Fortigate Securité – Infrastructure

★★★★★

SII-414 **5 Jours (35 Heures)**

Description

Cette formation FortiGate sécurité et infrastructure vous apportera toutes les connaissances liées à la gestion unifiée des menaces (Unified Threath Management ou UTM) sur une même plateforme. La partie "sécurité" vous fournira les acquis sur les pratiques liées aux règles générales de gestion et de protection contre les malwares. La partie "infrastructure" permettra, quant à elle, la maîtrise des fonctions d'architectures avancées du FortiGate.

À qui s'adresse cette formation ?

Pour qui

Ingénieurs/administrateurs et techniciens réseau et toute personne impliquée dans la conception d'architectures réseau et de sécurité basées sur les matériels FortiGate.

Prérequis

Connaissances de base en sécurité informatique ainsi que de bonnes connaissances de TCP/IP.

Les objectifs de la formation

- Déployer le mode de fonctionnement approprié à son réseau (proxy, flow, NGFW…)
- Utiliser conjointement les interfaces graphique et CLI pour l'administration
- Contrôler l'accès réseau aux réseaux configurés à l'aide de politiques de pare-feu
- Appliquer la redirection de port, le Network Address Translation (NAT) source et le NAT destination
- Authentifier les utilisateurs à l'aide de politiques de pare-feu
- Comprendre les fonctions de chiffrement et les certificats
- Déchiffrer le trafic sécurisé SSL/TLS afin de l'inspecter
- Configurer des profils de sécurité pour neutraliser les menaces et les abus
- Appliquer des techniques de contrôle des applications réseau
- Utiliser des protocoles et des ports standard ou non standard
- Lutter contre le piratage et le déni de service (DoS)
- Collecter et interpréter les items collectés dans les journaux

- Identifier les caractéristiques du tissu de sécurité Fortinet (Security Fabric)
- Analyser une table de routage FortiGate
- Acheminer les paquets à l'aide de routes statiques et de routes basées sur des règles
- Déployer les multichemins à charge équilibrée
- Diviser FortiGate en deux ou davantage d'appareils virtuels
- Configurer des domaines virtuels (VDOM)
- Comprendre les principes fondamentaux et les avantages de l'utilisation de ZTNA
- Proposer un VPN SSL pour un accès sécurisé à votre réseau privé
- Établir un tunnel VPN IPsec entre deux appareils FortiGate
- Implémenter un VPN maillé ou partiellement redondant
- Diagnostiquer les échanges IKE ayant échoués
- Offrir un accès Single Sign-On (FSSO) aux services réseau en adossant l'accès à Microsoft Active Directory (AD)
- Déployer des appareils FortiGate en cluster haute disponibilité
- Améliorer la tolérance aux pannes et fournir des performances élevées
- Déployer l'interface virtuelle SD-WAN
- Mettre en œuvre une répartition dynamique des flux selon des performances mesurées sur les interfaces membres
- Diagnostiquer et corriger les problèmes courants

Programme de la formation

Sécurité - Introduction et réglages initiaux

- Fonctionnalités de haut niveau.
- Les décisions initiales.
- Administration de base.
- Maintenance de base.

Sécurité - Politique de pare-feu

- Configuration de politiques.
- Gestion des politiques.
- Meilleures pratiques et dépannage.

Sécurité - Network Address Translation

- Introduction.
- NAT adossé à la politique versus NAT central.
- Meilleures pratiques et dépannage.

Sécurité - Authentification par firewall

- Méthodes d’authentification de pare-feu.
- Groupes d’utilisateurs.
- Règles de pare-feu avec authentification.

Sécurité - Logging et monitoring

- Notions de base sur les journaux.
- Journalisation locale ou distante.
- Réglages de journalisation, recherche dans les journaux.
- Protection des données de journalisation.

Sécurité - Opérations de certificat

- Authentifier et sécuriser les données à l'aide de certificats.
- Inspecter les données chiffrées.

Sécurité - Filtrage web

- Modes d'inspection.
- Bases du filtrage web.
- Fonctionnalités supplémentaires de filtrage web basées proxy.
- Filtrage Vidéo.
- Meilleures pratiques et dépannage.

Sécurité - Contrôle des applications

- Bases du contrôle des applications.
- Configuration du contrôle des applications.
- Journalisation et surveillance des événements de contrôle des applications.

Sécurité - Antivirus

- Fondamentaux.
- Modes d’analyse.
- Configuration de l’antivirus.

Sécurité - Prévention des intrusions

- Le système de prévention des intrusions.
- Déni de service.

Sécurité - Tissu de sécurité (Security Fabric)

- Notion de tissu de sécurité.
- Déploiement.
- Étendre le tissu de sécurité.
- Système de notation du tissu de sécurité et vue de la topologie.

Infrastructure - Routage

- Routage sur FortiGate.
- Surveillance du routage et attributs de routage.
- Partage de charge à coût égal.
- Test Reverse Path Forwarding (RPF), lutte contre l’usurpation d’adresse.
- Sondes de santé des liens et bascule de routes.
- Diagnostics.

Infrastructure - Domaines virtuels

- Concepts VDOM.
- Administrateurs VDOM.
- Configuration des VDOM.
- Liens interVDOM.
- Meilleures pratiques et dépannage.

Concepts VDOM. Administrateurs VDOM. Configuration des VDOM. Liens interVDOM. Meilleures pratiques et dépannage.

- Fonction et déploiement.
- FSSO avec Active Directory.
- Réglages et dépannage.

Infrastructure - Zero Trust Network Access (ZTNA)

- Introduction.
- Comparer ZTNA aux VPNs IPsec et SSL.

Infrastructure - VPN SSL

- Modes de déploiement.
- Configuration.
- Surveillance et dépannage.

Infrastructure - IPsec VPN

- Introduction.
- Configuration.
- Routage et règles de pare-feu.
- VPN redondants, VPN maillé.
- Surveillance, journalisation.

Infrastructure - Haute disponibilité

- Modes de fonctionnement actif/passif versus actif/actif.
- Synchronisation du cluster HA.
- Basculement HA.

Infrastructure - SD-WAN

- Motivation, répartition de flux dynamique.
- Implémentation.
- Sondes de performance.
- Règles SD-WAN.
-

Infrastructure - Diagnostics

- Généralités.
- Débogage de flux.
- Processeur et mémoire.
- Micrologiciel et matériel.