

Implementing Secure Solutions with Virtual Private Networks

Durée: 5 Jours **Réf de cours: SVPN** **Version: 1.1** **Méthodes d'apprentissage: Classe à distance**

Résumé:

The Implementing Secure Solutions with Virtual Private Networks (SVPN) 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 is worth 40 Continuing Education (CE) Credits

Public visé:

Network engineers responsible for selecting, designing and deploying secure solutions using VPNs

Objectifs pédagogiques:

- | | |
|---|---|
| <ul style="list-style-type: none">■ After completing 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 | <ul style="list-style-type: none">■ Review site-to-site and remote access VPN design options■ Review troubleshooting processes for various VPN options available on Cisco router and firewalls |
|---|---|

Pré-requis:

Attendees should meet the following prerequisites:

- 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
- CCNA - Mettre en oeuvre et administrer des solutions réseaux Cisco
- SCOR - Mettre en oeuvre et gérer les solutions de sécurité Cisco

Test et certification

Recommended as preparation for the following exams:

- **300-730** - Implementing Secure Solutions with Virtual Private Networks (SVPN) exam.
After you pass the **300-730 SVPN** exam, you will earn the Cisco® Certified Specialist - Network Security VPN Implementation certification and satisfy the concentration exam requirement for the CCNP Security certification.

Contenu:

Introducing VPN Technology Fundamentals

- Role of VPNs in Network Security
- VPNs and Cryptography

Implementing Site-to-Site VPN Solutions

- Site-to-Site VPN Solutions Overview
- Cisco IOS VPN Point-to-Point Solutions
- Cisco ASA VPN Point-to-Point Solutions
- Cisco IOS VTI Point-to-Point Solutions
- Cisco DMVPN Solutions

Implementing Cisco Internetwork Operating System (Cisco IOS®) Site-to-Site FlexVPN Solutions

- Overview of the Cisco FlexVPN Solution
- Point-to-Point FlexVPN
- Hub-and-Spoke FlexVPN
- Spoke-to-Spoke FlexVPN

Implement Cisco IOS Group Encrypted Transport (GET) VPN Solutions

- Overview of Cisco GET VPN Solution
- Configure GET VPN

Implementing Cisco AnyConnect VPNs

- Remote Access Overview
- Design Remote Access Solutions
- Basic Cisco AnyConnect VPN on Cisco ASA
- Advanced Cisco AnyConnect TLS VPN on Cisco ASA
- Advanced AAA in Cisco AnyConnect VPNs
- Cisco AnyConnect IKEv2 VPNs

Implementing Clientless VPNs

- Remote Access Overview
- Design Remote Access Solutions
- Clientless TLS VPN Overview
- Basic Cisco AnyConnect TLS VPN on Cisco ASA
- Application Access in Cisco ASA Clientless VPN
- Advanced AAA in Clientless VPN

Labs

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

Autres moyens pédagogiques et de suivi:

- Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
- Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
- En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

- Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
- Votre place sera confirmée à la réception d'un devis ou "booking form" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
- Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

- En cas de handicap : plus d'info sur globalknowledge.fr/handicap
- Le Règlement intérieur est disponible sur globalknowledge.fr/reglement