FortiGate administrator : configurer, gérer et sécuriser FortiGate (NSE4)

Date et durée

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

Description

Formation avec certification FCP in Network Security (anciennement NSE 4)
La configuration et la gestion efficace des équipements de sécurité sont primordiales pour **protéger les données et assurer la continuité des activités**. Des systèmes de sécurité mal configurés peuvent entraîner des vulnérabilités critiques et des pertes de données importantes. C'est là qu'intervient **l'administrateur FortiGate certifié *Network Security*** , un professionnel garantissant la sécurité et le fonctionnement optimal de l'infrastructure réseau.
Notre formation vous prépare à devenir un professionnel certifié Fortinet. Vous développerez une expertise solide dans **la configuration, la gestion, la surveillance et le dépannage des solutions de sécurité FortiGate**, en vous basant sur les meilleures pratiques. Vous serez capable de mettre en œuvre des politiques de sécurité robustes, de gérer l'accès des utilisateurs, de configurer des VPN sécurisés et d'utiliser les fonctionnalités avancées de FortiGate pour protéger efficacement les réseaux. Ce programme est conçu pour les professionnels souhaitant **acquérir les compétences fondamentales et avancées pour administrer les firewalls FortiGate** et obtenir une certification reconnue dans le domaine de la sécurité réseau.
À l'issue de ce programme de 5 jours, vous maîtriserez les compétences clés pour **réussir l'examen FCP - FortiGate 7.6 Administrator** (*en savoir plus dans l'onglet certification*). Vous bénéficierez d'une préparation complète, incluant des exercices pratiques intensifs et une compréhension approfondie des sujets d'examen pour vous assurer une réussite optimale.

Objectifs

*À l'issue de la **formation FortiGate administrateur**, vous atteindrez les objectifs suivants :*

- acquérir une compréhension solide dans l'utilisation des fonctionnalités les plus courantes de FortiGate ;
- mettre en œuvre et gérer efficacement les politiques de pare-feu pour contrôler le trafic réseau ;
- comprendre et configurer les méthodes d'authentification des utilisateurs pour un accès sécurisé au réseau ;
- déployer des clusters FortiGate en haute disponibilité pour assurer la tolérance aux pannes et la performance ;
- configurer des VPN SSL et IPsec site à site pour établir des connexions d'accès distant sécurisées ;
- utiliser efficacement le Fortinet Security Fabric pour mettre en place une architecture de sécurité intégrée ;
- configurer et utiliser les profils de sécurité, tels que l'IPS, l'antivirus, le filtrage web et le contrôle d'application ;
- diagnostiquer et résoudre les problèmes courants avec FortiGate ;
- se préparer à l'examen FCP - FortiGate 7.6 Administrator.

Points forts

- **Formateur expert Fortinet certifié :** bénéficiez de l'expertise d'un formateur reconnu et certifié par Fortinet dans le domaine de la sécurité réseau. Vous aurez la garantie d'une connaissance approfondie des solutions FortiGate et d'une préparation optimale à la certification FCP.
- **Exercices pratiques et études de cas concrets :** maîtrisez les techniques et outils d'administration FortiGate à travers des exercices pratiques et des études de cas réels. Vous serez préparé aux défis concrets de la gestion de la sécurité réseau avec FortiGate.
- **Acquisition des compétences clés pour la certification FCP :** le contenu de la formation est rigoureusement aligné sur les objectifs de l'examen FCP - FortiGate 7.6 Administrator. Vous développerez les compétences essentielles pour réussir la certification.
- **Préparation ciblée à l'examen avec simulations :** bénéficiez d'une préparation complète à l'examen FCP, incluant des QCM et des exercices pratiques fidèles au format et aux exigences de l'examen. Vous vous familiariserez avec le déroulement et le type de questions.

Certification

Cette formation vous prépare de manière intensive à l'examen de certification professionnelle Fortinet Certified Professional (FCP) en Network Security, en se concentrant sur l'examen FCP - FortiGate 7.6 Administrator. Un code coupon vous sera fourni à la fin du cours pour que vous puissiez programmer votre examen .

Modalités de l'examen FCP - FortiGate 7.6 Administrator :

- **Type d’examen :** QCM (Questions à Choix Multiples)
- **Nombre de questions :** 50
- **Durée :** 90 minutes
- **Lieu :** Centre de test Pearson VUE et via la plateforme OnVUE (en ligne).
- **Langue :** Anglais
- **Note de passage :** 100%.

Si vous réussissez l'examen, vous obtiendrez la certification FCP Network Security et recevrez un badge numérique.
À savoir : *la certification Fortigate Network Security a une durée de validité de 2 ans et nécessite un renouvellement.*

Modalités d'évaluation

Travaux Pratiques
Etude de cas

Pré-requis

Suivre cette formation Fortigate nécessite les prérequis suivants :

- **Maîtriser les fondamentaux des protocoles réseau :** vous devez avoir une solide compréhension des protocoles réseau essentiels, tels que TCP/IP, UDP, DNS, DHCP, HTTP/HTTPS, et être capable de comprendre comment ils interagissent dans un environnement réseau.
- **Posséder une compréhension de base des concepts de pare-feu :** vous devez être familier avec les concepts fondamentaux des pare-feu, notamment les principes de filtrage de trafic, les règles de pare-feu, les zones de sécurité, et la manière dont les pare-feu protègent les réseaux.
- **Savoir lire et comprendre l'anglais** pour accéder au support de cours officiel et passer l'examen.

