



- **Protection complète** de votre réseau contre les menaces malveillantes
- **Véritable prévention des attaques « zero day »** pour bloquer les menaces nouvelles de façon proactive
- **Nouveau ! VPN SSL intégré**
- **Administration rationalisée de la sécurité réseau** qui vous fait gagner du temps
- **Abonnements de sécurité continuellement mis à jour** pour vous offrir une protection instantanée
- **Fonctions intégrées évolutives** plus rentables
- **Équipe internationale d'experts de la sécurité** disponibles quand vous en avez besoin



Technologie écologique

Solution complète de gestion unifiée des menaces

Les solutions de gestion unifiée des menaces (unified threat management ou UTM) Firebox® X Core™ vous offrent la sécurité la plus complète de leur catégorie, en protégeant votre réseau des spywares, spam, virus, chevaux de Troie, exploits sur Internet et autres logiciels malveillants. Elles vous assurent une protection multicouche qui exige un investissement en temps et en argent bien moins élevé que celui engendré par l'administration de solutions à points multiples, tout en augmentant considérablement votre protection contre les menaces mixtes. Parallèlement, leurs fonctions réseau avancées, gérées par une interface utilisateur intuitive, garantissent une connectivité rapide et sécurisée pour les données de l'entreprise dans une même appliance simple d'emploi.

Une sécurité multicouche fiable

Le Firebox X Core est bâti sur l'architecture Intelligent Layered Security (ILS). En d'autres termes, les couches de sécurité fonctionnent ensemble pour renforcer votre protection globale. La communication entre les couches réduit et affine le traitement requis par les fonctions de sécurité. Le résultat : vous bénéficiez du degré de protection dont vous avez besoin pour assurer votre sécurité sans faire de compromis sur la performance.

Véritable prévention des attaques « 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.

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.

Des fonctions de sécurité intégrées pour une protection plus granulaire

Renforcez 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.

- **Antivirus de passerelle/service de prévention d'intrusions**
Bloque les virus, spywares, chevaux de Troie et exploits sur Internet par une solide protection fondée sur la signature au niveau de la passerelle.
- **spamBlocker avec protection contre les virus émergents**
Profitez de la meilleure solution antispam et de protection du courrier électronique du secteur. Elle bloque presque 100 % des e-mails indésirables et assure une protection en temps réel contre les virus émergents.
- **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.

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 :

- IPSec
- VPN SSL
- PPTP

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

Conseils et support par une équipe d'experts

Le Service LiveSecurity® de WatchGuard met à votre service une équipe internationale d'experts en matière de sécurité pour faciliter la gestion informatique de votre entreprise. Votre abonnement LiveSecurity inclut une garantie avec un remplacement anticipé du matériel, des mises à jour logicielles, une assistance technique avec une réponse rapide, des alertes de vulnérabilité de dernière minute et des ressources innovantes sur le plan de la formation.

Protection de votre investissement

Si vous examinez les coûts entraînés par le déploiement, l'administration et la mise à jour de multiples solutions, vous comprenez immédiatement pourquoi les solutions de gestion unifiée des menaces du Firebox X Core sont plus rentables. Avec une protection multifacette entièrement intégrée sur une même appliance, vous économisez sur tous les aspects du coût total de possession, de l'achat initial aux contrats de support technique.

Au fur et à mesure de l'expansion de vos besoins, vous pouvez ajouter facilement de nouvelles fonctions pour renforcer la sécurité de votre entreprise. Si vous avez besoin d'une capacité accrue, rien ne vous empêche d'évoluer vers un modèle supérieur en téléchargeant une simple clé logicielle. Enfin, pour les réseaux plus exigeants, vous pouvez monter en gamme du Firewall® vers le logiciel d'exploitation avancé Firewall® Pro doté de fonctions réseau étendues : prise en charge de VLAN, haute disponibilité et qualité de service (QoS). Tout ceci sans devoir acquérir de nouveau matériel. Aucun produit sur le marché n'est capable d'assurer une telle protection de votre investissement dans la sécurité sous autant de facettes.

Notre engagement sur le plan environnemental

WatchGuard crée des produits performants qui réduisent la consommation d'énergie et utilise des appliances et du matériel d'emballage recyclables. Nous respectons toutes les directives internationales 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 de cache Domain Name Service), de buffer overflows (dépassements de tampon) et d'attaques de dénis de service (DoS).

Ce qu'il vous faut

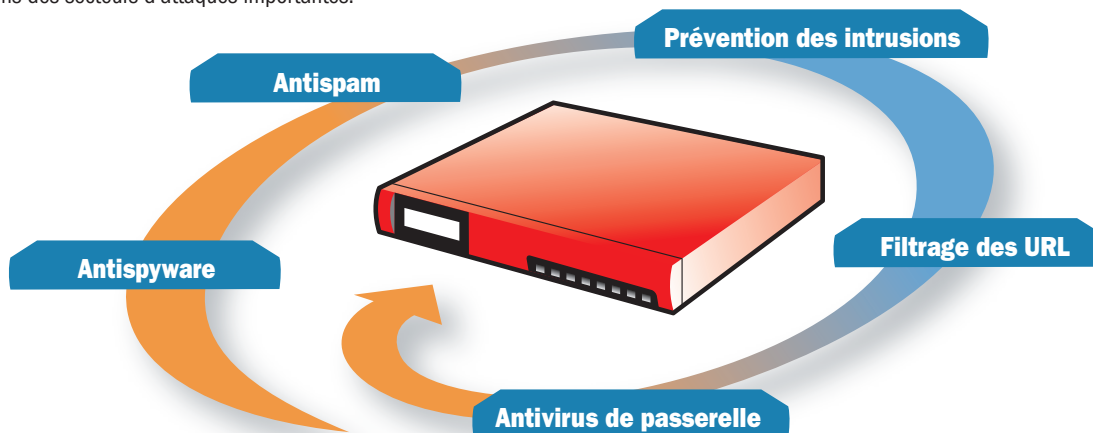
- Démarrez avec le **Firebox X Core** pour avoir une vraie protection contre les attaques « zero day ».
- Souscrivez un abonnement à **WebBlocker** pour contrôler la navigation non autorisée sur Internet et à l'**antivirus de passerelle/service de prévention d'intrusions** pour bloquer en temps réel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

Comment renforcer votre protection

- La **protection « zero day »** défend votre réseau contre de nombreuses menaces 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, assurant 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 à Internet des employés 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 Layered Security) opère 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 Core renforcent votre protection dans des secteurs d'attaques importantes.



