WatchGuard fireware v12.11 : maîtriser la sécurité avancée des réseaux d'entreprise

Date et durée

Code formation : WGF01FR
Durée : 4 jours
Nombre d'heures : 28 heures

Description

WatchGuard se positionne comme un leader en sécurité réseau, offrant des **solutions robustes pour la protection des infrastructures d'entreprise**. Avec son système d'exploitation Fireware, WatchGuard propose une suite complète de fonctionnalités incluant un pare-feu de nouvelle génération, des services de prévention des intrusions, le contrôle des applications, et des capacités avancées de détection des menaces. Ces outils permettent aux organisations de **sécuriser leurs données et leurs accès** tout en garantissant la continuité des opérations et en se protégeant contre les cybermenaces évolutives.
Cette formation de 4 jours vous fournira les compétences pratiques pour maîtriser l'**administration des solutions WatchGuard (Fireware v12.11)**. Vous explorerez en profondeur la configuration des politiques de sécurité, la gestion des VPN, l'optimisation des performances réseau, et l'utilisation des outils de supervision et de journalisation comme WatchGuard Dimension. À travers de nombreux exercices pratiques et des démos, vous apprendrez à **déployer, configurer et dépanner efficacement les Firebox** dans des environnements d'entreprise réels.
À l'issue de ce programme, vous développerez l'expertise nécessaire pour **comprendre et appliquer la sécurité WatchGuard de manière autonome et efficace** au sein de votre organisation. Vous maîtriserez les concepts clés, les meilleures pratiques et les outils essentiels pour exploiter pleinement le potentiel de ces technologies dans la protection de votre infrastructure réseau.

Objectifs

À l'issue de cette formation WatchGuard, vous atteindrez les objectifs de compétences suivants :

- remettre à l'état d'usine un Firebox et restaurer une sauvegarde de configuration ;
- comprendre, configurer et dépanner les paramètres réseau de base, incluant les interfaces, le routage statique et dynamique, et le DHCP ;
- maîtriser la création, la modification et l'optimisation des règles de pare-feu pour contrôler le trafic réseau et appliquer les politiques de sécurité ;
- comprendre en profondeur les différents types de translation d'adresses (NAT) et leur application dans divers scénarios de réseau ;
- utiliser les outils de journalisation et de surveillance en temps réel pour vérifier le fonctionnement du Firebox, diagnostiquer les problèmes et assurer la sécurité du réseau ;
- concevoir, déployer et dépanner différents types de VPN, incluant IPsec site-à-site, Mobile VPN with IPsec, et Mobile VPN with SSL, pour établir des connexions sécurisées ;
- mettre en œuvre et gérer les méthodes d'authentification des utilisateurs, incluant l'authentification locale, l'intégration avec Active Directory et les solutions d'authentification multi-facteurs (MFA) ;
- configurer et optimiser les services de sécurité avancés, tels que WebBlocker, Application Control, SpamBlocker, Gateway AntiVirus, Intrusion Prevention Service (IPS), Data Loss Prevention (DLP), et

Advanced Threat Protection (ATP) ;
- comprendre l'architecture de WatchGuard System Manager (WSM) et WatchGuard Cloud pour la gestion centralisée de plusieurs Firebox ;
- configurer et gérer les points d'accès sans fil WatchGuard, incluant les paramètres de sécurité Wi-Fi et l'intégration avec les politiques de sécurité réseau ;
- utiliser WatchGuard Dimension pour la visibilité du réseau, la génération de rapports et l'analyse de la sécurité ;
- mettre en œuvre des stratégies de haute disponibilité (HA) et de clustering pour assurer la redondance et la continuité des activités ;
- comprendre les concepts et la configuration du SD-WAN pour optimiser l'utilisation de la bande passante et améliorer les performances du réseau ;
- diagnostiquer et résoudre des problèmes courants de réseau et de sécurité liés aux Firebox WatchGuard.

Points forts

- **Maîtrise complète et actualisée :** vous allez acquérir une expertise approfondie des dernières fonctionnalités de WatchGuard Fireware (v12.11), qui vous permettront de gérer et de sécuriser efficacement des réseaux d'entreprise complexes.
- **Approche pratique et concrète :** vous bénéficierez de nombreux travaux pratiques et de démonstrations live qui consolideront votre compréhension des concepts et faciliteront l'application des connaissances techniques en situation réelle.
- **Compétences opérationnelles immédiates :** vous développerez des compétences directement applicables pour le déploiement, la configuration, l'optimisation et le dépannage des solutions de sécurité WatchGuard, vous rendant autonome rapidement.

