Qu'est-ce qu'une solution WatchGuard vous apportera concrètement ?

A noter :

- ***Ce document est loin d'être exhaustif.***
- *Un document beaucoup plus complet (en 130 pages et en français) est disponible.*
- *Nos équipes sont aussi à votre disposition pour tout complément d'information.*

TABLE DES MATIÈRES

1. 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 société WatchGuard Technologies a été créée en 1996 aux Etats-Unis.

Notre siège se situe à Seattle et nous sommes 500 employés dans le monde.

Plus de **1 000 000 d'appliances WatchGuard** sont installées dans le monde avec en général un fort attachement des équipes techniques aux solutions WatchGuard chez nos clients.

38% de nos ventes sont réalisées sur la zone EMEA.

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

2. Les Appliances de sécurité WatchGuard

Les partenariats technologiques

Notre architecture permet de nous appuyer sur des **partenariats technologiques** avec des éditeurs de solutions de sécurité leaders de leurs marchés respectifs afin de bénéficier du meilleur de chaque service de sécurité dans une appliance tout-en-un.

Voici les partenaires technologiques avec qui nous travaillons :

Anti-virus :	AVG sur la base Enterprise	
Anti-Spam :	Cyren (ex Comm Touch)	
Filtrage d'URL :	Websense	
IPS :	Trend Micro	
Contrôle d'Application :	Trend Micro	
DLP (Contrer la fuite d'Informations) :	Sophos	
APT Blocker (Anti-Cryptolockers) :	Lastline	

Cette **architecture ouverte** nous permet de pouvoir rajouter des nouveaux services de sécurité simplement ; ou même de pouvoir remplacer un éditeur facilement si un jour ses solutions venaient à ne plus nous convenir.

Des services spécifiques développés par nos équipes

Nous développons aussi des services de sécurité nous-même **quand nous ne trouvons pas forcément de solution sur le marché qui convienne à nos attentes**.

Quelques exemples :

- nous avons développé le service RED (**Reputation Enabled Defense**).
  Ce service de sécurité permet de dégrader la note d'un site internet quand un boitier dans le monde (parmi notre base d'un million de boitier WatchGuard) détecte une menace de type virus ou malware sur un site web. A partir d'un certain score (configurable) l'administrateur peut décider que ses utilisateurs ne pourront plus y accéder tant que le problème n'aura pas été résolu.

- **Dimension**, notre outil de visibilité, a été développé dans le même état d'esprit. Vous trouverez plus d'informations sur cet outil, fondamental dans une architecture WatchGuard, au chapitre suivant.

Fireware

Tous nos boitiers fonctionnent avec le même code (Fireware) et disposent des mêmes fonctionnalités et des mêmes interfaces de configuration et de monitoring. Fireware repose sur un système d'exploitation Linux sécurisé (WatchGuard Linux).

La gamme d'appliances de sécurité WatchGuard

La gamme des boitiers WatchGuard est composée de modèles destinés aux entreprises de toutes les tailles, **de moins de 5 utilisateurs jusqu'à 10 000 et plus.**

	Firebox T10 T10-W*, T10-D*	Firebox T30/T30-W	Firebox T50/T50-W	Firebox M200	Firebox M300	Firebox M400	Firebox M440	Firebox M500	XTM 850	XTM 860	XTM 870/870-F	XTM 1520-RP	XTM 1525-RP	XTM 2520
Débit et connexions														
Débit du pare-feu	400 Mbit/s	620 Mbit/s	1,2 Gbit/s	3,2 Gbit/s	4 Gbit/s	8 Gbit/s	6,7 Gbit/s	8 Gbit/s	8 Gbit/s	11 Gbit/s	14 Gbit/s	14 Gbit/s	25 Gbit/s	35 Gbit/s
Débit VPN	100 Mbit/s	150 Mbit/s	270 Mbit/s	1,2 Gbit/s	2 Gbit/s	4,4 Gbit/s	3,2 Gbit/s	5,3 Gbit/s	8 Gbit/s	8 Gbit/s	10 Gbit/s	10 Gbit/s	10 Gbit/s	10 Gbit/s
Débit AV	120 Mbit/s	180 Mbit/s	235 Mbit/s	620 Mbit/s	1,2 Gbit/s	2,5 Gbit/s	2,2 Gbit/s	3,2 Gbit/s	4 Gbit/s	5,5 Gbit/s	7 Gbit/s	8 Gbit/s	9 Gbit/s	9,7 Gbit/s
Débit IPS	160 Mbit/s	240 Mbit/s	410 Mbit/s	1,4 Gbit/s	2,5 Gbit/s	4 Gbit/s	2,2 Gbit/s	5,5 Gbit/s	5 Gbit/s	7 Gbit/s	9 Gbit/s	11 Gbit/s	13 Gbit/s	15 Gbit/s
Débit UTM	90 Mbit/s	135 Mbit/s	165 Mbit/s	515 Mbit/s	800 Mbit/s	1,4 Gbit/s	1,6 Gbit/s	1,7 Gbit/s	3 Gbit/s	4 Gbit/s	5,7 Gbit/s	6,7 Gbit/s	6,7 Gbit/s	jusqu'à 10 Gbit/s
Interfaces 10/100/1000	3	5[IX]	7[IX]	8	8	8 (dont 2 SFP)[IX]	25 1G cuivre[IX] 2 10G SFP+	8 (dont 2 SFP)[IX]	14	14	14 [IX]	14	6 cuivre et 4 10G SFP+[IX]	12 cuivre et 4 10G SFP+[IX]
Interfaces E/S	1 série / 1 USB	1 série / 2 USB	1 série / 2 USB	1 série / 2 USB	1 série / 2 USB	1 série / 2 USB	1 série / 2 USB	1 série / 2 USB	1 série / 2 USB	1 série / 2 USB	1 série / 2 USB	1 série / 2 USB	1 série / 2 USB	1 série / 2 USB
Nombre de connexions simultanées	50 000	200 000	300 000	1 700 000	3 300 000	3 800 000	4 000 000	9 200 000	5 000 000	7 000 000	9 000 000	10 000 000	15 000 000	15 000 000
Nouvelles connexions par seconde	2 300	3 400	4 600	20 000	48 000	84 000	62 000	95 000	70 000	80 000	90 000	135 000	135 000	135 000
Prise en charge VLAN	10	50	75	100	200	300	400	500	750	750	1 000	2 000	3 000	4 000
Nombre d'utilisateurs authentifiés	200	500	500	500	500	Illimité	Illimité	Illimité	Illimité	Illimité	Illimité	Illimité	Illimité	Illimité
Tunnels VPN														
VPN pour succursale	5	40	50	50	75	100	300	500	5 000	6 000	7 000	10 000	10 000	Illimité
VPN IPSec mobiles	5	40	55	75	100	150	300	500	10 000	12 000	14 000	15 000/15 000	20 000/20 000	Illimité
VPN SSL / L2TP mobiles	5	25	50	75	100	150	300	500	10 000	12 000	14 000	15 000	20 000	Illimité
Caractéristiques du système d'exploitation														
Généralités	Attribution des adresses IP : statique, DynDNS, PPPoE, DHCP (serveur, client, relais) / Indépendance des ports / Prise en charge VLAN / Mode transparent/de transfert													
Fonctions réseau avancées[IX]	Routage dynamique (BGP, OSPF, RIPv1,2) / Routage basé sur des stratégies / NAT : statique, dynamique, 1:1, IPSec Traversal, PAT basé sur des stratégies / Modélisation du trafic et QoS : 8 files d'attente prioritaires, DiffServ, file d'attente stricte modifiée / IP virtuelle pour l'équilibrage de charge côté serveur													
Disponibilité[IX]	Haute disponibilité (active/passive et active/active pour le clustering) (non disponible avec les modèles sans fil) / Basculement VPN / Basculement multi-WAN / Équilibrage de charge multi-WAN / Agrégation de liens (802.3ad dynamique, statique, active/sauvegarde) / Basculement WAN sans fil disponible avec l'accessoire de pont sans fil WatchGuard Broadband													
Sans fil														
Sans fil intégré	802.11a/b/g/n intégré disponible pour le Firebox T10-W. 802.11/ac intégré disponible pour les Firebox T30-W et T50-W													
Points d'accès sans fil	Tous les modèles prennent en charge les points d'accès sans fil AP100, AP102 et AP200 afin d'étendre les fonctions de sécurité UTM et NGFW au réseau WLAN / Comprend le filtrage des adresses MAC, les rapports client, la technologie des portails captifs, l'authentification 802.1X, ainsi que l'analyse et les rapports de conformité PCI / L'AP102 permet un accès WLAN en intérieur et en extérieur													
Services de sécurité														
Bundle NGFW	Contrôle d'application / Service de prévention d'intrusions / Support 24 h/24, 7 j/7 — Disponible pour le Firebox T30 et modèles supérieurs / Disponible pour le XTM 830 et modèles supérieurs													
Bundle UTM	Contrôle d'application / Service de prévention d'intrusions / Gateway AntiVirus / WebBlocker (filtrage d'URL) / spamBlocker (antispam) / Autorité de réputation (Reputation Enabled Defense) / Support 24 h/24, 7 j/7 — Disponibles pour tous les modèles Firebox et XTM													
Autres services de sécurité	APT Blocker, Prévention des pertes de données — Disponibles pour tous les modèles Firebox et XTM													
Mises à niveau de gestion	Dimension Command est une suite d'outils de management pour WatchGuard Dimension qui permet aux administrateurs de gérer les politiques directement depuis les tableaux de bord de visibilité de Dimension. Contactez votre revendeur WatchGuard pour voir une démonstration et obtenir des informations sur la promotion en cours.													

