IMPLEMENTING CISCO THREAT CONTROL SOLUTIONS (CI-SITCS)

This subtopic provides an overview of how the course is organized. The course contains these components:

Cisco ASA (CX) NGFW Services

Cisco Web Security Appliance

Cisco Cloud Web Security

Cisco Email Security Appliance

Cisco Intrusion Prevention Systems

Lab 1-1: Explore the Cisco ASA (CX) NGFW and PRSM

Lab 1-2: Configure Cisco ASA (CX) NGFW Access Policy

Lab 1-3: Configure Cisco ASA (CX) NGFW Identity Policy

Lab 1-4: Configure Cisco ASA (CX) NGFW Decryption Policy

Lab 2-1: Configure Cisco Web Security Appliance Explicit Proxy and User Authentication

Lab 2-2: Configure Cisco Web Security Appliance Acceptable Use Controls

Lab 3-1: Configure Cisco Cloud Web Security Connector on ISR G2 and on AnyConnect

Lab 4-1: Configure Cisco Email Security Appliance Basic Policies

Lab 5-1: Configure Cisco ASA IPS Software Module

Detailed Course Outline

Module 1: Cisco ASA (CX) NGFW Services

Module Objective: Implement the Cisco Next Generation Firewall Services

Lesson 1: Describing the Cisco ASA (CX) NGFW Services

Lesson Objective: Describe the Cisco ASA (CX) NGFW solution

This lesson includes these topics:

Cisco Modular Network Architecture and Cisco (CX) NGFW Services

Cisco ASA (CX) NGFW Benefits and Components

Cisco ASA (CX) NGFW Broad and Web AVC

Cisco ASA (CX) NGFW Policy Types

Cisco ASA (CX) NGFW Compatibility with Existing Cisco ASA Features

Cisco ASA 5585-X NGFW CX-SSP Hardware Module

Cisco ASA 5500-X (CX) NGFW Software Module

Summary

Lesson 2: Describing the Cisco ASA (CX) NGFW Management Architecture

Lesson Objective: Describe the Cisco ASA (CX) NGFW management architecture and protocols

This lesson includes these topics:

Cisco ASA (CX) NGFW Management Architecture

On-Box and Off-Box Cisco PRSM

Cisco PRSM GUI Basic Functions

Cisco ASA (CX) NGFW Management Interface

Cisco ASA (CX) NGFW CLI Operations

Cisco ASA (CX) NGFW Licenses

Cisco Off-Box PRSM License

Cisco ASA (CX) NGFW and Off-Box Cisco PRSM License Management

Summary

Lesson 3: Configuring Cisco ASA (CX) NGFW Policy Objects

Lesson Objective: Describe how to configure Cisco ASA (CX) NGFW policy objects

This lesson includes these topics:

Cisco ASA-to-Cisco ASA (CX) NGFW Traffic Redirection

Cisco ASA (CX) NGFW Policy Structure

Cisco ASA (CX) NGFW Policy Object Types

Cisco ASA (CX) NGFW Network Objects

Cisco ASA (CX) NGFW Service Objects and Service Groups

Cisco ASA (CX) NGFW Application Objects and Application Service Objects

Cisco ASA (CX) NGFW URL Objects

Cisco ASA (CX) NGFW User Agent Objects

Cisco ASA (CX) NGFW Identity Objects

Cisco ASA (CX) NGFW Source Object and Destination Object Groups

Cisco ASA (CX) NGFW Secure Mobility Objects

Cisco ASA (CX) NGFW Action Profile Objects

Policy Objects in Cisco ASA (CX) NGFW Policies

Tags, Ticket IDs, and Metadata

Summary

Lesson 4: Monitoring Cisco ASA (CX) NGFW Operations

Lesson Objective: Explain how to monitor Cisco ASA (CX) NGFW operations by using Cisco PRSM

This lesson includes these topics:

Cisco PRSM Dashboards and Reports

Cisco PRSM Event Viewer

Cisco SIO Update Verifications

Summary

Lab 1-1: Explore the Cisco ASA (CX) NGFW and PRSM

Lab Objective: Verify the Cisco ASA (CX) NGFW status

This lab includes these tasks:

