Formation : Implementing Secure Solutions with Virtual Private Networks (SVPN) v1.1

Cours officiel, préparation à l'examen 300-730 SVPN

Cours pratique - 5j - 35h00 - Réf. AQJ
Prix : 4440 € H.T.

Avec cette formation, vous apprendrez à mettre en œuvre, configurer, surveiller et dépanner des solutions VPN d'entreprise. Vous déploierez des VPN IPsec, DMVPN, FlexVPN et des VPN d'accès distant pour garantir la sécurité, la confidentialité et l'accessibilité des données via des connexions chiffrées.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Présenter les options de VPN site-à-site disponibles sur les routeurs et pare-feux Cisco
- Présenter les options de VPN d'accès distant disponibles sur les routeurs et pare-feux Cisco
- Examiner les options de conception des VPN site-à-site et d'accès distant
- Revoir les processus de dépannage des différentes options VPN sur les routeurs et pare-feux Cisco

Public concerné

Ingénieurs sécurité réseau, candidats à la certification CCNP Security, partenaires Cisco et clients de Cisco.

Prérequis

Maîtrise des routeurs et pare-feux Cisco, connaissance des modes de commande et des VPN site-à-site et accès distant, acquises via les formations CCNA ou SCOR.

Méthodes et moyens pédagogiques

Méthodes pédagogiques

Animation de la formation en français. Support de cours officiel en anglais.

PARTICIPANTS

Ingénieurs sécurité réseau, candidats à la certification CCNP Security, partenaires Cisco et clients de Cisco.

PRÉREQUIS

Maîtrise des routeurs et pare-feux Cisco, connaissance des modes de commande et des VPN site-à-site et accès distant, acquises via les formations CCNA ou SCOR.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils sont agréés par l'éditeur et sont certifiés sur le cours. Ils ont aussi été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Évaluation des compétences visées en amont de la formation.
Évaluation par le participant, à l'issue de la formation, des compétences acquises durant la formation.
Validation par le formateur des acquis du participant en précisant les outils utilisés : QCM, mises en situation...
À l'issue de chaque formation, ITTCERT fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques. Les participants réalisent aussi une évaluation officielle de l'éditeur.
Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Programme de la formation

1 Programme officiel

- Introduction aux fondamentaux des technologies VPN.
- Mise en œuvre de solutions VPN site-à-site.
- Mise en œuvre de solutions Cisco IOS Flex VPN site-à-site.
- Mise en œuvre de solutions Cisco IOS GET VPN.
- Mise en œuvre des VPN Cisco AnyConnect.
- Mise en œuvre des VPN sans client (Clientless VPNs).

2 Travaux pratiques officiels

- Explorer les technologies IPsec.
- Mettre en œuvre et vérifier un VPN point à point Cisco IOS.
- Mettre en œuvre et vérifier un VPN point à point sur Cisco ASA.
- Mettre en œuvre et vérifier un VPN VTI sur Cisco IOS.
- Mettre en œuvre et vérifier un DMVPN.
- Dépanner un DMVPN.
- Mettre en œuvre et vérifier FlexVPN avec les paramètres par défaut intelligents.
- Mettre en œuvre et vérifier un FlexVPN point à point.
- Mettre en œuvre et vérifier un FlexVPN en étoile (Hub-and-Spoke).
- Mettre en œuvre et vérifier un FlexVPN entre sites (Spoke-to-Spoke).
- Dépanner un FlexVPN Cisco IOS.
- Mettre en œuvre et vérifier un VPN AnyConnect TLS sur ASA.
- Mettre en œuvre et vérifier une AAA avancée sur un VPN Cisco AnyConnect.
- Mettre en œuvre et vérifier un VPN sans client (Clientless) sur ASA.

Options

Certification : 350 € HT

Pour l'obtention de la certification Cisco Certified Network Professional Security (CCNP Security), la réussite de l'examen 350-701 SCOR est requise ainsi que la réussite de l'un des examens suivants (au choix) : 300-710 SNCF, 300-715 SISE, 300-720 SESA, 300-725 SWSA, 300-730 SVPN, 300-740 SCAZT ou 300-745 SDSI.

Comment passer votre examen ?

L'option de certification se présente sous la forme d'un voucher ou d'une convocation qui vous permettra de passer l'examen à l'issue de la formation.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les ressources pédagogiques utilisées sont les supports et les travaux pratiques officiels de l'éditeur.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.