Les débits sont calculés en envoyant plusieurs flux via plusieurs ports et peuvent varier en fonction de l'environnement et de la configuration. Contactez votre revendeur WatchGuard ou appelez directement WatchGuard au 01 40 90 30 35 pour vous aider à choisir le bon modèle pour votre réseau.

Proxy transparent

Les appliances de sécurité WatchGuard sont bâties sur une technologie robuste de **Proxy transparent**, fondamentalement plus sûre qu'un filtrage dynamique de paquets (Packet-filtering).

Spécificités liées au modèle d'entrée de gamme T10

Deux spécificités sur le modèle T10 d'entrée de gamme :

- C'est le seul modèle de la gamme à ne pas être multi-WAN
- Il n'est pas non plus disponible en cluster.

Multi-WAN et Cluster sur le reste de la gamme

Tous les autres modèles de la gamme sont **multi-WAN** et peuvent être mis en **cluster** actif/passif et actif/actif.

La gestion de plusieurs accès Internet (multi-WAN) est possible dans les modes suivants :

- Partage de charge
- Tolérance de panne
- Aiguillage des flux manuel (Policy Based Routing)
- Surcharge d'interface

Solutions virtuelles

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

Bornes Wifi

Nous fournissons aussi des **bornes Wifi** WatchGuard qui permettent de mettre en place une **politique de sécurité** pour vos visiteurs Wifi, une conservation des **logs** pour répondre aux contraintes légales et une **visibilité** et un **contrôle** des usages des utilisateurs.

Les bornes Wifi WatchGuard sont gérées par nos appliances qui sont toutes contrôleur Wifi de base et sans surcoût.

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

3. Dimension : l'outil de visibilité très apprécié de nos clients

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 demandons juste à ce que votre appliance soit sous maintenance.

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.

Dimension est une **machine virtuelle** comprenant un OS optimisé avec les services de logs, rapports et de tableaux de bord ; et s'installe en une dizaine de minutes :

- dans une machine virtuelle en local
- une VM hébergée dans le Cloud
- ou un VM hébergée par votre prestataire WatchGuard et sauvegardée par ses soins.

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

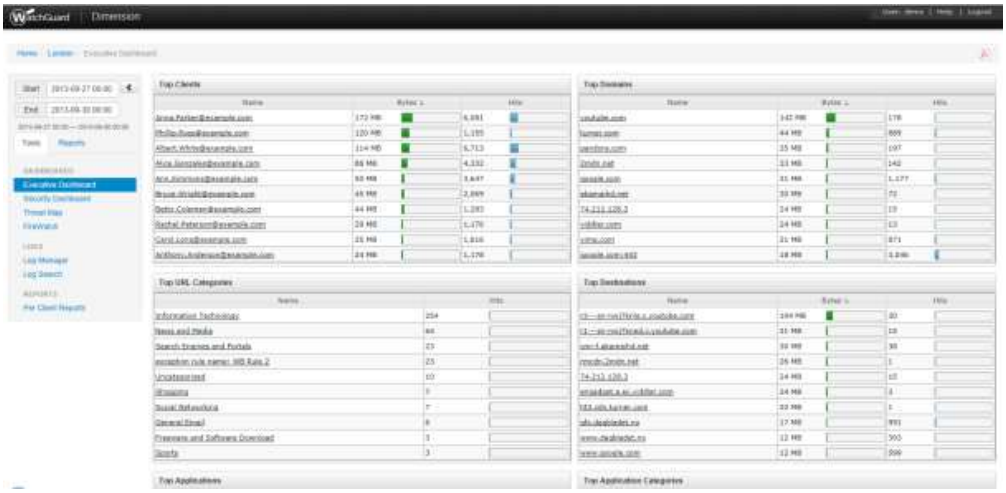
Divers profils peuvent utiliser Dimension :

- 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...

Le tableau de bord global :



Il vous permet de savoir qui sont **les utilisateurs les plus actifs** :

- En consommation de bande passante
- En nombre de visites

Vous pouvez visualiser **l'usage d'internet** dans votre structure :

