IMPLEMENTING CORE CISCO ASA SECURITY (CI-SASAC)

Course Introduction

The Course Introduction provides learners with the course objectives and prerequisite learner skills and knowledge. The Course Introduction presents the course flow diagram and the icons that are used in the course illustrations and figures. This course component also describes the curriculum for this course, providing learners with the information that they need to make decisions regarding their specific learning path.

Overview

Module 1: Cisco ASA Adaptive Security Appliance Essentials

Lesson 1: Evaluating Cisco ASA Adaptive Security Appliance Technologies

Lesson Objective: Evaluate Cisco ASA Adaptive Security Appliance technologies

This lesson includes these topics:

Firewall Technologies

Cisco ASA Adaptive Security Appliance Features

Summary

Lesson 2: Identifying Cisco ASA Adaptive Security Appliance Models

Lesson Objective: Describe Cisco ASA adaptive security appliance models

This lesson includes these topics:

Cisco ASA Adaptive Security Appliance Hardware

Summary

Lesson 3: Identifying Cisco ASA Adaptive Security Appliance Licensing Options

Lesson Objective: Identify Cisco ASA adaptive security appliance licenses

This lesson includes these topics:

Cisco ASA Adaptive Security Appliance Licensing Options

Cisco ASA Adaptive Security Appliance Licensing Requirements
Summary

Lab 1-1: Accessing the Remote Lab Environment

Lab Objective: Describe how to access the Learning@Cisco-hosted ASA remote lab environment for your assigned pod

This lab includes these tasks:
C-12 Implementing Core Cisco ASA Security © 2014 Cisco Systems, Inc.

Task 1: Access the Learning@Cisco-Hosted ASA Remote Lab

Lesson 4: Module Summary

This lesson includes these topics:

References

Module 2: Basic Connectivity and Device Management

Module Objective: Describe how to configure and verify Cisco ASA security appliance network integration

Lesson 1: Preparing the Cisco ASA Adaptive Security Appliance for Network Integration

Lesson Objective: Describe how to configure initial device management features of a Cisco ASA security appliance to prepare for network integration

This lesson includes these topics:

Managing the Cisco ASA Adaptive Security Appliance Boot Process

Managing the Cisco ASA Adaptive Security Appliance Using the CLI

Managing the Cisco ASA Adaptive Security Appliance Using Cisco ASDM

Navigating Basic Cisco ASDM Features

Managing the Cisco ASA Adaptive Security Appliance Basic Upgrade

Summary

Lesson 2: Managing Basic Cisco ASA Adaptive Security Appliance Network Settings

Lesson Objective: Describe how to configure and troubleshoot Cisco ASA security appliance connectivity to the network environment

This lesson includes these topics:

Managing Cisco ASA Adaptive Security Appliance Security Levels

Configuring and Verifying Basic Connectivity Parameters

Configuring and Verifying Interface VLANs

Configuring a Default Route

Configuring and Verifying the Cisco ASA Security Appliance DHCP Server

Troubleshooting Basic Connectivity

Summary

Lab 2-1: Configuring the Cisco ASA Adaptive Security Appliance

Lab Objective: Verify the Cisco ASA security appliance and Cisco ASDM versions

This lab includes these tasks:

Task 1: Verify Cisco ASA Adaptive Security Appliance and Cisco ASDM Versions
Task 2: Initialize the Cisco ASA Adaptive Security Appliance from the CLI
Task 3: Launch Cisco ASDM and Test SSH Access
Task 4: Configure and Verify Interfaces
Task 5: Configure System Management Parameters

Lesson 3: Module Summary

Module 3: Network Integration

Lesson 1: Configuring Cisco ASA Adaptive Security Appliance NAT Features

Lesson Objective: Choose, configure, and troubleshoot Cisco ASA security appliance NAT features

This lesson includes these topics:

NAT on Cisco ASA Security Appliances

Configuring Object (Auto) NAT

Configuring Manual NAT

Tuning and Troubleshooting NAT on the Cisco ASA Adaptive Security Appliance

Summary

Lab 3-1: Configuring NAT

Lab Objective: Configure object NAT for the inside network and DMZ server

This lab includes these tasks:

Task 1: Configure Object NAT for the Client Network and DMZ Server

Task 2: Configure Manual NAT for the DMZ Server and Client Network

Lesson 2: Configuring Cisco ASA Adaptive Security Appliance Basic Access Control Features

Lesson Objective:

This lesson includes these topics:

Connection Table and Local Host Table

Configuring and Verifying Interface ACLs

Configuring and Verifying Global ACLs

Configuring and Verifying Object Groups

Configuring and Verifying Public Servers

Configuring and Verifying Other Basic Access Controls

Troubleshooting ACLs

Summary

Lab 3-2: Configuring Basic Cisco Access Control Features

Lab Objective: Troubleshoot basic connectivity using packet capture, ping, and Cisco Packet Tracer

