

SIMOS (IMPLEMENTING CISCO SECURE MOBILITY)

Objetivo

Implementing Cisco Secure Mobility Solutions (SIMOS) v1.0 é um treinamento que faz parte da grade de certificação CCNP Security. Este curso visa preparar os engenheiros em segurança de rede com os conhecimentos e as habilidades que eles precisam para proteger os dados que atravessam em uma infraestrutura de rede pública ou compartilhada, como por exemplo, a Internet, através da implantação e manutenção de soluções Cisco VPN. O aluno vai aprender os conceitos de VPN, e os procedimentos e configurações necessárias para disponibilizar soluções para acesso remoto de usuários (Remote Access VPN) e acesso para redes (Site-to-Site VPN), configuradas em roteadores Cisco e Cisco ASA Firewall. São abordadas soluções envolvendo os protocolos e arquiteturas IPSEC e SSL VPN. Após a conclusão deste curso, o aluno será capaz de atender aos seguintes objetivos gerais: Descrever as várias tecnologias e implantações em VPN, bem como os algoritmos de criptografia e protocolos que fornecem segurança em uma solução de VPN; Implantar e prestar suporte em soluções de VPN Cisco Site-to-Site; Implantar e prestar suporte em soluções de VPN Cisco Site-to-Site; Implantar e prestar suporte em soluções Remote Access VPN SSL na arquitetura Portal (ClientLess); Implantar e prestar suporte em soluções Remote Access VPN SSL e IPSEC utilizando software cliente (Cisco AnyConnect e VPN Client); Implantar e prestar suporte em soluções de acesso VPN utilizando as políticas de segurança fornecidas pelas ferramentas Cisco DAP e Cisco Secure Desktop.

Público Alvo

O público principal deste curso são os responsáveis em projetar, implantar e fornecer suporte em segurança, em soluções VPN IPsec e SSL. Esse curso faz parte dos cursos preparatórios para a certificação CCNP Security.

Pré-Requisitos

Para aproveitar ao máximo este curso, é recomendável que os alunos possuam as seguintes habilidades e conhecimentos: Ter participado no curso ICND 1 ou possuir conhecimentos equivalentes abrangido pelo curso; Ter participado no curso IINS ou possuir conhecimentos equivalentes em segurança abrangido pelo curso; Conhecimento do sistema operacional Microsoft Windows

Carga Horária

40 horas (5 dias).

Conteúdo Programático

- Fundamentals of VPN Technologies and Cryptography
- The Role of VPNs in Network Security
- VPN Definition
- Key Threats to WANs and Remote Access
- Cisco Modular Network Architecture and VPNs

VPN Types and components

VPNs and Cryptography

Secure Communication and Cryptographic Services

Cryptographic Algorithms

Cryptography and Confidentiality

Cryptography and Integrity

Cryptography and Authentication

Cryptography and Nonrepudiation

Keys in Cryptography

Public Key Infrastructure

Next-Generation Encryption

Dependencies in Cryptographic Services

Cryptographic Controls Guidelines

Deploying Secure Site-to-Site Connectivity Solutions

Site-to-Site VPN Topologies

Site-to-Site VPN Technologies

IPsec VPN Overview

Internet Key Exchange v1 and v2

Encapsulating Security Payload

IPsec Virtual Tunnel Interface

Dynamic Multipoint VPN

Cisco IOS FlexVPN

Deploying Point-to-Point IPsec VPNs on the Cisco ASA

Overview of Point-to-Point IPsec VPNs on the Cisco ASA

Configuration Tasks for Basic Point-to-Point Tunnels on the Cisco ASA

Enable IKE on an Interface

Configure IKE Policy

Configure PSKs

Choose Transform Set and VPN Peer

Choose Traffic for VPN

Configuring Site-to-Site VPN with Connection Profiles Menu Troubleshoot Basic Point-to-Point Tunnels on the Cisco ASA

