

Implementing Secure Solutions with Virtual Private Networks (SVPN) v1.0

What you'll learn in this course

The **Implementing Secure Solutions with Virtual Private Networks (SVPN) v1.0** 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.

Course duration

- Instructor-led training: 5 days in the classroom
- Virtual instructor-led training: 5 days of web-based classes
- E-learning: Equivalent to 5 days of classroom instruction

How you'll benefit

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

What to expect in the exam

The **300-730 SVPN** exam certifies your knowledge and skills related to implementing secure remote communications with Virtual Private Network (VPN) solutions including secure communications, architectures, and troubleshooting.

After you pass **300-730 SVPN** exam, you earn the **Cisco® Certified Specialist - Network Security VPN Implementation** and you satisfy the concentration exam requirement for this professional-level certification:

- [CCNP® Security](#)

Who should enroll

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

- Network security engineer
- CCNP Security candidate
- Channel Partner

How to enroll

- For instructor-led training, visit the [Cisco Learning Locator](#).
- For private group training, visit [Cisco Private Group Training](#).
- For e-learning, visit the [Cisco Learning Network Store](#).
- For digital library access, visit [Cisco Learning Library](#).
- For other ways to purchase e-learning, contact us at: learning-bdm@cisco.com.

Technology areas

- Security

Course details

Objectives

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

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

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)**

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




Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

 Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Course content is dynamic and subject to change without notice.

© 2020 Cisco and/or its affiliates. All rights reserved.

SVPN_1-0

C22-743468-00 02/20