This lab includes these tasks:

Task 1: Troubleshoot Basic Connectivity
Task 2: Configure Network and Service Object Groups
Task 3: Configure Access Lists
Task 4: Configure Public Servers
Task 5: Configure Global Access Lists
Task 6: (Optional) Configure Unicast Reverse Path Forwarding Check

Lesson 3: Configuring Cisco ASA Adaptive Security Appliance Routing Features

Lesson Objective: Choose and configure routing features on the Cisco ASA security appliance

This lesson includes these topics:

Static Routing
Dynamic Routing
EIGRP Configuration and Verification

Multicast Support
Summary

Lesson 4: Module Summary

This lesson includes these topics:

References

Module 4: Cisco ASA Adaptive Security Appliance Policy Controls

Lesson 1: Defining the Cisco ASA Adaptive Security Appliance MPF

This lesson includes these topics:

Cisco MPF Overview

Configuring and Verifying Layer 3 and Layer 4 Policies

Configuring and Verifying a Policy for Management Traffic

Summary

Lab 4-1: Configuring MPF, Basic Stateful Inspections, and QoS

Lab Objective: Configure ICMP and FTP inspection

This lab includes these tasks:

Task 1: Configure ICMP and FTP Inspection
Task 2: Enable TTL Decrement and Disable TCP Initial Sequence Randomization
Task 3: Tune TCP Timeouts, Enable TCP DCD, and Configure TCP Normalization
Task 4: Configure a Priority Queue and Traffic Policing

Lesson 2: Configuring Cisco ASA Adaptive Security Appliance Advanced Application Inspections

This lesson includes these topics:

Layer 5 to Layer 7 Policy Control Overview

Configuring and Verifying HTTP Inspection

Configuring and Verifying FTP Inspection

Supporting Other Layer 5 to Layer 7 Applications

Troubleshooting Application Layer Inspection

Summary

Lab 4-2: Configuring MPF Advanced Application Inspections

Lab Objective: Configure HTTP inspection to verify conformance to the HTTP protocol and to prevent HTTP requests containing certain file types

This lab includes these tasks:

Task 1: Configure HTTP Inspection to Protect the DMZ Server
Task 2: Configure FTP Inspection to Protect the DMZ Server
Task 3: Return the Cisco ASA Security Appliance to the Default Inspection Policies

Lesson 3: Module Summary

This lesson includes these topics:

References

Module 5: Cisco ASA Adaptive Security Appliance VPN Common Components

Lesson 1: VPN Overview

Lesson Objective: Describe the role of VPNs in network security

This lesson includes these topics:

VPN Definition

Key Threats to WANs and Remote Access

VPN Types

VPN Components

Summary

Lesson 2: Implementing Profiles, Group Policies, and User Policies

This lesson includes these topics:

Cisco ASA VPN Policy Configuration

Cisco ASA Adaptive Security Appliance Connection Profiles

Cisco ASA Adaptive Security Appliance Group Policies

Cisco ASA VPN AAA and External Policy Storage

Cisco ASA Adaptive Security Appliance User Attributes
Access Control Methods

VPN Accounting Using External Servers

DAP for SSL VPN

Summary

Lesson 3: Implementing PKI Services

This lesson includes these topics:

Using PKI

Provisioning Server-Side Certificates on the Cisco ASA Adaptive Security Appliance

CA Servers

Deploying Client-Based Certificate Authentication

SCEP Proxy Operations

Enable Certificate Authentication in Connection Profile

Configuring Certificate-to-Connection Profile Mappings

Summary

Lesson 4: Module Summary

Module 6: Cisco Clientless VPN Solution

Lesson 1: Introducing Clientless SSL VPN

Lesson Objective: Describe the clientless SSL VPN solution and provide a general description of the SSL/TLS protocol

This lesson includes these topics:

Cisco Clientless SSL VPN

Cisco Clientless SSL VPN Use Cases

Cisco Clientless SSL VPN Resource Access Methods

Secure Sockets Layer and Transport Layer Security

SSL Session Setup and Key Management

SSL Server Authentication

SSL Client Authentication
SSL Transmission Protection

Summary

Lesson 2: Deploying Basic Cisco Clientless SSL VPN on the Cisco ASA Adaptive Security Appliance

Lesson Objective: Configure and verify baseline clientless SSL VPN remote access features of the Cisco ASA security appliance

This lesson includes these topics:

