Appendix B

CCNA Security 210-260 (IINS) Exam Updates

Over time, reader feedback enables Cisco Press to gauge which topics give our readers the most problems when taking the exams. To assist readers with those topics, the authors create new materials clarifying and expanding upon those troublesome exam topics. As mentioned in the introduction, the additional content about the exam is contained in a PDF document on this book’s companion website, at http://www.ciscopress.com/title/9781587205668.

This appendix is intended to provide you with updated information if Cisco makes minor modifications to the exam upon which this book is based. When Cisco releases an entirely new exam, the changes are usually too extensive to provide in a simple update appendix. In those cases, you might need to consult the new edition of the book for the updated content.

This appendix attempts to fill the void that occurs with any print book. In particular, it does the following:

* Mentions technical items that might not have been mentioned elsewhere in the book

Covers new topics if Cisco adds new content to the exam over time

Provides a way to get up-to-the-minute current information about content for the exam

Always Get the Latest at the Companion Website

You are reading the version of this appendix that was available when your book was printed. However, because the main purpose of this appendix is to be a living, changing document, it is important that you look for the latest version online at the book’s companion website.

To do so, follow these steps:

Step 1. Browse to http://www.ciscopress.com/title/9781587205668.

Step 2. Select the Updates tab.

Step 3. Download the latest “Appendix B” document.

NOTE Note that the downloaded document has a version number. Comparing the version of the print Appendix B (version 1.0) with the latest online version of this appendix, you should do the following:

* Same version: Ignore the PDF that you downloaded from the companion website.
* Website has a later version: Ignore this Appendix B in your book and read only the latest version that you downloaded from the companion website.

Technical Content

The version for this appendix is version 2.0. The version history is as follows:

Version 1.0: No technical content; the appendix was a placeholder to inform readers to check the website for future updates.

Version 2.0: Added the following.

Next-Generation Firewalls and Next-Generation IPS

In Chapters 14, 15, and 16 you learned the fundamentals of firewalls, how to configure the Cisco ASA and Cisco IOS zone-based firewalls. After writing those chapters Cisco introduced the Cisco ASA FirePOWER module, the Cisco Firepower Threat Defense (FTD) unified image, and the Cisco Firepower 4100 series appliances as part of the integration of the Sourcefire technology.

NOTE Cisco has acquired several security companies, including Sourcefire, Threat Grid, OpenDNS, and CloudLock, to expand its security portfolio.

The Cisco ASA FirePOWER module provides NGIPS, Application Visibility and Control (AVC), URL filtering, and Advanced Malware Protection (AMP). This module runs as a separate application from the classic Cisco ASA software. The Cisco ASA FirePOWER module can be a hardware module on the ASA 5585-X only or a software module that runs in an SSD in all other models.

The Cisco ASA FirePOWER module can be managed by the Firepower Management Center (FMC), formerly known as the FireSIGHT Management Center. The Firepower Management Center and the Cisco ASA FirePOWER module require additional licenses. In all Cisco ASA models except the 5506-X, 5508-X, and 5516-X, the licenses are installed in the FirePOWER module. No additional licenses are required in a Cisco ASA device. FirePOWER Services running on the Cisco ASA 5506-X, 5508-X, and 5516-X can be managed using Adaptive Security Device Manager (ASDM), and the licenses can be installed using ASDM. In all Cisco ASAs with FirePOWER Services managed by a Firepower Management Center, the license is installed on the Firepower Management Center and used by the module.

Next-generation firewalls do not focus solely on detection and traditional defenses but also provide the capability to mitigate the impact of an attack after it happens. Organizations must maintain visibility and control across the extended network during the full attack continuum:

* Before an attack takes place

During an active attack

After an attacker starts to damage systems or steal information

The Cisco ASA with FirePOWER Services, Cisco FTD, and Cisco AMP provide a security solution that helps you discover threats and enforce and harden policies before an attack takes place. These technologies and solutions can help you detect, block, and defend against attacks that have already taken place. In Chapter 16 you learned that the Cisco ASA family has members in many shapes and sizes, and you learned about their uses in small, medium, and large organizations. Cisco ASA FirePOWER Services and Cisco FTD provide the following key capabilities:

* Access control: This policy-based capability enables a network security administrator to define, inspect, and log the traffic that traverses a firewall. Access control policies determine how traffic is permitted or denied in a network. For example, you can configure a default action to inspect all traffic or to block or trust all traffic without further inspection. You can also achieve a more complete access control policy with enrichment data based on security threat intelligence. Whether you configure simple or complex rules, you can control traffic based on security zones, network or geographical locations, ports, applications, requested URLs, and per user.

