x
  - Cisco Identity Services Engine (ISE)
  - Bring Your Own Device (BYOD)
  - Cisco Cloud Web Security (CWS)
  - Cloud & Virtualization
- Updated examples of security risks, more closely aligned with today's common security threats.
- References to some standards and technologies have also been brought up to date.
  - DES and MD5 are replaced with more current algorithms.
- The curriculum used to prepare for the exam has all new labs, with dynamic topology based on the subject matter covered in a particular lab exercise.

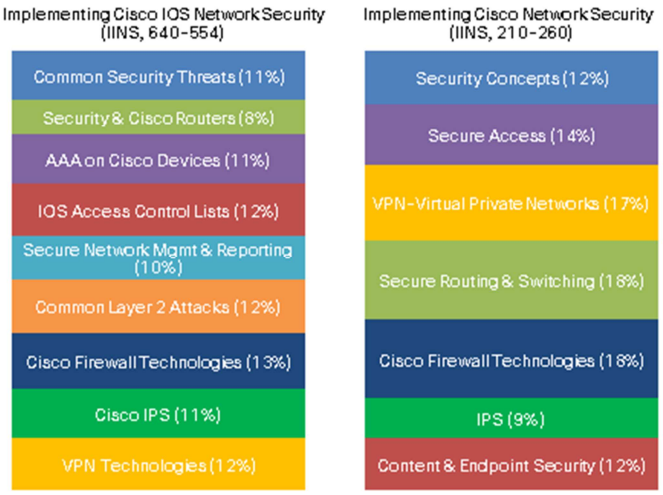

Figure 1: Current Exam Topics versus New Exam Topics

Detailed Exam Topic Comparison

A detailed comparison of the current 640-554 IINS exam and the new 210-260 IINS exam is shown below.

640-554: Implementing Cisco IOS Network Security	210-260: Implementing Cisco Network Security
11% 1.0 Common Security Threats **1.1 Describe common security threats** 1.1.a Common threats to the physical installation 1.1.b Mitigation methods for common network attacks 1.1.c Email-based threats 1.1.d Web-based attacks 1.1.e Mitigation methods for Worm, Virus, and Trojan Horse attacks 1.1.f Phases of a secure network lifecycle 1.1.g Security needs of a typical enterprise with a comprehensive security policy 1.1.h Mobile/remote security 1.1.i DLP (Data Loss Prevention)	**12% 1.0 Security Concepts** **1.1 Common Security Principles** 1.1.a Describe Confidentiality, Integrity, Availability (CIA) 1.1.b Describe SIEM technology 1.1.c Identify common security terms 1.1.d Identify common network security zones **1.2 Common Security Threats** 1.2.a Identify Common network attacks 1.2.b Describe Social Engineering 1.2.c Identify Malware 1.2.d Classify the vectors of Data Loss/Exfiltration **1.3 Cryptography Concepts** 1.3.a Describe Key Exchange 1.3.b Describe Hash Algorithm 1.3.c Compare & Contrast Symmetric and Asymmetric Encryption 1.3.d Describe Digital Signatures, Certificates and PKI **1.4 Describe network topologies** 1.4.a Campus Area Network (CAN) 1.4.b Cloud, Wide Area Network (WAN) 1.4.c Data Center 1.4.d Small office/Home office (SOHO) 1.4.e Network security for a virtual environment
8% 2.0 Security and Cisco Routers **2.1Implement security on Cisco routers** 2.1.a CCP Security Audit feature 2.1.b CCP One-Step Lockdown feature 2.1.c Secure router access using strong encrypted passwords, and using IOS login enhancements, IPV6 security 2.1.d Multiple privilege levels 2.1.e Role-based CLI 2.1.f Cisco IOS image and configuration files **2.2 Describe securing the control, data and management plane** **2.3 Describe CSM** **2.4 Describe IPv4 to IPv6 transition** 2.4.a Reasons for IPv6 2.4.b Understanding IPv6 addressing 2.4.c Assigning IPv6 addresses 2.4.d Routing considerations for IPv6	**14% 2.0 Secure Access** **2.1 Secure management** 2.1.a Compare In-band and out of band 2.1.b Configure secure network management 2.1.c Configure and verify secure access through SNMP v3 using an ACL 2.1.d Configure and verify security for NTP

11% 3.0 AAA on Cisco Devices

3.1Implement authentication, authorization, and accounting (AAA)
- 8.1.a AAA using CCP on routers
- 8.1.b AAA using CLI on routers and switches
- 8.1.c AAA on ASA

3.2 Describe TACACS+

3.3 Describe RADIUS

3.4 Describe AAA
- 3.4.a Authentication
- 3.4.b Authorization
- 3.4.c Accounting

3.5 Verify AAA functionality.

12% 4.0 IOS ACLs

4.1 Describe standard, extended, and named IP IOS ACLs to filter packets
- 4.1.a IPv4
- 4.1.b IPv6
- 4.1.c Object groups
- 4.1.d ACL operations
- 4.1.e Types of ACLs (dynamic, reflexive, time-based ACLs)
- 4.1.f ACL wild card masking
- 4.1.g Standard ACLs
- 4.1.h Extended ACLs
- 4.1.i Named ACLs
- 4.1.j VLSM