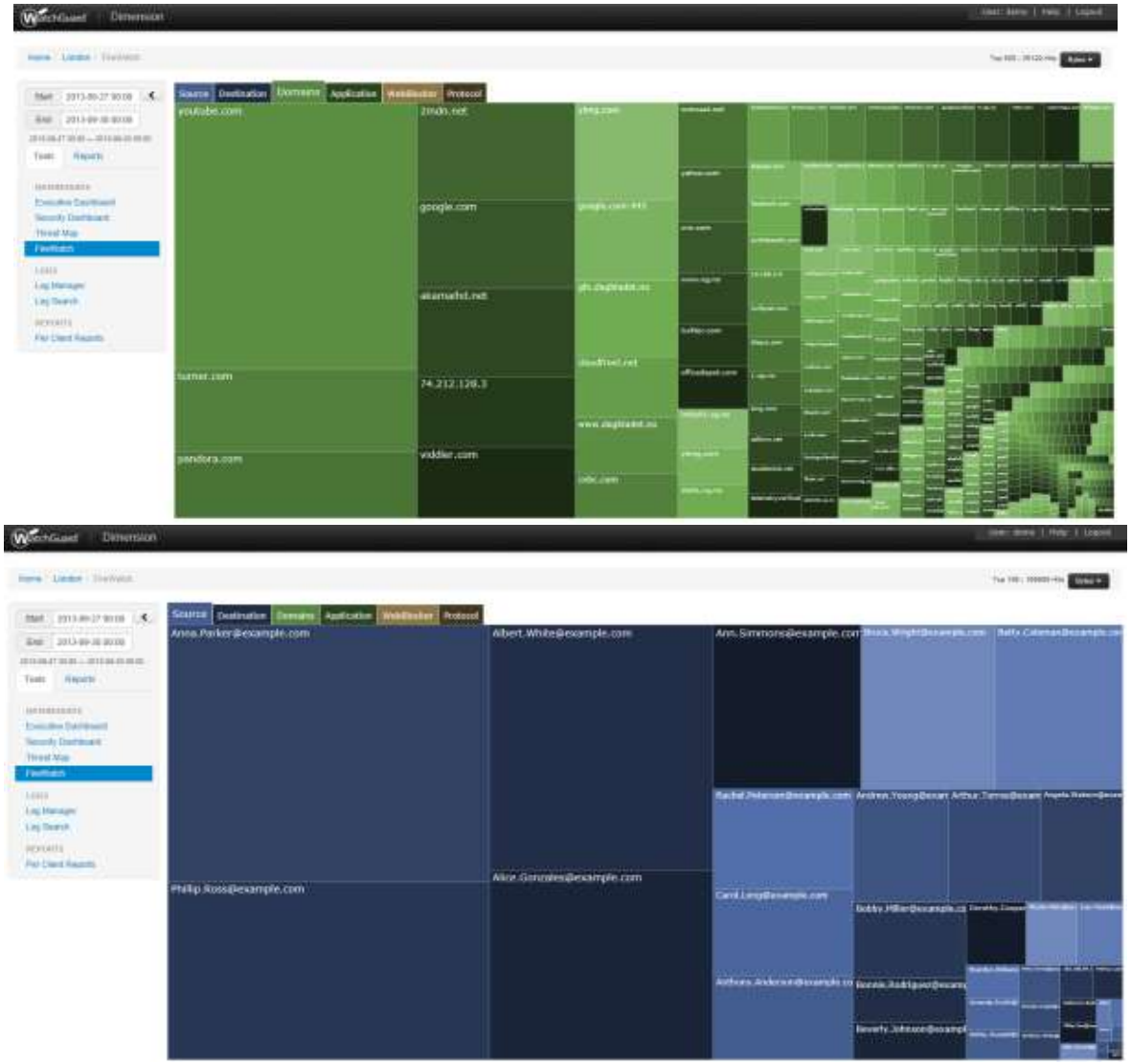
- Les sites internet les plus visités
- Les catégories correspondantes

Les applications les plus utilisées dans votre structure sont aussi mises en lumière.

Vous pourrez créer automatiquement un **rapport de synthèse** au format PDF afin de donner à des cibles non-techniques la visibilité sur ces informations.

A noter : Plus vous avez de services activés sur votre appliance WatchGuard et plus vous aurez de rapports disponibles.

FireWatch :



FireWatch filtre le trafic de sorte à instantanément **attirer votre attention graphiquement sur les informations les plus critiques relatives aux connexions et utilisateurs actifs**.

Par exemple :

- *Qui consomme le plus de bande passante ?*
- *Y a-t-il des modèles de trafic inhabituel ?*
- *Quels sont les sites Web les plus visités ?*
- *Quelles sont les applications utilisées par quels collaborateurs ?*
- *Quelles applications consomment le plus de bande passante ?*

Le tableau de bord de sécurité :

Le tableau de bord de sécurité présente **les éléments bloqués** sur votre réseau :

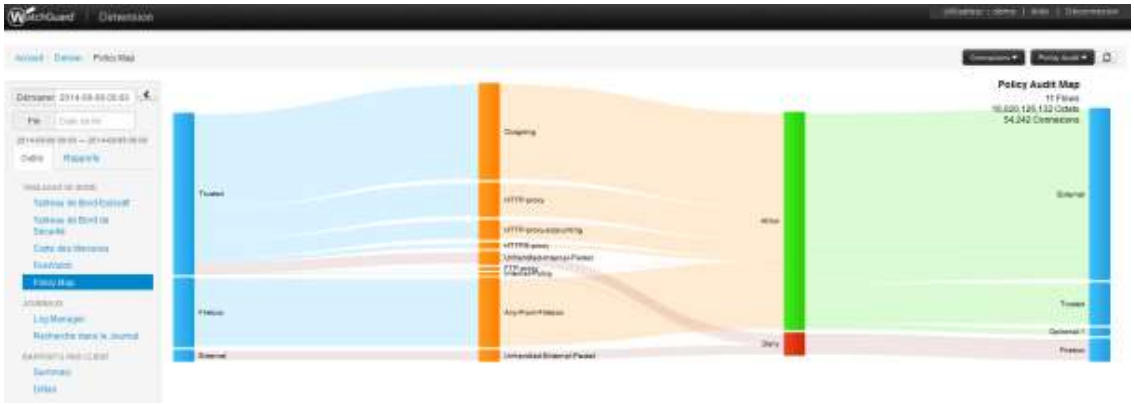
- Les utilisateurs
- Les machines
- Les destinations
- Les applications non autorisées par votre structure
- Les tentatives d'intrusion
- Les virus
- Etc…

Il est aisé de **contrôler les anomalies** qui ont été bloquées sur votre réseau et de croiser les données pour remédier aux différents problèmes comme une machine vérolée ou une application bloquée par mégarde pour un utilisateur.

La cartographie des menaces :

Identifiez instantanément **d'où viennent les menaces**, par emplacement. Il suffit de quelques clics pour savoir exactement quelle adresse IP bloquer pour protéger votre réseau.

Policy Map :



Policy Map est l'outil qui permet de voir les **flux** qui passent au travers du boitier UTM.

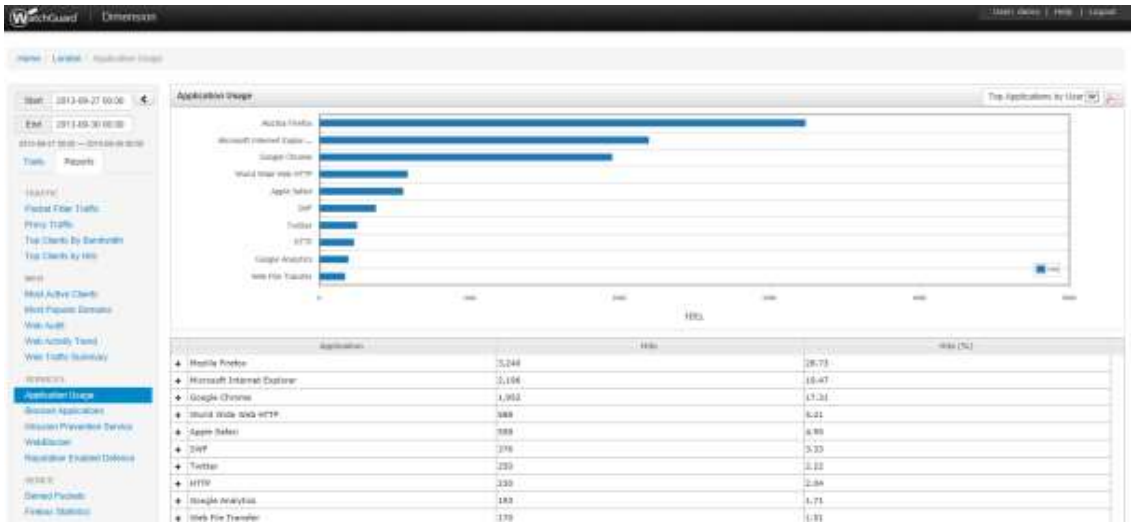
Ces flux peuvent être affichés en fonction :

- Des règles de Firewall
- Des services de sécurité
- Des catégories Web
- Du contrôle d'application
- Des attaques détectées par l'IPS
- Des malwares (Antivirus ou APT Blocker)
- Des violations DLP

Policy Map vous permet surtout d'**optimiser votre politique de sécurité** en affinant les règles jusqu'à ce que la situation corresponde à vos attentes.

