

## WatchGuard® XTM 1050

### Idéal pour les sièges/centres de données (jusqu'à 5 000 utilisateurs)

Les entreprises qui dépendent de réseaux à haut débit « always-on » devaient payer jusqu'à maintenant des sommes élevées pour assurer leur sécurité. Aujourd'hui, elles disposent d'une nouvelle appliance de sécurité ultra performante, le WatchGuard® XTM 1050, qui offre une sécurité de niveau entreprise entièrement extensible à un prix abordable.

### Quel est l'avantage d'une solution de sécurité tout-en-un ?

Réduire la perte de temps et les coûts liés à la gestion de multiples produits de sécurité. Votre personnel informatique peut se consacrer davantage à d'autres aspects de l'administration réseau et vos coûts de matériel et de support technique sont moins élevés.

**« Un pare-feu XTM est un pare-feu UTM dopé, avec une kyrielle de nouvelles fonctions qui exigeraient, pour des produits concurrents, une seconde appliance. »**

*TechWorld Magazine*  
sur le nouveau super  
pare-feu XTM.



### Un WatchGuard XTM 1050 garantit à votre réseau :

#### SÉCURITÉ

- L'inspection de contenu « Layer 7 » détecte et bloque les menaces que ne peuvent déceler les pare-feu dynamiques
- La protection étendue est due à une sécurité avancée sur HTTP, HTTPS, FTP, SMTP, POP3, DNS et TCP/UDP
- Les abonnements de sécurité renforcent la protection dans les zones d'attaques principales et assurent une gestion unifiée complète des menaces
- Inclut le VPN SSL intégré qui assure un accès simple au réseau, partout et à tout moment

#### PUISSANCE

- Débit du pare-feu de 10 Gbps et débit du VPN de 2 Gbps
- 12 ports Gigabit Ethernet avec architecture Line-Speed et 4 ports Gigabit fibre en option
- Chacun des 12 ports peut être configuré comme Interne, Externe ou Optionnel, ce qui optimise leur utilisation
- Gère un cluster de deux appliances comme une seule unité logique avec des fonctions de haute disponibilité et d'équilibrage de la charge qui doublent presque la performance d'un seul boîtier

#### EFFICACITÉ

- L'interpréteur de commandes (CLI) contrôlable par script prend en charge l'interopérabilité et simplifie l'intégration à l'infrastructure existante, ce qui facilite les déploiements importants
- Le contrôle et la production de rapports interactifs en temps réel vous donnent une vue sans précédent sur l'activité de sécurité de votre réseau, ce qui vous permet de lancer immédiatement les actions préventives ou correctives
- Une console de gestion intuitive administre de façon centralisée toutes les fonctions de sécurité
- Le contrôle d'accès à base de rôles (RBAC) inclut des rôles prédéfinis et des séries de privilèges, et permet à l'administrateur principal de créer des rôles personnalisés pour assurer un contrôle granulaire
- La création de VPN pour succursales/bureaux distants par simple « drag-and-drop » assure la connectivité des bureaux distants en 3 clics

#### FLEXIBILITÉ

- La sécurité de l'établissement de la communication pour la voix sur IP fait que vous n'avez pas à « cloisonner le pare-feu » pour profiter des avantages de coût générés par la voix sur IP
- Le routage dynamique et la régularisation du trafic optimisent la flexibilité et l'efficacité du réseau
- Le routage en fonction de règles vous permet de spécifier l'interface sortante par service pour améliorer la gestion de la bande passante et réduire les coûts
- L'équilibrage de la charge des serveurs facilite la protection des « fermes de serveur » pour le commerce électronique à destination du grand public
- L'équilibrage de charge à travers de multiples connexions WAN, la haute disponibilité (active/active) et les liens de secours WAN et VPN augmentent la performance, la redondance et la fiabilité
- Le grand choix de VPN permet un accès distant flexible

#### CAPACITÉ

- Une sécurité à multiples couches assure la sécurité de votre réseau
- La puissance et la performance du XTM 1050 vous permettent de gérer un volume de trafic élevé
- Sa gestion centralisée et intuitive vous apporte le contrôle nécessaire pour une administration efficace de votre réseau
- Ses fonctions réseau avancées garantissent le bon fonctionnement de votre réseau

## Spécifications techniques du XTM 1050

### Sécurité

**Pare-feu** Inspection dynamique, inspection de la couche applicative, pare-feu de proxy HTTP, HTTPS, SMTP, FTP, DNS, TCP, POP3

**Proxies d'application** HTTP, HTTPS, SMTP, FTP, DNS, TCP, POP3

**Protection contre les menaces** Bloque les spywares, les attaques de déni de service/déni de service distribué, les attaques via les paquets fragmentés ou mal formés et d'autres