4.2 Describe considerations when building ACLs
- 4.2.a Sequencing of ACEs
- 4.2.b Modification of ACEs

4.3 Implement IP ACLs to mitigate threats in a network
- 4.3.a Filter IP traffic
- 4.3.b SNMP
- 4.3.c DDoS attacks
- 4.3.d CLI
- 4.3.e CCP
- 4.3.f IP ACLs to prevent IP spoofing
- 4.3.g VACLs

10% 5.0 Secure Network Management and Reporting

5.1Describe secure network management
- 5.1.a In-band
- 5.1.b Out of band
- 5.1.c Management protocols
- 5.1.d Management enclave
- 5.1.e Management plane

5.2 Implement secure network management
- 5.2.a SSH
- 5.2.b syslog
- 5.2.c SNMP
- 5.2.d NTP
- 5.2.e SCP
- 5.2.f CLI
- 5.2.g CCP
- 5.2.h SSL
- 2.1.e Use SCP for file transfer

2.2 AAA Concepts
- 2.2.a Describe RADIUS & TACACS+ technologies
- 2.2.b Configure administrative access on a Cisco router using TACACS+
- 2.2.c Verify connectivity on a Cisco router to a TACACS+ server
- 2.2.d Explain the integration of Active Directory with AAA
- 2.2.e Describe Authentication & Authorization using ACS and ISE

2.3 802.1x Authentication
- 2.3.a Identify the functions 802.1x components

2.4 BYOD (Bring-Your-Own-Device)
- 2.4.a Describe the BYOD architecture framework
- 2.4.b Describe the function of Mobile Device Management (MDM)

17% 3.0 Virtual Private Networks (VPN)

3.1 VPN Concepts
- 3.1.a Describe IPSec Protocols and Delivery Modes (IKE, ESP, AH, Tunnel mode, Transport mode)
- 3.1.b Describe Hairpinning, Split Tunneling, Always-on, NAT Traversal

3.2 Remote Access VPN
- 3.2.a Implement basic Clientless SSL VPN using ASDM
- 3.2.b Verify clientless connection
- 3.2.c Implement basic AnyConnect SSL VPN using ASDM
- 3.2.d Verify AnyConnect connection
- 3.2.e Identify Endpoint Posture Assessment

3.3 Site-to-Site VPN
- 3.3.a Implement an IPSec site-to-site VPN with pre-shared key authentication on Cisco routers and ASA firewalls
- 3.3.b Verify an IPSec site-to-site VPN

18% 4.0 Secure Routing and Switching

4.1 Security on Cisco Routers
- 4.1.a Configure multiple privilege levels
- 4.1.b Configure IOS Role-based CLI Access
- 4.1.c Implement IOS Resilient Configuration

4.2 Securing Routing Protocols
- 4.2.a Implement routing update authentication on OSPF

4.3 Securing the Control Plane
- 4.3.a Explain the function of Control Plane Policing

4.4 Common Layer 2 Attacks
- 4.4.a Describe STP attacks
- 4.4.b Describe ARP Spoofing
- 4.4.c Describe MAC spoofing
- 4.4.d Describe CAM Table (MAC Address Table) Overflows
- 4.4.e Describe CDP/LLDP Reconnaissance
- 4.4.f Describe VLAN Hopping
- 4.4.g Describe DHCP Spoofing

4.5 Mitigation Procedures
- 4.5.a Implement DHCP Snooping
- 4.5.b Implement Dynamic ARP Inspection
- 4.5.c Implement Port Security
- 4.5.d Describe BPDU Guard, Root Guard, Loop Guard
- 4.5.e Verify mitigation procedures

4.6 VLAN Security
- 4.6.a Describe the security implications of a PVLAN
- 4.6.b Describe the security implications of a Native VLAN

12% 6.0 Common Layer 2 Attacks

6.1 Describe Layer 2 security using Cisco switches
- 6.1.a STP attacks
- 6.1.b ARP spoofing
- 6.1.c MAC spoofing
- 6.1.d CAM overflows
- 6.1.e CDP/LLDP

6.2 Describe VLAN Security
- 6.2.a Voice VLAN
- 6.2.b PVLAN
- 6.2.c VLAN hopping
- 6.2.d Native VLAN

6.3 Implement VLANs and Trunking
- 6.3.a VLAN definition
- 6.3.b Grouping functions into VLANs
- 6.3.c Considering traffic source to destination paths
- 6.3.d Trunking
- 6.3.e Native VLAN
- 6.3.f VLAN trunking protocols
- 6.3.g Inter-VLAN routing

6.4 Implement Spanning Tree
- 6.4.a Potential issues with redundant switch topologies
- 6.4.b STP operations
- 6.4.c Resolving issues with STP