Task 1: Verify the ASA (CX) NGFW Software Module Status
Task 2: Shut Down and Uninstall the IPS Software Module (Perform only if CX is not Installed)
Task 3: Install and Set Up the ASA (CX) NGFW Software Module (Perform only if CX is not Installed)
Task 4: Explore the ASA (CX) NGFW CLI

Task 5: Explore the On-Box PRSM GUI
Task 6: Redirect Traffic from the ASA to ASA (CX) NGFW
Task 7: Explore the System Predefined Default ASA (CX) NGFW Policy Objects
Task 8: Configure ASA (CX) NGFW Policy Objects

Lesson 5: Configuring Cisco ASA (CX) NGFW Access Policies

Lesson Objective: Describe how to configure Cisco ASA (CX) NGFW access policies to match security requirements

Cisco ASA (CX) NGFW Access Policy Configuration

Cisco ASA (CX) NGFW Application Control Configuration

Cisco ASA (CX) NGFW URL Filtering Configuration

Cisco ASA (CX) NGFW File Filtering Profile Configuration

Cisco ASA (CX) NGFW Web Reputation Profile Configuration

Cisco ASA (CX) NGFW Access Policies Troubleshooting

Summary

Lab 1-2: Configure Cisco ASA (CX) NGFW Access Policy

Lab Objective: Configure and verify Cisco ASA (CX) NGFW access policies per the given security requirements

This lab includes these tasks:

Task 1: Configure the ASA CX Access Policy to Deny Access to Unacceptable Websites
Task 2: Configure the ASA CX Access Policy to Deny Any Executable File Download
Task 3: Configure an ASA CX Access Policy to Deny Access to Any Websites with a Bad Reputation
Task 4: Optional Challenge Lab Task: Configure ASA CX Access Policies

Lesson 6: Configuring Cisco ASA (CX) NGFW Identity Policies

Lesson Objective: Describe how to configure Cisco ASA (CX) NGFW identity policies to match security requirements

This lesson includes these topics:

Cisco ASA (CX) NGFW Active and Passive Authentications

Cisco ASA (CX) NGFW Authentication Realms

Cisco ASA (CX) NGFW ADI

Cisco ASA (CX) NGFW Identity-Based Policy Configuration

LDAP Authentication Realm and Server Configurations

Active Directory Authentication Realm and Server Configurations

Cisco ASA (CX) NGFW-to-Cisco CDA Integration Configurations

Cisco ASA (CX) NGFW Identity Policies with Active Authentication

Cisco ASA (CX) NGFW Identity Policies with Passive Authentication

Cisco ASA (CX) NGFW Authentication Settings Configuration

Cisco ASA (CX) NGFW Access and Decryption Policies with Identity Objects

Cisco ASA (CX) NGFW User Identity in Event Viewer

Cisco ASA CX Identity Policy Troubleshooting

Summary

Lab 1-3: Configure Cisco ASA (CX) NGFW Identity Policy

Lab Objective: Configure and verify Cisco ASA (CX) NGFW Identity Policies using active authentication

This lab includes these tasks:

Task 1: Configure an ASA CX Identity Policy Using Active Authentication

Task 2: Configure an ASA CX Identity Policy Using Passive Authentication

Task 3: Configure an ASA CX Access Policy Using an Identity Object per the Given Requirements

Lesson 7: Configuring Cisco ASA (CX) NGFW Decryption Policies

Lesson Objective: Describe how to configure Cisco ASA (CX) NGFW decryption policies to match security requirements

This lesson includes these topics:

Cisco ASA (CX) NGFW Decryption Policies

Cisco ASA (CX) NGFW Decryption Configurations

Cisco ASA (CX) NGFW Decryption Policy Configuration

Cisco ASA CX Decryption Policy Troubleshooting

Cisco ASA (CX) NGFW Identity, Decryption, and Access Policy Interactions

Summary

Lab 1-4: Configure Cisco ASA (CX) NGFW Decryption Policy

Lab Objective: Configure and verify decryption policy based on given security policy requirements

This lab includes these tasks:

Task 1: Enable Cisco ASA (CX) NGFW Decryption
Task 2: Configure a Cisco ASA (CX) NGFW Decryption Policy per Security Requirements

Lesson 8: Module Summary

This lesson includes these topics:

