

Global Knowledge Course Name: CSVPN (Cisco Secure Virtual Private Networks) Code 5726

Course Overview:

Cisco Course v4.7 | Prepares you for Cisco Exam 642-511 CSVPN

In this Authorized Cisco class, you will learn the skills necessary to securely extend your computing environment using Cisco VPN solutions. With instruction based on the latest VPN technology, you will learn how to most effectively install and configure VPN connections to leverage your investment in these important security products and technologies.

We have enhanced our 4-day hands-on delivery of CSVPN by adding depth to the existing Cisco-developed hands-on labs. Over 20 advanced hands-on labs guide you through using the VPN Concentrator, VPN Software Client, and VPN Hardware Client to set up secure network connectivity in both LAN-to-LAN and Remote Access scenarios. A PIX Firewall-based VPN lab is included as a refresher on IPSec VPN principles. The labs include using the VPN 3000 Series Concentrator to host remote access VPN connections using the Cisco VPN Software Client and VPN 3002 Hardware Client with Pre-Shared Keys and digital certificates, integrated firewall features of the Software Client, and LAN-to-LAN IPSec VPN connections using the VPN 3000 Series Concentrator. New features in the 4.7 version of the Concentrator code, such as SSL VPN and Secure Desktop, are demonstrated.

Our exclusive labs include configuring and testing split tunneling, bandwidth management, pre-configuring and customizing the Cisco VPN Software Client, RADIUS and TACACS-based authentication, and configuring a Windows 2000 Server as a Certificate Authority. This course gives you the most relevant, hands-on, and real-world experience available anywhere, all based on an enhanced topology designed to simulate a typical production network instead of a classroom.

What You'll Learn:

- Features, functions, and benefits of Cisco Secure VPN products
- Cisco Secure VPN 3000 Series Concentrator
- Cisco Secure VPN Software Client version 4.x
- Cisco Secure VPN 3002 Hardware Client
- IPSec fundamentals and operation
- Public Key Infrastructure (PKI) organization and concepts
- Processes involved in the creation and use of digital certificates
- VPN 3000 Series Concentrator Redundancy and Load Balancing (Clustering)
- VPN Software Client firewall features and how to create and apply centrally managed firewall policies
- Configure and use split tunneling and split DNS
- Configure Certificate Revocation List (CRL) caching



- Configure and apply bandwidth policing or bandwidth reservation policies
- Monitoring functions, including use of the Filterable Event Log
- Reverse Route Injection
- Differences between Client Mode and Network Extension Mode when using the VPN 3002 Hardware Client
- How and why to configure IPsec over UDP, NAT Traversal, and IPsec over TCP
- Configure and use WebVPN clientless connectivity
- Configure and use the Cisco SSL VPN Client (new in Concentrator version 4.7)
- Configure and use the Cisco Secure Desktop (new in Concentrator version 4.7)

Who Needs to Attend?

- Networking professionals tasked with ensuring the effective use of Cisco VPN technologies within their networks; those seeking the Cisco Certified Security Professional (CCSP) or Cisco VPN Specialist certifications.

Course Content:

Security Fundamentals

- Need for Network Security
- Network Security Policy
- The Security Wheel
- Network Attack Taxonomy
- Management Protocols and Functions

Overview of Virtual Private Networks and IPsec Technologies

- VPN Products
- IPsec Overview
- IPsec Protocol Framework
- How IPsec Works

Cisco Virtual Private Network 3000 Concentrator Series Hardware Overview

- Cisco VPN 3000 Series Concentrator Models
- Benefits and Features of the Cisco VPN 3000 Series Concentrator
- Cisco VPN 3000 Series Concentrator Client Support

VPN 3000 Series Concentrator Remote Access Using Pre-Shared Keys

- Overview of Remote Access using Pre-Shared Keys
- Initial Configuration of the Cisco VPN 3000 Series Concentrator for Remote Access
- Browser Configuration of the Cisco VPN 3000 Series Concentrator
- Configuration of Users and Groups



- In-Depth Configuration Information
- Configuration of Cisco VPN Software Client for Windows

VPN 3000 Series Concentrator Remote Access Using Digital Certificates

- CA Support Overview
- Certificate Generation
- Validating Certificates
- Configuring the Cisco VPN 3000 Series Concentrator for CA Support

VPN Firewall Feature for the Software Client

- Overview of the Software Client's Firewall Feature
- AYT Feature
- Stateful Firewall Feature
- CPP Feature
- Firewall Statistics
- Customizing Firewall Policy

VPN Client Auto-Initiation Feature

- Overview of the Cisco VPN Software Client Auto-Initiation Feature
- Configure the Cisco VPN Software Client Auto-Initiation Feature

Monitor and Administer the Cisco VPN 3000 Series Concentrator Remote Access Networks

- Monitoring
- Administration
- Bandwidth Management

VPN 3002 Hardware Client for Remote Access Using Pre-Shared Keys

- Hardware Client Modes (Client and Network Extension)
- Quick Configuration Mode

VPN 3002 Hardware Client for Unit and User Authentication

- Overview of the Hardware Client Interactive Unit and User Authentication Features
- Configuring the Hardware Client Interactive Unit Authentication Feature
- Configuring the Hardware Client User Authentication Feature
- Monitoring the Hardware Client User Statistics

VPN 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

VPN 3002 Hardware Client for Software Auto-Update



- Overview and Configuration of the VPN 3002 Hardware Client Software Auto-Update Feature
- Monitoring the VPN 3002 Hardware Client Software Auto-Update Feature

VPN 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

VPN 3000 Series Concentrator LAN-to-LAN with Pre-Shared Keys

- VPN 3000 Series Concentrator IPSec LAN-to-LAN
- Configuring the VPN 3000 Series Concentrator Via the Quick Configuration Wizard
- LAN-to-LAN Configuration

VPN 3000 Series Concentrator LAN-to-LAN with NAT

- LAN-to-LAN NAT Overview
- Configuring the Concentrator LAN-to-LAN NAT Feature

VPN 3000 Series Concentrator LAN-to-LAN Using Digital Certificates

- SCEP Support Overview
- Root Certificate Installation
- Identity Certificate Installation

Configure the Cisco VPN 3000 Series Concentrator for WebVPN

- WebVPN Support Overview
- Configure WebVPN Servers and URLs
- Configure WebVPN for Port Forwarding
- Configure WebVPN for Email Proxy

Using Cisco SSL VPN Client

- Cisco SSL VPN Client - An Overview
- Installing Cisco SSL VPN Client
- Configuring Cisco VPN 3000 Series Concentrator v4.7

Installing and Configuring Cisco Secure Desktop

- Cisco Secure Desktop - An Overview
- Installing Cisco Secure Desktop
- Identifying Secure Desktop Manager Options
- Configuring Secure Desktop Manager Options
- Enabling Cisco Secure Desktop