Basic Cisco Clientless SSL VPN

Server Authentication in Basic Clientless SSL VPN

Client-Side Authentication in Basic Clientless SSL VPN

Clientless SSL VPN URL Entry and Bookmarks

Basic Access Control for Clientless SSL VPN

Disabling Content Rewriting

Basic Clientless SSL VPN Configuration Tasks

Basic Clientless SSL VPN Configuration Scenario

Configuring Basic Cisco Clientless SSL VPN

Verifying Basic Cisco Clientless SSL VPN

Troubleshooting Basic Clientless SSL VPN Operations

Summary

Lab 6-1: Implementing Basic Clientless SSL VPN on the Cisco ASA

Lab Objective: Enable basic clientless SSL VPN connections on the Cisco ASA

This lab includes these tasks:

Task 1: Configure the Cisco ASA to Use DNS
Task 2: Enable Clientless SSL VPN Connections
Task 3: Provision an Identity Certificate for the Cisco ASA
Task 4: Configure Local User Authentication
Task 5: Configure Bookmarks and Access Control

Lesson 3: Deploying Application Access in Cisco Clientless SSL VPN

Lesson Objective: Deploy and manage advanced application-access features of a clientless Cisco SSL VPN

This lesson includes these topics:

Cisco Clientless SSL VPN Application Access Overview

Application Plug-Ins

Configuring Application Plug-ins

Verify Clientless SSL VPN Application Plug-Ins

Troubleshooting Clientless SSL VPN Application Plug-Ins

Smart Tunnels

Configuring Smart Tunnels

Verifying Smart Tunnels

Troubleshoot Smart Tunnels

Summary

Lab 6-2: Configuring Application Access for Clientless SSL VPN on the Cisco ASA

Lab Objective: Deploy application plug-ins in the clientless SSL VPNs

This lab includes these tasks:

Task 1: Configure Application Access Using Plug-ins
Task 2: Configure Application Access Using Smart Tunnels

Lesson 4: Deploying Client-Side Authentication and Authorization in Clientless SSL VPN

Lesson Objective: Deploy and manage advanced authentication and authorization features of a clientless Cisco SSL VPN

This lesson includes these topics:

Client-Side Authentication Options

Client-Side Authentication and Authorization Using AAA Server

Double Client-Side Authentication Using AAA Servers

Troubleshooting Client-Side AAA Authentication

Summary

Lab 6-3: Implementing External Authentication and Authorization for Clientless SSL VPNs

Lab Objective: Configure the Cisco ASA to use a Microsoft Active Directory LDAP server for user authentication

This lab includes these tasks:

Task 1: Configure External Authentication Using Microsoft Active Directory
Task 2: Configure External Authorization Using Microsoft Active Directory

Lesson 5: Module Summary

This lesson includes these topics:

References

Module 7: Cisco AnyConnect Full Tunnel VPN Solutions

Module Objective:

Lesson 1: Deploying Basic Cisco AnyConnect SSL VPN on Cisco ASA

Lesson Objective: Configure, verify, and troubleshoot a basic Cisco AnyConnect SSL VPN on a Cisco ASA security appliance

This lesson includes these topics:

Basic Cisco AnyConnect SSL VPN

SSL VPN Clients Authentication

SSL VPN Client IP Address Assignment

SSL VPN Split Tunneling

Configuration Scenario

Configuration Tasks

Enable Cisco AnyConnect SSL VPNs

Define IP Address Pool

Configure Identity NAT

Configure Group Policy

Configure Group Policy: Split Tunneling

Configure Connection Profile

Monitor Cisco AnyConnect VPN on Client Endpoint

Monitor Cisco AnyConnect VPN on Server

Summary

Lab 7-1: Implementing Basic Cisco AnyConnect SSL VPN on the Cisco ASA

Lab Objective: Enable Cisco AnyConnect SSL VPN connections

This lab includes these tasks:

Task 1: Enable Cisco AnyConnect SSL VPN Connections
Task 2: Configure the VPN IP Address Pool and Identity NAT
Task 3: Configure a VPN User and Create a Connection Profile
Task 4: Configure Group Policy: IP Pool, DNS, and Split Tunneling
Task 5: Test Cisco AnyConnect SSL VPNs

Lesson 2: Deploying Advanced Cisco AnyConnect SSL VPN on Cisco ASA

Lesson Objective: Configure, verify, and troubleshoot advanced features of Cisco AnyConnect SSL VPNs

This lesson includes these topics:

Cisco AnyConnect SSL VPN Solution Components

DTLS Overview

Parallel DTLS and TLS Tunnels

Configure DTLS

Verify DTLS

Cisco AnyConnect Client Configuration Management

Managing Cisco AnyConnect Software from Cisco ASA

Cisco AnyConnect Client Operating System Integration Options

Deploying Cisco AnyConnect Trusted Network Detection

Cisco AnyConnect Start Before Logon

Deploying Cisco AnyConnect Start Before Logon

Summary

Lesson 3: Deploying Advanced Authentication and Authorization in Cisco AnyConnect VPNs