References

Lesson 9: Module Self-Check

Module 2: Cisco Web Security Appliance

Module Objective: Implement the Cisco Web Security Appliance

Lesson 1: Describing the Cisco Web Security Appliance Solutions

Lesson Objective: Describe the Cisco Web Security Appliance main features

This lesson includes these topics:

Cisco Modular Network Architecture and Cisco WSA

Cisco WSA Overview

Cisco WSA Architecture

Cisco WSA Malware Detection and Protection

Cisco Web-Based Reputation Score

Cisco WSA Acceptable Use Policy Enforcement

Cisco WSA GUI Management

Cisco WSA Committing the Configuration Changes

Cisco WSA Policy Types Overview

Cisco WSA Access Policies

Cisco WSA Identity: For Whom Does This Policy Apply To?

Cisco WSA Identity Example

Cisco WSA Policy Assignment Using Identity

Cisco WSA Identity and Authentication

Cisco WSA Policy Trace Tool

Summary

Lesson 2: Integrating the Cisco Web Security Appliance

Lesson Objective: Describe the two Cisco WSA integration methods (Explicit Proxy and Transparent Proxy)

This lesson includes these topics:

Explicit vs. Transparent Proxy Mode

Explicit Proxy Mode

PAC Files

PAC File Deployment Options

PAC File Hosting on Cisco WSA

Traffic Redirection In Transparent Mode

Connecting the Cisco WSA to a WCCP Router

Verifying WCCP

Summary

Lesson 3: Configuring Cisco Web Security Appliance Identities and User Authentication Controls

Lesson Objective: Configure identities and user authentication

This lesson includes these topics:

Configure Identities to Group Client Transactions

Configure Policy Groups

The Need for User Authentication

Authentication Protocols and Schemes

Basic Authentication in Explicit Proxy and Transparent Proxy Mode

Configure Realms and Realm Sequences

Configure NTLM Realm for Active Directory

Join Cisco WSA to Active Directory

Configure Global Authentication Settings

Configure an Identity to Require Authentication (Basic or NTLMSSP)

Configure an Identity to Require Transparent User Identification

Configure LDAP Realm for LDAP Servers

Define How User Information Is Stored in LDAP

Bind Cisco WSA to the LDAP Directory

LDAP Group Authorization

Allowing Guest Access to Users Who Fail Authentication

Testing Authentication Settings

Authenticated Users in Reports

Summary

Lab 2-1: Configure Cisco Web Security Appliance Explicit Proxy and User Authentication

Lab Objective: Implement the Cisco WSA in Explicit Proxy Mode

This lab includes these tasks:

Task 1: Verify Basic Cisco WSA Settings
Task 2: Implement the Cisco WSA in Explicit Proxy Mode
Task 3: Implement User Authentication with Active Directory using Basic Authentication
Task 4: Implement User Authentication using Transparent User Identification

Lesson 4: Configuring Cisco Web Security Appliance Acceptable Use Controls

Lesson Objective: Configure URL filtering and application visibility and control

This lesson includes these topics:

Acceptable Use Controls

URL Categorizing Process

Application Visibility and Control Overview

Streaming Media Bandwidth Control Overview

Enable Acceptable Use Controls

Using the Policies Table

Configure URL Filtering

Enable Safe Search and Site Content Ratings

Configure Custom URL Categories

URL Category Reports

Configuring AVC

Configure Media Bandwidth Limits

AVC Reports

Summary

Lab 2-2: Configure Cisco Web Security Appliance Acceptable Use Controls

Lab Objective: Implement the Cisco WSA in transparent proxy mode

This lab includes these tasks:

Task 1: Implement the Cisco WSA in Transparent Proxy Mode

Task 2: Configure the Access Policy

Task 3: Configure URL Filtering for the Access Policy

Task 4: Configure Application Visibility Control for the Access Policy

Lesson 5: Configuring Cisco Web Security Appliance Anti-Malware Controls

Lesson Objective: Configure inbound and outbound anti-malware controls

This lesson includes these topics:

