Programme de formation

FortiGate Security et FortiGate Infrastructure, préparation à la certification Fortinet NSE4

Objectifs

Cette formation permet d'acquérir les connaissances pour assurer les opérations quotidiennes de configuration, surveillance et gestion d'appareils FortiGate. A l'issue des 5 jours de formation, les participants seront en mesure de soutenir les politiques de sécurité de leur organisation, grâce à la maîtrise de l'ensemble des bonnes pratiques Fortinet. Chaque module de formation est ponctué par une série d'exercices pratiques, pour une mise en application immédiate des principes théoriques. A noter que cette formation est la nouvelle version groupée des cours FortiGate 1 et FortiGate 2. A l'issue de la formation, les participants seront en mesure de passer la certification NSE4 Network Security Professional (le passage de l'examen n'est pas obligatoire et n'est pas inclus dans la formation).

Pré requis

Notions sur le protocole TCP/IP, familiarité avec les concepts firewall et connaissance des couches du modèle OSI.

Durée

5 jours

Public

Administrateurs, Ingenieurs, Responsable-securite

Plan de formation

Introduction à la formation Fortinet NSE4
Présentation générale et objectifs de cette formation Network Security Expert 4

PREMIERE PARTIE : FortiGate Security (3 jours)

FortiGate et les UTM
Fonctionnalités haut niveau
Considérations pour l'installation et la configuration
Les interfaces GUI et CLI
Tâches d'administration de base
Serveurs intégrés
Maintenance
La Security Fabric

Règles firewall
Vue d'ensemble des règles de sécurité
Configurer et maintenir les règles
Les bonnes pratiques pour la résolution de problèmes

Le NAT (Network Address Translation)
Introduction à la traduction d'adresse réseau
La fonctionnalité Central NAT
Sessions Helpers et sessions

Règles firewall avec authentification des utilisateurs
Les différentes méthodes d'authentification
Serveurs d'authentification à distance
Groupes d'utilisateurs
Utiliser les règles firewall pour l'authentification des utilisateurs
L'authentification via les Captive Portals
Surveillance et dépannage

Logs et supervision
Principes et structure des logs
Connexion locale et à distance
Gestion des paramètres de logs
Visualiser, rechercher et surveiller les logs
Stocker et protéger les données de

journalisation

Certificats
Utiliser les certificats pour authentifier et sécuriser des données
Inspecter les données cryptées
Gérer les certificats digitaux dans FortiGate

Filtrage d'URL
Modes d'inspection
Principes fondamentaux du filtrage web
Fonctionnalités additionnelles (proxy)
Filtrage DNS

Contrôle applicatif
Principes de base
Configuration du contrôle applicatif
Surveiller les événements Application Control

Contrôle d'intrusion et protection DoS (déni de service)
Le système de prévention des intrusions
Denial of Service
Firewall d'application web
Les bonnes pratiques à connaître

VPN SSL et VPN IPSEC
Comprendre le VPN SSL FortiGate
Les modes de déploiement
Configurer le VPN SSL, options et sécurité
Retour sur IPsec
Paramètres Phase 1 et Phase 2
Le mode dial-up

Data Leak Prevention (DLP)
Vue d'ensemble
Flitres
Empreintes
Archives

DEUXIEME PARTIE : FortiGate Infrastructure (2 jours)

Routage
Le routage sur FortiGate
Surveiller le routage, attributs de route
Le protocole de routage ECMP (Equal-Cost Multi-Path)
La technique du Reverse Path Forwarding (RPF)
Effectuer des diagnostics

Le SD-WAN (Software-Defined Wide Area Network)
Introduction au SD-WAN
Considérations pour la performance et SLA
Règles SD-WAN

Domaines virtuels (VDOM)
Concepts de virtualisation et bénéfices des domaines virtuels
Administrateurs VDOM
Configuration
Liens entre domaines virtuels

Analyse L2
Réseaux locaux virtuels (VLAN)
Le mode transparent
Utiliser un virtual wire pair
Commutateur logiciel
Transfert STP (Spanning Tree Protocol)

Le VPN IPSec en mode site à site
Les différentes topologies VPN
Configuration d'un VPN site à site

Le FSSO (Fortinet Single Sign-On)
Intérêt et déploiement
FSSO avec Active Directory
Authentification NTLM
Paramètres FSSO

Haute disponibilité
Les différents mode d'Haute Disponibilité (HA)
Synchronisation des configurations
Failover et montée en charge

Proxy Web
Concepts
Configuration du proxy explicite
Authentification et autorisation

Diagnostics
Diagnostic général
Flux de debug
Mémoire et CPU
Firmware et hardware