FortiGate Administrator

Lien : https://innov-systems.com/formation/fortigate-administrator

DURÉE
5 jours (35h)

RÉFÉRENCE
SEC328

CATÉGORIE
Fortinet

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Implémenter le 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
- Mettre en pratique le 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)
- Identifier 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
- Pratiquer des techniques de contrôle des applications pour surveiller et contrôler les applications réseau susceptibles d'utiliser des protocoles et des ports standards ou non standards
- Proposer un VPN SSL pour un accès sécurisé à votre réseau privé
- Etablir un tunnel VPN IPsec entre deux équipements FortiGate
- Configurer 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.

POUR QUI ?

- Ingénieurs techniques et/ou toute personne occupant ou ayant à vocation d'occuper un poste technique dans le domaine de l'IT.

Programme détaillé

1 / Paramètres du système et du réseau

- Configuration initiale de FortiGate via GUI et CLI
- Paramétrage des interfaces réseau, VLANs et zones
- Gestion de l'heure, des administrateurs et des profils d'accès

2 / Stratégies de pare-feu et NAT

- Création et hiérarchisation des règles de pare-feu
- Configuration de la NAT source, destination et IP Pool
- Mise en œuvre des objets (adresses, services, groupes) pour la simplification des règles

3 / Routage

- Configuration du routage statique et dynamique (OSPF, BGP)
- Utilisation des routes blackhole, de surveillance de lien (link health monitoring)
- Résolution des conflits de routes et vérification des chemins (traceroute, debug route)

4 / Authentification du pare-feu

- Création des utilisateurs locaux et groupes
- Intégration LDAP, RADIUS et TACACS+ pour l’authentification externe
- Application de l’authentification dans les politiques

5 / FSSO (Fortinet Single Sign-On)

- Architecture FSSO : DC Agent, Collector Agent
- Intégration avec Active Directory pour la remontée des sessions utilisateur
- Dépannage des scénarios FSSO et vérification des logs

6 / Opérations de certificat

- Génération et gestion des certificats auto-signés et CA externes
- Déploiement des certificats pour l’inspection SSL et les VPN
- Dépannage des erreurs de certificat et vérification des chaînes de confiance

7 / Antivirus

- Activation du moteur AV et inspection proxy/flow-based
- Configuration des actions (bloquer, mettre en quarantaine, alerter)
- Analyse des journaux et détection des faux positifs

8 / Filtrage Web

- Création de profils de filtrage Web (static, catégorie, rating)
- Fonctionnement du FortiGuard Web Filtering et override
- Surveillance et ajustement des politiques de filtrage

9 / Prévention des intrusions et contrôle des applications

- Configuration des profils IPS et mise à jour des signatures
- Activation du contrôle applicatif : catégorisation et actions
- Analyse des journaux d’événements de sécurité (violations IPS, tentatives d’intrusion)

10 / SSL VPN

- Configuration en mode Web et Tunnel
- Gestion des utilisateurs, portails et permissions
- Dépannage : certificat, authentification, connectivité VPN

11 / IPSec VPN

- Configuration site-to-site et dial-up VPN
- Négociation de phase 1 & 2, sélection de l’algorithme de chiffrement

- Surveillance des tunnels et résolution des problèmes courants (IKE, MTU, routes)

12 / Configuration et surveillance SD-WAN

- Création de zones SD-WAN, ajout de membres WAN
- Définition de règles SD-WAN basées sur SLA (latence, gigue, perte)
- Tableau de bord SD-WAN et surveillance du trafic en temps réel

13 / Security Fabric

- Architecture du Security Fabric et interconnexion des équipements Fortinet
- Activation et configuration de la topologie
- Visibilité du réseau, des menaces et intégration avec FortiAnalyzer

14 / Haute disponibilité (HA)

- Modes de HA : Actif-Passif vs Actif-Actif
- Configuration des synchronisations et surveillance de l’état
- Scénarios de basculement (failover), diagnostics et vérification

15 / Diagnostic et dépannage

- Outils CLI : diagnose, execute, get, show, debug
- Lecture des journaux système, sécurité et trafic
- Étude de cas de dépannage : boucle de routage, NAT incorrect, policy mismatch
- Ingénieurs techniques et/ou toute personne occupant ou ayant à vocation d'occuper un poste technique dans le domaine de l'IT.

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

13 au 17 Juil. 2026	Présentiel -
20 au 24 Juil. 2026	Présentiel -
14 au 18 Sep. 2026	Présentiel -
21 au 25 Sep. 2026	Présentiel -
09 au 13 Nov. 2026	Présentiel -

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com