Cette vision unique sur le marché vous permet aussi d'analyser l'usage de votre Firewall en fonction des flux de différentes natures et d'en voir la consommation en terme de connexions ou de bande passante.

Rapports et Logs dans WatchGuard Dimension :



Vous avez donc le choix entre plus de **70 rapports** complets, avec la possibilité de **préprogrammer des rapports à envoyer par e-mail** aux acteurs clés de votre entreprise.

Le **rapport exécutif** est un rapport global synthétique créé spécialement pour les cadres supérieurs, les directeurs informatiques, les responsables de la conformité et les dirigeants de petites entreprises.

Gestion Mutualisée :

Dimension permet la création d'utilisateurs avec des **droits spécifiques** par rapport aux différents boîtiers remontant leurs logs. Ainsi Dimension pourra être utilisé dans un cadre mutualisé pour plusieurs clients ou infrastructures avec la possibilité de ne permettre l'accès à certaines appliances qu'à certains utilisateurs. Cette utilisation est particulièrement adaptée pour un hébergement multi-clients.

Si vous souhaitez tester Dimension :

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

http://demo.watchguard.com

- login : demo
- mot de passe : visibility

Cliquez sur le boitier DENVER :

Puis sélectionnez les dates suivantes en haut à gauche de l'interface :

Bonne découverte !!!
(Est-ce que vous souhaitez convoquer Alice dans votre bureau tout de suite ?)

4. 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 illégalement à du contenu protégé par des droits 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.

WebBlocker fonctionne sur la base de données de WebSense qui est mise à jour régulièrement. La base permet de choisir parmi **130 catégories** pour le blocage des accès et l'administrateur peut voir dans l'interface de management le descriptif de chacune.

L'administrateur peut créer des **listes d'exceptions** URL pour les sites de confiance ou mettre sur **liste noire** des adresses IP ou des URLs spécifiques afin de bénéficier d'une protection personnalisée.

5. 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.

- autoriser l'utilisation de **Windows Live Messenger** pour la messagerie instantanée, mais refuser son utilisation pour le transfert de fichiers

- limiter les applications de diffusion **multimédia** à des moments spécifiques de la journée.

- signaler l'utilisation (ou la **tentative d'utilisation**) des applications par utilisateur au sein de l'entreprise

- bloquer l'utilisation de **YouTube, Skype et MSN** 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**.

La base d'applications permet de contrôler les applications par :

- **Catégorie** d'Applications
- **Application**
- **Comportement** de l'application

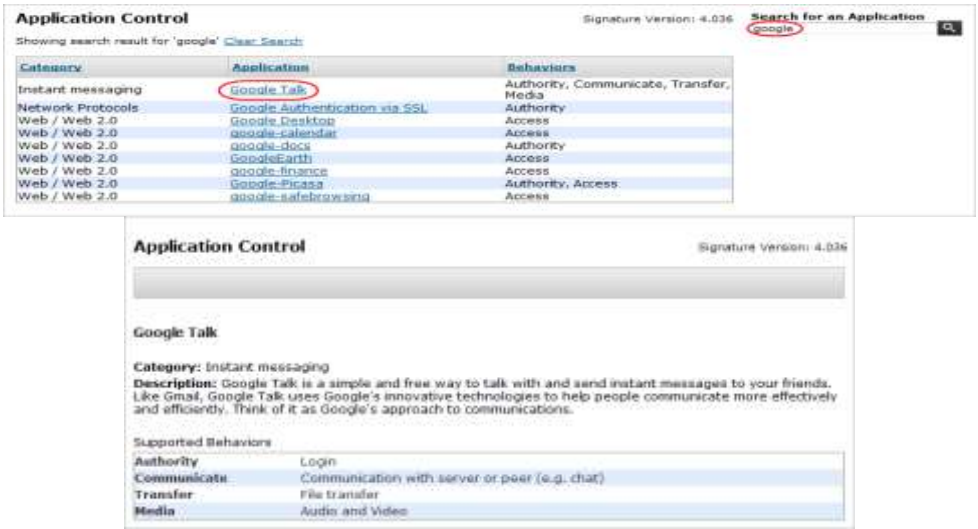
Il y a **20 catégories** différentes pour classer les applications, plus de **1800 applications** et bien plus de signatures pour différencier les comportements de chaque application.

Certaines applications (comme MSN par exemple) peuvent ainsi être **contrôlées finement** par leurs comportements :

- Authentification de l'application
- Transfert de fichiers via l'application
- Chat (conversation)
- Media (Webcam, audio etc)
- Jeux intégrés à l'application

L'interface d'administration propose également une fonction de **recherche** pour retrouver rapidement une application dans la base sans avoir à tout faire défiler.

D'autre part, nous avons mis en place un **portail internet** permettant de visualiser toutes les signatures de la base avec les explications pour chaque application et les comportements disponibles. Un administrateur peut donc vérifier à tout moment si une application est légitime ou non sur son réseau et peut la bloquer rapidement.



Enfin, la fonction de rapports intégrée aux Appliances WatchGuard fournit **5 rapports** différents concernant le contrôle d'applications.

6. L’anti-virus de passerelle

Les boitiers WatchGuard disposent d’un **moteur de détection des virus** en anti-virus de passerelle. Ce moteur et ses signatures sont basés sur la base Enterprise de AVG.

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.

Les signatures sont stockées sur la mémoire flash du Firebox et permettent d’analyser les flux HTTP, HTTPS, SMTP, POP3, FTP et les archives (ZIP, RAR, etc…)

L’activation de l’antivirus peut se faire par un assistant qui active l’antivirus sur l’ensemble des actions possibles du protocole. L’administrateur peut ensuite affiner s’il le souhaite.

Un expert en sécurité pourra se passer de l’assistant et configurer directement les différentes fonctions.

Cela permet au boitier d’avoir **deux niveaux d’administration** : expert ou normal.

Assistant d’activation de l’antivirus

7. 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 visibilité du comportement des logiciels malveillants et s'avère être le plus difficile à détecter par les logiciels malveillants avancés.

Voici les **types de fichiers analysés** par APT Blocker :

- tous les fichiers exécutables Windows
- les fichiers Adobe PDF
- les fichiers Microsoft Office, notamment Excel, Word, Visio, PowerPoint
- les fichiers Android Application Installer (.apk)

Les fichiers compressés, tels que les fichiers Windows .zip, sont décompressés.

Près de 88 % des logiciels malveillants actuels peuvent prendre une autre forme pour ne pas être détectés par les solutions antivirus basées sur les signatures...

« Malwise », IEEE Computers

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

A noter : Les manipulations effectuées dans cette vidéo sont effectuées dans un environnement virtuel, étanche et sécurisé. Nous vous déconseillons de les reproduire sur un PC standard.

8. L'Anti-Spam

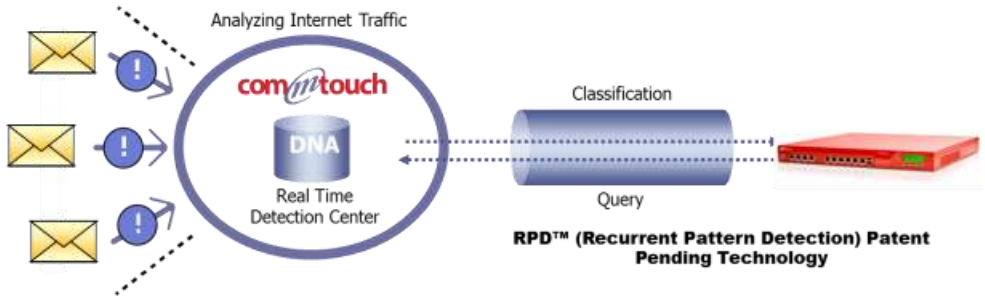
Le spam représente une part sans cesse croissante du trafic de courrier électronique mondial et reste la méthode la plus courante pour diffuser les virus. Il entrave le trafic sur le réseau et conduit des utilisateurs peu prudents vers des sites Internet malveillants conçus pour dérober des données sensibles sur les personnes ou les entreprises.

