Cisco Secure
Virtual Private Networks

Length
4 days

Format
Lecture/lab

Version
4.0

CSVPN

Course Description
CSVPN 4.0 is a 4-day lab-intensive course that provides you with the knowledge and skills needed to configure, verify, and manage the Cisco VPN 3000 Concentrator, Cisco VPN Software Client, and Cisco VPN 3002 Hardware Client feature set.

Who Should Attend
This course is designed for anyone tasked with implementing or maintaining a secure network using Cisco VPN solutions.

Recommended Prerequisites
- CCNA certification or equivalent knowledge
- Basic knowledge of the Windows operating system
- Familiarity with the networking and security terms and concepts

Learning Objectives
After completing this course, you will be able to:
- Describe the features, functions, and benefits of Cisco VPN products
- Explain the IPSec and IKE component technologies in Cisco secure VPN products
- Install and configure the Cisco IPSec VPN software client
- Configure Cisco VPN 3000 for remote access using preshared keys and using digital certificates
- Configure Cisco VPN 3000 firewall feature
- Configure Cisco VPN 3000 for IPSec over TCP or IPSec over UDP
- Configure Cisco VPN 3000 for LAN-to-LAN with preshared keys
- Configure Cisco VPN 3000 for LAN-to-LAN with digital certificates
- Configure CISCO VPN 3000 for LAN-to-LAN with Network Address Translation
- Configure Cisco VPN Windows Client auto-initiate feature
- Configure Cisco VPN 3002 for remote access using preshared keys
- Configure Cisco VPN 3002 for software auto-update, and for interactive unit and individual user authentication
- Configure Cisco VPN 3002 for backup server and load balancing

Cisco Secure
Virtual Private Networks

Cisco Secure
Virtual Private Networks

Course Outline

Lesson 11: Configure the Cisco Virtual Private Network Client Backup Server, and Load Balancing
Configuring the Cisco VPN Client Backup Server Feature
Configuring the Cisco VPN Client Load-Balancing Feature
Overview of the Cisco VPN Client Reverse Route Injection Feature

Lesson 12: Configure the Cisco Virtual Private Network 3002 Hardware Client for Software Auto-Update
Overview and Configuration of the Cisco VPN 3002 Hardware Client Software Auto Update Feature
Monitoring the Cisco VPN 3002 Hardware Client Software Auto-Update Feature

Lesson 13: Configure the Cisco Virtual Private Network 3000 Series Concentrator for IPSec over UDP and IPSec over TCP
Overview of Port Address Translation
Configuring IPSec over UDP
Configuring NAT Traversal
Configuring IPSec over TCP
Monitoring Session Statistics

Lesson 14: Cisco Virtual Private Network 3000 Series Concentrator LAN-to-LAN with Preshared Keys
Cisco VPN 3000 Series Concentrator IPSec LAN-to-LAN
Configuring the Cisco VPN 3000 Series Concentrator
LAN-to-LAN Configuration

Lesson 15: Configure the Cisco VPN 3000 Series Concentrator for LAN-to-LAN with NAT
LAN-to-LAN NAT Overview
Configuring the Concentrator LAN-to-LAN

Lesson 16: Configure the Cisco Virtual Private Network 3000 Series Concentrator for LAN to-LAN Using Digital Certificates
SCEP Support Overview
Root Certificate Installation
Identity Certificate Installation

Lab 1: Configure Cisco VPN 3000 for Remote Access Using Pre-Shared Keys

Lab 2: Configure the Cisco VPN 3000 Concentrator for Remote Access Using DigitalCertificates

Lab 3: Configure VPN IPSec Client Firewall

Lab 4: Configure VPN Client Auto-Initiate

Lab 5: Cisco VPN 3000 Concentrator Monitoring and Administration

Lab 6: Configure Cisco VPN 3002 Hardware Client Remote Access

Lab 7: Configure IPSec Hardware Client using user and unit authentication

Lab 8: Configure IPSec Hardware Client for backup server and reverse route injection

Lab 9: Configure VPN 3002 for auto-update

Lab 10: Configure Cisco VPN 3000 Concentrators for LAN-to-LAN Using Pre-Shared Keys

Lab 11: Configure Cisco VPN 3000 Concentrators for LAN-to-LAN Using NAT

Lab 12: Configure Cisco VPN 3000 Concentrators for LAN-to-LAN Using Digital Certificates