



Une sécurité Gigabit 10/100/1000 pour les réseaux exigeants

- **Une solution complète de gestion unifiée des menaces** qui protège les réseaux des attaques malveillantes
- **Véritable protection « zero day »** bloquant de façon proactive les nouvelles menaces
- **Nouveau ! VPN SSL intégré**
- **Huit ports Ethernet Gigabit 10/100/1000** pour une connectivité à haut débit
- **Fonctions réseau avancées** permettant le contrôle des ressources, la régularisation du trafic et l'augmentation de la disponibilité du réseau
- **Configuration et administration simples** des appliances Firebox X et de leurs fonctions
- **Abonnements de sécurité intégrée** pour une protection plus granulaire



Technologie écologique

Firebox® X Peak™ est la gamme la plus performante d'appiances de gestion unifiée des menaces (unified threat management ou UTM) de WatchGuard®. Prêts à l'emploi, ces appareils vous offrent une protection « zero day », avec un débit du pare-feu atteignant plusieurs gigabits par seconde. Intégrant des fonctions de sécurité puissantes et des capacités réseau avancées, ils forment une solution globale exceptionnelle, parfaitement adaptée aux environnements réseau les plus exigeants.

Solution complète de gestion unifiée des menaces

Le Firebox X Peak assure la sécurité la plus complète dans sa catégorie. Il conjugue des proxies applicatifs intégrés, un pare-feu dynamique et un réseau privé virtuel complet avec des abonnements de sécurité, offrant ainsi des défenses multicouches avancées. Les fonctions antispyware, prévention des intrusions, antivirus, antispam avec détection des virus émergents et filtrage des URL sont harmonieusement intégrées à une même appliance fiable. Le résultat : un investissement en temps et en argent bien moins élevé que celui engendré par l'administration de solutions à points multiples.

Une véritable protection « zero day »

Quand des vulnérabilités logicielles ouvrent la voie à de nouvelles attaques possibles, les défenses proactives du Firebox X Core garantissent la protection de votre réseau et de ses utilisateurs. Leurs technologies de proxy sophistiquées assurent une inspection profonde de la couche applicative afin d'identifier et de bloquer les menaces émergentes. Ceci assure une protection automatique de votre réseau contre les spywares, chevaux de Troie, vers, dénis de service (DoS), dénis de service distribué (DDoS), DNS poisoning, dépassements de la mémoire tampon et autres attaques.

Des performances élevées

Équipé d'un pare-feu dont le débit peut atteindre plusieurs gigabits et d'un VPN allant jusqu'à 600 Mbps, le Firebox X Peak est la solution UTM la plus performante dans notre gamme de produits. Tous les modèles Firebox X Peak comprennent 8 ports Ethernet Gigabit 10/100/1000 afin de supporter les infrastructures de la dorsale LAN et les connexions Gigabit WAN. Pour optimiser leur utilisation, chacun d'eux peut être configuré comme Interne, Externe ou En option.

Fonctionnalités réseau avancées

Les fonctionnalités réseau avancées du Firebox X Peak gèrent intelligemment les ressources et optimisent le trafic, tout en vous assurant une connectivité fiable qui augmente la disponibilité de votre réseau.

- **La prise en charge de VLAN** réduit les exigences en termes de matériel et améliore l'interopérabilité
- **L'équilibrage de charge multi-WAN, la haute disponibilité et les liens de secours** augmentent la performance, la redondance et la fiabilité
- **Le routage dynamique et la régularisation du trafic** optimisent la flexibilité et l'efficacité du réseau
- **Le routage en fonction des règles (PBR)** 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 serveurs » face au grand public dans le commerce électronique

Administration centralisée et intuitive

Grâce au WatchGuard® System Manager (WSM), la gestion centralisée des déploiements sur le Firebox X est intuitive, indépendamment de leur taille. En utilisant cette interface pour créer et déployer facilement les changements de configuration, contrôler les données en temps réel et produire des rapports, les administrateurs gagnent du temps et de l'argent.