Intrusion detection and prevention: Intrusion detection and prevention help you detect attempts from an attacker to gain unauthorized access to a network or a host, create performance degradation, or steal information. You define intrusion detection and prevention policies based on your access control policies. You can create and tune custom policies at a very granular level to specify how traffic in a network is inspected.

AMP and file control: You can detect, track, capture, analyze, and optionally block the transmission of files, including malware files and nested files inside archive files in network traffic. File control also enables you to detect and block users from sending or receiving files of different specified types over a multitude of application protocols. You can configure file control as part of the overall access control policies and application inspection.

Application programming interfaces (API): Cisco ASA FirePOWER Services supports several ways to interact with the system using APIs.

The Cisco ASA FirePOWER module can be a hardware module on the ASA 5585-X only or a software module that runs in a solid state drive (SSD) in all other Cisco ASA 5500-X models.

NOTE The Cisco ASA FirePOWER Services module is not supported in the 5505. For the 5512-X through ASA 5555-X, you must install an SSD. The SSD is standard on the 5506-X, 5508-X, and 5516-X.

Several options are available for network security administrators to manage the Cisco ASA FirePOWER module. The Cisco ASA FirePOWER module provides a basic command-line interface (CLI) for initial configuration and troubleshooting only. Network security administrators can configure security policies on the Cisco ASA FirePOWER module using either of these methods:

* Administrators can configure the Cisco Firepower Management Center hosted on a separate appliance or deployed as a virtual machine (VM).

Administrators can configure the Cisco ASA FirePOWER module deployed on Cisco ASA 5506-X, 5508-X, and 5516-X using the Cisco Adaptive Security Device Manager (ASDM).

Cisco Firepower Licenses

You have already learned that the Cisco ASA FirePOWER module can be managed by the Firepower Management Center or ASDM, in the case of the Cisco ASA 5506-X and 5508-X. The Firepower Management Center and Cisco ASA FirePOWER module require different licenses. These licenses are installed in the Cisco FirePOWER module and the Cisco Firepower Management Center. No additional licenses are required in the Cisco ASA.

The following are the different types of Cisco ASA FirePOWER Services licenses:

* Protection

Control

Malware

URL Filtering

The Protection License

The Protection license enables a network security administrator to perform intrusion detection and prevention, file control, and security intelligence filtering. The intrusion detection and prevention capabilities are used to analyze network traffic for intrusions and exploits, to alert the network security administrator, and optionally block offending packets. File control enables network security administrators to detect and (optionally) block users from sending or receiving files of specific types over specific application protocols.

NOTE The Malware license also enables you to inspect and block a set of file types, based on malware intelligence and dispositions. The Malware license is covered later in this chapter.

Security intelligence filtering enables network security administrators to blacklist different hosts/IP addresses before the traffic is analyzed by access control rules. Cisco provides dynamic feeds, allowing a network security administrator to immediately blacklist connections based on the Cisco threat intelligence capabilities, fueled by the Cisco research organization Talos. You can also configure this to be monitor only.

TIP You can configure access control policies without a license; however, if you do so, you will not be able to apply the policy until the Protection license is added to the Cisco ASA FirePOWER module. If the Protection license is for some reason deleted, the Cisco ASA FirePOWER module ceases to detect intrusions and file events, and it cannot reach the Internet for either Cisco-provided or third-party security intelligence information.

A Protection license is required with all the other licenses (Control, Malware, and URL Filtering). If the Protection license is disabled or deleted, this has a direct effect on any other licenses installed.

The Control License

The Control license enables a network security administrator to implement user and application control by adding user and application settings to access control rules. As with the Protection license, you can add user and application conditions to access control rules without a Control license. You cannot apply the policy until the Control license is installed and enabled in the Cisco ASA FirePOWER module, however.

The URL Filtering License

The URL Filtering license enables a network security administrator to implement access control rules that determine what traffic can pass through the firewall, based on URLs requested by monitored hosts. The Cisco ASA FirePOWER module obtains information about those URLs from the Cisco cloud.

You can configure individual URLs or groups of URLs to be allowed or blocked by the Cisco ASA FirePOWER module without a URL Filtering license; however, you cannot use URL category and reputation data to filter network traffic without a URL Filtering license. If the FMC manages the Cisco ASA FirePOWER module, Cisco receives the URL categorization and reputation information from the FMC and then sends it to the managed devices (that is, Cisco ASA FirePOWER modules, NGIPS, FTD, and so on).

NOTE The URL Filtering license is a subscription-based license.

The Malware License

The Malware license enables Advanced Malware Protection (AMP) in the Cisco ASA FirePOWER module. With AMP, you can detect and block malware potentially being transmitted over the network.

Malware detection is configured as part of a file policy, which you then associate with one or more access control rules.

