Administration et Sécurisation des Pare-feux FortiGate

Lien : https://innov-systems.com/formation/administration-et-securisation-des-pare-feux-fortigate

DURÉE	RÉFÉRENCE	CATÉGORIE
5 jours (35h)	**SEC273**	**Fortinet**

OBJECTIFS DE LA FORMATION

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

- Maîtriser les principes fondamentaux et avancés de la configuration des pare-feux FortiGate
- Savoir concevoir, déployer et administrer une infrastructure Fortinet sécurisée
- Comprendre et mettre en œuvre les mécanismes de routage, d'authentification et de VPN
- Déployer des politiques de sécurité adaptées aux environnements hybrides et multi-sites
- Diagnostiquer et résoudre efficacement les incidents de sécurité et de connectivité
- Optimiser la performance et la résilience de l'infrastructure via le SD-WAN, la haute disponibilité et la Security Fabric

POUR QUI ?

- Administrateurs réseau et sécurité responsables du déploiement et de la maintenance des pare-feux FortiGate
- Ingénieurs systèmes en charge de la sécurisation des infrastructures IT
- Responsables techniques d'équipes infrastructure ou sécurité souhaitant approfondir leur expertise sur FortiGate

Innov Systems

Programme détaillé

1 / INTRODUCTION À L'ARCHITECTURE FORTIGATE

- Présentation de l'écosystème Fortinet et des versions FortiOS
- Architecture matérielle et logicielle du pare-feu FortiGate
- Modes de déploiement : NAT/Route, Transparent, et Virtual Wire Pair

2 / CONFIGURATION DE BASE ET ACCÈS ADMINISTRATIF

- Initialisation à partir des paramètres d'usine
- Configuration réseau et interfaces système
- Sécurisation de l'accès administrateur (GUI, CLI, HTTPS, SSH)
- Gestion des comptes, des profils et des permissions administratives

3 / EXPLORATION DE L'INTERFACE ET DES OUTILS D'ADMINISTRATION

- Utilisation de la console CLI et de la Web GUI
- Introduction au FortiCloud et au FortiAnalyzer pour le monitoring
- Sauvegarde et restauration de la configuration

4 / POLITIQUES DE PARE-FEU ET CONTRÔLE D'ACCÈS

- Création et gestion des politiques de sécurité
- Filtrage du trafic entrant et sortant
- Gestion des objets réseau (adresses, groupes, services)

5 / NAT ET TRADUCTIONS D'ADRESSES

- Configuration du NAT source et destination
- Transfert de port et redirection de service
- Étude des cas d'usage en environnement multi-zone

Innov Systems

6 / ROUTAGE ET CONNECTIVITÉ RÉSEAU

- Routage statique et dynamique (OSPF, BGP)
- Routage basé sur les règles et équilibrage de charge
- Analyse et diagnostic de la table de routage

7 / AUTHENTIFICATION DES UTILISATEURS

- Authentification locale et distante (RADIUS, LDAP)
- Intégration Fortinet Single Sign-On (FSSO) avec Active Directory
- Gestion des politiques basées sur les identités

8 / GESTION DES CERTIFICATS ET CHIFFREMENT

- Fonctionnement du chiffrement SSL/TLS
- Création et déploiement de certificats internes et externes
- Inspection SSL pour la détection des menaces chiffrées

9 / PROTECTIONS AVANCÉES ET FILTRAGE CONTENU

- Mise en place des profils de sécurité (AV, IPS, Web Filter, Application Control)
- Blocage des contenus malveillants et des sites inappropriés
- Analyse comportementale et détection d’anomalies réseau

10 / CONFIGURATION DES VPN SSL ET IPSEC

- Création d’un accès distant via SSL VPN
- Mise en place de tunnels IPsec site-à-site
- Surveillance et dépannage des connexions VPN

11 / CONFIGURATION DU SD-WAN ET OPTIMISATION DU TRAFIC

- Principes du SD-WAN et scénarios d’usage

Innov Systems

- Politique de répartition du trafic et priorisation applicative
- Surveillance des performances et SLA

12 / MISE EN ŒUVRE DE LA SECURITY FABRIC

- Concept et architecture de la Fortinet Security Fabric
- Intégration de FortiAnalyzer, FortiManager et FortiSwitch
- Visibilité, automatisation et réponse aux incidents

13 / HAUTE DISPONIBILITÉ ET RÉSILIENCE

- Mise en cluster HA actif-actif et actif-passif
- Synchronisation et basculement automatique
- Bonnes pratiques pour la continuité de service

14 / SUPERVISION ET DIAGNOSTIC

- Analyse des logs, sessions et événements système
- Outils de dépannage CLI et GUI (ping, sniffer, diagnose)
- Analyse des performances et détection d’incidents réseau

15 / ÉTUDES DE CAS ET BONNES PRATIQUES D’ADMINISTRATION

- Scénarios pratiques de déploiement et de sécurisation
- Méthodologie de gestion du changement et sauvegarde
- Bonnes pratiques d’audit et de maintenance proactive

Inov Systems

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

12 au 18 Jan. 2027	Présentiel - Casablanca
08 au 12 Mars 2027	Présentiel - Casablanca
03 au 07 Mai 2027	Présentiel - Casablanca
28 Juin au 02 Juil. 2027	Présentiel - Casablanca
23 au 27 Août 2027	Présentiel - Casablanca

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

Innov Systems — Tous droits réservés