Dynamic Vectoring and Streaming Engine Overview

Contrast Webroot with Sophos or McAfee Malware Scanning

Adaptive Scanning Overview

Web Reputation Filtering Overview

Enable Web Reputation Filtering, Adaptive Scanning and Malware Scanning

Configure Inbound Web Reputation Filtering and Malware Scanning

Configure Outbound Malware Scanning

Malware Reports

Summary

Lesson 6: Configuring Cisco Web Security Appliance Decryption

Lesson Objective: Configure decryption policies

This lesson includes these topics:

HTTPS Proxy Operations Overview

Enable HTTPS Proxy

Invalid Destination Web Server Certificate Handling

Configure Decryption Policies

Summary

Lesson 7: Configuring Cisco Web Security Appliance Data Security Controls

Lesson Objective: Configure data security controls to implement data loss prevention

This lesson includes these topics:

Cisco WSA Data Security Overview

Data Security Policies

Control Uploaded Content

External Data Loss Prevention

Add an ICAP Server

Summary

Lesson 8: Module Summary

This lesson includes these topics:

References

Lesson 9: Module Self-Check

Module 3: Cisco Cloud Web Security

Module Objective: Implement the Cisco Cloud Web Security Connectors

Lesson 1: Describing the Cisco Cloud Web Security Solutions

Lesson Objective: Describe the main features of the Cisco Cloud Web Security

This lesson includes these topics:

Cisco Modular Network Architecture and Cisco Cloud Web Security (CWS)

Cisco Cloud Web Security Overview

Cisco Cloud Web Security Traffic Flow Overview

Cisco Cloud Web Security URL Filtering, AVC and Reporting Features Overview

Cisco Cloud Web Security Scanning Processes and Day Zero Outbreak Intelligence Overview

Cisco ScanCenter Overview

Summary

Lesson 2: Configuring Cisco Cloud Web Security Connectors

Lesson Objective: Describe traffic redirection to Cloud Web Security through connectors, how to configure them on Cisco ASA, Cisco WSA and Cisco IOS, and how to configure AnyConnect web security module

This lesson includes these topics:

Cisco Cloud Web Security Traffic Redirection Overview

Cisco Cloud Web Security Authentication Key

Authentication Key Generation from the Cisco ScanCenter

Verifying Traffic Redirection to CWS Using Special URL

Cisco ASA Cloud Web Security Overview

Cisco ASA Cloud Web Security Basic Configuration Using ASDM

Cisco ASA Cloud Web Security Basic Configuration Using the CLI

Cisco ASA Cloud Web Security Configuration with the Whitelist and Identity Options Using the CLI

Verifying Cisco ASA Cloud Web Security Operations Using the Cisco ASDM

Verifying Cisco ASA Cloud Web Security Operations Using the CLI

Cisco AnyConnect Web Security Module Overview

Cisco AnyConnect Web Security Module for Standalone Use Overview

Configure Cisco AnyConnect Web Security Module for Standalone Use

Configure Cisco ASA to Download the Web Security Module to the Client Machine

Verifying Cisco AnyConnect Web Security Module Operations

Cisco ISR G2 Cloud Web Security Overview

Cisco ISR G2 Cloud Web Security Configuration

Cisco ISR G2 Cloud Web Security Verification

Cisco WSA Cloud Web Security Overview

Summary

Lesson 3: Describing the Web Filtering Policy in Cisco ScanCenter

Lesson Objective: Implement basic web filtering policy in Cisco ScanCenter

This lesson includes these topics:

ScanCenter Web Filtering Policy Overview

ScanCenter Web Filtering Policy Configuration

HTTPS Inspection Configuration Overview

ScanCenter Web Filtering Verification

ScanCenter Web Filtering Reporting

Summary

Lab 3-1: Configure Cisco Cloud Web Security Connector on ISR G2 and on AnyConnect

Lab Objective: Configure and verify the CWS connector on the Cisco ISR G2 router

This lab includes these tasks:

Task 1: Enable the CWS Connector on the Partner ISR G2 Router
Task 2: Enable the CWS Connector on the AnyConnect Secure Mobility Client

Lesson 4: Module Summary

This lesson includes these topics:

References

Lesson 5: Module Self-Check

Module 4: Cisco Email Security Appliance

Module Objective: Implement the Cisco Email Security Appliance

Lesson 1: Describing the Cisco Email Security Solutions

Lesson Objective: Illustrate the SMTP flows and conversations and provides a high level overview of the Cisco Email Security Appliance services

