Formation **Fortigate Administrator, préparation à l'examen Fortinet FCP (NSE4)**

Découvrez notre formation sur FortiGate, conçue pour vous enseigner l'utilisation des fonctionnalités les plus répandues, notamment les profils de sécurité. À travers des ateliers pratiques, vous apprendrez à gérer les politiques de pare-feu, l'authentification des utilisateurs, le VPN SSL, le VPN IPsec de site à site, ainsi que la Security Fabric de Fortinet. Vous verrez également comment renforcer la sécurité de votre réseau avec des profils de sécurité comme l'IPS, l'antivirus, le filtrage Web, et le contrôle des applications. Cette formation vous offrira une compréhension approfondie des principales fonctionnalités de FortiGate, essentielles pour une administration efficace. A l'issue de la formation, les participants seront en mesure de passer l'examen Fortinet FCP - FortiGate 7.4 Administrator (NSE4). Le passage de l'examen n'est pas obligatoire et n'est pas inclus dans le coût de la formation.

Durée
4 jours

Objectifs pédagogiques

- Configurer et administrer l'infrastructure initiale
- Gérer les accès et les stratégies de pare-feu
- Analyser et gérer le routage et le trafic
- Appliquer le NAT et le transfert de port
- Comprendre et utiliser les fonctions de sécurité et de cryptage
- Configurer les profils de sécurité et le contrôle des applications

Public
Administrateurs systèmes et réseaux,
Responsables de la sécurité des systèmes d'information (RSSI),
Ingénieurs télécoms et réseaux

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

Programme de formation

Phase d'inclusion

Accueil des participants, présentation des objectifs et contextes professionnels de chacun.

Chapitres du cours FortiGate Administrator

1. System and Network Settings
2. Firewall Policies and Network Address Translation
3. Routing
4. Firewall Authentication
5. Fortinet Single Sign-On (FSSO)
6. Certificate Operations
7. Antivirus
8. Web Filtering
9. Intrusion Prevention and Application Control
10. SSL VPN
11. IPSec VPN
12. SD-WAN Configuration and Monitoring
13. Security Fabric
14. High Availability
15. Diagnostics and Troubleshooting

Moyens et méthodes pédagogiques

- La formation alterne entre présentations des concepts théoriques et mises en application à travers d'ateliers et exercices pratiques (hors formation de type séminaire).
- Les participants bénéficient des retours d'expérience terrains du formateur ou de la formatrice
- Un support de cours numérique est fourni aux stagiaires

Modalités d'évaluation

- **En amont de la session de formation**, un questionnaire d'auto-positionnement est remis aux participants, afin qu'ils situent leurs connaissances et compétences déjà acquises par rapport au thème de la formation.

- **En cours de formation**, l'évaluation se fait sous forme d'ateliers, exercices et travaux pratiques de validation, de retour d'observation et/ou de partage d'expérience, en cohérence avec les objectifs pédagogiques visés.

- **En fin de session**, le formateur évalue les compétences et connaissances acquises par les apprenants grâce à un questionnaire reprenant les mêmes éléments que l'auto-positionnement, permettant ainsi une analyse détaillée de leur progression.