Connectivité distante sécurisée

Avec le Firebox X Core, la protection des employés distants est plus simple, où qu'ils soient. Il offre le plus large éventail de fonctions d'accès à distance de sa catégorie. Par conséquent, les utilisateurs distants peuvent accéder en toute sécurité au réseau de l'entreprise via :

- un VPN IPsec, un VPN SSL et les clients PPTP

Inclut le Single Sign-On (SSO) qui rationalise l'authentification.

Fonctions de sécurité intégrées pour une protection plus granulaire

Trenforcez votre défense dans les zones d'attaque critiques en ajoutant des abonnements de sécurité performants à votre Firebox X. Tous ces abonnements sont gérés de façon centrale avec WSM et sont constamment mis à jour pour vous assurer une protection immédiate.

■ WebBlocker

Renforce la productivité et diminue les risques pour la sécurité de votre réseau en bloquant l'accès HTTP ou HTTPS au contenu malveillant ou inadéquat sur Internet.

- **spamBlocker avec protection contre les virus émergents** Bloque presque 100 % des mails indésirables et des virus qu'ils transportent.

■ Antivirus de passerelle/service de prévention d'intrusions avec antispyware

Bloquez les spywares, virus, chevaux de Troie et exploits connus sur Internet, avec une protection basée sur la signature.

Évolutivité et montée en gamme des modèles

Lorsque les exigences de votre réseau se renforcent, vous pouvez augmenter la capacité de votre modèle ou vous abonner à des options de sécurité avec une simple clé logicielle à télécharger.

Notre engagement sur le plan environnemental

WatchGuard s'engage à créer des produits performants qui réduisent la consommation d'énergie et à utiliser des appliances et du matériel d'emballage recyclables. Nous respectons toutes les directives européennes relatives à l'utilisation de substances toxiques et la responsabilité environnementale est un élément important de notre stratégie d'entreprise.

Blocage des exploits sur Internet

Internet est l'un de vos plus précieux outils commerciaux, mais il peut aussi représenter une sérieuse menace pour votre réseau. Des utilisateurs non administrés peuvent, délibérément ou par inadvertance, créer des brèches et introduire des bots et des spywares mettant en danger vos données sensibles et augmentant considérablement le nombre des appels au service d'assistance. Les réseaux vulnérables peuvent faire l'objet de DNS cache poisoning (corruption des caches Domain Name Service), de buffer overflows (dépassements de tampon) et d'attaques de déni de service (DoS).

Ce qu'il vous faut

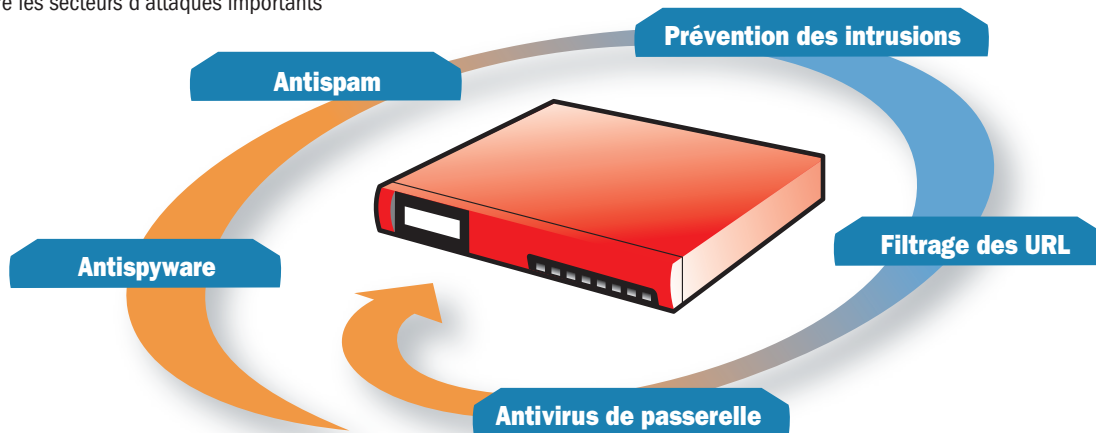
- Démarrez avec le **Firebox X Peak** pour avoir une vraie protection contre les attaques « zero day » et une performance se mesurant en multigigabits.
- Souscrivez un abonnement à **WebBlocker** pour contrôler la navigation non autorisée sur Internet et à l'**antivirus de passerelle/service de prévention d'intrusions** pour bloquer en temps réel le trafic Internet malveillant et les téléchargements nuisibles.