This lesson includes these topics:

Cisco Modular Network Architecture and Cisco ESA

Cisco Hybrid Email Security Solution Overview

SMTP Terminologies

SMTP Flow

SMTP Conversation

Cisco ESA Services Overview

Cisco ESA GUI Management

Cisco ESA Committing the Configuration Changes

Cisco ESA Licensing

Incoming Mail Processing Overview

Outgoing Mail Processing Overview

Cisco ESA LDAP Integration Overview

Cisco Registered Envelope Service (CRES) Overview

Summary

Lesson 2: Describing the Cisco Email Security Appliance Basic Setup Components

Lesson Objective: Describe the basic configuration components to setup the Cisco ESA, which includes the listener, LDAP queries, HAT, RAT, Mail Flow Policies and SMTP Routes table

This lesson includes these topics:

Cisco ESA Listener Overview

Cisco ESA Listener Type: Private and Public

Cisco ESA One Interface/One Listener Deployment Example

Cisco ESA Two Interfaces/Two Listeners Deployment Example

Cisco ESA Listener Major Components: HAT and RAT

Cisco ESA One Listener Deployment Scenario

One Listener Deployment Scenario: Interfaces and Listener

One Listener Deployment Scenario: LDAP Accept Query

One Listener Deployment Scenario: HAT

One Listener Deployment Scenario: HAT > Sender Group

One Listener Deployment Scenario: HAT > Sender Group SBRS

One Listener Deployment Scenario: HAT > BLACKLIST Sender Group

One Listener Deployment Scenario: HAT > RELAYLIST Sender Group

One Listener Deployment Scenario: HAT > Add Sender Group

One Listener Deployment Scenario: HAT > Mail Flow Policy

One Listener Deployment Scenario: HAT > Mail Flow Policy > Anti-Spam and Anti-Virus

One Listener Deployment Scenario: HAT > Mail Flow Policies Summary

One Listener Deployment Scenario: RAT

One Listener Deployment Scenario: SMTP Routes

One Listener Deployment Scenario: Email Relaying on Internal Mail Server

Summary

Lesson 3: Configuring Cisco Email Security Appliance Basic Incoming and Outgoing Mail Policies

Lesson Objective: Explain how to configure the different features within the incoming and outgoing mail policies (anti-spam, anti-virus, content filters, outbreak filters, data loss prevention)

This lesson includes these topics:

Cisco ESA Incoming and Outgoing Mail Policies Overview

Cisco ESA Mail Policies Matching

Anti-Spam Overview

Anti-Spam Configuration

Spam Quarantine Configuration

Policy, Virus, Outbreak Quarantines Configuration

Anti-Virus Overview

Anti-Virus Configuration

Content Filters Overview

Content Filters Configuration

Outbreak Filters Overview

Outbreak Filters Configuration

Data Loss Prevention Overview

Data Loss Prevention Configuration

Reporting Overview

Message Tracking

Trace

Summary

Lab 4-1: Configure Cisco Email Security Appliance Basic Policies

Lab Objective: Verify the initial email exchange without the ESA

This lab includes these tasks:

Task 1: Verify the Initial Email Exchange Without the Cisco ESA
Task 2: Deploy the Cisco ESA Mail Proxy
Task 3: Integrate the Cisco ESA with LDAP and Enable LDAP Accept Query
Task 4: Configure Incoming Content Filters and Mail Policies
Task 5: Configure Outbound Data Loss Prevention

Lesson 4: Module Summary

This lesson includes these topics:

References

Lesson 5: Module Self-Check

Module 5: Cisco Intrusion Prevention Systems

Module Objective: Implement the Cisco IPS Appliance and Modules

Lesson 1: Describing Cisco IPS Solutions

Lesson Objective: Describe the basic definitions and approaches to traditional intrusion prevention/detection systems and next generation IPS

This lesson includes these topics:

Cisco Modular Network Architecture and Cisco IPS

Intrusion Detection Systems vs. Intrusion Prevention Systems

Intrusion Prevention Systems Terminologies

Traditional Network Intrusion Prevention Systems

Sourcefire NGIPS Benefits Overview

ASA NGFW Services with NGIPS Overview

ASA NGFW Services NGIPS Threat Profile

Apply NGIPS Threat Profile in NGFW Services Access Policy

NGFW Services NGIPS Global Settings

Viewing NGIPS Threat Information in PRSM Event Viewer

Summary

Lesson 2: Integrating Cisco IPS Sensor into a Network

Lesson Objective: Configure the different Cisco IPS sensor interface modes

This lesson includes these topics:

