



FORMATION EXPERTISES : POLITIQUE DE SÉCURITÉ & FIREWALLS

OBJECTIFS

Ce cours apporte au stagiaire, les bases théoriques et pratiques de maîtrise de la politique de sécurité, par la mise en œuvre de Firewalls.

À l'issue de la formation, les stagiaires seront capables de :

- appréhender les menaces et les attaques internes et externes du monde IP, les vulnérabilités
- déterminer les points clefs d'une politique de sécurité,
- comprendre les bons choix pour une architecture sécurisée, tout en conservant un bon niveau de performance
- décrire les principales vulnérabilités,
- décrire les fonctions d'un firewall,
- classifier les différentes catégories de firewalls,
- décrire les techniques à la base des firewalls,
- déployer et administrer des firewalls.

MÉTHODE

Les exposés théoriques sont illustrés d'exemples concrets, de représentations schématiques et d'exercices pratiques sur Firewalls. Tout au long de la formation, du temps sera consacré aux exercices et aux questions permettra d'intégrer les notions de base et de les manipuler en groupe.

L'atteinte des objectifs est contrôlée au fur et à mesure du stage.

PERSONNES CONCERNÉES, PRÉREQUIS

Directeurs, responsables du système d'information, ingénieurs, techniciens, administrateurs systèmes et réseaux ayant des connaissances de base en informatique, bases de transmission de données, Internet et TCP/IP.

DURÉE

Deux journées de formation en intra-entreprise pour 3 à 10 participants.

Introduction

- concepts de sécurité: les points clefs
- la sécurité dans les réseaux IP

Rappels sur TCP/IP et les services Internet

- points clefs de l'adressage IP
- le routage
- les services TCP/IP: les ports et les sockets
- mécanismes d'une session TCP/IP

Vulnérabilités et attaques

- IP, TCP
- services (SMTP, DNS, SNMP, NFS, HTTP, FTP, etc.)

Fonctions et limites d'un firewall

- concepts et définitions, protections d'un réseau par un firewall
- le filtrage et ses limites, NAT, PAT, ports

Firewall et performances des réseaux

- la répartition de charges
- la haute disponibilité

Les catégories de firewalls

- routeurs filtrants
- Firewalls à états
- Proxies et firewalls

Architecture de sécurité

- les zones démilitarisées
- architectures classiques et ses différentes variantes
- déploiement

Administration des firewalls

- architecture d'un firewall, règles de sécurité
- le traitement des logs
- supervision et sécurité d'un firewall

Les offres du marché et du domaine public

- exemples concrets
- conseils pratiques et sources d'information