Vous pouvez **bloquer le spam**, malgré son caractère envahissant, avec le service spamBlocker.

SpamBlocker s'appuie sur une **détection en temps réel** pour vous protéger instantanément contre les vagues de spam. Il bloque en temps réel le spam et les virus qu'il transporte**.** La technologie Recurrent Pattern Detection (RPD™) de Cyren détecte les vagues de spam dès qu'elles émergent afin d'assurer une protection immédiate et constante.

SpamBlocker bloque le spam **indépendamment de la langue, du format ou du contenu du message**, même le spam basé sur des **images** que d'autres produits antispam laissent souvent passer. De plus, le **taux de faux positifs** de spamBlocker est proche de zéro, ce qui réduit considérablement la tache de l'administrateur ou de l'utilisateur dans la gestion des spams.

SpamBlocker peut s'appliquer sur les flux SMTP ou POP. Quand le Firebox reçoit un email, il en fait un hash qu'il envoie aux centres de détection de Cyren qui classifie le mail et renvoie l'information aux boitiers WatchGuard (Spam, Bulk, suspect ou Ham). En fonction de cette classification, une action est appliquée pour traiter l'email (suppression, quarantaine, tag ou autorisation).



Classification par Commtouch

SpamBlocker peut également utiliser un **serveur de quarantaine** (Quarantine Server). Il s'installe avec le WatchGuard Server Center sur une machine Windows pour pouvoir stocker les spams ou messages suspects. La quarantaine antispam est disponible uniquement pour le SMTP, pas pour le POP3.

Le Quarantine Server fournit des outils à la fois **pour les utilisateurs et les administrateurs**.

Les **utilisateurs** reçoivent des **notifications** d'e-mails périodiques à partir de Quarantine Server, indiquant qu'ils possèdent des messages stockés sur Quarantine Server.

Les utilisateurs peuvent alors cliquer sur une **URL** dans l'e-mail pour accéder à Quarantine Server en **mode web**.

Dans la quarantaine, l'expéditeur et l'objet des e-mails suspects sont affichés.
Dans le cas de courrier indésirable, ils peuvent libérer tous les messages électroniques de leur choix dans leur boîte de réception et supprimer les autres messages.

Les **administrateurs** peuvent configurer la quarantaine pour qu'elle supprime automatiquement les futurs messages provenant d'un domaine ou d'un expéditeur spécifique, ou ceux dont la ligne Objet contient une expression spécifique.

Vous pouvez afficher des **statistiques** sur l'activité de la quarantaine, telles que le nombre de messages mis en quarantaine au cours d'une plage de dates spécifique ou le nombre de messages réputés indésirables.

9. La prévention d'intrusions (IPS)

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

Ce moteur et ses signatures sont basés sur la technologie BroadWeb / TrendMicro.

Les signatures sont stockées sur la mémoire flash du Firebox et permettent d'analyser **tous les flux sur tous les protocoles**.

L'administrateur peut choisir des **actions spécifiques en fonction du niveau de sévérité** d'une signature. Ces actions sont :

- Autoblocage (mise en quarantaine de l'IP)
- Refus de la connexion
- Autorisation

L'administrateur peut également définir une **liste d'exception** des signatures qu'il ne veut pas voir actives.

L'apport de l'IPS WatchGuard est fondamentalement différent de nombreux autres produits du marché. En effet, l'IPS peut s'activer en plus des proxies et leur est donc complémentaire. Le proxy bloquera des attaques Zero Day pour compléter l'IPS.

En effet, le **proxy** bloque les attaques de manière immédiate par le fait de réécrire le protocole de manière saine et bloque donc par la même des attaques zero day. L'efficacité contre les attaques est donc une **mécanique combinée Proxies et IPS** tout en générant beaucoup moins de faux positifs qu'une technologie basée exclusivement sur les signatures.

10. Empêcher la fuite de données sensibles = DLP

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

Contrairement aux solutions DLP UTM des autres fournisseurs, 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.**

Principaux avantages :

• Configuration rapide des stratégies.
Une bibliothèque intégrée de plus de 200 règles permet au service informatique de rapidement créer et mettre à jour les stratégies DLP de l'entreprise.

• Protection automatique.
Toutes les données transmises par messagerie, Web ou FTP sont automatiquement analysées en fonction de votre ensemble de règles.

• Couverture étendue.
Le service WatchGuard DLP peut analyser les données issues de plus de 30 types de fichiers, y compris les fichiers Excel, Word, Visio, PowerPoint et PDF.

• La conformité en toute simplicité.
Des détecteurs sont intégrés pour le respect des normes de conformité PCI DSS et HIPAA.

• Contrôles internes.
Maintenez le flux des communications d'entreprise vitales grâce à différentes options de correction. Vous pouvez choisir de bloquer ou journaliser les transmissions signalées, ou de les mettre en quarantaine à des fins d'analyse.

• Simplicité d'administration.
Utilisez la même console intuitive pour administrer le service DLP que celle que vous utilisez déjà pour tous les autres services exécutés sur votre plateforme UTM de WatchGuard.

• Règle spécifique à votre structure :
Il est possible de définir une custom rule pour le DLP avec une recommandation de 15 phrases maximum d'une longueur maximum de 127 caractères.

11. VPN

Le VPN (réseau privé virtuel) permet de réaliser des interconnexions privées à travers un réseau public comme Internet par exemple.

Les boitiers WatchGuard supportent les deux types de VPN :

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

Voici le **nombre de connexions VPN disponibles de base** sur les boitiers WatchGuard :

	Firebox T10/T10-W	Firebox T30/T30-W	Firebox T50/T50-W	Firebox M200	Firebox M300	Firebox M400	Firebox M440	Firebox M500	XTM 850	XTM 860	XTM 870	XTM 870-F
VPN tunnels												
Branch Office VPN	5	40	50	50	75	100	300	500	5000	6000	7000	7000
Mobile VPN IPSec	5	25	50	75	100	150	200	500	10000	12000	14000	14000
Mobile VPN SSL/L2TP	5	25	50	75	100	150	200	500	10000	12000	14000	14000

Le **Branch Office VPN** permet de relier des sites d'une compagnie entre eux (Intranet) ou bien de plusieurs compagnies différentes (Extranet). Cette interconnexion se réalise sur un réseau public et nécessite donc une sécurisation forte par des techniques de chiffrement, authentification et contrôle d'intégrité. Cela nécessite également des mécanismes de Pare-feu pour se protéger du réseau public en tant que tel. Les Branch Office VPN sont réalisés avec le protocole IPSEC. Il est possible de faire du Failover de VPN en coupure.

Le **VPN Mobile** permet à un utilisateur de se connecter aux ressources de l'entreprise, par exemple dans le cadre du télétravail ou d'un utilisateur en déplacement. L'utilisateur se connecte à un réseau public via une connexion locale à un fournisseur d'accès. Il utilise ensuite un logiciel Client **IPSEC** ou **SSL** pour créer un tunnel jusqu'au site de sa société. WatchGuard fournit les deux types de clients.

En plus des clients fournis par WatchGuard (Shrewsoft pour le client IPSEC), WatchGuard supporte également les clients IPSEC et L2TP natifs sur les Iphone et Ipad ainsi que sur Android.

Client IPSEC du Firebox

Client léger SSL

12. Quelques caractéristiques additionnelles

Traitement multi-cœur

En exploitant la puissance du traitement multi-cœur, la plateforme exécute simultanément tous les moteurs d'analyse, assurant une protection optimale et un débit ultrarapide.

