Microtel
Training institute

NSE4 FORTIGATE SECURITY – FORTIGATE INFRASTRUCTURE

CURSUS:
FORTINET
SÉCURITÉ DES SYSTÈMES D'INFORMATION

TYPE DE FORMATION:
INTER-ENTREPRISES

CODE DE LA FORMATION:
FT-SC-NSE4

ÉDITEUR OU CONSTRUCTEUR:
FORTINET

DURÉE:
5 JOURS

PRÉREQUIS:

Des notions TCP/IP et des concepts firewall. Connaissance des couches du modèle OSI. Connaissance des concepts de firewall.

PUBLIC:

Tous ceux qui administrent régulièrement un firewall Fortigate et à tous ceux qui participent au design des architecture réseau et sécurité reposant sur des matériels Fortigate

OBJECTIFS:

- Décrire les fonctionnalités des UTM du Fortigate,
- Neutraliser les menaces véhiculées au travers des malwares, les applications nocives et limiter les accès aux sites inappropriés,
- Contrôler les accès au réseau selon les types de périphériques utilisés,
- Authentifier les utilisateurs au travers des règles firewalls,
- Mettre en oeuvre un VPN SSL pour l'accès des utilisateurs nomades au réseau de l'entreprise,
- Déployer un tunnel IPSEC entre deux boîtiers Fortigate,
- Comparer les tunnels IPSEC de type « policybased » et « tunnel-based »,
- Appliquer de la PAT, de la source NAT et de la destination NAT,
- Interpréter les logs,
- Générer des rapports,
- Utiliser la GUI et la CLI,
- Mettre en oeuvre le proxy explicit, le cache et l'authentification des utilisateurs,
- Maîtriser l'utilisation des applications au sein de votre réseau…
- Déployer un cluster de Fortigate,
- Inspecter le trafic réseau en mode transparent,
- Analyser la table de routage d'un Fortigate,
- Utiliser les PBR (Policy Based Routing),
- Réaliser du load balancing de trafic sur plusieurs opérateurs,
- Mettre en oeuvre les Virtual Domain,
- Implémenter une architecture de VPN IPSec redondée
- Dépanner et diagnostiquer,
- Mettre en oeuvre des politiques anti DoS,
- Mettre en oeuvre le FSSO,
- Déchiffrer les flux chiffrés,
- Déployer des profils de DLP,
- Implémenter IPv6 et le dual stack IPv4/IPv6,

- Comprendre le fonctionnement de l’accélération matérielle…

CONTENU:

1. Introduction sur Fortigate et les UTM
2. Gestion des logs et supervision
3. Les règles firewall
4. Le NAT
5. Les règles firewall avec authentification des utilisateurs
6. Le VPN SSL
7. Introduction au VPN IPSEC
8. L’antivirus
9. Le proxy explicit
10. Le filtrage d’URL
11. Le contrôle applicatif
12. Le routage
13. La virtualisation
14. Le mode transparent
15. La haute disponibilité
16. Le VPN IPSec avancé
17. L’IPS
18. Le FSSO
19. Les certificats, la cryptographie
20. Le DLP
21. Les diagnostics
22. L’accélération matérielle
23. IPv6