

SVPN

The **Implementing Secure Solutions with Virtual Private Networks (SVPN)** training 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 training prepares you for the 300-730 SVPN v1.1 exam. If passed, you earn the Cisco Certified Specialist – Network Security VPN Implementation certification and satisfy the concentration exam requirement for the CCNP Security certification. This training also earns you 40 Continuing Education (CE) credits towards recertification.

How You'll Benefit

This training 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

Who Should Enroll

- Network Security Engineers
- CCNP Security Candidates
- Channel Partners
- Cisco Customers

What to Expect in the Exam

Implementing Secure Solutions with Virtual Private Networks (300-730 SVPN v1.1) is a 90-minute exam associated with the Cisco Certified Specialist – Network Security VPN Implementation certification and satisfies the concentration exam requirement for the CCNP Security certification.

The exam tests your knowledge of implementing secure remote communications with VPN solutions, including:

- Secure communications
- Architectures
- Troubleshooting

Course Objectives

- 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

Course Prerequisites

The knowledge and skills you are expected to have before attending this training are:

- 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

These skills can be found in the following Cisco Learning Offerings:

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

Course Outline

1. Introducing VPN Technology Fundamentals
2. Implementing Site-to-Site VPN Solutions
3. Implementing Cisco IOS Site-to-Site Flex VPN Solutions
4. Implement Cisco IOS GET VPN Solutions
5. Implementing Cisco AnyConnect VPNs
6. Implementing Clientless VPNs

Lab Outline

1. Explore IPsec Technologies
2. Implement and Verify Cisco IOS Point-to-Point VPN
3. Implement and Verify Cisco ASA Point-to-Point VPN
4. Implement and Verify Cisco IOS VTI VPN
5. Implement and Verify DMVPN
6. Troubleshoot DMVPN
7. Implement and Verify FlexVPN with Smart Defaults
8. Implement and Verify Point-to-Point FlexVPN
9. Implement and Verify Hub-and-Spoke FlexVPN
10. Implement and Verify Spoke-to-Spoke FlexVPN
11. Troubleshoot Cisco IOS FlexVPN
12. Implement and Verify AnyConnect TLS VPN on ASA
13. Implement and Verify Advanced AAA on Cisco AnyConnect VPN
14. Implement and Verify Clientless VPN on ASA