Comment renforcer votre protection

- Une véritable protection « zero day » défend votre réseau contre de nombreuses menaces nouvelles ou inconnues, lorsque des vulnérabilités dans les logiciels d'application ouvrent la voie à d'autres types d'attaques, grâce à de puissantes technologies de proxy applicatif intégrées.

- La fonction **antispyware multicouche** bloque l'accès aux sites de spywares connus, empêche les téléchargements intempestifs sur le réseau liés à la navigation sur Internet et évite que le spyware n'essaie de contacter son hôte.
- L'**antivirus de passerelle/service de prévention d'intrusions avec antispyware** inspecte le trafic Internet à la recherche des virus, chevaux de Troie, bots et autres logiciels malveillants afin d'assurer une protection granulaire contre les menaces connues.
- Le **cloaking (dissimulation) des serveurs Internet** empêche les pirates d'utiliser vos informations système pour attaquer votre réseau.
- **WebBlocker** vous permet de limiter l'accès des employés à Internet depuis leur bureau de façon à accroître leur productivité et éviter que votre responsabilité légale ne soit mise en jeu, tout en protégeant votre réseau des sites malveillants.
- Le **filtrage URL du trafic HTTPS** empêche les utilisateurs de passer par une voie dérobée pour surfer sur Internet en dehors des limites.
- L'**architecture ILS (Intelligent Security Layer) fonctionne avec le proxy DNS** pour vous protéger contre les intrusions sur votre réseau, les attaques de déni de service (DoS) et le DNS cache poisoning.
- La **production intégrée de journaux, rapports et alertes** vous offre une vue détaillée de l'activité de votre réseau et vous permet de prendre immédiatement des mesures de correction ou de prévention.

Les abonnements de sécurité intégrée du Firebox X Peak vous protègent contre les secteurs d'attaques importants



Sécuriser vos bureaux distants et vos utilisateurs mobiles

Étant donné le nombre croissant de télétravailleurs ou d'employés travaillant dans des bureaux satellites, le besoin d'avoir des connexions distantes fiables et sûres n'a jamais été aussi grand. Les considérations comme l'administration et la production centralisées de rapports, l'établissement de règles de sécurité uniformes, l'interopérabilité avec votre réseau, vos ressources et vos applications et une connectivité distante fiable doivent être soigneusement pesées. Il est indispensable de vous assurer que vos appareils distants respectent vos règles de sécurité avant d'accéder à votre réseau.

Ce qu'il faut

- Démarrez avec le **Firebox X Peak** pour une gestion unifiée des menaces et une performance se mesurant en gigabits.
- Ajoutez des appliances **Firebox X Edge** afin d'avoir une protection exceptionnelle du périmètre de votre réseau filaire ou sans fil pour vos bureaux distants et de gérer toutes vos fonctions de façon centralisée à l'aide du logiciel convivial **WatchGuard System Manager**.

