Introduction à l'offre WatchGuard

WatchGuard Technologies

WatchGuard développe des **appliances de sécurité combinant pare-feu, VPN et services de sécurité** pour protéger les réseaux contre les spams, les virus, les logiciels malveillants et les intrusions.

La gamme des boitiers WatchGuard est composée de modèles destinés aux entreprises de toutes les tailles, **de moins de 10 utilisateurs jusqu'à 10 000 et plus.**

Il existe aussi des **versions virtuelles** de nos solutions s'installant sur des hyperviseurs VMware et Hyper-V.

Plus de **1 000 000 d'appliances WatchGuard** sont installées dans le monde.

Nos interfaces sont traduites en **français**, tout comme les documentations techniques et l'aide en ligne.

Dimension : l'outil de visibilité intégré gratuitement

Dimension est un outil de visibilité qui vous permet de comprendre ce qui a pu se passer sur une période définie sur votre appliance, ses services de sécurité et par extension sur votre réseau (sur le dernier mois, sur les 5 dernières minutes, etc...)

Il vous permet :

- de maîtriser votre **politique de sécurité**
- de contrôler que votre **bande passante** n'est pas gaspillée inutilement par trop d'usages non-productifs.
- De conserver une année de **logs** afin de répondre aux contraintes légales

Dimension Visibility est **gratuit et intégré de base** dans toutes nos appliances de sécurité.

Nous avons fait le choix de rendre cet outil gratuit car il permet à nos clients d'avoir une meilleure visibilité et d'améliorer leur niveau de sécurité.

Les utilisateurs accèdent à Dimension via un navigateur internet et visualisent des informations présentées sous une forme aisément compréhensible et en français.

Divers profils peuvent utiliser Dimension :

- la direction générale, les équipes RH, etc… : dans les rapports adaptés à cette typologie d'utilisateurs, les informations importantes sur les usages sautent aux yeux sans connaissances techniques.
- Un profil technique utilisera d'autres rapports de Dimension : Par exemple des rapports de corrélation, difficilement accessibles par de simples logs et permettant d'avoir une compréhension fine d'une situation.

Dimension est un outil **dynamique** :

- cliquer sur le nom d'une personne permet de connaître l'ensemble de ses usages
- cliquer sur le nom d'un des malwares que cette personne a fait rentrer, permet de situer la criticité de ce malware, par quelle connexion il est arrivé, par quelle règle.
- etc...

Anonymisation des rapports

Nouveauté Dimension 2.1

Cette fonction permet aux entreprises de se conformer aux réglementations relatives à la protection de la vie privée, telles que le règlement GDPR (General Data Protection Regulation) de l'Union Européenne.

Lorsque le mode d'anonymisation est enclenché, l'administrateur réseau ne peut pas voir le nom des utilisateurs qui sont remplacés par des pseudonymes aléatoires.

Subscription Services Dashboard :

Nouveauté Dimension 2.1

Ce tableau de bord donne aux entreprises un aperçu complet des performances en matière de sécurité, avec des statistiques qui montrent ce qui a été scanné et les attaques qui ont été évitées.

Si vous souhaitez tester Dimension :

Il vous est possible de tester Dimension grâce à la démo en ligne suivante :

https://demo.watchguard.com/

- login : demo
- mot de passe : visibility

Nouvelle démo

Cliquez sur le boitier WEBDEMO :

Botnet Detection

Nouveauté Fireware 11.11

Botnet Detection permet de détecter les machines zombies (les machines infectées contrôlées à distance par un hacker et ses serveurs de commande). L'administrateur a alors la visibilité sur ces machines pour pouvoir les nettoyer.

Network Discovery

Nouveauté Fireware 11.11

Ce service disponible sur les Firebox de dernière génération permet de scanner le réseau pour donner une visibilité sur les postes sur le réseau, leur système d'exploitation ainsi que les ports ouverts.

