

## IMPLEMENTING CISCO SECURE MOBILITY

Cette formation permet d'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.

Les participants acquièrent de l'expérience pratique dans la configuration et le dépannage de l'accès distant et des solutions VPN site à site, avec les «appliances» de sécurité Cisco ASA et les routeurs Cisco IOS.

### PRÉREQUIS:

Les participants doivent posséder le niveau de certification [CCNA](#) et [CCNA Sécurité](#).

### PUBLIC:

Cette formation s'adresse aux ingénieurs sécurité réseau.

### OBJECTIFS:

- Les différentes technologies de VPN et leurs déploiements
- Les algorithmes de cryptographie et protocoles qui fournissent la sécurité VPN
- Les solutions VPN Cisco site à site
- Le "flexVPN" Cisco pour une configuration «IPSec» en «point à point», «hub and spoke» et «spoke-to-spoke»
- Le WebVPN «SSL/TLS» Cisco en mode «clientless»
- Le client VPN Cisco AnyConnect en SSL/TLS et IPsec
- Les politiques de sécurité et d'accès dynamique (DAP) (Dynamic Access Policies)

### CONTENU:

L'essentiel des technologies VPN et de la cryptographie

- La responsabilité des VPNs dans la sécurité des réseaux
- Cryptographie et VPNs

Installer des solutions sécurisées de connectivité

- Présentation des solutions Cisco sécurisées de connectivité de site à site
- Installation des VPNs IPsec point à point sur Cisco ASA
- Installation des VPNs IPsec basé sur VTI sur Cisco IOS
- Installation des DMVPNs sur Cisco IOS

Installer sur Cisco IOS, les solutions FlexVPN

- Présentation des solutions FlexVPN Cisco
- Installation des VPNs IPsec point à point à l'aide de FlexVPN
- Installation des VPNs IPsec Hub-and-Spoke à l'aide de FlexVPN
- Installation des VPNs IPsec Spoke to Spoke à l'aide de FlexVPN

**CODE DE LA FORMATION:**  
CS-SC-SIMOS

**ÉDITEUR OU  
CONSTRUCTEUR:**  
CISCO

**VERSION:**  
1.0

**DURÉE:**  
5 JOURS

#### Installer les VPNs SSL Clientless

- Présentation des VPNs SSL Clientless
- Installation des VPNs SSL Clientless de base sur Cisco ASA
- Installation de l'accès aux applications sur des VPNs SSL Clientless Cisco ASA
- Installation de l'authentification avancée et des méthodes d'autorisation sur VPNs SSL Clientless

#### Installer les VPNs Cisco AnyConnect

- Installation des VPNs Cisco AnyConnect de base sur Cisco ASA
- Installation des VPNs Cisco AnyConnect avancés sur Cisco ASA
- Installation de l'authentification avancée et des méthodes d'autorisation sur VPNs Cisco Anyconnect Installation des VPNs IPSec/IKEv2 Cisco AnyConnect

#### Mise en place des protocoles d'accès dynamiques ainsi que la sécurité des équipements terminaux

- Installer Host Scan
- Installer les DAP pour VPNs SSLPage

#### **LAB:**

- Lab 1: Implement Site-to-Site Secure Connectivity on the Cisco ASA
- Lab 2: Implement Cisco IOS Static VTI Point-to-Point Tunnel
- Lab 3: Implement DMVPN
- Lab 4: Implement Site-to-Site Secure Connectivity Using Cisco IOS FlexVPN
- Lab 5: Implement Hub-to-Spoke Secure Connectivity Using Cisco IOS FlexVPN
- Lab 6: Implement Spoke-to-Spoke Secure Connectivity Using Cisco IOS FlexVPN
- Lab 7: Implement ASA Basic Clientless SSL VPN
- Lab 8: Configure Application Access for Cisco ASA Clientless SSL VPN
- Lab 9: Implement Local and AAA for Clientless SSL VPNs
- Lab 10: Implement ASA Basic AnyConnect SSL VPN
- Lab 11: Configure Advanced Authentication for Cisco AnyConnect SSL VPN
- Lab 12: Implement AnyConnect IPsec/IKEv2
- Lab 13: Implement Host Scan and DAP

#### **CERTIFICATION:**

La formation SIMOS prépare au passage de l'examen Cisco 300-209, nécessaire à l'obtention du titre de certification [CCNP Sécurité](#).

#### **COURS SUIVANT:**

Mettre en œuvre les solutions Cisco pour sécuriser son réseau d'entreprise (Cisco Edge Network)

Mettre en œuvre les solutions Cisco Secure Access

Implementing Cisco Threat Control Systems