kapedia
FORMATIONS INFORMATIQUES
systèmes | virtualisation | réseaux | messagerie | sécurité | développement | web | gestion de projets | sharepoint | SGBD | infographie | bureautique
www.kapedia.fr

FORMATION FORTINET - SECURITE RESEAUX

Code **SECU21**	**Objectifs** • Décrire les fonctionnalités du FortiGate • Installer et configurer le firewall • Mettre en oeuvre une stratégie de filtrage réseau et applicative • Mettre en oeuvre un VPN SSL et IPSEC • Mettre en œuvre la haute disponibilité des FortiGate •
	Public Techniciens, administrateurs et ingénieurs systèmes réseaux, sécurité.
	Prérequis Bonnes connaissances de TCP/IP. Connaissances de base en sécurité informatique.
Durée **4jours**	**Méthodes pédagogiques** Alternance d'apports théoriques et d'exercices pratiques.
	Moyens pédagogiques • 1 PC par personne avec logiciel installé • 1 Support de cours par personne

INTRODUCTION

- Technologies et caractéristiques des firewalls.
- L'architecture. La famille des produits FORTINET.
- Les composants de l'Appliance.

CONFIGURATION ET ADMINISTRATION

- Les tâches d'administration.
- Les modes CLI/GUI et FortiManager.
- La procédure d'installation.
- Prise en main de l'interface.

LE FILTRAGE RESEAU ET LE FILTRAGE APPLICATIF

- La politique de contrôle d'accès du firewall. Le filtrage des adresses et des ports.
- Définir une politique de filtrage. Gestion des règles.
- Le filtrage de contenu et détection de pattern.
- Le filtrage URL. Les options avancées.
- Les filtres anti-spam. Le contrôle du protocole SMTP.
- Les fichiers attachés. Les profils de protection. L'antivirus. Le blocage par extension de fichiers.

LE NAT ET LE ROUTAGE

- Les modes d'utilisation NAT/Route/Transparent.
- Le routage statique et le routage dynamique.
- Quelle politique de routage mettre en place ?

LES VLAN ET LE VIRTUALS DOMAINS (VDOM)

- Rappels sur le concept de VLAN. Quand l'utiliser ?
- Administration et supervision.
- Le routage InterVDOM.

LE VPN avec IPSEC

- Rappels d'IPSEC. Le VPN IPSEC site à site.
- Le mode interface et le mode tunnel.
- Le VPN IPSEC client à site.
- Le client "FortiClient". L'authentification Xauth.
- Les tunnels avec la clé prépartagée.

LE VPN AVEC SSL

- Rappels sur le protocole SSL.
- Le mode Tunnel et le mode Portail.
- Choisir le mode approprié.

HAUTE DISPONIBILITE

- Les concepts de haute disponibilité.
- Le mode actif-passif/actif-actif.
- Répondre au besoin de l'entreprise.

.