

Implementing Secure Solutions with Virtual Private Networks (SVPN)

Implementing Secure Solutions with Virtual Private Networks (SVPN)

In this Implementing Secure Solutions with Virtual Private Networks course provides a comprehensive, hands-on exploration of virtual private network technologies used to securely connect users, sites, and applications across enterprise and hybrid environments. The curriculum begins with core VPN and IPsec fundamentals, including cryptographic concepts, tunnel establishment, and secure data transport, establishing a strong foundation for understanding modern VPN architectures. Learners gain clarity on when and why different VPN models are used, such as site-to-site, remote-access, and clientless VPNs, and how these models support secure connectivity in distributed networks.

The course then moves into practical implementation of site-to-site VPN solutions across Cisco platforms, including Cisco IOS, Cisco IOS Virtual Tunnel Interfaces, and Cisco Adaptive Security Appliance deployments. Advanced architectures such as Dynamic Multipoint VPN, Group Encrypted Transport VPN, and Cisco FlexVPN are explored in depth, allowing students to design scalable hub-and-spoke and spoke-to-spoke topologies using both static and dynamic approaches. Emphasis is placed on configuration best practices, verification techniques, and troubleshooting methodologies to ensure reliable and secure VPN operations.

The final portion of the course focuses on secure remote access solutions, including Cisco AnyConnect SSL/TLS VPNs and clientless VPN deployments. Learners configure advanced authentication, authorization, and accounting integrations, verify secure access for remote users, and troubleshoot common connectivity and policy issues. A comprehensive lab program reinforces all concepts through real-world scenarios, enabling students to confidently deploy, verify, and troubleshoot Cisco VPN solutions in enterprise production environments.

How you'll benefit

This class will help you:

- Acquire the knowledge and skills to enhance internet privacy, speed, and performance
- Gain hands-on experience using the tools to ensure premium data security
- Prepare for the 300-730 SVPN v1.1 exam
- Earn 40 CE credits toward recertification

Why Attend with Current Technologies CLC

- Our Instructors are in the top 10% rated by Cisco
- Our Lab has a dedicated 1 Gig Fiber Connection for our Labs
- Our Labs run up to Date Code for all our courses

Who Should Attend

The primary audience for this course is as follows:

- Network Security Engineer
- CCNP Security Candidate
- Channel Partner
- Cisco Customers

Course Duration

5 days

Course Price

\$4,295.00 or 43 CLCs

Methods of Delivery

- Instructor Led
- Virtual ILT
- On-Site

Prerequisites

Before taking this course, you should have the following knowledge and skills:

- Familiarity with the various Cisco router and firewall command modes
- Experience navigating and managing Cisco routers and firewalls
- Clear understanding of the benefits of site-to-site and Remote Access VPN options

OUTLINE

Module 1: Introducing VPN Technology Fundamentals

Module 2: Implementing Site-to-Site VPN Solutions

Module 3: Implementing Cisco Internetwork Operating System (Cisco IOS®) Site-to-Site Flex VPN Solutions

Module 4: Implement Cisco IOS Group Encrypted Transport (GET) VPN Solutions

Module 5: Implementing Cisco AnyConnect VPNs

Module 6: Implementing Clientless VPNs

LAB OUTLINE

- Lab 1: Explore IPsec Technologies
- Lab 2: Implement and Verify Cisco IOS Point-to-Point VPN
- Lab 3: Implement and Verify Cisco Adaptive Security Appliance (ASA) Point-to-Point VPN
- Lab 4: Implement and Verify Cisco IOS Virtual Tunnel Interface (VTI) VPN
- Lab 5: Implement and Verify Dynamic Multipoint VPN (DMVPN)
- Lab 6: Troubleshoot DMVPN
- Lab 7: Implement and Verify FlexVPN with Smart Defaults
- Lab 8: Implement and Verify Point-to-Point FlexVPN
- Lab 9: Implement and Verify Hub and Spoke FlexVPN
- Lab 10: Implement and Verify Spoke-to-Spoke FlexVPN
- Lab 11: Troubleshoot Cisco IOS FlexVPN
- Lab 12: Implement and Verify AnyConnect Transport Layer Security (TLS) VPN on ASA
- Lab 13: Implement and Verify Advanced Authentication, Authorization, and Accounting (AAA) on Cisco AnyConnect VPN
- Lab 14: Implement and Verify Clientless VPN on ASA