Fortinet NSE 4 - FortiGate Security et Infrastructure

Lien : https://innov-systems.com/formation/fortinet-nse-4-fortigate-security-et-infrastructure

DURÉE
5 jours (35h)

RÉFÉRENCE
SEC221

CATÉGORIE
Fortinet

OBJECTIFS DE LA FORMATION

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

- Assurer les opérations quotidiennes de configuration, surveillance et gestion d'appareils FortiGate
- Acquérir l'ensemble des techniques et des méthodologies nécessaires au passage de l'examen Fortinet NSE4

POUR QUI ?

- Administrateurs
- Ingénieurs
- Responsable sécurité

Innov Systems

Programme détaillé

1 / Introduction sur FortiGate et les UTM

- Fonctionnalités haut niveau
- Considérations pour l’installation et la configuration
- Les interfaces GUI et CLI
- Administration de l'équipement, compte et authentification
- Fichier de configuration et mise à niveau du firmware
- Serveurs DHCP et DNS
- L'antivirus : filtre antiviral de flux web et de messagerie
- Le filtrage web
- L'IPS Applicatives. Le contrôle applicatif
- La protection DoS (le Déni de Service)
- FortiGate dans le Security Fabric

2 / Règles firewall

- Vue d’ensemble des règles de sécurité
- Configurer et maintenir les règles de pare-feu
- Contrôle des postes de travail
- Journal et analyse
- Meilleures pratiques pour la résolution de problèmes

3 / NAT, la translation d'adresses IP

- Introduction au NAT
- Politique de pare-feu NAT
- La fonctionnalité Central NAT
- Sessions Helpers et sessions
- Meilleures pratiques et dépannage

Innov Systems

4 / Les règles de firewall avec authentification des utilisateurs

- Les différentes méthodes d’authentification
- Serveurs d’authentification à distance
- Groupes d’utilisateurs
- Utilisation des règles de pare-feu pour l'authentification
- L’authentification via les Captive Portals
- Surveillance et dépannage

5 / Gestion des logs et supervision

- Principes et structure des logs
- Connexion locale et à distance
- Gestion des paramètres de logs
- Afficher, rechercher et surveiller les logs
- Protéger les données du log

6 / Certificats et cryptographie

- Authentifier et sécuriser les données à l'aide de certificats
- Inspecter les données chiffrées
- Les certificats digitaux
- Inspection du contenu SSL

7 / Le filtrage d’URL

- Modes d’inspection
- Principes de base du filtrage Web
- Fonctionnalités additionnelles (proxy)
- Filtrage DNS
- Meilleures pratiques et dépannage

8 / Le contrôle applicatif

Inov Systems

- Principes de base du contrôle des applications
- Configuration du contrôle applicatif
- Journalisation et surveillance des événements de contrôle des applications
- Meilleures pratiques et dépannage

9 / Le contrôle d'intrusion et le Déni de Service (DoS)

- Système de prévention des intrusions
- Déni de service
- Pare-feu d’application web
- Les bonnes pratiques à connaître
- Les meilleures pratiques
- Dépannage

10 / Le VPN SSL

- Topologies VPN
- Comprendre le VPN SSL FortiGate
- Modes de déploiement SSL-VPN
- Configuration des VPN SSL
- Hardening SSL-VPN Access
- Renforcement de l'accès SSL-VPN
- Surveillance et dépannage

11 / Le VPN IPSEC

- Introduction à IPsec
- Configuration du VPN IPSec
- Paramètres Phase 1 et Phase 2
- VPN IPsec commuté
- Surveillance du VPN IPSec
- VPN Dialup, redondants

Innov Systems

- Meilleures pratiques

12 / Data Leak Prevention (DLP)

- Présentation de DLP
- Filtres DLP
- Empreintes digitales DLP
- Archivage DLP
- Les meilleures pratiques

1 / Le routage

- Le routage sur FortiGate
- Surveiller le routage, attributs de route
- Le protocole de routage ECMP (Equal-Cost Multi-Path)
- La technique du Reverse Path Forwarding (RPF)
- Effectuer des diagnostics

2 / Le SD-WAN (Software-Defined Wide Area Network)

- Introduction au SD-WAN
- Considérations pour la performance et SLA
- Règles SD-WAN
- Diagnostics SD-WAN

3 / La virtualisation

- Concepts VDOM
- Administrateurs VDOM
- Configuration des VDOM
- Liens entre domaines virtuels

4 / Analyse L2

Innov Systems

- Réseaux locaux virtuels (VLAN)
- Le mode transparent
- Utiliser un virtual wire pair
- Commutateur logiciel
- Transfert STP (Spanning Tree Protocol)

5 / Le VPN IPSec en mode site à site

- Les différentes topologies VPN
- Configuration d’un VPN site à site

6 / Le FSSO (Fortinet Single Sign-On)

- Intérêt et déploiement
- FSSO avec Active Directory
- Authentification NTLM
- Paramètres FSSO
- Dépannage

7 / Haute disponibilité

- Les différents modes d’Haute Disponibilité (HA)
- La synchronisation entre les équipements
- Les options de Clustering
- Surveillance et dépannage

8 / Proxy Web

- Concepts de proxy Web
- Configuration du proxy explicite
- Authentification et autorisation du proxy Web

Innov Systems

9 / Diagnostics

- Diagnostic général
- Flux de debug
- Mémoire et CPU
- Les outils de diagnostic

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

25 au 29 Jan. 2027	Présentiel - Casablanca
22 au 26 Mars 2027	Présentiel - Casablanca
17 au 21 Mai 2027	Présentiel - Casablanca
12 au 16 Juil. 2027	Présentiel - Casablanca
06 au 10 Sep. 2027	Présentiel - Casablanca

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

Innov Systems

Réservation & Renseignements

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

Innov Systems — Tous droits réservés