Deploying Cisco IOS Router VTI-Based Point-to-Point IPsec VPNs

Overview of Cisco IOS VTIs

Configure Static VTI Point-to-Point Tunnels

Configure Dynamic VTI Point-to-Point Tunnels

Troubleshoot Basic Dynamic VTI Point-to-Point Tunnels

Deploying Cisco IOS Router DMVPNs

Overview of Cisco IOS DMVPN

DMVPN Solution Components

GRE and NHRP

DMVPN Operations

Types of Authentication

- Configure DMVPN on Hub
- Configure DMVPN on Spoke
- Configure Routing in DMVPN
- Troubleshoot Basic DMVPN

- Introducing Cisco FlexVPN Solution
- FlexVPN Overview
- Public Key Infrastructure (PKI)
- Site-to-Site VPN Topologies
- FlexVPN Architecture
- FlexVPN Configuration
- FlexVPN Capabilities
- IKEv2 vs. IKEv1 and Comparison
- IKEv2 Message Exchange
- IKEv2 DoS Prevention
- FlexVPN Use Cases

- Deploying Point-to-Point IPsec VPNs Using Cisco IOS FlexVPN
- Point-to-Point FlexVPN
- FlexVPN Configuration Blocks
- IKEv2 Profile
- Negotiating IKEv2 Proposals
- Point-to-Point VPN Scenario with IPv4 Static Routes
- Configure and Verify Point-to-Point VPN with IPv4 Static Routes
- Point-to-Point VPN Scenario with OSPFv3
- Configure and Verify Point-to-Point VPN with OSPFv3
- Enroll Devices to ECDSA PKI
- Configure Router for ECDSA
- Configure ASA for ECDSA
- Verify EC Key Pairs and Certificates
- Verify IKEv2 and IPsec SA
- Verify Point-to-Point FlexVPN
- Deploying Hub-and-Spoke IPsec VPNs Using Cisco IOS FlexVPN
- Cisco IOS Hub-and-Spoke FlexVPN IKEv2 Configuration Payload
- Locally Managed Hub-and-Spoke Scenario
- Configure a Spoke in a Hub-and-Spoke Scenario
- Configure a Hub in a Hub-and-Spoke Scenario
- Configuration Exchange
- Verify and Troubleshoot Hub-and-Spoke FlexVPN

- Deploying Spoke-to-Spoke IPsec VPNs Using Cisco IOS FlexVPN
- Spoke-to-Spoke Shortcut Scenario
- NHRP in FlexVPN
- Configure and Verify a Spoke in a Spoke-to-Spoke Shortcut Scenario
- Configure and Verify a Hub in a Spoke-to-Spoke Shortcut Scenario
- RADIUS-Managed FlexVPN Scenario
- Verify Spoke-to-Spoke Shortcut Switching
- Troubleshoot Spoke-to-Spoke Shortcut Switching

Deploying Clientless SSL VPN

Clientless SSL VPN Overview

SSL VPN Components

SSL/TLS

Overview of group policies and connection profiles

Deploying Basic Cisco Clientless SSL VPN

Basic Cisco Clientless SSL VPN

Solution Components

Configure ASA gateway

Configure basic authentication

Configure access control (including URL entry and bookmarks)

Troubleshoot basic clientless SSL VPN

Deploying Application Access in Clientless SSL VPN

Application Access options (plug-ins, smart tunnels)

Configure and verify plugins

Configure and verify smart tunnels

Troubleshoot plugins and smart tunnels

Deploying Advanced Authentication in Clientless SSL VPN

Advanced Authentication in Cisco Clientless SSL VPN Solution Components

Configure and verify Certificate based Authentication

Configure and Verify External Authentication (mention multiple auth)