Mobile Security

Nouveauté Fireware 11.11

Mobile Security permet de vérifier la conformité d'un smartphone avec des prérequis définis par l'administrateur – Pour ainsi par exemple :

- interdire les smartphones jailbreakés/rootés
- interdire des devices qui téléchargent des applications à partir d'une source non identifiée
- détecter les malwares sur Android

Si la conformité n'est pas respectée, il est alors impossible au smartphone de se connecter en VPN ou en WIFI sur le réseau de l'entreprise.

Le filtrage d'URL

WebBlocker limite les sites auxquels vos employés peuvent accéder sur Internet :

- Il permet d'accroître la **productivité** des salariés :
  par exemple en interdisant la catégorie Jeux pendant les horaires de travail.

- Il permet d'éviter que votre **responsabilité légale** ne soit mise en jeu
  par exemple en interdisant à des lycéens d'accéder à des sites permettant de construire une bombe artisanale ou d'accéder à du contenu protégé par le droit d'auteur.

- Il permet protéger votre réseau des **sites malveillants** :
  Par exemple en interdisant l'accès à des sites de téléchargements de logiciels contenant généralement beaucoup de malwares.

Le contrôle d'application

Le Contrôle d'application permet aux administrateurs informatiques de surveiller et de **contrôler l'accès aux applications web et aux applications d'entreprise** afin de faire respecter la politique de sécurité et de protéger la productivité et la bande passante du réseau.

Vous pouvez soit **autoriser, bloquer ou refuser l'accès** aux applications en fonction du **groupe** d'un utilisateur, de ses **tâches** et du **moment de la journée**, et générer des **rapports** d'utilisation.

Par exemple, vous pourriez choisir :

- d'autoriser à votre service marketing l'accès à **Facebook** et aux autres sites de réseaux sociaux (car c'est un outil de communication) mais pas aux jeux Facebook ; ni au chat Facebook – Il est même possible d'aller jusqu'à interdire les Like Facebook.

- vous pouvez tolérer l'usage de **YouTube** mais en limitant sa consommation à 10% de la bande passante au maximum par exemple.

- limiter l'utilisation de toutes les applications de **Peer2Peer** à une bande passante ridicule (56 Kbits par exemple) afin de dégouter les utilisateurs de télécharger du contenu illégal.

- bloquer l'utilisation des messageries personnelles de type **Gmail** à tout moment, pendant les heures de bureau, ou jamais

- Plus globalement, s'assurer que 70% de la bande passante (par exemple) soit réservée à vos **applicatifs métiers**.

Il y a **20 catégories** différentes pour classer les applications, plus de **1800 applications** et bien plus de signatures pour différencier les comportements de chaque application.

L’Anti-Spam

Vous pouvez **bloquer le spam**, **indépendamment de la langue, du format ou du contenu du message**, même le spam basé sur des **images**. Le **taux de faux positifs** est proche de zéro, ce qui réduit considérablement la tache de l’administrateur ou de l’utilisateur dans la gestion des spams.

L’anti-virus de passerelle

Les boitiers WatchGuard disposent d’un **moteur de détection des virus** en anti-virus de passerelle. Un anti-virus reste nécessaire sur les postes clients. L’intérêt de rajouter un anti-virus de passerelle est, entre-autre, de pouvoir contrer les virus qui sont construits pour détecter quel est l’antivirus sur les postes de travail, le désactiver et attaquer.

APT Blocker : Pour lutter contre les malwares avancés

Les menaces actuelles sont de plus en plus dangereuses en partie du fait qu'elles peuvent aisément **se déguiser en code qui passe inaperçu** auprès des produits basés sur signature (anti-virus) qui recherchent un modèle de logiciel malveillant reconnaissable.

Le module APT Blocker se concentre sur l'**analyse des comportements** pour déterminer si un fichier est malveillant.