Cisco FTD

The Cisco FTD is unified software that includes Cisco ASA features, legacy FirePOWER Services, and new features. FTD can be deployed on Cisco Firepower 4100 and 9300 appliances to provide next-generation firewall (NGFW) services. In addition to being able to run on the Cisco Firepower 4100 Series and the Firepower 9300 appliances, FTD can run natively on several Cisco ASA models. The following Cisco ASA 5500-X models support a reimage to run the FTD software:

* ASA 5506-X

ASA 5506W-X

ASA 5506H-X

ASA 5508-X

ASA 5512-X

ASA 5515-X

ASA 5516-X

ASA 5525-X

ASA 5545-X

ASA 5555-X

Cisco FTD is not supported in the ASA 5505 or the 5585-X. In the Cisco ASA, you can use FTD in single context mode and in routed or transparent mode. Multiple context mode is not supported at this writing.

To reimage one of the aforementioned Cisco ASA models, you must meet the following prerequisites:

* You must have a Cisco Smart Account. You can create one at Cisco Software Central (https://software.cisco.com).

You must review the FTD software version release notes to become familiar with the supported features, because Cisco continues to add features regularly.

Add at least a base FTD license to your Smart Account (for example, L-ASA5516T-BASE=).

You must have access to an FMC (virtual or physical).

You must have access to the console port of the Cisco 5500-X appliance on which FTD software will be installed, either directly from the computer being used for installing FTD software or through a terminal server.

It is a best practice to back up your existing configuration.

Understand that when you reimage and install FTD software on your Cisco ASA, all previous files and configurations saved on the ASA are lost.

You must have the required minimum free space (3 GB plus the size of the boot software) available on the flash (disk0).

You must have an SSD in your Cisco ASA.

You must have access to a TFTP server to host the FTD images.

Cisco Firepower 4100 Series

The Cisco Firepower 4100 Series appliances are next-generation firewalls that run the Cisco FTD software and features. There are four models:

* Cisco Firepower 4110, which supports up to 20 Gbps of firewall throughput

Cisco Firepower 4120, which supports up to 40 Gbps of firewall throughput

Cisco Firepower 4140, which supports up to 60 Gbps of firewall throughput

Cisco Firepower 4150, which supports more than 60 Gbps of firewall throughput

All the Cisco Firepower 4100 Series models are one rack-unit (1 RU) appliances and are managed by the Cisco Firepower Management Center.

Cisco Firepower 9300 Series

The Cisco Firepower 9300 appliances are designed for very large enterprises or service providers. They can scale beyond 1 Tbps and are designed in a modular way, supporting Cisco ASA software, Cisco FTD software, and Radware DefensePro DDoS mitigation software.

NOTE The Radware DefensePro DDoS mitigation software is available and supported directly from Cisco on Cisco Firepower 4150 and Cisco Firepower 9300 appliances.

Radware’s DefensePro DDoS mitigation software provides real-time analysis to protect the enterprise or service provider infrastructure against network and application downtime due to distributed denial of service (DDoS) attacks.

Cisco FTD for Cisco Integrated Services Routers (ISR)

The Cisco FTD can run on Cisco Unified Computing System (UCS) E-Series blades installed on Cisco ISR routers. Both the FMC and the FTD are deployed as virtual machines. Two internal interfaces connect a router to an UCS E-Series blade. On ISR G2, Slot0 is a Peripheral Component Interconnect Express (PCIe) internal interface, and UCS E-Series Slot1 is a switched interface connected to the backplane Multi Gigabit Fabric (MGF). In Cisco ISR 4000 Series routers, both internal interfaces are connected to the MGF.

A hypervisor is installed on the UCS E-Series blade, and the Cisco FTD software runs as a virtual machine on it. FTD for ISRs is supported on the following platforms:

* Cisco ISR G2 Series: 2911, 2921, 2951, 3925, 3945, 3925E, and 3945E

Cisco ISR 4000 Series: 4331, 4351, 4451, 4321, and 4431

Network Infrastructure Security Updates

802.1X Components

802.1X is a protocol developed to enforce authentication and authorization of devices to access a network, both wired and wireless. The 802.1X framework consists of a client endpoint (supplicant), a network device (authenticator) that provides network connectivity to the client endpoint, and a host providing backend authentication/authorization supporting RADIUS/EAP protocols (authentication server). Until the client endpoint is successfully authenticated the only network traffic allowed by the authenticator will be Extensible Authentication Protocol over LAN (EAPOL) traffic. Once the client endpoint is authenticated, network traffic will be allowed to or from the client via the authenticator; that is, the network device, based on the authorization profile sent back to the network device from the authentication server.

802.1X uses the following protocols:

* Extensible Authentication Protocol (EAP): EAP is the message format and framework defined by RFC 4187 that provides a way for the supplicant and the authenticator to negotiate an authentication method (the EAP method).

