Réseau
Cisco

Administrateur Firewalls PIX/ASA certifié Cisco

ASA | 5 JOURS

Description

La sécurité des données est une condition indispensable aux échanges sur les réseaux locaux et distants. Il est primordial, pour un administrateur, de connaître et de réévaluer en permanence les risques qu'encourent les systèmes informatiques. Les premières étapes dans la sécurisation d'un réseau informatique concernent l'accès aux dispositifs actifs du réseau (routeurs, commutateurs), la mise en place et la configuration d'un pare-feu.

Déroulement

Le cursus de formation Firewall permet d'atteindre ces deux objectifs, tout en répondant à une demande importante de profils formés et certifiés dans les domaines de la sécurité. De l'installation physique d'une infrastructure réseau à la configuration des mécanismes avancés de routage, le cursus de formation alterne les présentations théoriques et les ateliers pratiques.

Public

- Administrateurs et ingénieurs réseau
- Responsables sécurité

Pré-requis

- Avoir déjà réalisé la configuration de base d'un routeur Cisco
- Savoir utiliser un système d'exploitation Windows ou Unix/Linux

Certifications

- 642-504 SNRS
- 642-524 SNAF

Programme

Configuration d'un système de sécurité de base

- Description de la sécurité logicielle et physique
- Utilisation des commandes show
- Mise en place d'une route par défaut
- Configuration des options de log
- Description des technologies de pare-feu
- Configuration d'un NAT statique
- Limitation des connexions embryonnaires

Configuration d'une solution de sécurité

- Configuration des ACL basées sur les adresses, l'heure et les protocoles
- Configuration des groupes d'objets pour optimiser les ACL
- Configuration du filtrage de java/activeX
- Configuration de l'URL filtering
- Vérification des restrictions de trafic entrant

Configuration VPN

- Les certificats
- Configuration de IKE
- Configuration des paramètres IPSec
- Configuration des crypto-map
- EasyVPN
- Configuration de WebVPN

Firewall transparent et virtuel, options de haute disponibilité

- Les firewall transparents
- Configuration d'un parefeu transparent
- Monitoring et maintien du parefeu virtuel
- Le fail-over
- Configuration du système de sécurité pour le fail-over

Configuration d'une politique modulaire de sécurité

- Configuration d'une class-map
- Configuration d'une policy-map
- Configuration d'une service-policy
- Configuration d'une ftp-map
- DNS-guard

Vous serez capable de...

Gérer et mettre en place des Firewalls Cisco

- Comprendre les mécanismes fondamentaux pour la sécurisation d'une infrastructure réseau
- Connaître les principales menaces sur les réseaux modernes
- Sécuriser les dispositifs réseau
- Configurer un PIX Firewall
- Configurer un firewall ASA
- Configurer le support d'AAA
- Configurer un système de détection d'intrusion sur un routeur Cisco
- Créer un VPN site à site
- Configurer un VPN pour les accès distants
- Configurer un serveur de certificats
- Configurer un IOS Firewall
- Analyser et restreindre le flux (entrant et sortant)
- Analyser les statistiques
- Optimiser les règles de sécurité

egilia® LEARNING