+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 12/06/2026

S'inscrire

Formation Watchguard Network Security Essential

2 jours (14 heures)

Présentation

WatchGuard Firebox est une solution de sécurité réseau permettant de protéger les infrastructures d'entreprise grâce à des fonctions de firewall, filtrage, VPN, inspection du trafic, services UTM, supervision et reporting.

Notre formation WatchGuard Network Security Essentials vous permettra de maîtriser les fondamentaux de l'installation, de la configuration et de l'administration d'un environnement WatchGuard Firebox.

Vous apprendrez à configurer les interfaces réseau, les politiques de sécurité, le NAT, la segmentation, les services UTM, l'authentification, les accès distants et les VPN site-à-site.

À l'issue de cette formation, vous serez en mesure d'administrer un Firebox au quotidien, de sécuriser les accès, d'analyser les logs, de superviser l'activité réseau et de diagnostiquer les incidents courants.

Cette formation aborde également les bonnes pratiques de durcissement : mises à jour, sauvegardes, comptes administrateurs, politiques minimales, sécurité VPN, certificats, logs et configuration sécurisée.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Comprendre l'architecture WatchGuard Firebox et les fondamentaux Fireware
- Configurer les interfaces, routes, DNS, DHCP et paramètres réseau
- Créer des politiques de sécurité, règles NAT et services de filtrage

- Mettre en place les services UTM : IPS, WebBlocker, Application Control et proxies
- Configurer les VPN d’accès distant et les tunnels site-à-site
- Exploiter les logs, rapports, outils de monitoring et méthodes de dépannage

Public visé

- Administrateurs réseaux
- Administrateurs systèmes et réseaux
- Ingénieurs réseaux
- Ingénieurs sécurité réseaux
- Techniciens réseaux avancés
- Responsables infrastructure et consultants intégration sécurité

Pré-requis

- Connaissances de base en réseaux TCP/IP
- Notions de routage, DNS, DHCP, NAT et adressage IP
- Compréhension générale des principes de sécurité réseau

Pré-requis techniques

- Disposer d’un ordinateur avec navigateur web récent
- Prévoir une connexion Internet stable

Programme de notre formation WatchGuard Network Security Essentials

[Jour 1 - Matin]

Découvrir WatchGuard Firebox et les fondamentaux Fireware

- Comprendre le rôle de WatchGuard Firebox dans une architecture de sécurité réseau
- Identifier les composants clés : Fireware, Web UI, WatchGuard System Manager, WatchGuard Cloud et services de sécurité
- Comprendre les modes de déploiement : routeur, bridge, drop-in, réseau local, DMZ et segmentation
- Configurer les interfaces, adresses IP, DNS, DHCP, routes statiques et passerelles
- Découvrir les bonnes pratiques de configuration initiale, sauvegarde, restauration et mise à jour Fireware
- Atelier pratique : initialiser un Firebox, configurer les interfaces réseau et valider la connectivité de base

[Jour 1 - Après-midi]

Politiques de sécurité, NAT et contrôle du trafic

- Comprendre le fonctionnement des firewall policies dans Fireware
- Créer et organiser des règles de filtrage selon sources, destinations, ports, protocoles et services
- Configurer le NAT, le SNAT, le DNAT, les redirections de ports et les règles de publication
- Appliquer les bonnes pratiques de segmentation entre LAN, WAN, DMZ, invités et réseaux métiers
- Tester, diagnostiquer et ajuster les règles pour éviter les ouvertures excessives
- Atelier pratique : créer des politiques de sécurité, configurer une règle NAT et valider les flux autorisés ou bloqués

Services de sécurité et protection UTM

- Comprendre les services de sécurité WatchGuard : Gateway AntiVirus, IPS, WebBlocker, Application Control et spamBlocker
- Configurer les proxies HTTP, HTTPS, SMTP, DNS ou FTP selon les besoins de filtrage
- Mettre en place le filtrage web, le contrôle applicatif et la prévention d'intrusion
- Activer les profils de sécurité adaptés aux utilisateurs, réseaux et risques métier
- Identifier les impacts des services de sécurité sur la performance et l'expérience utilisateur
- Atelier pratique : appliquer des services UTM sur une politique de trafic et analyser les événements générés

[Jour 2 - Matin]

VPN, accès distant et interconnexion de sites

- Comprendre les usages des VPN dans WatchGuard : accès distant, site-à-site et interconnexion sécurisée
- Configurer un Mobile VPN pour les utilisateurs distants
- Mettre en place un Branch Office VPN pour connecter plusieurs sites
- Comprendre les paramètres IKE, tunnels, réseaux autorisés, routage et règles associées
- Appliquer les bonnes pratiques de sécurité VPN : authentification, chiffrement, droits et supervision
- Atelier pratique : configurer un VPN d'accès distant ou un tunnel site-à-site et valider les communications

[Jour 2 - Après-midi]

Authentification, administration et durcissement

- Configurer l'authentification des utilisateurs et groupes pour contrôler les accès réseau
- Gérer les comptes administrateurs, rôles, permissions, mots de passe et accès distants
- Sécuriser l'administration locale et distante du Firebox
- Appliquer les bonnes pratiques : mises à jour, sauvegardes, certificats, comptes, interfaces et politiques minimales
- Préparer une configuration conforme aux besoins d'exploitation et de maintenance
- Atelier pratique : durcir une configuration Firebox et appliquer une checklist de sécurisation

Monitoring, logs, reporting et dépannage

- Exploiter les logs Firebox pour comprendre les flux autorisés, bloqués ou inspectés
- Utiliser les outils de monitoring, tableaux de bord, alertes et rapports WatchGuard
- Diagnostiquer les problèmes courants : connectivité, politiques, NAT, VPN, DNS et services de sécurité
- Analyser les événements liés aux proxies, IPS, filtrage web, authentification et VPN
- Mettre en place une méthode de troubleshooting structurée pour l'exploitation quotidienne
- Atelier pratique : résoudre un incident réseau ou sécurité à partir des logs, outils de diagnostic et rapports disponibles

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.