VPN (DEPLOYING CISCO ASA VPN SOLUTIONS) 2.0

Objetivo

Este treinamento tem como objetivo fornecer conhecimento necessário para Implantar e manter soluções de segurança Cisco ASA utilizando os recursos para soluções em VPN. Ao final do curso, o aluno estará apto a: •Descrever as propriedades gerais de segurança do ASA com soluções em VPN •Implantar e manter o Cisco clientless remote access Secure Sockets Layer (SSL) VPNs •Implantar e manter uma solução em remote access VPN IPsec •Implantar e manter uma solução site-to-site VPN IPSec •Implantar segurança nos dispositivos remotos utilizando as ferramentas Cisco Secure Desktop e Dynamic Access Policy (DAP), •Implantar e gerenciar alta disponibilidade no ASA em uma solução de VPN

Público Alvo

Este treinamento é recomendado para profissionais que buscam conhecimentos no equipamento Cisco ASA 5500 Series, suas soluções, configurações e Administração. Também a Engenheiros de Sistema que prestam suporte a vendas.

Pré-Requisitos

Para total aproveitamento neste treinamento é altamente recomendado que o aluno possua certificação Cisco CCNA Security (Curso IINS) e ICND1 (conhecimentos básicos de rede). Também é recomendado que o profissional tenha realizado o treinamento Cisco FIREWALL (Firewall 1.0/2.0) ou possua conhecimentos equivalentes, e bons conhecimentos no sistema operacional Windows.

Carga Horária

40 horas (5 dias).

Conteúdo Programático

Cisco ASA Adaptive Security Appliance VPN Architecture and Common Components
Evaluating the Cisco ASA Adaptive Security Appliance VPN Subsystem Architecture
Evaluating the Cisco ASA Adaptive Security Appliance Software Architecture
Implementing Profiles, Group Policies, and User Policies
Implementing PKI Services

Cisco ASA Adaptive Security Appliance Clientless Remote Access SSL VPN Solutions
Deploying Basic Clientless VPN Solutions
Deploying Advanced Application Access for Clientless SSL VPNs
Deploying Advanced Authentication and SSO for Clientless SSL VPNs
Customizing the Clientless SSL VPN User Interface and Portal

Cisco AnyConnect Remote Access SSL Solutions
Deploying a Basic Cisco AnyConnect Full-Tunnel SSL VPN Solution
Deploying an Advanced Cisco AnyConnect Full-Tunnel SSL VPN Solution
Deploying Advanced Authentication, Authorization, and Accounting in Cisco Full-Tunnel VPNs

Cisco ASA Adaptive Security Appliance Remote Access IPsec VPNs
Deploying Cisco Remote Access VPN Clients
Deploying Basic Cisco Remote Access IPsec VPN Solutions

Cisco ASA Adaptive Security Appliance Site-to-Site IPsec VPN Solutions
Deploying Basic Site-to-Site IPsec VPNs
Deploying Advanced Site-to-Site IPsec VPNs

Endpoint Security and High Availability for Cisco ASA VPNs
Implementing Cisco Secure Desktop and DAP for SSL VPNs
Deploying High-Availability Features in Cisco ASA Adaptive Security Appliance VPNs

Labs
Lab 2-1: Configuring Basic Clientless VPN Access on the Cisco ASA Security Appliance
Lab 2-2: Configuring Advanced Application Access for Clientless SSL VPNs
Lab 2-3: Customizing the SSL VPN Portal on the Cisco ASA Security Appliance
Lab 3-1: Configuring Basic Cisco AnyConnect Client Full-Tunnel SSL VPNs Using Local Password Authentication
Lab 3-2: Deploying the Cisco AnyConnect Client with Centralized Management
Lab 3-3: Configuring Basic Cisco AnyConnect Full-Tunnel SSL VPNs Using Local CA and SCEP Proxy
Lab 4-1: Deploying Basic Remote Access IPsec VPN with IKEv2
Lab 5-1: Deploying a Basic Cisco ASA Security Appliance IPsec IKEv1 Site-to-Site VPN
Lab 6-1: Deploying Cisco Secure Desktop in Cisco SSL VPNs
Lab 6-2: Configuring a Load-Balancing SSL VPN Cluster