EAP method: The EAP method defines the authentication method; that is, the credential type and how it is submitted from the supplicant to the authentication server using the EAP framework. Examples of EAP methods include EAP-Transport Layer Security (EAP-TLS) and Protected EAP-Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MSCHAPv2).

EAP over LAN (EAPoL): EAPoL is the Layer 2 encapsulation protocol used for the transport of the EAP from the supplicant to the switch.

RADIUS: RADIUS is the standard protocol used for communication between the authenticator (network device) and the authentication server.

802.1X consists of the following components:

* Supplicant: The supplicant is the component of 802.1X that runs on the endpoint device; that is, the device that is attempting to gain access to the network. The supplicant can be software that is installed on the endpoint, such as the Cisco AnyConnect Secure Mobility Client, or it can come embedded within the operating system itself, such as Microsoft Windows.

Authenticator: The authenticator is the component of 802.1X that provides the actual network connectivity to the endpoint once the endpoint has been successfully authenticated and authorized to use the network by the authentication server. 802.1X port-based authentication is configured on the network device (authenticator) to prevent unauthorized endpoints (supplicants) from gaining access to the network. The network device includes the RADIUS client, which is responsible for encapsulating and decapsulating the EAP frames and interacting with the authentication server. Examples of authenticators include routers, switches, and wireless access points.

Authentication Server: The authentication server is the component of 802.1X that validates the credentials of the supplicant on the endpoint to determine (a) whether the endpoint has the necessary authentication credentials to access the network and (b) what actions on the network the endpoint is authorized to perform. Examples of authentication servers include servers that support the RADIUS protocol, such as Cisco Secure Access Control Server (ACS) and the Cisco Identity Services Engine (ISE).

For more information on 802.1X please reference the following:

Wired 802.1X Deployment Guide: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec\_1-99/Dot1X\_Deployment/Dot1x\_Dep\_Guide.html

Campus 802.1X Authentication Technology Design Guide: http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2014/CVD-CampusDot1XDesignGuide-AUG14.pdf

Configuring IEEE 802.1X Port-Based Authentication: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x\_3560x/software/release/12-2\_55\_se/configuration/guide/3750xscg/sw8021x.html

Private VLANs (PVLAN)

PVLANs belong to the same overall primary VLAN. PVLANs segregate Layer 2 traffic by subdividing a primary VLAN into multiple secondary VLANs that are isolated from each other.

Switch ports within a Private VLAN can be configured for one of three modes:

* Promiscuous: A port that is configured to be in promiscuous mode can communicate with all ports associated with the Private VLAN (that is, secondary VLANs) as well as with ports outside the Private VLAN. A promiscuous port is considered to be in the primary VLAN so it can communicate with other primary VLANs on the switch as well as the secondary VLANs, of which community and isolated ports are members (community and isolated ports are described in the following paragraphs). The ports where routers and firewalls are connected are promiscuous ports because those ports can forward traffic coming from every secondary VLAN defined in the mapping as well as the primary VLAN. The ports connected to each host can only forward the traffic coming from the primary VLAN and the secondary VLAN configured on that port.

Community: A port that is configured to be in a community VLAN can communicate with ports within the same community VLAN as well as with a port configured as a promiscuous port in the primary VLAN. A community port is considered to be in the secondary VLAN.

Isolated: A port that is configured to be in an isolated VLAN can communicate only with a port that is configured as a promiscuous port in the primary VLAN. An isolated port is considered to be in the secondary VLAN.

The primary VLAN carries traffic from the promiscuous ports to the host ports, both isolated and community in secondary VLANs, and to other promiscuous ports in primary VLANs. Traffic that comes to a switch from a promiscuous port can go out on all the ports that belong to the same primary VLAN. Traffic that comes to a switch from a port mapped to a secondary VLAN (secondary VLAN ports are configured as either isolated or community ports) can be forwarded to a promiscuous port or a port belonging to the same community VLAN. Multiple ports mapped to the same isolated VLAN cannot exchange any traffic.

Figure B-1 depicts a PVLAN deployment consisting of a router, a Layer 2 switch, and several different endpoint devices. The router and the Layer 2 switch are connected via a primary VLAN configured on the promiscuous port on the Layer 2 switch. The Layer 2 switch then also has four additional PVLANs configured on it. There are three separate isolated VLANs (Isolated VLANs A, B, and C) and a community VLAN (Community VLAN A). The three workstations in Community VLAN A can communicate with each other as well as with the Layer 2 switch over the promiscuous (primary) VLAN. Each device on the isolated VLANs can only communicate with the Layer 2 switch over the promiscuous VLAN and cannot communicate with either the other devices in their respective isolated VLANs or with the devices in the community VLAN.



Figure B-1 Private VLAN Deployment

For more information on private VLANs please reference the following:

Configuring Private VLANs: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/PrivateVLANs.html