Programme de cours
FortiGate Administrator (FGT-ADM)

Durée :	4 jours soit 28 heures	Référence :	FL-FO-FGT-ADM

Public visé :

Les professionnels des réseaux et de la sécurité impliqués dans la gestion, la configuration, l'administration et la surveillance des dispositifs FortiGate utilisés pour sécuriser les réseaux de leurs organisations devraient suivre ce cours.

Pré-requis :

- Connaissance des protocoles de réseau
- Compréhension de base des concepts de pare-feu

Objectifs pédagogiques :

Après avoir suivi ce cours, vous serez en mesure de :

- Implémentation du paramétrage de base réseau à partir de la configuration usine
- Configurer et contrôler les accès administrateur au Fortigate
- Utiliser l'interface graphique et le CLI pour l'administration
- Contrôler l'accès aux réseaux configurés à l'aide de stratégies de pare-feu
- Appliquer le transfert de port, le NAT à la source et le NAT à la destination
- Analyser une table de routage FortiGate
- Routage des paquets à l'aide de routes statiques et basées sur des règles pour les déploiements à trajets multiples et à charge équilibrée
- Authentifier les utilisateurs à l'aide de stratégies de pare-feu
- Monitorer les utilisateurs à l'aide de la GUI
- Offrir un accès Fortinet Single Sign-On (FSSO) aux services du réseau, intégré à Microsoft Active Directory (AD)
- Comprendre les fonctions de cryptage et les certificats
- Inspecter le trafic sécurisé SSL/TLS pour empêcher le cryptage utilisé pour contourner les politiques de sécurité
- Configurer les profils de sécurité pour neutraliser les menaces et les abus, y compris les virus, les torrents et les sites web inappropriés
- Appliquer des techniques de contrôle des applications pour surveiller et contrôler les applications réseau susceptibles d'utiliser des protocoles et des ports standard ou non standard
- Proposer un VPN SSL pour un accès sécurisé à votre réseau privé
- Établir un tunnel VPN IPsec entre deux équipements FortiGate
- Configuration du SD-WAN
- Identifier les caractéristiques de la Security Fabric de Fortinet
- Déployer les équipements FortiGate en tant que cluster HA pour la tolérance aux pannes et la haute performance
- Diagnostiquer et corriger les problèmes courants

Compétences acquises à l'issue de la formation :

- Configurer les paramètres réseau de base, les accès administrateur et l'administration via GUI et CLI.
- Déployer et gérer des stratégies de pare-feu, le NAT, le routage statique ou avancé, ainsi que le SD-WAN.
- Authentifier et contrôler les utilisateurs via politiques, FSSO et intégration Active Directory.
- Mettre en œuvre des profils et techniques de sécurité (SSL/TLS inspection, antivirus, filtrage web, contrôle applicatif).
- Assurer la connectivité sécurisée par la configuration de VPN SSL et IPsec.
- Optimiser la résilience et la performance en déployant la Security Fabric, un cluster HA et en diagnostiquant les incidents.

Modalités pédagogiques :

Session dispensée en présentiel ou téléprésentiel, selon la modalité inter-entreprises ou intra-entreprises sur mesure.
La formation est animée par un(e) formateur(trice) durant toute la durée de la session et présentant une suite de modules théoriques clôturés par des ateliers pratiques validant l'acquisition des connaissances. Les ateliers peuvent être accompagnés de Quizz.
L'animateur(trice) présente la partie théorique à l'aide de support de présentation, d'animation réalisée sur un environnement de démonstration.
En présentiel comme en téléprésentiel, l'animateur(trice) accompagne les participants durant la réalisation des ateliers.

Moyens et supports pédagogiques :

Cadre présentiel
Salles de formation équipées et accessibles aux personnes à mobilité réduite.
- Un poste de travail par participant
- Un support de cours numérique ou papier (au choix)
- Un bloc-notes + stylo
- Vidéoprojection sur tableau blanc
- Connexion Internet
- Accès extranet pour partage de documents et émargement électronique

Cadre téléprésentiel
Session dispensée via notre solution iClassroom s'appuyant sur Microsoft Teams.
- Un compte Office 365 par participant
- Un poste virtuel par participant
- Un support numérique (PDF ou Web)
- Accès extranet pour partage de documents et émargement électronique

Informations sur l'accessibilité :

Nos formations sont, dans la mesure du possible, conçues pour être accessibles à toutes et à tous. Afin de garantir les meilleures conditions d'accueil et d'apprentissage pour les personnes en situation de handicap, nous vous invitons à contacter notre référente handicap certifiée :
Céline SOLATGES – 05 61 34 39 80 – csolatges@iform.fr
Nous vous remercions de bien vouloir nous communiquer toute information utile à ce sujet en amont de la formation, afin de mettre en place les adaptations nécessaires et d'assurer un accompagnement optimal.
Pour en savoir plus sur les dispositifs d'accompagnement existants, vous pouvez consulter les sites suivants :

- AGEFIPH
- FIPHFP
- MDPH de votre département

Description / Contenu

Cette formation remplace le cours NSE4 - FortiOS - Fortigate Sécurité & Infrastructure I & II (FORT-BUNDL)

Résumé du cours :

Dans ce cours, vous apprendrez à utiliser les fonctionnalités les plus courantes de FortiGate, y compris les profils de sécurité. Dans les laboratoires interactifs, vous explorerez les politiques de pare-feu, l'authentification des utilisateurs, le VPN SSL, le VPN IPsec de site à site, la Security Fabric de Fortinet, et comment protéger votre réseau en utilisant des profils de sécurité, tels que l'IPS, l'antivirus, le filtrage Web, le contrôle des applications, et plus encore. Ces bases de l'administration vous permettront d'acquérir une solide compréhension des fonctionnalités les plus courantes de FortiGate. Versio : FortiOS 7.4

Contenu

- 1. Paramètres du système et du réseau
- 2. Stratégies de pare-feu et traduction d'adresses réseau
- 3. Routage
- 4. Authentification du pare-feu
- 5. Signature unique Fortinet (FSSO)
- 6. Opérations de certificat
- 7. Antivirus
- 8. Filtrage Web
- 9. Prévention des intrusions et contrôle des applications
- 10. VPN SSL
- 11. VPN IPSec
- 12. Configuration et surveillance du SD-WAN
- 13. Structure de sécurité
- 14. Haute disponibilité
- 15. Diagnostic et dépannage