

Implementing Secure Solutions with Virtual Private Networks

The **Cisco** authorized course **SVPN - Implementing Secure Solutions with Virtual Private Networks** course teaches you how to implement, configure, monitor, and support enterprise Virtual Private Network (VPN) solutions. Through a combination of lessons and hands-on experiences you will acquire the knowledge and skills to deploy and troubleshoot traditional Internet Protocol Security (IPsec), Dynamic Multipoint Virtual Private Network (DMVPN), FlexVPN, and remote access VPN to create secure and encrypted data, remote accessibility, and increased privacy.

This course will prepare you for the **300-730 Implementing Secure Solutions with Virtual Private Networks (SVPN)** exam.



Purpose of the training

This course is designed for professionals in the following job roles:

- Network security engineer
- CCNP Security candidate
- Channel Partner



Benefits of completing the training

This course 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** exam
- Earn 40 CE credits toward recertification



Exam description

The training prepares you for the **300-730 SVPN** exam, which can be taken for an additional fee at the PearsonVUE center. You can also take the exam on-line.

Details are available at: <https://home.pearsonvue.com/cisco/onvue>



Expected Listener Preparation

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

The following Cisco courses can help you gain the knowledge you need to prepare for this course:

- **Implementing and Administering Cisco Solutions (CCNA®)**
- **Implementing and Operating Cisco Security Core Technologies (SCOR)**



Training Language

- Training: English
- Materials: English



Training Includes

5 days of web-based classes

Duration

5 days / 35 hours

Training agenda

After taking this course, you should be able to:

- Introduce site-to-site VPN options available on Cisco router and firewalls
- Introduce remote access VPN options available on Cisco router and firewalls
- Review site-to-site and remote access VPN design options
- Review troubleshooting processes for various VPN options available on Cisco router and firewalls

Outline

- Introducing VPN Technology Fundamentals
- Implementing Site-to-Site VPN Solutions
- Implementing Cisco Internetwork Operating System (Cisco IOS®) Site-to-Site FlexVPN Solutions
- Implement Cisco IOS Group Encrypted Transport (GET) VPN Solutions
- Implementing Cisco AnyConnect VPNs
- Implementing Clientless VPNs

Lab outline

- Explore IPsec Technologies
- Implement and Verify Cisco IOS Point-to-Point VPN
- Implement and Verify Cisco Adaptive Security Appliance (ASA) Point-to-Point VPN
- Implement and Verify Cisco IOS Virtual Tunnel Interface (VTI) VPN
- Implement and Verify Dynamic Multipoint VPN (DMVPN)
- Troubleshoot DMVPN
- Implement and Verify FlexVPN with Smart Defaults
- Implement and Verify Point-to-Point FlexVPN
- Implement and Verify Hub and Spoke FlexVPN
- Implement and Verify Spoke-to-Spoke FlexVPN
- Troubleshoot Cisco IOS FlexVPN
- Implement and Verify AnyConnect Transport Layer Security (TLS) VPN on ASA
- Implement and Verify Advanced Authentication, Authorization, and Accounting (AAA) on Cisco AnyConnect VPN
- Implement and Verify Clientless VPN on ASA