

Formation WatchGuard

Network Security Essential

Public visé

Toute personne adulte concernée par l'administration au quotidien de boitiers WatchGuard.
Aucune durée minimale d'activité professionnelle n'est demandée.

Cette formation peut faire l'objet d'une demande de prise en charge au titre de la formation continue auprès de votre OPCA. no. d'agrément D2B: 11 93 05082 93.

Pré-requis

- Connaissances de base sur les réseaux et TCP/IP
- Etre à l'aise avec un PC sous Windows (7, 8 ou 10)
- Les connaissances en sécurité informatique sont un plus mais ne sont pas obligatoires

Objectifs

A l'issue de cette formation l'apprenant sera capable de :

- remettre en configuration usine un pare-feu et recharger une sauvegarde de la configuration
- mettre en place les configurations réseaux adaptées à son entreprise
- comprendre et modifier les règles et paramètres les plus usuels
- comprendre et mettre en œuvre les différentes translations d'adresses
- vérifier le bon fonctionnement du pare-feu au travers des journaux et du suivi temps réel
- mettre en place et gérer des authentifications
- choisir et mettre en œuvre les fonctions optionnelles de sécurité (WebBlocker, SpamBlocker, Application Control, RED, IPS, Anti-Virus, DLP,...)
- mettre en place un VPN Site à Site (BOVPN) simple en IPsec
- mettre en place un VPN nomade (MUVPN en IPsec et en SSL)
- gérer des interfaces WAN multiples
- gérer la bande passante

Contenu de la formation

- Présentation des composants matériels
 - Les gammes WatchGuard
 - Les interfaces (RJ45, USB, ...)
- Présentation des composants logiciels
- Installation des boitiers
 - La configuration d'usine
 - Les assistants de configuration
- Connexion au firewall via le client WSM – Accès à Policy Manager
- Paramétrages des interfaces et des règles de base
- Gestion des licences
- Gestion des mises à jour
- Utilisation des alias
- Gestion par défaut des menaces
- Réglages généraux (NTP, DNS, ...)
- Mise en place des polices
 - From et TO
 - Journalisation
 - personnalisation
- Les outils de supervision
 - Firebox System manager
 - Les journaux
- Les interfaces et les VLAN
- SD-WAN (Multi-WAN)
- Les translations d'adresses (SDNAT, SNAT, 1 to 1)
- Gestion de la bande passante
- Gestion de la journalisation
- Gestion avancée des polices (schedule, precedence, ...)
- Les services de sécurité globaux : Botnet Detection
- Les services de sécurité pour polices
 - DNSWatch
 - IPS

- Application Control
- Geolocation
- Les proxies et leurs services de sécurité
 - FTP, SMTP, HTTP, HTTPS
 - APT Blocker, DLP, RED, SpamBlocker, WebBlocker, AntiVirus
 - Inspection de contenu
- Sécurisation des terminaux : TDR
- Les authentifications (locale et via AD)
- Les VPN site à site (BOVPN IPsec, BOVPN-VIF, BOVPN-TLS)
- Les VPN Nomades (Mobile VPN L2TP, IPsec/IKEv2 et SSL)
- Résolution de problèmes VPN
- Dimension : statistiques et rapports
- Bilan de la formation – Remise des attestations

Moyens et méthodes pédagogiques

La formation se déroule avec une alternance d'exposés ou de présentations, de travaux pratiques/dirigés et de quiz.

Chaque participant a accès à un PC et un boîtier WatchGuard pour la mise en pratique des notions abordées.

Un support de cours (essentiellement en anglais) est fourni sous format papier à chaque participant.

Les compétences acquises sont vérifiées au travers de mises en situation et/ou de quiz.

Durée : 28 heures sur 4 jours

Formateur : Qualification et compétences

La formation est assurée par Jean-Paul ARCHIER qui travaille depuis plus de 30 ans dans le domaine des réseaux informatiques, dont 20 ans à utiliser, configurer et administrer des solutions WatchGuard. Jean-Paul ARCHIER est WCT (WatchGuard Certified Trainer). Il est l'auteur de plusieurs ouvrages portant sur les réseaux (Cisco ASA, VPN, IPv6, ...) et il intervient régulièrement, en France et à l'étranger, pour des formations liées à ces domaines.



Taille du groupe de participants

Afin d'assurer un parfait suivi des participants et une grande interactivité entre le formateur et les apprenants chaque session ne dépassera pas 8 personnes.

Suivi des participants

L'assiduité des participants est attestée par la signature pour chaque ½ journée d'une feuille de présence par le participant et le formateur.

Evaluation de la formation

L'évaluation de la formation se fait à chaud par un questionnaire de satisfaction ainsi que des échanges directs entre le formateur et les participants.

Les points principaux à évaluer portent sur la qualité pédagogique du formateur, la qualité et le contenu du support de cours ainsi que la qualité de l'infrastructure utilisée.

Une partie du questionnaire portera également sur l'atteinte des objectifs initiaux du participant et sur ses souhaits en matière de formations complémentaires.

La formation sera sanctionnée par la remise d'une attestation individuelle.