Fortinet NSE 4 - FortiGate Network Security Professional

- **Référence :** NSE 4
- **Durée : 5 jours**

RESUME

Avec des menaces informatiques de plus en plus sophistiquées et soutenues, les entreprises sont contraintes de s'équiper d'outils de sécurité complexes à déployer, à administrer et à maintenir. **FORTINET, l'un des leaders en matière de solutions de sécurité UTM (Unified Threat Management)** et propose une gamme de firewalls qui intègrent de multiples services de sécurité au sein d'une seule et même plateforme, les FortiGate.

Cette formation NSE4 **découpée en deux parties FortiGate I & II** vous permettra, au cours des 2 premiers jours **de prendre en main les principales fonctions de l'UTM du FortiGate**. Vous apprendrez à configurer le pare-feu, différents VPN (IPSEC, SSL..), à contrer les malwares et à créer des filtres d'URL. Dans la seconde partie de la formation qui dure 3 jours, vous apprendrez **à configurer le FortiGate dans ses fonctions avancées** (virtualisation, IPS, FSSO, DLP, …)

PARTICIPANTS

Ce cours s'adresse à ceux qui doivent administrer un firewall FortiGate (Technicien, administrateur et ingénieur systèmes/réseaux/sécurité.) ou qui désirent passer la certification NSE 4 - FortiGate Network Security Professional.

Cette formation s'adresse aux profils suivants

Administrateur Système / Réseaux / Télécom

Ingénieur Système / Réseaux / Télécom

Responsable Sécurité / RSSI

Prérequis

Des notions TCP/IP et des concepts firewall sont demandées pour démarrer ce stage.

La connaissance des couches du modèle OSI et des concepts de firewall est nécessaire pour aborder la partie Infrastructure.

OBJECTIFS

Concrètement à l'issue de ces 5 jours de formation FortiGate Security et Infrastructure, vous saurez :

- Décrire les fonctionnalités des UTM du FortiGate
- 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
- Authentifier les utilisateurs au travers du portail captif personnalisable
- Mettre en œuvre un VPN SSL pour l'accès des utilisateurs nomades au réseau de l'entreprise
- Mettre en œuvre un VPN IPsec pour l'accès des utilisateurs nomades au réseau de l'entreprise
- Appliquer de la PAT, de la source NAT et de la destination NAT
- Interpréter les logs et générer des rapports
- Utiliser la GUI et la CLI
- Mettre en œuvre la protection anti-intrusion
- Maîtriser l'utilisation des applications au sein de votre réseau
- Configurer de la SD-Wan
- Monitorer le statut de chaque lien de la SD-Wan
- Configurer de la répartition de charge au sein de la SD-Wan
- Déployer un cluster de FortiGate
- Inspecter et sécuriser le trafic réseau sans impacter le routage
- Analyser la table de routage d'un FortiGate
- Diviser un FortiGate physique en plusieurs FortiGates virtuels indépendants, via la mise en œuvre des Virtual Domains
- Étudier et choisir une architecture de VPN IPsec
- Comparer les VPN IPsec en mode Interface (route-based) ou Tunnel (Policy-based)
- Implémenter une architecture de VPN IPSec redondée
- Troubleshooter et diagnostiquer des problématiques simples sur le FortiGate
- Mettre en œuvre l'identification utilisateur ou l'authentification transparente dans les environnements Active Directory.

CONTENU

FortiGate Security (3 jours)

Introduction sur FortiGate et les UTM

High-Level Features
Setup Decisions
Basic Administration
Built-In Servers
Fundamental Maintenance
FortiGate Within the Security Fabric

Les règles de firewall

Firewall Policies
Configuring Firewall Policies
Manaing Firewall Policies
Best Practices and Troubleshooting

Le NAT

Introduction to NAT
Firewall Policy NAT
Central NAT
Session Helpers
Sessions
Best Practices and Troubleshooting

Les règles de firewall avec authentification des utilisateurs

Methods of Firewall Authentification
Remote Authentification Servers
User Groups
Using Firewall Policies for Authentification
Authenticating Through Captive Portal
Monitoring and Troubleshooting

Gestion des logs et supervision

Log Basics
Local Logging
Remote Logging
Log Settings

View, Search, and Monitor Logs
Protecting Log Data

Les Certificats

Authenticate and Secure Data Using Certificates
Inspect Encrypted Data
Manage Digital Certificates in FortiGate

Le filtrage d'URL

Inspection Modes
Web Filtering Basics
Additional Proxy-Based Web Filtering Features
DNS Filtering
Best Practices and Troubleshooting

Le contrôle applicatif

Application Control Basics
Application Control Configuration
Logging and Monitoring Application Control Events
Best Practices and Troubleshooting

Le contrôle d'intrusion et le déni de service

Intrusion Prevention System
Denial of Service
Web Application Firewall
Best Practices
Troubleshooting

Le VPN SSL

Describe SSL-VPN
SSL-VPN Deployment Modes
Configuring SSL-VPNs
Realms and Personal Bookmarks
Hardening SSL-VPN AccessMonitoring and Troubleshooting

Le VPN IPSEC en mode dial-up

IPsec Introduction
IKE Phase 1 and IKE Phase 2

Dialup IPsec VPN
Best Practices and VPN Logs

Data Leak Prevention (DLP)

DLP Overview
DLP Filters
DLP Fingerprinting
DLP Archiving
Best Practices

FortiGate Infrastructure (2 jours)

Le routage

Routing on FortiGate
Routing Monitor and Route Attributes
Equal Cost Multipath Routing
Reverse Path Forwarding
Best Practices
Diagnostics

La SD-Wan

Introduction to Software-Defined WAN
SD-WAN Performance SLA
SD-WAN Rules
SD-WAN Diagnostics

La virtualisation

VDOM Concepts
VDOM Administrators
Configuring VDOMs
Inter-VDOM Links
Best Practices and Troubleshooting

L'analyse L2

Virtual Local Area Networks
Transparent Mode
Virtual Wire Pairing
Software Switch
Spanning Tree Protocol
Best Practices

Le VPN IPSec en mode site à site

VPN Topologies
Site-to-Site VPN Configuration
Best Practices and Troubleshooting

Le FSSO

FSSO Function and Deployment
FSSO With Active Directory
NTLM Authentication
FSSO Settings
Troubleshooting

La haute disponibilité

HA Operation Modes
HA Cluster Synchronization
HA Failover and Workload
Monitoring and Troubleshooting

Le Proxy Explicite

Web Proxy Concepts
Web Proxy Configuration
Web Proxy Authentication and Authorization

Les diagnostics

General Diagnosis
Debug Flow
CPU and Memory
Firmware and Hardware

Travaux Pratiques

Un formateur présente chacun des modules à la fin desquels vous mettrez la théorie en pratique par des cas concrets.

Certification NSE4

A l'issue de ce stage, les participants peuvent passer la certification NSE 4 - Network Security Professional.

L'examen n'est pas obligatoire et se passe après la formation.