Fortinet Network Security Associate (NSE4)

★★★★★

SII-429 **5 Jours (35 Heures)**

Description

Au cours de cette formation, vous apprendrez à maîtriser les principales fonctionnalités UTM des équipements FortiGate. Vous travaillerez directement sur des dispositifs accessibles via notre environnement de formation dédié. Les exercices pratiques vous permettront de configurer des règles de pare-feu, de mettre en place des tunnels VPN IPsec ainsi que des accès VPN SSL. Vous aborderez également la protection contre les malwares, la création de profils de filtrage d'URL et l'authentification des utilisateurs via un portail captif.

À qui s'adresse cette formation ?

Pour qui

- Ingénieurs/administrateurs et techniciens réseaux.

Prérequis

- Basic knowledge of IT security as well as good knowledge of TCP/IP.

Les objectifs de la formation

- Se préparer efficacement à l'examen de certification Fortinet NSE4 (FortiGate I et II)
- Comprendre et décrire les principales fonctionnalités UTM des équipements FortiGate
- Mettre en œuvre l'authentification des utilisateurs à travers les règles de pare-feu
- Déployer un tunnel VPN IPsec entre deux appliances FortiGate
- Analyser les journaux (logs) et générer des rapports pertinents

Programme de la formation

Fortigate UTM

- Administration de l'équipement, compte et authentification.
- Le Fortigate comme serveur DHCP, serveur DNS.
- Fichier de configuration et mise à niveau du firmware.
- L'antivirus : filtre antiviral de flux web (HTTP, HTTPS, FTP) et de messagerie (SMTP, SMTPS, IMAP, IMAPS, POP3, POP3S).
- Le filtrage web.
- L'IPS Applicatives. Le contrôle applicatif.
- La protection DoS (le Déni de Service).

Le firewall

- Les règles de sécurité.
- Contrôle des postes de travail.
- Journal et analyse.
- NAT, la translation d'adresses IP.
- Inspection du trafic.
- Diagnostique des règles de sécurité.

Le proxy

- Authentification Proxy et méthodes d'authentification.
- Authentification à deux facteurs.
- Types et règles d'authentification.
- Utilisateurs et groupes.
- Supervision des utilisateurs.

VPN SSL et IPSec

- Topologies VPN, comprendre le VPN SSL Fortigate.
- Options et sécurité VPN SSL.
- Configuration du VPN SSL, VPN IPSec.
- Monitoring VPN IPSec.
- VPN Dialup, redondants.

Journalisation et surveillance

- Comprendre la structure des Logs.
- Navigation dans les Logs.
- Alertes Email et paramètres de Logs.
- Monitoring et stockage des Logs.

Certificats et cryptographie

- Les certificats digitaux.
- Inspection du contenu SSL.

Haute disponibilité (HA)

- La synchronisation entre les équipements.
- Les options de Clustering.

Les outils de diagnostic

- Le diagnostic du HA.
- Diagnotics et Troubleshooting.