FIREWALL (DEPLOYING CISCO ASA FIREWALL SOLUTIONS) 2.0

Objetivo

Este treinamento proporciona ao profissional as habilidades necessárias para configurar, operar e prestar suporte aos recursos do Cisco ASA 5500 Series Adaptive Security Appliances (ASA) Firewall. As abordagens conceituais serão sempre acompanhadas de atividades práticas em laboratórios. Ao final do curso, o profissional estará apto a: Descrever a Tecnologia e recursos do Cisco ASA Firewall; Descrever a Família de produtos Cisco ASA; Aprender como o Firewall ASA protege os dispositivos de uma rede dos ataques; Realizar a Configuração Inicial; Utilizar o ASDM (Asa Security Device Manager) em atividades de configuração e monitoramento; Utilizar a linha de comando (CLI) para configuração e suporte; Integrar o ASA com ao Cisco Secure ACS para o processo AAA administrativo utilizando o protocolo TACACS+; Integrar o ASA ao Cisco Secure ACS para controle de acesso dos usuários à rede utilizando o protocolo RADIUS; Configurar Regras de NAT (Network Address Translation); Configurar uma política de acesso utilizando o recurso "Global Access Control List (ACL)"; Configurar uma política de acesso utilizando o recurso "Access Control List" (ACL) aplicadas nas interfaces; Utilizar grupos de objetos para simplificar a complexidade e manutenção das regras (ACL´s); Utilizar "Modular Policy Framework" (MFP) para prover políticas para inspeção das aplicações e serviços de rede; Realizar atividades de suporte através das ferramentas "TCP Ping", ¨Syslog¨, ¨Packet Tracer¨ e realizar a captura de pacotes; Configurar o dispositivo de segurança para operar como firewall de camada 2 denominado como "Transparent Firewall"; Habilitar, configurar e gerenciar múltiplos contextos para atender aos requisitos da política de segurança; Selecionar e configurar o tipo de recurso de alta disponibilidade (destacando o processo denominado de "Failover") que melhor se aplica a topologia da rede; Realizar atividade de monitoramento e gerência.

Público Alvo

Este treinamento é recomendado para profissionais que implementam e realizam atividades de suporte em dispositivos Cisco ASA Firewall.

Pré-Requisitos

Para maior aproveitamento deste treinamento é recomendado que o aluno: Tenha participado em treinamento ICND1 e ICND2, ou possua conhecimentos equivalentes; Tenha participado em treinamento IINS 2.0 (CCNA Security) ou possua conhecimentos equivalentes.

Carga Horária

40 horas (5 dias).

Conteúdo Programático

1. Cisco ASA Introduction
Cisco ASA Technologies
Cisco ASA Families
Cisco ASA Licensing Options

2. Basic Connectivity and Device Management
Preparing the Cisco ASA for Network Integration
Managing Basic Cisco ASA Network Settings
Configuring Cisco ASA Device Management Features

3. Network Integration
Configuring Cisco ASA NAT Features
Configuring Cisco ASA Basic Access Control Features
Configuring Cisco ASA Routing Features
Configuring the Cisco ASA Transparent Firewall

4. Cisco ASA Policy Control
Defining the Cisco ASA Modular Policy Framework (MPF)
Configuring Cisco ASA Connection Policy and QoS Settings
Configuring Cisco ASA Advanced Application Inspections
Configuring Cisco ASA User-Based Policies

5. Cisco ASA High Availability and Virtualization
Configuring Cisco ASA Interface Redundancy Features
Configuring Cisco ASA Active/Standby High Availability
Configuring Security Contexts on the Cisco ASA
Configuring Cisco ASA Active/Active High Availability

Labs
Lab 1: Enhanced - Preparing the ASA for Administration
Lab 2: Enhanced - Fundamental ASA Configuration
Lab 3: Enhanced - AAA for Administrative Access
Lab 4: Enhanced - Network Address Translation
Lab 5: Enhanced - Basic Access Control
Lab 6: Exclusive - ICMP, uRPF, and Troubleshooting Tools
Lab 7: Enhanced - Transparent Firewall
Lab 8: Enhanced - Basic Protocol Inspection
Lab 9: Enhanced - Advanced Protocol Inspection
Lab 10: Enhanced - User-Based Policies
Lab 11: Enhanced - Active/Standby Failover
Lab 12: Enhanced - Active/Active Failover