retengr

FortiGate Security

Durée : 11.5 jours

Date de mise à jour : 12/05/2026

Méthode pédagogique

Une évaluation quotidienne de l'acquisition des connaissances de la veille est effectuée.

Une synthèse est proposée en fin de formation.

Une évaluation à chaud sera proposée au stagiaire à la fin du cours.

Un support de cours (version électronique) sera remis à chaque participant comprenant les slides sur la théorie, les exercices.

Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de formation.

Notre outil de Visio intégré à notre plate-forme (ou autre) sera utilisé pour la partie Visio-Conférence (si formation en distanciel)

En ce qui concerne le matériel informatique du stagiaire, il est seulement préconisé un ordinateur et une connexion internet. Nous nous chargeons du reste.

Présentation

Au cours de cette formation, vous prendrez en main les fonctions UTM du FortiGate.

Au travers des exercices vous configurerez des règles pare-feu, des tunnels VPN IPSEC, des accès VPN SSL, la protection contre les malwares, des profils de filtrage d'URL, l'authentification des utilisateurs au travers d'un portail captif.

À l'issue de ces trois jours, vous aurez des bases solides qui vous permettrons d'aborder le cours FortiGate Infrastructure.

Durant les 2 derniers jours (FortiGate Infrastructure), vous prendrez en main les fonctions d'architectures avancées du FortiGate.

Vous aurez la main sur des équipements qui se trouvent sur notre environnement de formation. Et au travers des exercices vous configurerez de la SD-Wan, du routage avancé, la mise en haute

disponibilité des FortiGate, le mode transparent, des tunnels IPsec redondés, les VDOMS, le Single Sign On...

40 rue des Filatiers, 31000 Toulouse - Organisme de formation : 73 31 08023 31 - SIRET : 812 673 903 00017

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.

Audience

Tout public

Le formateur

Le formateur est un expert du domaine qui intervient sur le sujet depuis plusieurs années en formation mais aussi en conseil.

Doté d'une grande qualité d'écoute, sa pédagogie et sa compétence technique vous permettront d'acquérir les compétences sur le domaine de la formation.

Il saura alterner entre théorie, pratique, et retours d'expérience.

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.

Programme

FortiGate Security (3 jours) [3.5h]

Introduction sur FortiGate et les UTM [3.5h]

- High-Level Features
- Setup Decisions
- Basic Administration
- Built-In Servers
- Fundamental Maintenance

- FortiGate Within the Security Fabric

Les règles de firewall [3.5h]

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

Le NAT [3.5h]

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

Les règles de firewall avec authentification des utilisateurs [3.5h]

- 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 [3.5h]

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

40 rue des Filatiers, 31000 Toulouse - Organisme de formation : 73 31 08023 31 - SIRET : 812 673 903 00017

Les Certificats [3.5h]

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

Le filtrage d'URL [3.5h]

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

Le contrôle applicative [3.5h]

- 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 [3.5h]

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

Le VPN SSL [3.5h]

- 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 [3.5h]

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

Data Leak Prevention (DLP) [3.5h]

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

FortiGate Infrastructure (2 jours) [3.5h]

Le routage [3.5h]

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

La SD-Wan [3.5h]

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

40 rue des Filatiers, 31000 Toulouse - Organisme de formation : 73 31 08023 31 - SIRET : 812 673 903 00017

La virtualization [3.5h]

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

L'analyse L2 [3.5h]

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

Le VPN IPSec en mode site à site [3.5h]

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

Le FSSO [3.5h]

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

La haute disponibilité [3.5h]

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

Le Proxy Explicite [3.5h]

- Web Proxy Concepts
- Web Proxy Configuration
- Web Proxy Authentication and Authorization

Les diagnostics [3.5h]

- General Diagnosis
- Debug Flow
- CPU and Memory
- Firmware and Hardware

Modalités et délais d'accès à la formation

Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation, en interentreprises, dans la limite des places disponibles. Pour les formations organisées en intra entreprise, la liste des participants peut être modifiée jusqu'à 24h ouvrés avant le début de la formation.

40 rue des Filatiers, 31000 Toulouse - Organisme de formation : 73 31 08023 31 - SIRET : 812 673 903 00017

Accessibilité

RETENGR facilite l'accessibilité de ses formations.

Cette formation est accessible aux personnes en situation de handicap.

Si vous avez un besoin d'accès spécifique, contactez Céline BOURREIL (celine.bourreil@retengr.com) qui étudiera avec Handifiel's (notre référent handicap) votre demande et vous proposera les meilleures solutions

Vous allez nous adorer si comme nous vous pensez que...

Une formation doit être au service de la performance du collaborateur et de l'entreprise

Ceci nécessite une quête constante d'excellence de la part de l'organisme formateur avec une adaptation systématique aux enjeux de l'entreprise, la mise à jour régulière des supports de cours et une veille technologique indispensables pour toujours être à la pointe du domaine.

L'expertise technique est aussi importante que les qualités pédagogiques

Nos formateurs sont tous des experts de leur domaine. Mais qu'ont-ils de plus que les autres ? Nous les sélectionnons en plus pour leurs qualités de pédagogue et leurs méthodes d'enseignements. Nous plaçons les qualités pédagogiques au même niveau que l'expertise afin que nos stagiaires tirent le meilleur de leurs formations.

L’excellence naît de l’excellence

Beaucoup de nos clients se classent parmi les leaders de leurs industries respectives ou parmi les start-ups les plus prometteuses. Nous savons que former les collaborateurs de telles entreprises nécessite de prêter attention à chaque détail en prodiguant un accompagnement à la hauteur de l’ambition de nos stagiaires. C’est pourquoi nous savons faire des leaders d’aujourd’hui les champions de demain !

retengr

Faire du leader d'aujourd'hui, le champion de demain