13% 7.0 Cisco Firewall Technologies

7.1 Describe operational strengths and weaknesses of the different firewall technologies
- 7.1.a Proxy firewalls
- 7.1.b Packet and stateful packet
- 7.1.c Application firewall
- 7.1.d Personal firewall

7.2 Describe stateful firewalls
- 7.2.a Operations
- 7.2.b Function of the state table

7.3 Describe the types of NAT used in firewall technologies
- 7.3.a Static
- 7.3.b Dynamic
- 7.3.c PAT

7.4 Implement Zone Based Firewall using CCP
- 7.4.a Zone to zone
- 7.4.b Self zone

7.5 Implement the Cisco Adaptive Security Appliance (ASA)
- 7.5.a NAT
- 7.5.b ACL
- 7.5.c Default MPF
- 7.5.d Cisco ASA sec level

7.6 Implement NAT and PAT
- 7.6.a Functions of NAT, PAT, and NAT Overload
- 7.6.b Translating inside source addresses
- 7.6.c Overloading Inside global addresses

18% 5.0 Cisco Firewall Technologies

5.1 Describe operational strengths and weaknesses of the different firewall technologies
- 5.1.a Proxy firewalls
- 5.1.b Application firewall
- 5.1.c Personal firewall

5.2 Compare Stateful vs. Stateless Firewalls
- 5.2.a Operations
- 5.2.b Function of the state table

5.3 Implement NAT on Cisco ASA 9.x
- 5.3.a Static
- 5.3.b Dynamic
- 5.3.c PAT
- 5.3.d Policy NAT
- 5.3 e Verify NAT operations

5.4 Implement Zone Based Firewall
- 5.4.a Zone to zone
- 5.4.b Self zone

5.5 Firewall features on the Cisco Adaptive Security Appliance (ASA) 9.x
- 5.5.a Configure ASA Access Management
- 5.5.b Configure Security Access Policies
- 5.5.c Configure Cisco ASA interface security levels
- 5.5.d Configure Default Modular Policy Framework (MPF)
- 5.5.e Describe Modes of deployment (Routed firewall, Transparent firewall)
- 5.5.f Describe methods of implementing High Availability
- 5.5.g Describe Security contexts
- 5.5.h Describe Firewall Services

9% 6.0 Intrusion Prevention Systems (IPS)

6.1 Describe IPS Deployment Considerations
- 6.1.a Network Based IPS vs. Host Based IPS
- 6.1.b Modes of deployment (Inline, Promiscuous - SPAN, tap)
- 6.1.c Placement (positioning of the IPS within the network)
- 6.1.d False Positives, False Negatives, True Positives, True Negatives

6.2 Describe IPS Technologies
- 6.2.a Rules/Signatures
- 6.2.b Detection/Signature Engines
- 6.2.c Trigger Actions/Responses (drop, reset, block, alert, monitor/log, shun)
- 6.2.d Blacklist (Static & Dynamic)

12% 7.0 Content and Endpoint Security

7.1 Describe Mitigation Technology for Email-based Threats
- 7.1.a SPAM Filtering, Anti-Malware Filtering, DLP, Blacklisting, Email Encryption

7.2 Describe Mitigation Technology for Web-based Threats
- 7.2.a Local & Cloud Based Web Proxies
- 7.2.b Blacklisting, URL-Filtering, Malware Scanning,

11% 8.0 Cisco IPS

8.1 Describe IPS deployment considerations
- 8.1.a SPAN
- 8.1.b IPS product portfolio
- 8.1.c Placement
- 8.1.d Caveats

8.2 Describe IPS technologies
- 8.2.a Attack responses
- 8.2.b Monitoring options
- 8.2.c syslog
- 8.2.d SDEE
- 8.2.e Signature engines
- 8.2.f Signatures
- 8.2.g Global correlation and SIO
- 8.2.h Network-based
- 8.2.i Host-based

8.3 Configure Cisco IOS IPS using CC
- 8.3.a Logging
- 8.3.b Signatures

12% 9.0 VPN Technologies

9.1 Describe the different methods used in cryptography
- 9.1.a Symmetric
- 9.1.b Asymetric
- 9.1.c HMAC
- 9.1.d Message digest
- 9.1.e PKI

9.2 Describe VPN technologies
- 9.2.a IPsec
- 9.2.b SSL

9.3 Describe the building blocks of IPSec
- 9.3.a IKE
- 9.3.b ESP
- 9.3.c AH
- 9.3.d Tunnel mode
- 9.3.e Transport mode

9.4 Implement an IOS IPSec site-to-site VPN with pre-shared key authentication
- 9.4.a CCP
- 9.4.b CLI

9.5 Verify VPN operations.

9.6 Implement SSL VPN using ASA device manager
- 9.6.a Clientless
- 9.6.b AnyConnect

URL Categorization, Web Application Filtering, TLS/SSL Decryption

7.3 Describe Mitigation Technology for Endpoint Threats
- 7.3.a Anti-Virus/Anti-Malware
- 7.3.b Personal Firewall/HIPS
- 7.3.c Hardware/Software Encryption of local data

Learn More

Get more information on the Cisco CCNA Security certification and available security training.