Blocage des menaces liées aux e-mails

Votre activité est fortement liée au courrier électronique. Il faut donc que celui-ci puisse circuler de façon fluide et fiable, sans mettre en cause la sécurité de votre réseau. Parallèlement, l'e-mail reste aussi le moyen principal de diffusion d'un code malveillant sur votre réseau. Si vous ajoutez à cela le spam incessant, votre environnement de courrier électronique risque de devenir l'un de vos fardeaux informatiques les plus pesants.

Ce qu'il vous faut

- Démarrez avec le **Firebox X Core** pour bénéficier d'une vraie protection « zero day ».
- Souscrivez un abonnement à un **antivirus de passerelle/service de prévention d'intrusions** qui scanne le trafic e-mail afin de bloquer vers, virus, chevaux de Troie et autres programmes malveillants connus.
- Activez l'abonnement **spamBlocker**, la meilleure solution du secteur pour différencier en temps réel le courrier légitime des attaques de spam. spamBlocker inclut une couche de protection antivirus efficace qui reconnaît les virus propagés par le courrier électronique et les bloque avec presque 100 % d'exactitude.

Comment renforcer votre protection

- La **protection « zero day » intégrée** s'appuie sur de puissantes technologies de proxy applicatif pour bloquer de façon proactive les types de fichiers qui transportent généralement le malware par e-mail.
- **spamBlocker** procède à la détection du spam en temps réel pour vous assurer une protection immédiate, et bloque les e-mails indésirables, indépendamment de leur contenu, leur langue et leur format, y compris le spam basé sur des images.
- La **quarantaine spam et antivirus** isole le spam et les e-mails suspects de votre réseau, tout en offrant à l'administrateur et aux utilisateurs des outils pour l'administrer.
- Le **cloaking (dissimulation) des serveurs SMTP** empêche les pirates d'utiliser vos informations système pour attaquer votre réseau.
- L'**antivirus de passerelle intégré** vous donne une protection plus granulaire des fichiers et des pièces jointes, en bloquant les virus, vers et autres programmes malveillants avant qu'ils ne pénètrent dans votre réseau et ne désactivent vos applications de sécurité.
- Le **scan antivirus des e-mails sortants** empêche votre entreprise d'envoyer des virus, vers et chevaux de Troie à ses partenaires, clients et autres destinataires en dehors de son réseau.

Spécifications

	Firebox® X550e WG50550 Bundle X550e UTM WG50553	Firebox® X750e WG50750 Bundle X750e UTM WG50753	Firebox® X1250e WG51250 Bundle X1250e UTM WG51253
Débit du pare-feu†	300+ Mbps	750 Mbps	1,5 Gbps
Débit du VPN†	35 Mbps	50 Mbps	100 Mbps
Débit de l'antivirus†	50 Mbps	70 Mbps	100 Mbps
AV de passerelle/IPS avec antispyware	En option	En option	En option
Filtrage des URL sur HTTP et HTTPS	En option	En option	En option
Antispam avec détection des virus émergents	En option	En option	En option
Interfaces 10/100	4	8	0
Interfaces 10/100/1000	0	0	8
Port série	1	1	1
Prise en charge (VLAN)*	25	25	25
Zones de sécurité (incl.)	4	8	8
Sessions concomitantes	25 000	75 000	200 000
Nœuds pris en charge (LAN IP)	Illimité	Illimité	Illimité
Tunnels de VPN pour succursale (incl./max.)	35/45	100/100	600/600
Tunnels de VPN pour utilisateur mobile - IPSec (incl./max.)	5/75	50/100	400/400
Tunnels de VPN pour utilisateur mobile - SSL (incl./max.)	1/75	1/300	1/500
Limite d'authentification DB de l'utilisateur local	250	1 000	5 000
Montée en gamme	Oui	Oui	Non
Logiciel avancé Firewall® Pro	En option	En option	En option

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

* Disponible avec la montée en gamme vers le logiciel avancé Firewall Pro.

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 et 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 et 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
- RSA SecurID®
- Basée sur Internet
- Authentification locale

Attribution d'adresse IP

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

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)
 - Lien de secours
 - Fonction ECMP
 - Round Robin pondéré**

Régulation du trafic**

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

Routing

- Routes statiques
- Routing dynamique**
 - BGP4, OSPF, RIPv1 et v2
- Routing 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 et multi-WAN
- 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
- WebBlocker

Modes d'exploitation

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

Translation d'adresses

- 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 de logs SQL
- Canal de communication des logs 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
- IPSec ICSA
- Pare-feu ICSA
- Certification Checkmark West Coast Labs

Support et maintenance

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

** Disponible avec la montée en gamme vers le logiciel d'exploitation avancé Firewall Pro

†† Le Firebox X 550e est livré avec une licence WSM à un seul nœud. Pour créer des tunnels « drag-and-drop » ou gérer de façon centrale plusieurs appliances Firebox X Edge avec un Firebox X550e, des licences de mise à niveau WSM sont nécessaires.