**Voix sur IP** H.323, SIP, sécurité de l'établissement de la communication et de la session

**spamBlocker** Disponible avec le Bundle Sécurité

**WebBlocker** Disponible avec le Bundle Sécurité

**Antivirus de passerelle** Disponible avec le Bundle Sécurité

**Service de prévention d'intrusions** Disponible avec le Bundle Sécurité

**VPN et authentification** Disponible avec le Bundle Sécurité

**Chiffrement** DES, 3DES, AES 128, 192 et 256 bits

**IPSec** SHA-1, MD5, clé IKE prépartagée, importation de certificats de tiers

**SSL** Client léger, Web Exchange

**PPTP** Serveur et passthrough

**Lien de secours VPN** Oui

**Single Sign-On** Authentification transparente sur Active Directory

**XAUTH** Radius, LDAP, Windows® Active Directory

**Autre authentification des utilisateurs** VASCO, RSA SecurID, basée sur Internet, locale

**Performance**

**Débit du pare-feu\*** 10 Gbps

**Débit du VPN\*** 2 Gbps

**Sessions concomitantes** 2 500 000

**Nœuds pris en charge (LAN IP)** Illimités

**Tunnels de VPN pour succursale/bureau distant** 2 500

**Tunnels de VPN mobiles (IPSec/SSL)** 2 500/2 500

**Fonctions réseau**

**Système d'exploitation** Firewall™ Pro

**Affectation d'adresses IP** Statique, DynDNS, PPPoE et DHCP (serveur, client, relais)

**Routage** Statique, dynamique (BGP4, OSPF, RIP v1/v2) et basé sur des règles

**QoS** 8 files d'attente prioritaires, diffserv, Modified Strict Queuing

**Prise en charge VLAN** 500 VLAN en mode bridge, tagging et routé

**Haute disponibilité** Active/Passive, Active/Active avec FireCluster

**NAT** Statique, dynamique, 1:1, IPSec NAT Traversal, NAT basé sur des règles, IP virtuel

**Autres fonctions réseau** Indépendance des ports, lien de secours WAN, équilibrage de charge, mode transparent/drop-in

### Gestion

**Plate-forme de gestion** WatchGuard System Manager v.11

**Avertissements et notifications** SNMP, v2/v3, e-mail, alertes sur le système de gestion

**Prise en charge du serveur** Création de journaux/rapports, mise en quarantaine, WebBlocker, gestion

**Interface utilisateur Web** Prend en charge les systèmes d'exploitation Windows, Mac, Linux, Solaris et les navigateurs les plus courants

**CLI** Avec Direct Connect et scripts

\* Le débit varie selon l'environnement et la configuration

### Matériel

**Interfaces 10/100/1000** 12

**Port série** 1

**Port USB** 1

**Dimensions** 430 mm x 510 mm x 88 mm

**Dimensions sous emballage** 18,4 x 54,6 x 48,2 cm

**Poids emballé** 6,25 kg

**Tension** 100-240 VAC autosensing

**Consommation électrique** 312 watts (1060 BTU) max.

**Montage en rack** Monté en rack 2U, supports inclus (avec rails arrière 29')

**Accessoires** Module en fibre, sources d'alimentation universelles redondantes échangeables à chaud, ventilateurs remplaçables et échangeables à chaud

**Oui**

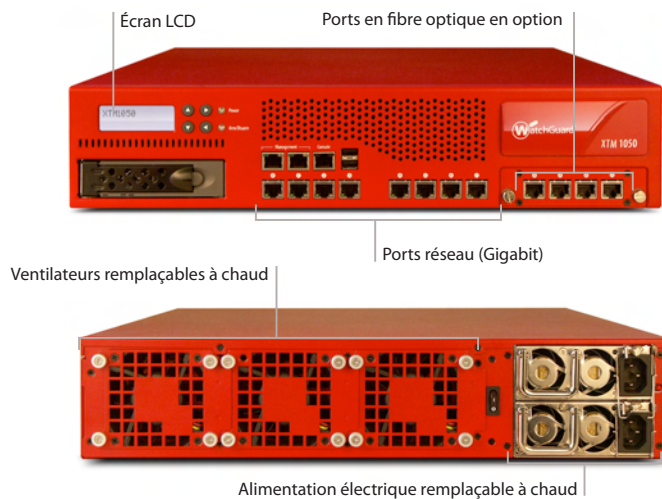
**Conformité DEEE/RoHS** ICESA, FIPS, EAL4 en instance

**Certifications des produits de sécurité** NRTL/C, CB

**Certifications de sécurité produit** Service LiveSecurity® avec garantie du matériel, support technique, mises à jour logicielles et alertes sur les menaces

**Support technique** Renouvelable par abonnement de 1, 2 et 3 ans

- Service de niveau Gold disponible pour un support 24h/24 7j/7 et un temps de réponse d'une heure



### Choisissez le bundle et profitez de tous ses avantages.

Le Bundle Sécurité de WatchGuard comprend tout ce qui suit :

- Une appliance WatchGuard® XTM 1050
  - spamBlocker\* avec détection des virus émergents
  - WebBlocker\* avec inspection HTTP et HTTPS
  - L'antivirus de passerelle\* pour une protection basée sur les signatures contre les menaces connues
  - Le service de prévention des intrusions\* pour une protection en ligne contre les attaques conformes aux normes du protocole, mais transportant du contenu malveillant
  - Le service LiveSecurity\*\* avec garantie du matériel, mises à jour logicielles gratuites, support technique expert et alertes de sécurité
- Une bonne affaire quand vous les achetez tous ensemble !

Adresse : WatchGuard Technologies France, La Grande Arche - Paroi Nord, 92042 Paris La Défense • Site Internet : [www.watchguard.fr](http://www.watchguard.fr) • Tél. : +33 1 40 90 30 35

• E-mail : [france@watchguard.com](mailto:france@watchguard.com) • Service commercial aux États-Unis : 1.800.734.9905 • Service commercial international : +1.206.613.0895

Ce document ne contient aucune garantie expresse ou tacite. Toutes les spécifications sont susceptibles de changer et tous les futurs produits, fonctionnalités et services attendus seront fournis à partir du moment où ils seront disponibles. ©2009 WatchGuard Technologies, Inc. Tous droits réservés. WatchGuard, le logo WatchGuard, Firebox, Firewall et LiveSecurity sont des marques déposées ou non déposées de WatchGuard Technologies, Inc. aux États-Unis et/ou dans les autres pays. Toutes les autres marques appartiennent à leurs propriétaires respectifs. Numéro de référence WGCE66570\_040309