Organisme de formation professionnelle continue
Numero agrément 91 30 03332 30
France : +33 (0)188 24 70 33 / 34
Site : www.oo2.fr
Mail : contact@oo2.fr

Fortinet ® NSE 4 - FortiGate Security et FortiGate Infrastructure

Date et durée

Code formation : NSE4FR
Durée : 5 jours
Nombre d'heures : 35 heures

Formation avec préparation à la certification

Fortinet Certified Professional

Description

Avec des menaces informatiques de plus en plus sophistiquées et soutenues, les entreprises doivent **intégrer des outils de sécurité** complexes à déployer, à administrer et à maintenir. Fortinet®, l'un des leaders en matière de solutions de sécurité informatique propose un **pare-feu nouvelle génération, FortiGate®**. Il s'intègre au sein d'un seul et même système d'exploitation, le FortiOS®. C'est donc un ensemble de services qui permet d'avoir une gestion unifiée des menaces (UTM).
Notre **formation Fortinet Fortigate NSE4** qui dure 5 jours se compose en 2 parties. La première partie est consacrée à la sécurité. Elle vous permettra au cours des 2 premiers jours de prendre en main les principales fonctions de l'UTM de FortiGate®. Vous apprendrez à configurer le pare-feu, à configurer le service VPN avec les protocoles IPSEC, SSL et pour finir, à **lutter contre les malwares** et créer des filtres d'URL. Dans la seconde partie dédiée à l'infrastructure qui dure 3 jours, vous apprendrez à configurer le FortiGate® dans ses fonctions avancées (virtualisation, IPS, FSSO, DLP, etc.).
Cette formation vous permettra également de **vous préparer à l'examen Fortinet NSE 4 - FortiOS 7.0**. Une fois que vous aurez atteint tout les objectifs de cette formation FortiOS, vous pourrez passer l'examen officiel dans notre centre PearsonVue Oo2. Il vous permettra d'obtenir par la suite la certification NSE 4 Network Security Professional.
En savoir + sur l'examen Fortinet NSE4 7.0

Objectifs

À l'issue de la **formation Fortinet NSE 4**, vous validerez les objectifs de compétences suivants :

- administrer Fortigate® en mode graphique GUI ou par ligne de commande CLI (génération de rapports, gestion des logs et diagnostics, analyse des tables de routage, inspection du trafic, déchiffrage de flux chiffré) ;
- neutraliser les différentes menaces issues de malwares ;
- mettre en place différents VPN de type SSL ou IPSEC ;
- authentifier les utilisateurs ;
- gérer l'antivirus ;
- configurer le proxy explicit ;
- déployer un cluster, faire du load balancing et comprendre l'accélération matérielle pour la haute disponibilité ;
- mettre en œuvre les Virtual Domain, les politiques antiDoS et le FSSO ;
- gérer le NAT et le routage ;
- implémenter l'IPv6 et le dual stack IPv4/IPv6 ;

- utiliser les Policy Based Routing(PBR) ;
- déployer des profils data leak prevention (DLP) ;
- être préparé pour le passage de l'examen FortiOS 7.0 Fortinet NSE4.

Points forts

Un formateur certifié NSE 4 - FortiGate Network Security Professional et des travaux pratiques via FortiOS® 6.x et FortiOS® 7.x basés sur des études de cas.

Certification

Cette formation vous permet une préparation à l'examen officiel **Fortinet NSE 4 : FortiOS 7.0** (*FortiGate Security and FortiGate Infrastructure*). Celui-ci peut-être passé dans notre centre PearsonVue.
Il s'agit d'un QCM d'une durée d'1 h 45 heure (105 minutes) composé de 60 questions **en anglais**. La certification NSE 4 est valable 2 ans.

Modalités d'évaluation

Travaux Pratiques
Etude de cas

Pré-requis

Suivre la **formation Fortinet NSE 4**, nécessite les prérequis suivants :

- une parfaite compréhension des couches du modèle OSI ;
- une connaissance de base des protocoles Internet TCP/IP ;
- une connaissance des concepts d'un firewall d'entreprise.

Public

Cette formation s'adresse aux publics suivants :

- tout professionnel de l'informatique qui doit administrer un firewall FortiGate® ou qui souhaite le découvrir ;
- tout professionnel de la sécurité informatique qui désire passer la certification NSE 4 - FortiGate Network Security Professional.

Cette formation s'adresse aux profils suivants

Administrateur système
Administrateur réseaux - télécoms
Ingénieur système

Programme

Tour de table

- Introduction individuelle
- Exploration des attentes et des objectifs de chaque participant
- Introduction au cadre de la formation
- Alignement avec les objectifs et enjeux spécifiques
- Identification des attentes et des perspectives individuelles des participants

---

Partie 1 : Sécurité de Fortigate® (2 jours)

- Compréhension de Fortigate et de l'UTM.
- Gestion des logs et la supervision des équipements.
- Gestion des règles du firewall sans l'authentification des utilisateurs.
- Mise en œuvre d'un VPN SSL pour permettre l’accès distant au réseau de l’entreprise.
- Mise en œuvre d'un VPN IPSec.
- Gestion et le paramétrage de l’antivirus.
- Gestion de l’authentification des utilisateurs.
- Mise en œuvre d'un proxy explicit et la mise en cache.
- Gestion du contrôle applicatif.

Partie 2 : Infrastructure Fortigate® (3 jours)

- Analyse de la table de routage de Fortigate®.
- Mise en œuvre de la virtualisation.
- Mode transparent.
- Load balancing de trafic sur plusieurs opérateurs (haute disponibilité).
- Configuration avancée d’un VPN IPSec.
- Mise en œuvre de l’Intrusion Prevention Systems (IPS).
- Configuration du Single-Sign-On (FSSO).
- Déchiffrage des flux chiffrés.
- Déploiement des profils data leak prevention (DLP).
- Gestion des diagnostics.
- Fonctionnement de l’accélération matérielle.
- Paramétrage de l'IPv6.

Fortinet®, FortiGate® et FortiOS® sont des marques déposée de la société Fortinet, Inc.