Formation FortiGate Administrator

FORTIADMIN

Version 7.4
4 Jours

Description du programme

Dans cette formation, vous apprendrez à utiliser les fonctionnalités réseau et infrastructure les plus courantes du FortiGate.

Les sujets abordés incluent des fonctionnalités couramment appliquées dans les réseaux d'entreprise ou MSSP complexes ou de grande taille, telles que le routage, l'infrastructure redondante, le VPN SSL, le VPN IPsec de site à site, l'authentification de type FSSO et la mise en place de différents diagnostics.

Vous apprendrez à utiliser les principales caractéristiques de FortiOS.

Vous découvrirez les politiques pare-feu, Fortinet Security Fabric, l'authentification de l'utilisateur et comment protéger votre réseau en utilisant des profils de sécurité et la mise en place des règles IPS et antivirales, du filtrage web et le contrôle des applications.

Ces fondamentaux vous permettront de comprendre la mise en place d'une sécurité réseau de base.

Objectifs pédagogiques

A l'issue de cette session, vous serez en mesure de :

- Configurer basiquement le paramétrage réseau d'un FortiGate en partant des paramètres d'usine
- Configurer et contrôler l'accès administrateur à FortiGate
- Utiliser l'interface graphique et la ligne de commande pour l'administration quotidienne d'un Fortigate
- Contrôler l'accès réseau aux réseaux configurés en utilisant les politiques pare feu
- Appliquer le port forwarding, le Source NAT source et le Destination NAT
- Analyser une table de routage FortiGate
- Acheminer les paquets à l'aide d'itinéraires statiques basés sur des règles multi path et également l'ECMP pour équilibrer les charges réseaux
- Authentifier les utilisateurs en utilisant les politiques pare-feu
- Surveiller les utilisateurs du pare-feu à partir de l'interface graphique FortiGate
- Proposer un accès Fortinet Single Sign-On (FSSO) intégré à Microsoft Active Directory
- Comprendre les fonctions de chiffrement et les certificats

- Inspecter le trafic sécurisé SSL/TLS pour empêcher l'utilisation du chiffrement pour contourner les politiques de sécurité
- Configurer des profils de sécurité pour neutraliser les menaces (virus, malwares) et l'utilisation abusive d'Internet (sites web inappropriés, torrents, applications indésirables, etc.)
- Appliquer des techniques de contrôle des applications pour surveiller et contrôler les applications réseau susceptibles d'utiliser des protocoles et des ports non-standard
- Offrir un accès réseau sécurisé de type VPN SSL
- Établir un tunnel VPN IPsec entre deux dispositifs FortiGate
- Configurer le routage statique
- Configurer le SD-WAN (Overlay, Underlay et échappement local)
- Identifier les caractéristiques de la "Security Fabric" de Fortinet
- Déployer les appareils FortiGate en tant que cluster HA pour la tolérance de panne et la haute performance
- Diagnostiquer et corriger les problèmes courants

Public Concerné

- Tout professionnel réseaux et sécurité chargé de la gestion, de la configuration, de l'administration et de la surveillance des éléments FortiGate utilisés pour sécuriser les réseaux
- Tout professionnel des réseaux et de la sécurité impliqué dans la conception, la mise en œuvre et l'administration d'une infrastructure utilisant des équipements FortiGate
- Cette formation est uniquement destinée aux professionnels de la cybersécurité.

Pré-requis

- Connaissance des protocoles réseaux
- Connaissance de base des concepts pare-feu
- Connaissance du procotole TCP/IP

Contenu de la formation :

Détails du jour 1 :

- Leçon 1 : Paramètres système et réseau
- Configurer FortiGate sur les paramètres d'usine par défaut
- Configurer FortiGate comme serveur DHCP