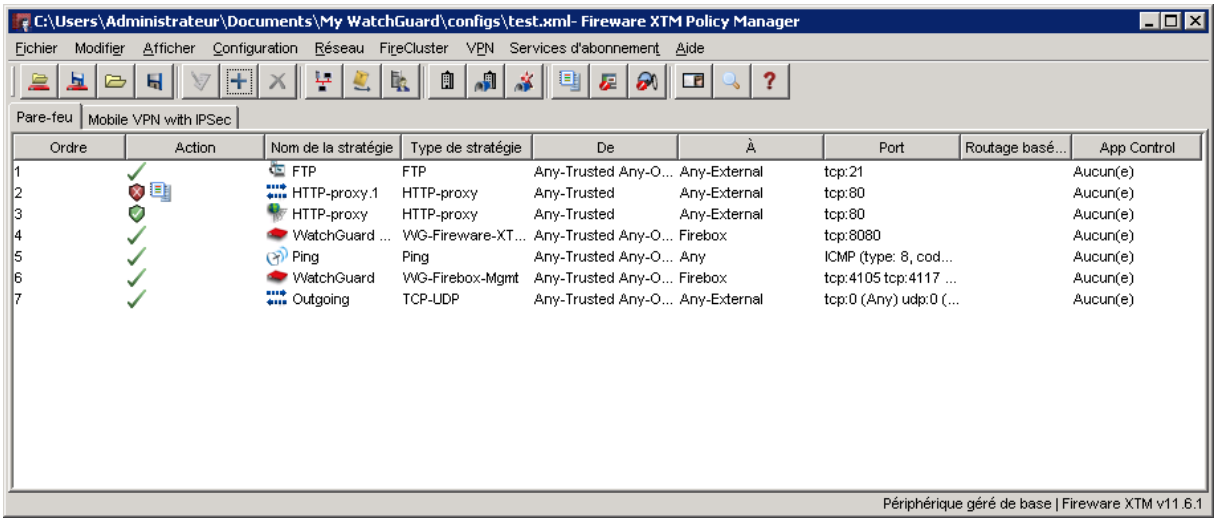
Les ressources sont allouées en fonction du flux de données et des services de sécurité requises par ces données.

Par exemple, si le filtrage Web a besoin de plus de puissance, des processeurs supplémentaires y sont automatiquement alloués pour que le trafic Internet reste fluide et votre entreprise protégée.

Ordonnancement automatique

La gestion des règles de sécurité est réalisée par WatchGuard de manière unique sur le marché des firewalls.

En effet les stratégies de sécurité qui composent la politique de sécurité sont par défaut **classées dans un ordre automatique**.



Quand on ajoute une nouvelle règle, celle-ci vient automatiquement se placer au bon endroit pour garantir la cohérence de la politique de sécurité globale selon un système de précédence logique.

Ce système offre de nombreux avantages à l'administrateur. L'ajout d'une règle est bien plus rapide que sur un système traditionnel manuel. Ce système permet de se concentrer sur la règle elle-même et l'implémentation d'une règle de la politique de sécurité et enlève le fardeau du positionnement par rapport aux autres règles.

La gestion au jour le jour en est facilitée. Si la personne qui connait bien l'ensemble des règles est absente, cela n'empêche pas les autres administrateurs ou l'infogéreur de rajouter une règle rapidement sans risque de remettre en question le système de sécurité et sans avoir besoin de revoir et connaitre l'ensemble des règles existantes. C'est le Policy Manager qui se charge de conserver les règles dans le bon ordre.

L'ordonnancement automatique est également un très bon outil pour vérifier que l'implémentation d'une règle correspond bien à la politique de sécurité globale. Si une règle ne se positionne pas comme on l'aurait imaginé, il y a surement un delta entre son implémentation et la politique de sécurité voulue.

C'est aussi un mécanisme intéressant pour le support technique. En effet, lors de l'ouverture d'un incident technique, le support n'a pas besoin de vérifier l'ordre des règles. Si les règles sont automatiques, le support peut se focaliser sur le problème et n'a pas besoin de vérifier une potentielle erreur d'ordonnancement de la part de l'administrateur.

Bien sûr il est possible de désactiver cet ordonnancement automatique et de passer en mode manuel pour ceux qui voudraient vraiment gérer l'ordre par eux même.

Ajouté à ce système de classification des règles, le Policy Manager dispose d'un outil de recherche dans les règles pour trouver les règles qui utilisent un port spécifique, une IP spécifique etc.

Voix sur IP et Visioconférence

Si, dans l'entreprise, il est nécessaire de faire appel à la technique de voix sur IP, il est possible d'ajouter une règle de proxy afin d'ouvrir les ports nécessaires à l'activation de la voix sur IP par le biais du boitier WatchGuard.

Authentification Utilisateurs

L'authentification restreint l'accès aux ressources de votre choix à des utilisateurs ou groupes d'utilisateurs en fonction de leur compte (login/mot de passe).

Un boitier WatchGuard permet d'activer l'authentification avec les serveurs suivants :

- Firebox (base locale)
- Active Directory
- RADIUS
- LDAP
- SecurID

Le mécanisme d'authentification permet ainsi de définir une politique de sécurité en fonction des groupes d'utilisateurs et de leurs fonctions.

Traffic Management par Application

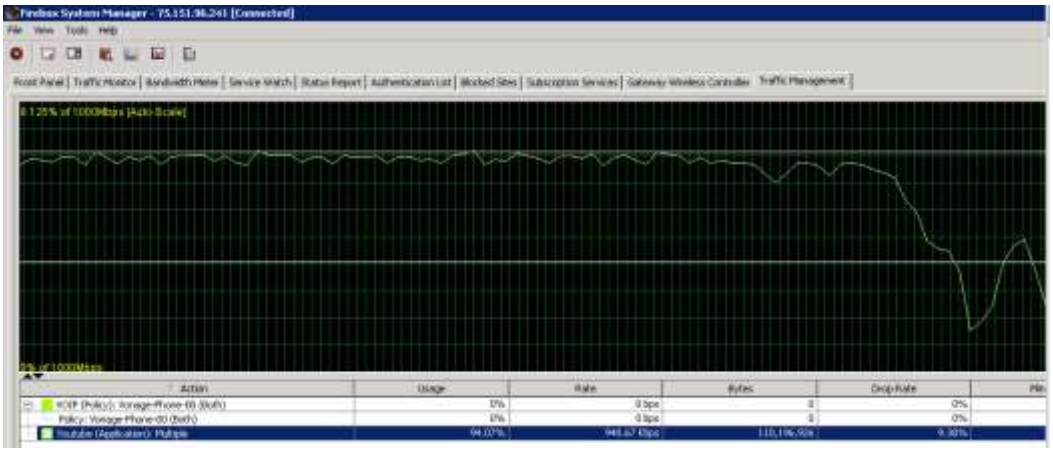
Il devient nécessaire de pouvoir fixer des limites de bande passante pour certaines applications spécifiques ou catégories d'applications.

Par exemple, de nombreux problèmes de bande passante peuvent venir d'un ou plusieurs utilisateurs abusant de streaming sur le réseau de l'entreprise.

Comme il est souvent difficile de tout interdire, la meilleure solution est de limiter l'usage de ce type de trafic.

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

Le boitier WatchGuard offre des outils permettant aussi de **contrôler** que les actions de Traffic Management sont bien respectées. Dans l'outil de Monitoring, un onglet spécifique permet de visualiser chaque action et d'en vérifier les effets graphiquement.



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.

13. Administration des Appliances Firebox

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

- Interface Web
- Client lourd installé sur un PC
- Commande en Ligne

Le client lourd

Le client lourd est très apprécié des administrateurs de solutions WatchGuard.