Lesson Objective: Configure, verify, and troubleshoot advanced authentication and authorization in Cisco AnyConnect VPNs

This lesson includes these topics:

Cisco AnyConnect Advanced Authentication Scenarios

Certificate-Based Server Authentication

Client Enrollment Methods

Methods for Revoking Credentials

Enable Certificate-Based Authentication

Enable Two-Factor Authentication

Two-Factor Authentication with Name Prefill

Local Authorization Overview

Local Authorization Configuration Procedure

Configure Local Authorization

Verify Local Authorization

External Authorization Scenario

Configure Authorization Using LDAP/AD

Verify External Authorization

Troubleshooting Cisco AnyConnect VPN

Summary

Lab 7-2: Configuring Advanced Authentication for Cisco AnyConnect SSL VPNs

Lab Objective: Deploy external authentication by using Microsoft Active Directory

This lab includes these tasks:

Task 1: Review LDAP and Active Directory Server Settings on the Cisco ASA
Task 2: Deploy Local Authorization for Local VPN Users
Task 3: Deploy External Authorization Using Microsoft Active Directory
Task 4: Deploy a Standalone Cisco AnyConnect Client on the Outside PC

Lesson 4: Deploying Cisco AnyConnect IPsec/IKEv2 VPNs

Lesson Objective: Configure, verify, and troubleshoot a Cisco AnyConnect IPsec/IKEv2 VPN on Cisco ASA security appliances

This lesson includes these topics:

Cisco AnyConnect Support for IKEv2

Internet Key Exchange v1 and v2

Making IPsec the Primary Protocol for a Host Entry

IKEv2 Configuration Procedure

Configure a Cisco AnyConnect IPsec VPN on a Cisco ASA Appliance

Verify and Troubleshoot Cisco AnyConnect IPsec VPN on Cisco ASA Appliance

Summary

Lab 7-3: Implementing Cisco AnyConnect IPsec/IKEv2 VPNs

Lab Objective: Implement Cisco AnyConnect IPsec/IKEv2 VPNs by using the WebLaunch method

This lab includes these tasks:

Task 1: Deploy Cisco AnyConnect IPsec/IKEv2 VPN with WebLaunch

Lesson 5: Module Summary

This lesson includes these topics:

References

Module 8: Cisco ASA Adaptive Security Appliance High Availability and Virtualization

Lesson 1: Configuring Cisco ASA Adaptive Security Appliance Interface Redundancy Features

Lesson Objective: Choose and configure interface redundancy features on the Cisco ASA security appliance

This lesson includes these topics:

Configuring and Verifying EtherChannel

Configuring and Verifying Redundant Interfaces

Troubleshooting EtherChannel and Redundant Interfaces

Summary

Lesson 2: Configuring Cisco ASA Adaptive Security Appliance Active/Standby High Availability

Lesson Objective: Configure and troubleshoot stateful active/standby high availability on the Cisco ASA security appliance

This lesson includes these topics:

Failover Overview

Configuration Choices, Basic Procedures, and Required Input Parameters

Configuring and Verifying Active/Standby Failover

Tuning and Managing Active/Standby Failover

Remote Command Execution

Troubleshooting Active/Standby Failover

Summary

Lesson 3: Configuring Security Contexts on the Cisco ASA Adaptive Security Appliance

Lesson Objective: Choose and configure virtual contexts on the Cisco ASA security appliance

This lesson includes these topics:

Multiple-Context Mode

Configuring Security Contexts

Verifying and Managing Security Contexts

Configuring and Verifying Resource Management

Troubleshooting Security Contexts

Summary

Lab 8-1: Configuring Active/Standby High Availability

Lab Objective: Prepare the secondary Cisco ASA security appliance for active/standby high availability

This lab includes these tasks:

Task 1: Prepare the Secondary Appliance for Failover Configuration via the CLI and Cisco ASDM
Task 2: Configure Active/Standby Failover
Task 3: Configure Standby IP Addresses on the Active Appliance and Test Failover
Task 4: Tune Active/Standby Failover
Task 5: Enable Stateful Active/Standby Failover

Lesson 4: Module Summary

This lesson includes these topics:

References

Lesson 5: (OPTIONAL) Configuring Cisco ASA Adaptive Security Appliance Active/Active High Availability (Optional/Self-study)

This lesson includes these topics:

Active/Active Failover

Configuring and Verifying Active/Active Failover

Tuning and Managing Active/Active Failover

Troubleshooting Active/Active Failover