Cisco IPS Sensor Deployment Modes Overview

Deploy Sensors in Promiscuous Mode

Deploy Sensors in Inline Interface Pair Mode

Deploy Sensors in Inline VLAN Pair Mode

Deploy Sensors in Inline VLAN Group Mode

Cisco IPS Management Options Overview

Configure Interfaces on IPS Sensor

Configure Promiscuous Interfaces

Configure Inline Interface Pairs

Configure Inline VLAN Pairs

Configure Inline VLAN Groups

Traffic Redirection to IPS Module Overview

Summary

Lesson 3: Configuring Basic Cisco IPS Operations

Lesson Objective: Configure basic Cisco IPS operations.

This lesson includes these topics:

IPS Signatures

IPS Signature Properties

IPS Actions

Configure a Virtual Sensor

IPS Threat Profiles Overview

Configure Basic Signature Properties

Risk Rating

Risk Rating Calculation

Threat Rating

Event Action Overrides Overview

Configure and Verify Event Action Overrides

Event Action Filters Overview

Configure and Verify Event Action Filters

Examine IPS Events using IDM

Summary

Lesson 4: Tuning Cisco IPS Signatures

Lesson Objective: Tune Cisco IPS signatures to reduce false positives and false negatives

This lesson includes these topics:

False Negatives

False Positives

False Positive Examples

Cisco IPS Tuning Approaches

Tune Cisco IPS to Reduce False Positives

Reduce False Positives: Narrow Search Context

Reduce False Positives: Narrow Header Values

Reduce False Positives: Limit Number of Matched Patterns

Reduce False Positives: Limit Number of Matched Patterns Example

Reduce False Positives: Decrease Attention Span

Reduce False Positives: Increase Number of Events

Tune Cisco IPS to Reduce False Negatives

Reduce False Negatives: IP Reassembly

Reduce False Negatives: TCP Reassembly

Reduce False Negatives: Deobfuscation

Summary

Lesson 5: Configuring Custom Cisco IPS Signatures

Lesson Objective: Configure custom Cisco IPS signatures.

This lesson includes these topics:

Custom Signatures Overview

Signature Engines

Custom Signature Creation Procedure

Custom Signature Matching Strategies

Configure Custom Signatures

Custom Signature Wizard

Custom Signature Wizard Options

Verify Custom Signatures

Summary

Lab 5-1: Configure Cisco ASA IPS Software Module

Lab Objective: Install the Cisco ASA IPS software module and configure basic IPS settings

This lab includes these tasks:

Task 1: Install the Cisco ASA IPS Software Module and Configure the Basic IPS Settings
Task 2: Verify the IPS Operations
Task 3: Tune Existing Signature
Task 4: Create Custom Signature

Lesson 6: Configuring Cisco IPS Anomaly Detection

Lesson Objective: Configure Cisco IPS anomaly detection.

This lesson includes these topics:

Anomaly Detection

Worm Scanning Methods

Scanners and Histograms

Anomaly Detection Zones

Anomaly Detection Learning and Knowledge Base

Anomaly Detection and Actions

Anomaly Detection Scenario

Anomaly Detection Configuration Procedure

Verify Knowledge Base Creation

Verify Anomaly Detection Operational Mode

Verify Anomaly Detection Statistics

Summary

Lesson 7: Configuring Cisco IPS Reputation-Based Features

Lesson Objective: Configure Cisco IPS global correlation features.

This lesson includes these topics:

Global Correlation and Reputation-Based Filtering Overview

IPS Processing Flow with Global Correlation and Reputation Filter

Reputation Filter Operations

Global Correlation Operations

Dynamic Updates from Cisco SensorBase

IPS Sensor Network Participation to Cisco SensorBase

Global Correlation Configurations

Verify Global Correlation and Reputation Filter

Summary

Lesson 8: Module Summary

This lesson includes these topics:

References

Lesson 9: Module Self-Check