Il se connecte à l'appliance et récupère le **fichier XML de configuration**. Une fois récupéré, il permet de modifier la configuration.

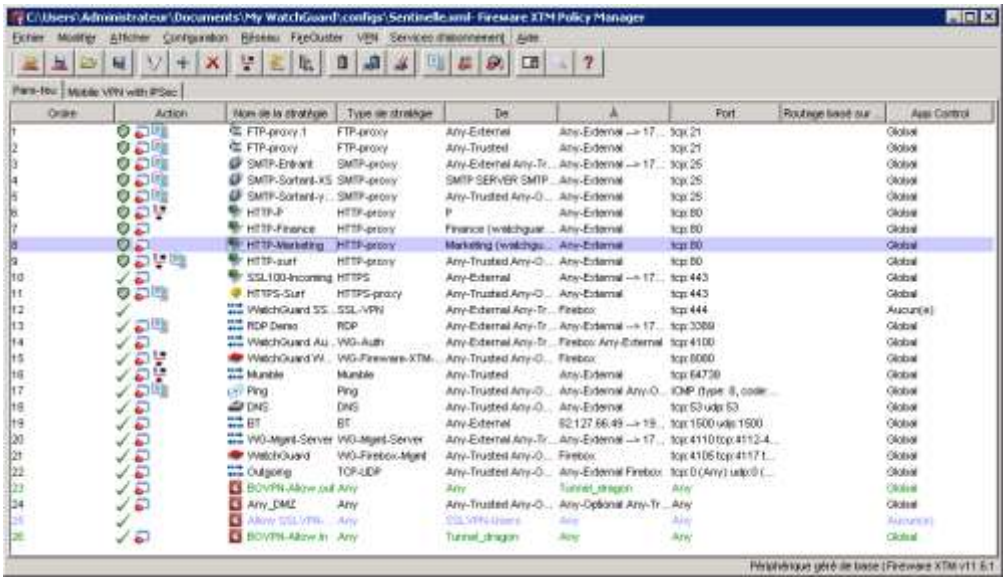
Ces modifications de configuration sont d'abord effectuées sur le fichier de configuration XML et ne sont appliquées que lorsque cette configuration est sauvegardée en retour sur l'appliance WatchGuard.

Cette philosophie de travail sur la configuration en mode « **offline** » est idéale pour gérer un équipement de sécurité en toute sérénité et sans latence.

Il permet également de gérer facilement **différentes versions** de la configuration ou même un **historique des configurations**.

Il permet aussi de **relire une configuration** ou même de **préparer une nouvelle configuration** sans avoir besoin d'accéder à l'appliance. Il suffit d'ouvrir le fichier XML localement ou d'en créer un nouveau comme on ouvrirait un document Word.

L'autre atout du client lourd est son intuitivité. La **lisibilité de la politique de sécurité** est une priorité pour permettre à l'administrateur de s'y retrouver vite. D'où les différentes fonctions simplifiant la vie de l'administrateur comme la classification automatique des règles, l'ajout de règle par simple bouton « + », les actions réutilisables sur les règles (action de proxy, de filtrage web, de qualité de service, de planification d'horaires), une barre d'outils pour accès rapide aux différentes fonctions (et même des raccourcis sur les fonctions), etc.…

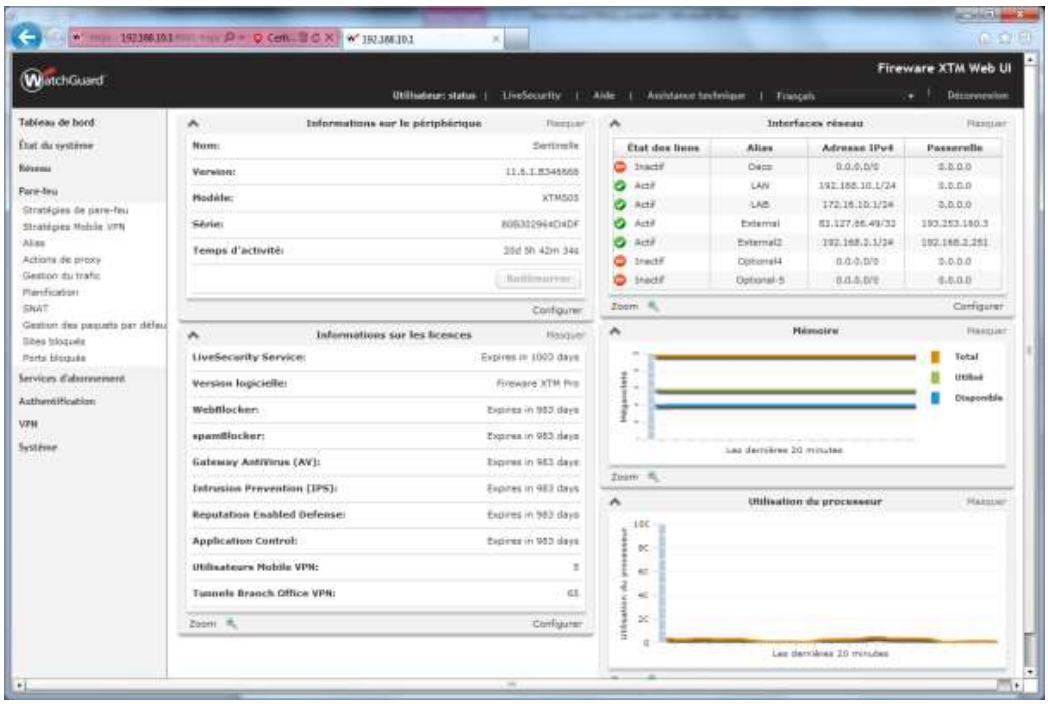


Interface de Management Web

A partir de Fireware en v11, tous les modèles peuvent être configurés via une **Interface WEB.**

L'interface WEB de configuration est un outil idéal complémentaire au client lourd quand l'administrateur a besoin d'effectuer une modification à partir d'un poste qui n'a pas de client installé, ou bien qui n'est pas un système Windows.

L'interface WEB est compatible avec le cluster (une fois celui-ci monté).



14. 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.

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**.

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.

Les points d’accès existent en trois modèles : AP100, AP102 et AP200. Elles permettent aux administrateurs d'appliquer facilement les stratégies de sécurité aux ressources filaires et sans fil simultanément, ce qui est essentiel lorsqu'il s'agit de renforcer les normes de sécurité sur l'ensemble de l'infrastructure réseau.

AP100, AP102 et AP200 supportent les normes Wifi 802.11a/b/g/n en mode MIMO 2x2 :2 (Multiple Input, Multiple Output), à savoir 2 antennes en réception et 2 antennes en émission pour 2 flux spectraux de données.

