SASAC (IMPLEMENTING CORE CISCO ASA SECURITY)

Objetivo

Este curso capacita um administrador de rede para implantar uma solução de firewall Cisco utilizando o ASA. Após a conclusão deste curso, o aluno será capaz de atender a esses objetivos gerais: • Explicar as características essenciais do núcleo de serviços do Cisco ASA 5500-X Firewalls; • Descrever e implantar a conectividade básica e o gerenciamento; • Descrever e implantar a integração básica na rede; • Descrever e implantar controles básicos de política; • Descrever e implantar os componentes de VPN mais comuns; • Descrever e implantar soluções de VPN Client-Less SSL; • Descrever e implantar soluções de VPN Full-Tunnel com Cisco AnyConnect.

Público Alvo

O público principal deste curso é composto por: • Os engenheiros de rede e operadores que prestam suporte em soluções utilizando a versão 9.x do Cisco ASA.

Pré-Requisitos

Os conhecimentos e habilidades que o aluno deve ter antes de participar deste curso são os seguintes: • Certificação CCNA ou conhecimentos equivalentes; • Ter participado nos cursos Firewall 1.0 ou firewall v2.0, ou possuír conhecimentos equivalentes.

Carga Horária

40 horas (5 dias).

Conteúdo Programático

Cisco ASA Adaptive Security Appliance Essentials
Evaluating Cisco ASA Adaptive Security Appliance Technologies
• Firewall Technologies
• Cisco ASA Adaptive Security Appliance Features

Identifying Cisco ASA Adaptive Security Appliance Models
• Cisco ASA Adaptive Security Appliance Hardware

Identifying Cisco ASA Adaptive Security Appliance Licensing Options
• Cisco ASA Adaptive Security Appliance Licensing Options
• Cisco ASA Adaptive Security Appliance Licensing Requirements

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 Public Servers
- 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
- Multicast Support

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 Clientless VPN Solution
Introducing Clientless SSL VPN
• 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

Deploying Basic Cisco Clientless SSL VPN on the Cisco ASA Adaptive Security Appliance
• 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 Opera

Deploying Application Access in Cisco Clientless SSL VPN
• 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

Deploying Client-Side Authentication and Authorization in Clientless SSL VPN
• Client-Side Authentication Options
• Client-Side Authentication and Authorization Using AAA Server
• Double Client-Side Authentication Using AAA Servers
• Troubleshooting Client-Side AAA Authentication

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 Advanced Authentication and Authorization in Cisco AnyConnect VPNs
• 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

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

Configuring Security Contexts on the Cisco ASA Adaptive Security Appliance
• Multiple-Context Mode
• Configuring Security Contexts
• Verifying and Managing Security Contexts
• Configuring and Verifying Resource Management
• Troubleshooting Security Contexts

LABS
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 Clientless SSL VPN on the Cisco ASA
Lab 8: Configuring Application Access for Clientless SSL VPN on the Cisco ASA
Lab 9: Implementing External Authentication and Authorization for Clientless SSL VPNs
Lab 10: Implementing Basic Cisco AnyConnect SSL VPN on the Cisco ASA
Lab 11: Configuring Advanced Authentication for Cisco AnyConnect SSL VPNs
Lab 12: Implementing Cisco AnyConnect IPsec/IKEv2 VPNs
Lab 13: Configuring Active/Standby High Availability