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

Fortinet – FortiGate III NSE 7 (Préparation à la certification NSE 7)

Date et durée

Code formation : NSE7FR
Durée : 3 jours
Nombre d'heures : 21 heures

Formation avec préparation à la certification

Fortinet Certified Solution Specialist

Description

FortiGate regroupe l'ensemble des services de sécurité de pointe mis au point par Fortinet. Le développement des technologies informatiques au sein des entreprises implique de maîtriser la sécurité des données pour éviter tout risque nuisible. Cette formation vous apprendra à déployer et administrer efficacement les programmes FortiGate. Elle vous préparera au cursus de **certification NSE7**

Objectifs

Cette formation a pour objectif **de vous enseigner l'architecture et le fonctionnement complet de FortiGate III et du pare-feu d'entreprise**. Vous apprendrez à utiliser l'administration centralisée de FortiGate pour gérer efficacement les différents programmes Fortinet et mettre en place une sécurité optimale de vos réseaux en entreprise. Ce cours se concentre sur l'implémentation, le diagnostic et la gestion centrale des services FortiGates. Il combine à la fois des modules théoriques et des exercices pratiques pour tester vos compétences en situation concrète de risque informatique. Cette formation fait partie du cursus de **certification NSE 7**.
A l'issue de cette formation, vous saurez :

- Exploiter tous les composants de la Security Fabric de Fortinet : FortiManager, FortiAnalyzer et les FortiGates.
- Opérer une administration centrale de l'analyse et du traitement de la sécurité de réseau.
- Optimiser l'utilisation des ressources FortiGates.
- Utiliser les outils de FortiGate pour dépanner et surveiller le trafic utilisateur.
- Utiliser la forte utilisation CPU, les règles de firewall, les sessions Helpers, l'IPsec, FortiGuard, l'inspection du contenu, le routage et la haute disponibilité pour examiner et résoudre les problèmes.
- Déployer des tunnels IPsec en simultané sur des sites multiples avec la console VPN de FortiManager.
- Activer les tunnels à la demande entre différents sites grâce à l'ADVPN.
- Router le trafic d'entreprise avec l'Open Shortest Path First et le Border Gateway Protocol.

Pré-requis

La participation à cette formation nécessite de maîtriser au préalable FortiGate I et II, FortiAnalyzer et FortiManager.

Public

Cette formation s’adresse aux professionnels IT impliqués dans la sécurité de réseau et l’administration des FortiGates en entreprise.

Cette formation s'adresse aux profils suivants

Administrateur système
Directeur des Systèmes d'Information (DSI)
Ingénieur système

Programme

Module 1 : Vue d’ensemble du pare-feu d’entreprise
Module 2 : Architecture et fonctionnement de FortiOS
Module 3 : Dépanner le système
Module 4 : Surveiller le trafic et les sessions
Module 5 : Le routage
Module 6 : FortiGuard
Module 7 : Administration centralisée
Module 8 : Le protocole Open Shortest Path First (OSPF)
Module 9 : Filtrage Web
Module 10 : Système de prévention d’intrusion (IPS)
Module 11 : Border Gateway Protocol (BGP)
Module 12 : Internet Protocol Security (IPSEC)
Module 13 : Auto-Discovery VPN (ADVPN)