Public

Cette formation s'adresse aux publics suivants :

- Les professionnelles des réseaux et de la sécurité informatique qui s’occupent de la gestion, de la configuration, de l’administration et de la supervision des équipements FortiGate, tels que :
    - Administrateurs de sécurité réseau ;
    - Ingénieurs réseaux ;
    - Ingénieurs en sécurité ;
    - Techniciens réseaux et sécurité ;
    - Spécialistes en cybersécurité.

Programme

Jour 1 : découvrir et configurer les fonctionnalités de base de FortiGate

Introduction à FortiGate et au Fortinet Security Fabric

- Présentation de Fortinet et de la gamme FortiGate.
- L'architecture de FortiGate et ses concepts clés.
- Les composants et les avantages de Fortinet Security Fabric.
- Les bases pour accéder et naviguer dans l'interface graphique (GUI) et utiliser la ligne de commande (CLI).
- La configuration initiale du système (réseau, DNS, NTP, etc.).

Gestion des objets et des politiques de Pare-feu

- La création et la gestion des objets (adresses, services, groupes et interfaces).
- Les principes fondamentaux des politiques de pare-feu.
- La configuration et la mise en œuvre de politiques de pare-feu de base.
- La gestion de l'ordre des politiques et des règles implicites.

Travaux pratiques :

- Création et test de politiques de pare-feu simples.

Jour 2 : authentifier les utilisateurs et diriger le trafic

Authentification des utilisateurs

- Les concepts d'authentification locale et distante.
- La configuration de l'authentification locale des utilisateurs et des groupes.
- L'intégration avec des serveurs d'authentification externes (LDAP, RADIUS).
- L'utilisation de Single Sign-On (SSO) avec FortiGate.

Travaux pratiques :

- Configuration de l'authentification locale et RADIUS.

Concepts de routage et routage statique

- Les principes de base du routage IP.
- La configuration du routage statique.
- La compréhension et la configuration des routes par défaut.

Travaux pratiques :

- Configuration de routes statiques pour différents scénarios.

Jour 3 : assurer la haute disponibilité et sécuriser l'accès distant avec SSL VPN

Mise en œuvre de la Haute Disponibilité (HA)

- Les concepts de la haute disponibilité et ses avantages.
- Les modes de HA FortiGate : Active-Passive et Active-Active.
- La configuration et la gestion d'un cluster HA Active-Passive.
- La surveillance et le dépannage des clusters HA.

Travaux pratiques :

- Déploiement et test d'un cluster HA Active-Passive.

Configuration des VPN SSL

- Introduction aux VPN SSL et à leurs cas d'utilisation.
- La configuration du mode Portail et du mode Tunnel.
- L'authentification des utilisateurs pour les VPN SSL.
- La personnalisation du portail VPN SSL.

Travaux pratiques :

- Configuration de VPN SSL en mode Portail et Tunnel.

Jour 4 : établir des VPN IPsec Site à Site et appliquer les profils de sécurité

Configuration des VPN IPsec Site à Site

- Introduction aux VPN IPsec et à leurs cas d'utilisation.
- Les concepts clés de la configuration IPsec (phases, propositions et clés).
- La configuration de VPN IPsec site à site basé sur des politiques.
- Le dépannage des connexions VPN IPsec.

Travaux pratiques :

- Configuration de VPN IPsec site à site entre deux FortiGate.

Introduction et configuration des profils de sécurité

- Présentation des profils de sécurité (IPS, antivirus, filtrage web et contrôle d'application).
- La configuration et l'application des profils de sécurité dans les politiques de pare-feu.
- Les options de configuration et les actions disponibles dans chaque profil.

Travaux pratiques :

- Application de profils de sécurité pour bloquer des menaces et contrôler l'accès.

Jour 5 : optimiser la sécurité, diagnostiquer et préparer la certification

Configuration avancée des profils de sécurité et des logs

- L'exploration des options avancées des profils de sécurité.
- L'utilisation des signatures et des filtres personnalisés.
- La configuration et la gestion des logs (locaux et distants avec FortiAnalyzer.
- L'analyse des logs pour le dépannage et la sécurité.

Travaux pratiques :

- Configuration avancée des profils et analyse des logs.

Diagnostic

- Les outils de diagnostic et de dépannage courants sur FortiGate (CLI).
- L'identification et la résolution des problèmes de connectivité, de pare-feu et de VPN.
- Les concepts clés et les meilleures pratiques.

Préparation à la certification FCP Network Security

- Conseils et ressources pour la préparation à l'examen FCP - FortiGate 7.6 Administrator.
- Questions/Réponses et discussion.

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