Comment renforcer votre protection

- La **politique centralisée et l'administration du VPN** vous permettent d'appliquer uniformément vos règles de sécurité sur tous vos sites et pour tous vos utilisateurs.
- L'**accès distant sécurisé aux ressources du réseau** sur des tunnels de VPN cryptés pour vos bureaux et utilisateurs mobiles optimisent la productivité et la flexibilité pour le personnel à l'extérieur du bureau principal.
- La **solution performante de gestion unifiée des menaces** pour vos bureaux distants et vos télétravailleurs protège votre réseau étendu et vos utilisateurs contre les spywares, virus, attaques de déni de service (DoS) et autres menaces dynamiques.
- La **configuration du VPN des bureaux distants par un simple « drag and drop »** vous permet d'assurer leur connectivité en trois clics de souris et réduit vos coûts informatiques.
- La **performance atteignant plusieurs gigabits** assure la fiabilité, la redondance et la flexibilité des divers environnements de connectivité réseau, y compris en cas d'augmentation des besoins de votre réseau.

Spécifications

	Firebox® X5500e WG55500 Bundle x5500e UTM WG55503	Firebox® X6500e WG56500 Bundle x6500e UTM WG56503	Firebox® X8500e WG58500 Bundle x8500e UTM WG58503	Firebox® X8500e-F WG58510 Bundle x8500e-F UTM WG58513
Débit du pare-feu*	2+ Gbps	2,3 Gbps	2,3 Gbps	2,3 Gbps
Débit du VPN*	400 Mbps	600 Mbps	600 Mbps	600 Mbps
Débit de l'antivirus*	140 Mbps	170 Mbps	200 Mbps	200 Mbps
AV de passerelle/IPS avec antispyware	En option	En option	En option	En option
Filtrage des URL sur HTTP et HTTPS	En option	En option	En option	En option
Antispam avec détection des virus émergents	En option	En option	En option	En option
Interfaces 10/100/1000	8	8	8	8 (4 cuivre/4 fibre)
Port série	1	1	1	1
Prise en charge VLAN	200	200	400	400
Zones de sécurité (incl.)	8	8	8	4 RJ45, 4 SFP GBIC
Sessions concomitantes	500 000	750 000	1 000 000	1 000 000
Nœuds pris en charge (IP LAN)	Illimité	Illimité	Illimité	Illimité
Tunnels de VPN pour bureaux distants (incl./max.)	750/750	750/750	750/750	750/750
Tunnels de VPN pour utilisateur mobile -IPSec (incl./max.)	600/600	600/600	600/600	600/600
Tunnels de VPN pour utilisateur mobile -SSL (incl./max.)	1 000/1 000	4 000/4 000	6 000/6 000	6 000/6 000
Limite d'authentification DB de l'utilisateur local	5 000	6 000	8 000	8 000
Montée en gamme	Oui	Oui	Non	Non

*Le débit peut varier selon la configuration et l'environnement.

Fonctions
Fonctions de sécurité

- Pare-feu dynamique
- Pare-feu avec inspection au niveau de la couche applicative
- Proxies applicatifs : HTTP, SMTP, FTP, DNS, TCP, POP3
- Blocage des spywares
- Prévention des DoS et DDoS
- Prévention progressive des DDoS
- Détection des anomalies du protocole
- Analyse des comportements
- Appariement de formes (pattern matching)
- Protection du réassemblage des paquets fragmentés
- Protection des paquets malformés
- Listes statique et dynamique des sources bloquées
- Règles basées sur le temps
- Autorise/refuse les messageries instantanées et le Peer-to-Peer

Réseaux privés virtuels

- VPN
 - Encryptage (DES, 3DES, AES 128, 192, 256 bits)
 - IPSec
 - SHA-1, MD5
 - IKE - clé pré-partagée, certificat tiers Firebox
 - SSL
 - Client léger, Web Exchange
- Serveur PPTP
- PPTP Passthrough
- Détection DPD ou Dead Peer Detection (RFC 3706)
- Encryptage basé sur le matériel
- Tunnels de VPN drag-and-drop avec règles de pare-feu

Authentification des utilisateurs

- Authentification Active Directory transparente (Single Sign-On)
- XAUTH
 - RADIUS®, LDAP, Windows® Active Directory
- VASCO
- RSA SecurID®
- Basée sur Internet
- Authentification locale