- Configurer et contrôler l'accès administrateur à FortiGate
- Sauvegarder et restaurer les fichiers de configuration du système
- Mettre à niveau le micrologiciel du FortiGate
- Vérifier les licences FortiGuard
- Leçon 2 : Politiques de pare-feu et NAT
- Configurer la politique de pare-feu IPv4
- Surveiller les journaux de trafic à partir de la politique de pare-feu
- Choisir les modes d'inspection pour les politiques de pare-feu
- Configurer le SNAT
- Configurer une politique de pare-feu pour effectuer le DNAT à l'aide d'une VIP
- Leçon 3 : Routage
- Configurer le routage statique
- Interpréter la table de routage sur FortiGate
- Implémenter la redondance des routes et l'équilibrage de charge
- Leçon 4 : Authentification pare-feu
- Configurer un serveur d'authentification LDAP distant sur le FortiGate
- Configurer un serveur d'authentification RADIUS distant sur le FortiGate
- Déployer l'authentification active et passive
- Surveillez les utilisateurs du pare-feu à l'aide de l'interface graphique du FortiGate

Détails du jour 2 :

- Leçon 5 : Fortinet Single Sign-On (FSS0)
- Installer FSSO en mode agent DC
- Installer l'agent collecteur
- Résoudre les problèmes de connexion FSSO
- Leçon6 : Certificate Operations
- Configurez FortiGate pour une inspection SSL/SSH complète
- Installer des certificats d'autorité de certification privés sur les points de terminaison
- Résoudre les problèmes de certificat
- Leçon 7 : Antivirus
- Configurer le profil antivirus en mode d'inspection basé sur les flux
- Configurer le profil antivirus en mode d'inspection basé sur proxy
- Configurer les options de protocole
- Consigner et surveiller les événements antivirus
- Résoudre les problèmes antivirus courants
- Leçon 8 : Filtre web
- Sélectionner le bon mode d'inspection (flux ou proxy) en fonction des besoins de sécurité
- Configurer l'inspection des certificats pour le filtrage Web
- Configurer un profil de filtre Web en mode d'inspection basé sur le flux
- Configurer un profil de filtre Web en mode d'inspection basé sur un proxy
- Configurer les catégories FortiGuard
- Configurer un filtre d'URL
- Résoudre les problèmes de filtrage Web

Détails du jour 3 :

- Leçon 9 : Prévention des intrusions et contrôle des applications
- Configurer un capteur de système de prévention d'intrusion (IPS)
- Dépanner l'utilisation élevée du processeur IPS
- Surveiller les événements de contrôle des applications
- Résoudre les problèmes de correspondance du trafic avec les problèmes de profil de contrôle des applications
- Leçon10 : SSL VPN
- Configurer les portails VPN SSL
- Configurer le VPN SSL en mode tunnel
- Surveiller les utilisateurs connectés au VPN SSL
- Résoudre les problèmes courants de VPN SSL
- Leçon 11 : IPsec VPN
- Configurer manuellement le VPN IPsec
- Configurer le VPN IPsec à l'aide de l'assistant IPsec
- Configurer un VPN redondant entre deux appareils FortiGate
- Surveiller les VPN IPsec et consulter les journaux
- Résoudre les problèmes de VPN IPsec
- Leçon 12 : SD WAN
- Comprendre ce qu'est le SD-WAN
- Identifier les principaux cas d'usage du SD-WAN
- Configurer le SD-WAN sur FortiGate
- Comprendre et analyser le comportement de routage dans un contexte SD-WAN
- Surveiller le comportement du SD-WAN, l'utilisation des liens et l'état de la qualité

Détails du jour 4 :

- Leçon 13 : Security Fabric
- Configurer la Security Fabric de Fortinet
- Surveiller les vues de topologie physique et logique
- Exécuter et analyser un rapport de notation Security Fabric
- Leçon 14 : Haute Disponibilité
- Configurer la haute disponibilité (FGCP)
- Configurer le basculement HA
- Configurer la synchronisation des sessions HA
- Configurer l'interface de gestion HA
- Vérifier le fonctionnement normal d'un cluster HA
- Mettre à niveau un cluster haute disponibilité
- Leçon 15 : Diagnostics et Dépannage
- Surveiller les comportements anormaux, tels que les pics de trafic
- Diagnostiquer les problèmes au niveau des couches physique et réseau
- Diagnostiquer les problèmes de connectivité à l'aide du renifleur et du flux de débogage
- Diagnostiquer les problèmes de ressources, tels qu'une utilisation élevée du processeur ou de la mémoire
- Diagnostiquer le mode de conservation de la mémoire