EduGroupe
Accompagner pour réussir

FORTINET NSE4 – Fortigate security & infrastructure

Référence : **SEC-FOR3** Durée : **5 jours (35 heures)** Certification : **NSE4**

Connaissances préalables

- 1-Avoir des notions de TCP/IP
- 2-Avoir des connaissances des concepts firewall

Profil des stagiaires

- Toute personne qui doit administrer régulièrement un firewall Fortigate

Objectifs

- Neutraliser les menaces véhiculées au travers des malwares, les applications nocives et limiter les accès aux sites inappropriés
- Contrôler les accès au réseau selon les types de périphériques utilisés
- Déployer un tunnel IPSEC entre deux boîtiers Fortigate
- Interpréter les logs et Générer des rapports
- Déployer un cluster de Fortigate
- Inspecter le trafic réseau en mode transparent
- Troubleshooter et diagnostiquer
- Mettre en œuvre des politiques antiDoS
- Réussir la Certification FortiOS NSE4 de Fortinet

Certification préparée

Certification FortiOS NSE4 de Fortinet

Méthodes pédagogiques

- Mise à disposition d'un poste de travail par participant
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques et de réflexions

Formateur·rice

- Consultant-Formateur expert Fortinet

Méthodes d'évaluation des acquis

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

Contenu du cours

1. Partie 1 : FortiGate Notions de bases (2 jours)

-

2. Gestion des logs et supervisions UTMs

-

3. Les règles firewall

-

4. Les règles firewall avec authentification des utilisateurs : Authentifier les utilisateurs au travers des règles firewalls

-

5. Le VPN SSL : Mettre en œuvre un VPN SSL pour l'accès des utilisateurs nomades au réseau de l'entreprise

-

6. Introduction au VPN IPSEC

-

7. L'antivirus

-

8. Le proxy explicit

-

9. Le filtrage d'URL : Mettre en œuvre le proxy explicit, le cache et l'authentification des utilisateurs

-

10. Le contrôle applicatif : Maîtriser l'utilisation des applications au sein de votre réseau

-

11. Partie 2 : Notions Avancées (3 jours)

-

12. Le routage : Analyser la table de routage d'un Fortigate

-

13. La virtualisation

-

14. Le mode transparent

-

15. La haute disponibilité : Réaliser du load balancing de trafic sur plusieurs opérateurs

-

16. Le VPN IPSec avancé : Implémenter une architecture de VPN IPSec redondée

-

17. L'IPS

-

18. Le FSSO : Mettre en œuvre le FSSO

-

19. Les certificats, la cryptographie : Déchiffrer les flux chiffrés

-

20. Le DLP : Déployer des profils de DLP

-

21. Les diagnostics

-

22. L’accélération matérielle : Comprendre le fonctionnement de l’accélération matérielle

-

23. IPV6

-

24. Certification FortiOS NSE4 de Fortinet

- Cette formation prépare au passage de la certification FortiOS NSE4 de Fortinet

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d’aménagements, afin de vous offrir la meilleure expérience possible.