ASACDO (CISCO ASA + CISCO DEFENSE ORCHESTRATOR) 1.0

Objetivo

Ao concluir este treinamento, o aluno serÃi capaz de cumprir estes objetivos gerais: â□¢ Explicar os principais recursos essenciais dos Cisco ASA 5500-X Next-Generation Firewalls; â□¢ Descrever como implementar a conectividade bÃisica Cisco ASA e o gerenciamento de dispositivos; â□¢ Implementar integraÃ§Ã£o do ASA junto a uma rede; â□¢ Descrever e implementar controles bÃisicos de polÃtica do Cisco ASA; â□¢ Descrever os componentes VPN comuns do Cisco ASA; â□¢ Descrever e implementar soluÃ§Ãµes VPN de tÃºnel completo Cisco ASA e Cisco AnyConnect; â□¢ Descrever as funcionalidades do CDO; â□¢ Explicar o processo de integraÃ§Ã£o do CDO junto ao Cisco ASA; â□¢ Descrever as funcionalidades e ferramentas do CDO.

PÃºblico Alvo

Profissionais de seguranÃ§a que necessitam de conhecimentos na instalaÃ§Ã£o, configuraÃ§Ã£o, operaÃ§Ã£o e administraÃ§Ã£o do Cisco ASA utilizando o ASDM/CLI, e a utilizaÃ§Ã£o do CDO e suas funcionalidades de integraÃ§Ã£o e gerÃªncia.

PrÃ©-Requisitos

Ã□ recomendado que os alunos possuam as seguintes habilidades e conhecimentos prÃ©vios ao treinamento: â□¢ Conhecimento prÃitico em redes IP (bÃisico); â□¢ Conhecimento bÃisico de firewall de seguranÃ§a.

Carga HorÃiria

40 horas (5 dias).

ConteÃºdo ProgramÃitico

Parte 1: Cisco ASA (ASDM + CLI) 24 horas

Course Introduction
Course Outline
Course Goals & Objectives

Cisco ASA Adaptive Security Appliance Essentials
Evaluating Cisco ASA Adaptive Security Appliance Technologies
Firewall Technologies
Cisco ASA Adaptive Security Appliance Features
Cisco ASA 5508 Architecture

Basic Connectivity and Device Management
Preparing the Cisco ASA Adaptive Security Appliance for Network Integration
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

Managing Basic Cisco ASA Adaptive Security Appliance Network Settings
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

Network Integration
Configuring Cisco ASA Adaptive Security Appliance NAT Features
NAT on Cisco ASA Security Appliances
Configuring Object (Auto) NAT
Configuring Manual NAT
Tuning and Troubleshooting NAT on the Cisco ASA Adaptive Security Appliance

Configuring Cisco ASA Adaptive Security Appliance Basic Access Control Features
Connection Table and Local Host Table
Configuring and Verifying Interface ACLs
Configuring and Verifying Global ACLs
Configuring and Verifying Object Groups
Configuring and Verifying Other Basic Access Controls
Troubleshooting ACLs

Configuring Cisco ASA Adaptive Security Appliance Routing Features
Static Routing
Dynamic Routing
EIGRP Configuration and Verification

Cisco ASA Adaptive Security Appliance Policy Controls
Defining the Cisco ASA Adaptive Security Appliance MPF
Cisco MPF Overview
Configuring and Verifying Layer 3 and Layer 4 Policies
Configuring and Verifying a Policy for Management Traffic

Configuring Cisco ASA Adaptive Security Appliance Advanced Application Inspections
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

Cisco ASA Adaptive Security Appliance VPN Common Components
VPN Overview
VPN Definition
Key Threats to WANs and Remote Access
VPN Types
VPN Components

Implementing Profiles, Group Policies, and User Policies
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

Implementing PKI Services
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

Cisco AnyConnect Full Tunnel VPN Solutions
Deploying Basic Cisco AnyConnect SSL VPN on Cisco ASA
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

Deploying Advanced Cisco AnyConnect SSL VPN on Cisco ASA
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

Deploying Cisco AnyConnect IPsec/IKEv2 VPNs
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

Cisco ASA Adaptive Security Appliance High Availability and Virtualization
Configuring Cisco ASA Adaptive Security Appliance Interface Redundancy Features
Configuring and Verifying EtherChannel
Configuring and Verifying Redundant Interfaces
Troubleshooting EtherChannel and Redundant Interfaces

Configuring Cisco ASA Adaptive Security Appliance Active/Standby High Availability
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

Labs Outline
Lab 1: Accessing the Remote Lab Environment
Lab 2: Configuring the Cisco ASA Adaptive Security Appliance
Lab 3: Configuring NAT
Lab 4: Configuring Basic Cisco Access Control Features
Lab 5: Configuring MPF, Basic Stateful Inspections, and QoS
Lab 6: Configuring MPF Advanced Application Inspections
Lab 7: Implementing Basic Cisco AnyConnect SSL VPN on the Cisco ASA
Lab 8: Configuring Advanced Authentication for Cisco AnyConnect SSL VPNs
Lab 9: Implementing Cisco AnyConnect IPsec/IKEv2 VPNs
Lab 10: Configuring Active/Standby High Availability

Parte 2: Cisco Defense Orchestrator (16 Horas)

Cisco Defense Orchestrator Architecture
Network Security Strategy
Security Management
Cisco Defense Orchestrator Solution

Licensing Options
Supported Platforms
Benefits of CDO

Deploy CDO
Initial Deployment
SDC: Secure Device Connector
SAL: Security Analytics & Logging
Cisco Devices Integration

Cisco CDO Tenant Management
General Settings
User Management
User Roles
Logging Settings

Managing Cisco ASA with CDO
CDO & Cisco Tenant
Using SDC on local Network
Integrating Cisco ASA & CDO
CDO Management Features for ASA Devices

Demonstration Cisco CDO Scenarios
Scenario 1. Network health status at-a-glance
Scenario 2. Onboard devices
Scenario 3. Clean up configurations and policies
Scenario 4. Use the Command-Line Interface (CLI)
Scenario 5. Schedule deployments
Scenario 6. Manage VPN
Scenario 7. Use the Logging and Security Analytics service
Scenario 8. Analytics and Detection
Scenario 9. Total Network Analytics and Detection
Scenario 10. Multi-Domain Management