

Cisco® Secure Virtual Private Networks (CSVPN)

(4 day Instructor-Led Course)

Course Overview

This task-oriented course teaches the knowledge and skills needed to describe, configure, verify, and manage the Cisco VPN 3000 concentrator, Cisco VPN software client, and Cisco VPN 3002 hardware client feature set.

Who Should Attend

- Cisco customers who implement and maintain Cisco Virtual Private Networks (VPNs)

Prerequisites

- *CCNA Training*
- *Basic knowledge of the Windows operating system*
- *Familiarity with the networking and security terms and concepts*

What You Will Accomplish

- Describe the features, functions, and benefits of Cisco VPN products
- Explain the IPSec and IKE component technologies that are implemented in Cisco Secure VPN products
- Install and configure the Cisco IPSec VPN Software client
- Configure Cisco VPN 3000 for remote access using pre-shared keys and digital certificates
- Configure Cisco VPN 3000 firewall feature
- Configure Cisco VPN 3002 for remote access using preshared keys
- Configure Cisco VPN 3002 for software auto-update
- Configure Cisco VPN 3002 for interactive unit and individual user authentication
- Configure Cisco VPN 3002 for backup server and load balancing
- Configure Cisco VPN 3000 for IPSec over TCP or IPSec over UDP
- Configure Cisco VPN 3000 for LAN-to-LAN with preshared keys and digital certificates

What You Will Receive

- *Student guide Cisco Secure Virtual Private Networks*

Certification Preparation

- This course helps prepare you for CCSP certification.

Course Outline: CSVPN™ (Cisco Secure Virtual Networks)	
<p>Presenting VPN and IPSec Technologies</p> <ul style="list-style-type: none"> ▪ Enabling a secure VPN ▪ Reviewing IPSec ▪ Studying IPSec crypto components ▪ Discussing IKE ▪ Working with IPSec security associations <p>Analyzing Cisco VPN 3000 Concentrator Series Hardware</p> <ul style="list-style-type: none"> ▪ Studying VPN 3000 concentrator series models ▪ Discussing benefits and features of the VPN 3000 concentrator series <p>Configuring Cisco VPN 3000 for Remote Access Using Pre-Shared Keys</p> <ul style="list-style-type: none"> ▪ Configuring VPN 3000 concentrator series ▪ Configuring the browser ▪ Setting up users and groups ▪ Establishing IPSec clients ▪ Monitoring <p>Using Digital Certificates and Cisco VPN 3000 for Remote Access</p> <ul style="list-style-type: none"> ▪ Getting CA support ▪ Generating certificates ▪ Validating certificates ▪ Configuring VPN 3000 for CA support <p>Setting Up Cisco VPN Firewall Feature for IPSec Software Client</p> <ul style="list-style-type: none"> ▪ Studying the software client's firewall features ▪ Working with are you there, stateful firewall, and Central policy protection features ▪ Analyzing firewall statistics ▪ Customizing firewall policy <p>Monitoring and Administering Cisco VPN 3000 Remote Access Networks</p> <ul style="list-style-type: none"> ▪ Monitoring ▪ Administering <p>Using Pre-Shared Keys and Cisco VPN 3002 for Remote Access</p> <ul style="list-style-type: none"> ▪ Configuring the "client mode" remote access ▪ Setting up "network extension mode" access 	<p>Authenticating Users and Units with Cisco 3002 Hardware Client</p> <ul style="list-style-type: none"> ▪ Setting up the interactive unit authentication ▪ Authenticating users ▪ Monitoring user statistics <p>Configuring Cisco 3002 Hardware Client for Backup Server, Load Balancing, and Reverse Route Injection</p> <ul style="list-style-type: none"> ▪ Setting up backup server features ▪ Allowing load balancing ▪ Performing reverse route injection <p>Configuring Cisco 3002 Hardware Client for Software Auto-Update</p> <ul style="list-style-type: none"> ▪ Monitoring for software updates <p>Configuring Cisco 3002 Hardware Client for IPSec Over TCP and UDP</p> <ul style="list-style-type: none"> ▪ Translating port addresses ▪ Configuring over UDP ▪ Monitoring session statistics <p>Employing VPN 3000 LAN-to-LAN with Pre-Shared Keys</p> <ul style="list-style-type: none"> ▪ Configuring the concentrator via quick configuration ▪ Monitoring LAN-to-LAN tunnels ▪ Setting up network lists ▪ Configuring network auto-discovery <p>Configuring Cisco VPN 3000 Site-to-Site Using Digital Certificates</p> <ul style="list-style-type: none"> ▪ Explaining the purpose of digital certificates ▪ Generating certificate requests