FortiGate Security

SYLLABUS

Au cours de cette session de 3 jours, vous prendrez en main les fonctions UTM du FortiGate. Au travers des exercices vous configurerez des règles pare-feu, des tunnels VPN IPSEC, des accès VPN SSL, la protection contre les malwares, des profils de filtrage d'URL, l'authentification au travers d'un portail captif, la prévention de fuites de données, le déchiffrement…

Certification

Ce cours ainsi que FortiGate Security préparent au passage de la certification NSE4.

Objectifs

A l'issue de cette session de trois jours vous serez en mesure de :

- 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 du portail captif personnalisable,

- mettre en oeuvre un VPN SSL pour l'accès des utilisateurs nomades au réseau de l'entreprise,

- mettre en oeuvre un VPN IPsec pour l'accès des utilisateurs nomades au réseau de l'entreprise,

- appliquer de la PAT, de la source NAT et de la destination NAT,

- interpréter les logs et générer des rapports

- utiliser la GUI et la CLI,

- mettre en oeuvre la protection anti-intrusion,

- maîtriser l'utilisation des applications au sein de votre réseau…

A qui s'adresse cette formation ?

A tous ceux qui administrent régulièrement un firewall FortiGate

Agenda

1. Introduction sur FortiGate et les UTMs
2. La « Security Fabric »
3. Les règles firewall
4. La NAT
5. Les règles firewall avec authentification des utilisateurs
6. Gestion des logs et supervision
7. Les Certificats
8. Le filtrage d'URL
9. Le contrôle applicatif
10. L'antivirus
11. Le contrôle anti-intrusion
12. Le VPN SSL
13. Le VPN IPSEC en mode dial-up

Format du cours

Instructeur qui présentera chacun des modules.

Exercices pratiques à la fin de chaque module.

Prérequis

Version produit

Des notions TCP/IP et des concepts firewall.

FortiOS 6.2

FortiGate Infrastructure

SYLLABUS

Au cours de cette session de 2 jours, vous prendrez en main les fonctions d'architectures avancées du FortiGate. Vous aurez la main sur des équipements qui se trouvent sur notre environnement de formation. Et au travers des exercices vous configurerez de la SD-Wan, du routage avancé, la mise en haute disponibilité des FortiGate, le mode transparent, des tunnels IPsec redondés, les VDOMS, le Single Sign On, …

Certification

Ce cours ainsi que FortiGate Infrastructure préparent au passage de la certification NSE4.

Objectifs

A l'issue de cette session de deux jours vous serez en mesure de :

- configurer de la SD-Wan,

- monitorer le statut de chaque lien de la SD-Wan

- configurer de la répartition de charge au sein de la SD-Wan

- déployer un cluster de FortiGate,

- inspecter et sécuriser le trafic réseau sans impacter le routage,

- analyser la table de routage d'un FortiGate,

- diviser un FortiGate physique en plusieurs FortiGates virtuels indépendants, via la mise en oeuvre des Virtual Domains,

- étudier et choisir une architecture de VPN IPsec

- comparer les VPN IPsec en mode Interface (route-based) ou Tunnel (Policy-based)

- implémenter une architecture de VPN IPSec redondée,

- troubleshooter et diagnostiquer des problématiques simples sur le FortiGate,

- mettre en oeuvre l'identification utilisateur ou l'authentification transparente dans les environnements Active Directory…

A qui s'adresse cette formation ?

A tous ceux qui participent au design des architectures réseaux et sécurité reposant sur des matériels FortiGate.

Agenda

1. Le routage
2. La SD-Wan
3. La virtualisation
4. L’analyse L2
5. Le VPN IPSec en mode site à site
6. Le FSSO
7. La haute disponibilité
8. Le Proxy Explicite
9. Les diagnostics

Format du cours

Instructeur qui présentera chacun des modules et des exercices pratiques à la fin de chaque module.

Version produit

FortiOS 6.2

Prérequis

Connaissance des couches du modèle OSI.

Connaissance des concepts de firewall.