	AP100	AP200	
Matériel - informations détaillées			
Nombre de radios	1	2	
Fréquences supportées	2,4 GHz ou 5 GHz (au choix)	Radio 1 = 5 GHz	Radio 2 = 2,4 GHz
Caractéristiques des radios	Deux flux spatiaux MIMO 2x2		
Fréquences supportées*	2,400-2,474 GHz, 5,150-5,250 GHz, 5,250-5,350 GHz, 5,470-5,725 GHz, 5,725-5,850 GHz		
Antenne	4 antennes internes, omnidirectionnelles		
Gain d'antenne de crête	3 dBi	4 dBi	3 dBi
Puissance d'émission maximale*	2,4 GHz = 17 dBm 5 GHz = 20 dBm	5 GHz = 20 dBm	2,4 GHz = 21 dBm
Débit	300 Mbps	600 Mbps	
SSID	8	16	
Boîtier plénum (résistant au feu)	Non	Oui	
Paramètres de sécurité	WPA-PSK, WPA2-PSK, WPA2-PSK mode mixte, WPA2-Enterprise 802.1x, TKIP, AES		
Ethernet	1 GbE		
Options d'alimentation	PoE, adaptateur secteur		
MTBF	> 500 000 heures		
Sécurité physique	Encoche de sécurité Kensington		
Normes IEEE prises en charge	802.11a/b/g/n, 802.11i, 802.11x, 802.11af/at		
Support et maintenance	Un abonnement de 1 an ou de 3 ans au service LiveSecurity® pour la garantie du matériel comprend le remplacement anticipé, le support technique et les mises à jour logicielles		
Déploiement	A l'intérieur		

Environnement	
Température de fonctionnement	0 à 40° C
Humidité relative de fonctionnement	5 % à 90 % sans condensation
Température de stockage	-40° à 70° C
Humidité relative hors fonctionnement	5 % à 90 % sans condensation
Adaptateur secteur	
Tension en entrée	100-240 Vca
Fréquence	50/60 Hz
Courant entrant maximal	400 mA
Tension de sortie	12 V
Courant sortant	1 250 mA
Injecteur PoE (en option)	
Norme IEEE	802.3af
Tension en entrée	100-240 Vca
Tension de sortie	56 V
Alimentation de sortie	15,4 W
Dimensions	
Dimensions du produit	16,5 x 4,4 cm
Dimensions du colis	17,8 x 18,4 x 11,4 cm
Poids du produit	0,34 kg
Poids du colis (comprend l'adaptateur AC, le kit de montage, etc.)	0,91 kg
Kit de montage	Inclus
Certifications	
Sans fil	FCC, IC, CE
Sécurité	NRTL/C, CB, CE
Contrôle des substances dangereuses	WEEE, RoHS, REACH

Nombre de Bornes Wifi recommandées par Contrôleur

Le **dimensionnement** du contrôleur associé avec les bornes dépend partiellement du nombre de bornes disposées sur le réseau. Ceci étant dit, la charge générée par la prise en compte des points d'accès eux-mêmes reste minime.

La recommandation suivante est donnée à titre indicatif uniquement, sans aucune limitation dans le code :

Modèles XTM	Série 2[**]	Série 3	Série 5	Série 5	Série 800	XTM 1050	Série 1500	XTM 2050	XTM 2520
Nombre[1] de points d'accès	jusqu'à 5	jusqu'à 15	jusqu'à 35	jusqu'à 70	jusqu'à 100	jusqu'à 100	jusqu'à 100	jusqu'à 100	jusqu'à 100

Dans la pratique, le contrôleur étant également le firewall de l'entreprise, on dimensionnera l'appliance WatchGuard en fonction de la charge de trafic (dimensionnement classique en Firewall ou UTM) tout en prévoyant un peu de marge pour tenir compte de la charge CPU et mémoire engendrée par la fonction de contrôleur (10-15% maximum du global).

Découverte Automatique

Le contrôleur Wifi WatchGuard est capable de **détecter automatiquement** les bornes Wifi nouvellement installées sur un réseau.

Normes Wireless supportées

Les Points d'accès Wifi WatchGuard supportent l'ensemble des normes 802.11a/b/g/n pour une compatibilité étendue avec les différents clients wifi.

La norme IEEE 802.11n est la plus récente (standardisée en 2009) et permet de fournir un accès wifi avec un débit de 300Mbps théorique (à partager et dans des conditions de propagation optimum).

Les Points d'accès Wifi WatchGuard peuvent se mettre en mode mixte pour supporter les différentes normes en même temps.

Radios

L'AP 100 et 102 peuvent diffuser sur une seule fréquence Radio (2.4Ghz ou 5Ghz).
L'AP 200 peut lui diffuser sur deux fréquences Radio différentes (2.4Ghz et 5Ghz)

La fréquence la plus couramment utilisée est la fréquence 2.4Ghz du fait de la portée supérieure.

La fréquence 5Ghz peut être utilisée pour diffuser dans des environnements ou la fréquence 2.4Ghz est congestionnée.

Roaming

Lorsque le même SSID est propagé sur les différentes bornes wifi, les clients Wifi (portables/smartphone etc.) peuvent passer de l'une à l'autre très rapidement et sans aucune reconfiguration ou reconnexion du client.

Les clients Wifi sélectionnent la borne la plus puissante pour basculer dessus et continuer ses transferts et communications de manière transparente.

Power Over Ethernet (PoE)

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

WatchGuard distribue également des injecteurs POE compatibles (disponible en option).

Ces équipements POE doivent suivent les spécifications **IEEE 802.3af**. Toute autre technologie POE pourra endommager la borne (ne pas utiliser des équipements IEEE 802.3at « High Power Over Ethernet » ou des équipements non-standards)

Injecteur POE

Nouvelles bornes : Les AP300, annoncées pour le 13-Jan-2016

Les caractéristiques de ces nouvelles bornes AP300 sont les suivantes :

- 802.11ac
- 3x3
- Dual Radio
- Avec support du Fast Roaming

Ce document sera remis à jour mi-janvier 2016 après la sortie de ces nouvelles bornes.

Reporting Wifi intégré à WatchGuard Dimension

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

Ces rapports permettent de vérifier l'installation de l'architecture Wifi et son bon dimensionnement ainsi que toutes ses évolutions. S'il y a trop d'utilisateurs sur une même borne et que la borne sature en débit, il sera très facile de le détecter et d'y remédier.

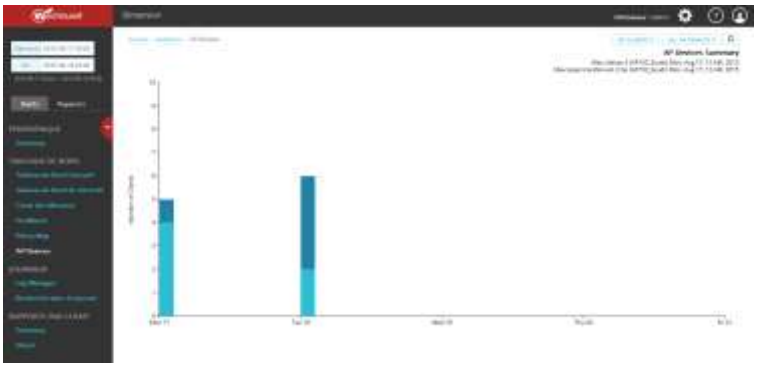


Tableau de Bord Wifi

Rapport de synthèse des AP

Evolution de l'usage sur plusieurs jours

15. Les modes d'acquisition d'un boitier WatchGuard :

En acquisition traditionnelle

Vous achetez le boitier avec une certaine durée de maintenance (1 an, 3 ans, etc…)

Il existe deux types de boitiers :

1 - Un boitier WatchGuard acquis en **Live Security / Standard Support** :

C'est un Firewall / Proxy / avec des connexions VPN mais sans services de sécurité additionnels.

2 – Un boitier acquis avec un **Security Bundle** :

Il intègre les services de sécurité suivants :

- Anti-virus
- Anti-spam
- IPS
- Filtrage d'URL
- Contrôle d'application
- Autorité de réputation web
- Dimension Visibility

En option, trois modules additionnels peuvent être acquis :

- APT Blocker
- DLP
- Dimension Command = Rajoute la possibilité de réaliser des taches d'administration dans Dimension Visibility

En mode locatif (MSSP) :

Il est aussi possible d'acquérir une appliance WatchGuard en mode locatif :

Il existe deux types de boitiers :

1 - En ALL SERVICES :
l'appliance WatchGuard
+ les composantes d'un Security Bundle
+ APT Blocker + DLP + Dimension Command

2 - En SUPPORT ONLY :
l'appliance WatchGuard en Firewall / Proxy / VPN uniquement