Troubleshoot Advanced Authentication in Clientless SSL VPN

Deploying Cisco AnyConnect VPNs

Overview of Cisco AnyConnect VPNs IP Address assignment

Split Tunneling

Deploying Basic Cisco AnyConnect SSL VPN on Cisco ASA

Basic Cisco AnyConnect SSL VPN

Solution Components

SSL VPN Server Authentication

SSL VPN Clients Authentication

SSL VPN Clients IP Address Assignment

SSL VPN Split Tunneling

Configure ASA for Basic AnyConnect SSL VPN

Configure Basic Cisco Authentication

Configure Access Control

Verify and Troubleshoot Basic Cisco AnyConnect SSL VPN

Deploying Advanced Cisco AnyConnect SSL VPN on Cisco ASA

DTLS Overview

Parallel DTLS and TLS Tunnels

Configure DTLS

Verify DTLS

- Cisco AnyConnect Client Configuration Management
- Cisco AnyConnect Client Operating System Integration Options
- Cisco AnyConnect Start Before Logon
- Cisco AnyConnect Trusted Network Detection
- Configure, Verify, and Troubleshoot Cisco AnyConnect Start Before Logon and Cisco AnyConnect Trusted Network Detection

Deploying Cisco AnyConnect IPsec/IKEv2 VPNs

- AnyConnect Support for IPsec/IKEv2
- Configure a Cisco AnyConnect IPsec/IKEv2 VPNs on a Cisco ASA Adaptive Security Appliance
- Verify and Troubleshoot Cisco AnyConnect IPsec/IKEv2 VPNs on Cisco ASA

Deploying Advanced Authentication, Authorization, and Accounting in Cisco AnyConnect VPNs

- Cisco AnyConnect Advanced Authentication Scenarios
- External Authentication
- Certificate-Based Server Authentication
- Configure and Verify Certificate-Based Client Authentication
- SCEP Proxy Overview
- SCEP Proxy Connection Flow
- SCEP Proxy Configuration Procedure
- Configure SCEP Proxy
- Verify SCEP Proxy
- Local Authorization Overview
- Local Authorization Scenario Local Authorization Configuration Procedure
- Configure Local Authorization
- External Authentication and Authorization Scenario
- Configure External Authentication and Authorization
- Troubleshoot Advanced Authentication and Authorization in AnyConnect VPNs
- Configure Accounting

Deploying Endpoint Security and Dynamic Access Policies

- Implementing Host Scan
- Cisco HostScan Overview
- Cisco HostScan Prelogin Assessment
- Install Cisco HostScan
- Configure Prelogin Criteria and Prelogin Policy
- Configure Host Scan Endpoint Assessment
- Configure Host Scan Advanced Endpoint Assessment
- Verify and Troubleshoot HostScan

Implementing DAP for SSL VPNs

- DAP Overview
- Integrating DAP with Host Scan
- Configuring DAP
- Verifying and Troubleshooting DAP

Roteiro de Laboratórios

- Lab 2-1: Implement Site-to-Site Secure Connectivity on the Cisco ASA
- Lab 2-2: Implement Cisco IOS Static VTI Point-to-Point Tunnel
- Lab 2-3: Implement DMVPN
- Lab 3-1: Implement Site-to-Site Secure Connectivity Using Cisco IOS FlexVPN
- Lab 3-2: Implement Hub-to-Spoke Secure Connectivity Using Cisco IOS Flex VPN
- Lab 3-3: Implement Spoke-to-Spoke Secure Connectivity Using Cisco IOS Flex VPN
- Lab 4-1: Implement ASA Basic Clientless SSL VPN
- Lab 4-2: Application Access clientless SSL
- Lab 4-3: Advanced AAA clientless SSL
- Lab 5-1: Implement ASA Basic AnyConnect SSL VPN
- Lab 5-2: Configure Advanced Cisco AnyConnect SSL VPN on Cisco ASA
- Lab 5-3: Configure Cisco AnyConnect IPsec/IKEv2 VPNs on Cisco ASA
- Lab 5-4: Configure Advanced Authentication for AnyConnect SSL VPN Cisco ASA
- Lab 6-1: Configure Hostscan and DAP for AnyConect SSL VPNs.