APT Blocker identifie et signale les fichiers suspects à une **Sandbox** (bac-à-sable) de nouvelle génération basée sur le Cloud, un environnement virtuel dans lequel le code est analysé, émulé et exécuté pour déterminer son potentiel de menace.

Les menaces avancées, notamment les APT (menaces persistantes avancées), sont conçues pour reconnaître les modes de détection et s'en cacher. **L'émulation système complète** d'APT Blocker (qui simule le matériel physique, notamment le processeur et la mémoire) offre le plus haut niveau de d’efficacité du marché à ce jour.

Nous vous conseillons de regarder la vidéo YouTube suivante :

https://youtu.be/ajkmA7pLIbE

Cette vidéo vous expliquera concrètement :

- Comme il est simple de trouver un malware avancé sur internet.
- Pourquoi les anti-virus ne sont plus forcément suffisants.
- Les solutions à mettre en place pour lutter contre ce type de menaces

La prévention d'intrusions (IPS)

Les boitiers WatchGuard disposent d'un **moteur de détection des attaques**.

Empêcher la fuite accidentelle de données = DLP

Le service WatchGuard DLP **évite les fuites accidentelles de données** en analysant automatiquement les données en transit afin d'y détecter la présence potentielle d'informations sensibles.

Le service de WatchGuard, fonctionnant sur la base d'un abonnement, comprend une bibliothèque prédéfinie de plus de **200 règles pour 18 pays**, et couvre aussi bien les **informations personnelles que les données bancaires et de santé.**

VPN

Les boitiers WatchGuard supportent deux types de VPN :

- **Branch Office** (Site à Site)
- **Mobile VPN** (Nomade)

Traffic Management par Application

Une appliance WatchGuard permet de fixer une **limite de bande passante (et/ou une garantie) par Application ou Catégorie d'application.**

Quota de temps et de volume pour les utilisateurs

Des **quotas de temps et de volume** peuvent être appliqués aux utilisateurs authentifiés à travers les règles de Firewall.

Les quotas sont **journaliers** et si un utilisateur dépasse son quota de volume ou son quota de temps, il se verra bloqué par un message spécifique.

Déchiffrer les contenus devient critique

Bientôt, 75% des sites internet auront basculé en https.

Une appliance de sécurité doit être puissante afin de déchiffrer, analyser et filtrer les contenus désormais chiffrés. Autrement, ces flux passent sans contrôle.

Administration des Appliances Firebox

Les appliances WatchGuard vous permettent de passer librement d'un environnement d'administration à un autre :

- Client lourd installé sur un PC, très apprécié des administrateurs de solutions WatchGuard
- Interface Web
- Commande en Ligne

Les points d'accès Wifi WatchGuard

WatchGuard propose des bornes d'accès WIFI pour permettre une sécurisation complète filaire et sans fil des réseaux privés, une conservation des **logs** pour répondre aux contraintes légales et une **visibilité** et un **contrôle** des usages des utilisateurs..

Ces bornes Wifi sont rattachées à leur **contrôleur Wifi** qui est implémenté directement dans les appliances WatchGuard de base et sans surcoût, permettant ainsi une intégration complète entre les bornes et la **politique de sécurité**.

Un **portail** est disponible pour générer des coupons Wifi. Vous pouvez laisser l'accès à cet applicatif à une personne non technique

Cela permet également une cohérence parfaite dans l'administration des équipements avec une **interface de configuration unique** de l'ensemble des équipements de sécurité et des bornes.

Grace à la fonctionnalité de Roaming, les clients Wifi (portables/smartphone etc.) sélectionnent la borne la plus puissante pour basculer dessus et continuer les transferts et communications de manière transparente.

Les Points d'accès Wireless WatchGuard peuvent être raccordés par des liens Ethernet alimentés par des injecteurs ou switch POE.

WatchGuard Dimension permet d'avoir un **tableau de bord Wifi** ainsi que des **rapports d'activités des bornes**