Cisco - Mettre en œuvre la sécurité pour la mobilité avec les produits Cisco v1.0

Référence : **SIMOS** Durée : **5 jours** Certification : **300-209**

Eligible CPF : 235895

CONNAISSANCES PREALABLES

• Avoir des connaissances sur le système d'exploitation Windows. • Posséder le niveau de certification CCNA, et CCNA Sécurité .

PROFIL DES STAGIAIRES

• Ingénieurs sécurité réseau.

OBJECTIFS

• Acquérir les compétences et connaissances nécessaires pour protéger les données au sein d'une infrastructure publique ou partagée, tel que internet, en mettant en œuvre et en assurant la maintenance des solutions VPN Cisco.

CERTIFICATION PREPAREE

- Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Sécurité CISCO

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Les fondamentaux de la cryptographie et des technologies VPN

- Le rôle des VPNs dans la sécurité des réseaux
- VPNs et Cryptographie

Déployer des solutions sécurisées de connectivité site à site

- Introduction aux solutions sécurisées de connectivité site à site Cisco
- Déployer les VPNs IPsec Point à Point sur ASA
- Déployer les VPNs IPsec VTI-Based sur Cisco IOS
- Déployer les DMVPNs sur Cisco IOS

Déployer les solutions FlexVPN site à site sur Cisco IOS

- Introduction aux solutions FlexVPN Cisco
- Déployer les VPNs IPsec point à point avec FlexVPN
- Déployer les VPNs IPsec Hub-and-Spoke avec FlexVPN
- Déployer les VPNs IPsec Spoke to Spoke avec FlexVPN

Déployer les VPNs SSL Clientless

- Introduction aux VPNs SSL Clientless
- Déployer les VPNs SSL Clientless standard sur ASA
- Déployer l'accès aux applications sur des VPNs SSL Clientless ASA

- Déployer l'authentification avancée et les méthodes d'autorisation sur VPNs SSL Clientless

Déployer les VPNs Cisco AnyConnect

- Déployer les VPNs Cisco AnyConnect standard sur ASA
- Déployer les VPNs Cisco AnyConnect avancés sur ASA
- Déployer l'authentification avancée et les méthodes d'autorisation sur VPNs Cisco Anyconnect
- Déployer les VPNs IPSec/IKEv2 Cisco AnyConnect

Politiques d'accès dynamiques et sécurité des équipements terminaux

- Implémenter Host Scan
- Implémenter les DAP pour VPNs SSL

Certification Cisco CCNP Security - Cisco Certified Network Professional

- La certification Cisco CCNP Security nécessite la réussite des examens : 300-206 préparé par la formation SENSS + 300-207 préparé par la formation STICS + 300-208 préparé par la formation SISAS + 300-209 préparé par ce cours SIMOS