METTRE EN ŒUVRE LA SÉCURITÉ AVEC LES FIREWALLS CISCO ASA - FONCTIONNALITÉS DE BASE

CODE DE LA FORMATION:
CS-SC-SASAC

ÉDITEUR OU CONSTRUCTEUR:
CISCO

VERSION:
1.0

DURÉE:
5 JOURS

Cette formation permet aux participants d'acquérir les connaissances et outils nécessaires pour mettre en oeuvre et administrer des pare-feu Cisco ASA (Adaptative Security Appliance).
Les participants seront capables de réduire les failles de sécurité de leur infrastructure informatique et d'accès aux données en implémentant les fonctionnalités des Cisco ASA.
Cette formation est basée sur les fonctionnalités de la version 9.x.

PRÉREQUIS:
Posséder le niveau de compétences CCNA Sécurité ou avoir suivi les cours ICND1 et IINS.

PUBLIC:
Cette formation s'adresse aux Ingénieurs sécurité en charge de l'installation et de la configuration des Cisco ASA.

OBJECTIFS:
- Décrire les fonctionnalités de base d'un pare-feux Série ASA 5500-X Next-generation
- Intégrer un ASA dans une infrastructure et utiliser les outils d'administration
- Implémenter les règles de filtrages basiques (Policy)
- Décrire les composants d'un VPN
- Décrire et implémenter les solutions VPN en mode clientless
- Décrire et implémenter les solutions full tunnel VPN IPsec et SSL avec des Cisco ASA et Cisco AnyConnect

CONTENU:

Les bases des Cisco ASA (Adaptative Security Appliance)
- Présentation des Cisco ASA et des fonctionnalités
- Identification de la gamme
- Gestion des licences

Connexion basique et management
- Intégration d'un Cisco ASA dans le réseau
- Configuration des paramètres réseaux de l'appliance

Configuration des fonctionnalités réseau
- Configuration de la translation d'adresse (NAT) sur l'appliance
- Configuration du contrôle d'accès sur l'appliance
- Configuration du routage sur l'appliance

Configuration des règles de filtrage

- Présentation du MPF(Modular Policy Framework)
- Configuration des règles d'inspection avancées

Composant d'un réseau VPN

- Présentation des composants d'un VPN
- Implémentation des Profil, des Groups Policies et des User Policies
- Implémentation des services PKI

VPN : Le mode clientless

- Introduction à la solution clientless SSL VPN
- Déploiement sur un Cisco ASA
- Configuration de l'authentification et de l'autorisation

VPN : Cisco Anyconnect Full Tunnel

- Déploiement basique d'un Cisco AnyConnect SSL VPN sur un ASA
- Déploiement avancé d'un Cisco AnyConnect SSL VPN sur un ASA
- Déploiement des méthodes d'authentification et d'autorisation avancées
- Déploiement des VPN IPSEC.IKEv2

Cisco ASA : Haute disponibilité et virtualisation

- Configuration de la redondance d'interfaces
- Configuration de la haute disponibilité en mode Actif/Passif
- Configuration des contextes
- Configuration de la haute disponibilité en mode Actif/Actif (EN OPTION)

COURS SUIVANT:
Mettre en œuvre la sécurité avec les firewalls Cisco ASA - Fonctionnalités avancées