FORTIGATE SÉCURITÉ

Public
Tous ceux qui administrent régulièrement un firewall FortiGate, également à tous ceux qui participent au design des architectures réseau et sécurité reposant sur des matériels FortiGate.

Durée
3 jours - 21 heures

Pré-requis
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
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.

Méthodes pédagogiques
Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire.
La formation est délivrée en présentiel ou distanciel (e-learning, classe virtuelle, présentiel et à distance). Le formateur alterne entre méthodes démonstratives, interrogatives et actives (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification.
Cette formation est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par Audit Conseil Formation.

Moyens techniques
1 poste de travail complet par personne
De nombreux exercices d'application
Mise en place d'ateliers pratiques
Remise d'un support de cours
Passage de certification(s) dans le cadre du CPF
Remise d'une attestation de stage

Modalité d'évaluation des acquis
Evaluation des besoins et objectifs en pré et post formation
Evaluation technique des connaissances en pré et post formation
Evaluation générale du stage

Planning
Du 10/09/2024 au 12/09/2024
Du 03/12/2024 au 05/12/2024
Du 03/02/2025 au 05/02/2025
Du 16/06/2025 au 18/06/2025

Délai d'accès
L'inscription à cette formation est possible jusqu'à 5 jours ouvrés avant le début de la session

Accessibilité handicapés
Au centre d'affaires ELITE partenaire d'ACF à 20 m. Guide d'accessibilité à l'accueil.

1. INTRODUCTION SUR FORTIGATE ET LES UTM

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

2. LES RÈGLES DE FIREWALL

- Firewall Policies
- Configuring Firewall Policies
- Managing Firewall Policies
- Best Practices and Troubleshooting

3. LE NAT

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

4. 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

5. GESTION DES LOGS ET SUPERVISION

- Log Basics
- Local Logging
- Remote Logging
- Log Settings
- View, Search, and Monitor Logs
- Protecting Log Data

6. LES CERTIFICATS

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

7. LE FILTRAGE D'URL

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

8. LE CONTRÔLE APPLICATIF

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

9. LE CONTRÔLE D'INTRUSION ET LE DÉNI DE SERVICE

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

10. LE VPN SSL

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

11. LE VPN IPSEC EN MODE DIAL-UP

- IPsec Introduction
- IKE Phase 1 and IKE Phase 2
- Dialup IPsec VPN
- Best Practices and VPN Logs

12. DATA LEAK PREVENTION (DLP)

- DLP Overview
- DLP Filters
- DLP Fingerprinting
- DLP Archiving
- Best Practices

NOUS CONTACTER

Siège social
16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

Centre de formation
87, RUE GÉNÉRAL MANGIN
38000 GRENOBLE

Téléphone
04 76 23 20 50 - 06 81 73 19 35

E-mail
contact@audit-conseil-formation.com

Suivez-nous sur les réseaux sociaux, rejoignez la communauté !

ACF Audit Conseil Formation @ACF_Formation ACFauditconseilformation