Attribution d'adresse IP

- Statique
- Client PPPoE
- Serveur, client, relais DHCP
- Client DNS dynamique

Interface fibre X8500e-F

- Fibre multimode (MMF)
- 1000 Base SX
- 850 nm
- Connecteurs LC

Haute disponibilité

- Haute disponibilité active/passive
- Synchronisation de la configuration
- Synchronisation des sessions
- Synchronisation des tunnels de VPN

Lien de secours WAN (failover)

- Lien de secours VPN
- Modes WAN
 - Spill-over
 - Round Robin (répartition de charge entre plusieurs serveurs), Round Robin pondéré
 - Lien de secours
 - Fonction ECMP

Régulation du trafic

- Qualité de service (QoS)
 - 8 files prioritaires
 - Diffserve
 - File d'attente stricte modifiée

Routages

- Routes statiques
- Routes dynamiques
 - BGP4, OSPF, RIP v1 et v2
- Routage en fonction de règles (PBR)

Mise en réseau

- Indépendance des ports
- Réseau local virtuel (VLAN)
 - Mode bridge, identificateur (tagging), mode routé
- Équilibrage de la charge des serveurs
- Prise en charge de la vidéoconférence et de la voix sur IP (VoIP)

Abonnements de sécurité

- spamBlocker
 - Mise en quarantaine du spam, des envois en masse et des e-mails suspects
 - Détection des virus émergents

- Antivirus de passerelle/service de prévention d'intrusions avec antispyware
 - Scan antivirus de fichiers de taille illimitée
- WebBlocker

Modes d'exploitation

- Mode transparent/Drop-in (couche 2)
- Mode routé (couche 3)

Translation d'adresses réseau

- NAT statique (Port Forwarding)
- NAT dynamique
- NAT one-to-one
- IPSec NAT Traversal
- NAT basé sur des règles
- IP virtuel pour l'équilibrage de la charge des serveurs

Journaux/Rapports

- Agrégation de journaux provenant de plusieurs appliances
- Rapports compatibles WebTrends® (WELF)
- Rapports aux formats HTML et PDF
- Base de données des logs SQL
- Log channel encrypté
- Syslog
- SNMP v2 et v3

Alertes/Notifications

- SNMP
- E-mail
- Alertes par le système d'administration

Logiciel

- WatchGuard System Manager (WSM)

Certifications

- Critères Communs EAL4
- Pare-feu ICASA et IPSec ICASA
- West Coast Labs Checkmark

Support et maintenance

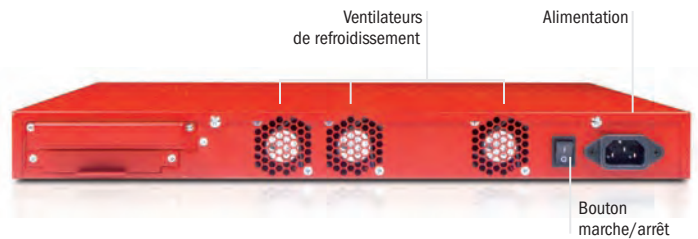
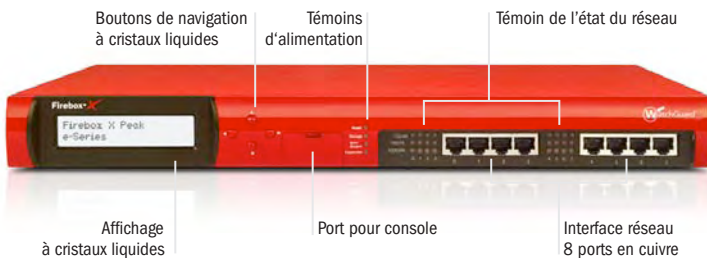
- Garantie du matériel : 1 an
- Abonnement de 90 jours ou 1 an au Service LiveSecurity®