Modalités d'évaluation

Travaux Pratiques

Pré-requis

Suivre cette formation nécessite les prérequis suivants :

- **des connaissances de base en réseau** (TCP/IP, routeurs, commutateurs, pare-feu et sécurité) ;
- **une expérience pratique de la gestion des périphériques réseau** ;
- **des compétences informatiques de base** (configuration de systèmes d'exploitation Windows ou Linux et utilisation avancée des lignes de commandes) ;
- **une compréhension de l'anglais technique.**

Public

Cette formation s'adresse aux publics suivants :

- **les administrateurs réseau et système** qui sont responsables de la gestion et de la sécurisation des infrastructures réseau ;
- **les ingénieurs sécurité** désirant maîtriser les fonctionnalités avancées des pare-feu WatchGuard pour renforcer la posture de sécurité de leur organisation ;
- **les architectes réseau** qui conçoivent des architectures sécurisées et ont besoin d'une connaissance approfondie des capacités des solutions WatchGuard ;
- **les techniciens en support informatique** amenés à diagnostiquer et résoudre des problèmes liés aux équipements de sécurité WatchGuard ;
- **toute personne travaillant dans un environnement IT** où les pare-feu WatchGuard sont déployés et qui souhaite monter en compétence sur cet équipement essentiel.

Programme

Module 1 : comprendre les bases de WatchGuard

- Les différents produits WatchGuard et leurs fonctionnalités.
- Les composants matériels et logiciels des Firebox.
- Présentation de Fireware OS.
- Les options de gestion (Web UI, CLI et WatchGuard System Manager).
- Les licences et l'activation des produits.
- La configuration et l'installation initiale de WatchGuard.

Module 2 : configurer la configuration initiale et la gestion de base

- La connexion et la navigation dans l'interface Web UI.
- La configuration des paramètres système de base (nom d'hôte, DNS et NTP).
- La configuration des interfaces réseau (VLAN et agrégation de liens).
- La configuration du routage statique et du routage dynamique (OSPF et BGP).
- Les services réseau (DHCP et relais DHCP).
- La gestion des objets et des alias.

Module 3 : gérer les politiques et les services de sécurité

- Les principes de base des politiques de pare-feu.
- La création, la modification et la gestion des politiques.
- L'inspection approfondie des paquets (Deep Packet Inspection).
- Les services de proxy (HTTP, HTTPS, FTP, SMTP et DNS).
- Le filtrage du contenu Web avec WebBlocker.
- Le contrôle des applications.
- La prévention des intrusions (IPS).
- L'antivirus au niveau de la passerelle.
- Le blocage du spam avec SpamBlocker.
- La protection avancée contre les menaces (ATP).
- La prévention de la perte de données (DLP).

Module 4 : comprendre la translation d'adresses réseau (NAT)

- Les concepts de base du NAT.
- Le NAT statique.
- Le NAT dynamique.
- Le Port Address Translation (PAT).
- Le NAT 1-à-1.
- La configuration du NAT pour les services hébergés.
- Le dépannage des problèmes de NAT.

Module 5 : gérer l'authentification et le contrôle d'accès

- L'authentification locale des utilisateurs.
- L'intégration avec Active Directory.
- L'authentification unique (SSO).
- L'authentification multi-facteurs (MFA) avec WatchGuard AuthPoint.
- La gestion des utilisateurs et des groupes.
- Les politiques d'authentification.
- Les protocoles d'authentification RADIUS et LDAP.

Module 6 : configurer les réseaux privés virtuels (VPN)

- Les concepts de base des VPN.
- Le VPN IPsec site-à-site (configuration, tunnels et politiques).
- Le Mobile VPN with IPsec (configuration du client et profils).
- Le Mobile VPN with SSL (configuration du portail et authentification).
- Le dépannage des VPN.
- Le VPN SSL Web.

Module 7 : gérer la journalisation, les rapports et la supervision

- La configuration de la journalisation (paramètres et serveurs Syslog).
- La surveillance du trafic en temps réel.
- L'utilisation de WatchGuard Dimension pour la visibilité et les rapports.
- La création de rapports personnalisés.
- L'analyse des journaux et le dépannage.

Module 8 : mettre en œuvre la gestion avancée du réseau

- La qualité de service (QoS) et la gestion de la bande passante.
- L'équilibrage de charge et le basculement.
- La haute disponibilité (HA) et le clustering.
- Le SD-WAN (concepts et configuration).
- La gestion des points d'accès sans fil WatchGuard.
- L'intégration de la sécurité Wi-Fi.

Module 9 : gérer la gestion centralisée

- La présentation de WatchGuard System Manager (WSM).
- L'ajout et la gestion des Firebox dans WSM.
- Le déploiement centralisé des politiques.
- Les mises à jour et la gestion des firmwares.
- Présentation de la gestion basée sur le cloud avec WatchGuard Cloud.
- L'automatisation et les APIs.

Module 10 : effectuer le dépannage et l'optimisation

- Les outils de diagnostic (Firebox System Manager et CLI).
- La capture de paquets et l'analyse.
- Le dépannage des problèmes courants.
- L'optimisation des performances du Firebox.
- Les meilleures pratiques de sécurité WatchGuard.
- Les mises à jour du firmware.