Dimensions et tension

Dimensions de l'appareil	14,5 x 42,6 x 36,2 cm
Dimensions de l'emballage	18,4 x 54,6 x 48,2 cm
Poids de l'appareil	5,62 kg
Poids total	6,25 kg
Poids DEEE	4,81 kg
Tension requise	100-240 VCA Autosensing
Consommation d'énergie	80 watts aux États-Unis Reste du monde : 1146 cal/min ou 273 BTU/h
Montable en rack	Oui

Environnement

Température de fonctionnement	0 à 45°C
Température à l'arrêt	-40 à 70°C
Humidité de fonctionnement	10-85 %
Humidité à l'arrêt	10-95 % sans condensation à 55°C
Vibrations aléatoires à l'arrêt	7-28 Hz 0,001 à 0,01 G2 par Hz
Bruit	54 dBA à 20-25°C
Choc mécanique en fonctionnement	20 G avec une durée de 11 ms dont la moitié d'ondes sinusoïdales
Conformité DEEE/RoHS	Oui



Le modèle X8500e-F est également disponible avec 4 ports en cuivre et 4 ports en fibre.

Conseils et support par une équipe d'experts

Le service LiveSecurity® de WatchGuard est l'offre de support technique et de maintenance la plus complète sur le marché. Vous savez que vous avez derrière vous une équipe internationale d'experts en matière de sécurité afin de vous simplifier la gestion informatique. Le Service LiveSecurity comprend :

- La garantie du matériel avec remplacement anticipé
- Les mises à jour logicielles
- Un support technique avec une réponse rapide
- Des alertes de sécurité immédiates avec des instructions claires sur la façon de gérer les nouvelles menaces et des liens vers les correctifs des fournisseurs pour gagner du temps
- Des ressources innovantes sur le plan de la formation, notamment des vidéos, des podcasts et des modules de formation à la sécurité pratiques pour l'utilisateur final

Quand vous achetez un Firebox X Peak, vous avez le choix entre abonnement de 90 jours ou d'un an au service LiveSecurity. Un service de support prestige est disponible pour les entreprises ayant de hautes exigences par rapport à Internet.

Bundle Peak™ UTM : une seule solution, un seul achat, un seul prix avantageux

Ce bundle intéressant réunit tout ce dont vous avez besoin pour assurer une gestion unifiée des menaces complète sur une appliance de sécurité ultra performante. Chaque bundle d'une valeur exceptionnelle comprend :

- Une appliance de sécurité Firebox X Peak e-Series
- WebBlocker*
- spamBlocker avec détection des virus émergents*
- Antivirus de passerelle/service de prévention d'intrusions avec antispyware*
- Service LiveSecurity®*

Meilleure solution de gestion unifiée des menaces de sa catégorie, le bundle Firebox X Peak e-Series UTM rationalise la gestion de la sécurité de votre réseau - de l'achat initial à la protection continue. Choisissez le bundle et faites des économies !

*Abonnement d'un an

Gratuit !

Essais de 30 jours

Essayez gratuitement pendant trente jours les options **spamBlocker**, **WebBlocker** et **antivirus de passerelle/service de prévention d'intrusions** avec l'achat d'un Firebox X Peak. Pour en savoir plus, contactez votre revendeur.

Pour de plus amples informations sur la gamme Firebox X Peak, rendez-vous sur www.watchguard.com/appliances

ADRESSE: 505 Fifth Avenue South, Suite 500, Seattle, WA 98104 · SITE INTERNET : www.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. ©2008 WatchGuard Technologies, Inc. Tous droits réservés. WatchGuard, le logo WatchGuard, Firebox, Firewall, LiveSecurity, Peak et Core sont des marques déposées ou non de WatchGuard Technologies, Inc. aux États-Unis et/ou dans d'autres pays. Tous les autres noms de marque et marques appartiennent à leurs propriétaires respectifs. Numéro de référence : WGC66358_071808

