

- **Prévention proactive et intégrée des attaques** pour vous protéger contre les nouvelles menaces
- **Abonnements de sécurité continuellement mis à jour** pour une protection immédiate
- **Options de gestion réseau fiables et flexibles** pour connecter et sécuriser vos bureaux distants
- **Gestion et priorisation simples** du trafic grâce à la qualité de service (QoS)
- **Gestion unifiée et intuitive de la sécurité** sécurité qui rationalise considérablement l'administration réseau
- **Appliance évolutive et régulièrement mise à jour** pour protéger votre investissement dans la sécurité
- **Une équipe internationale d'experts** à votre disposition dès que vous en avez besoin
- **Conformité RoHS et DEEE**



Technologie écologique



Protection solide et fiable pour les réseaux des PME

Les réseaux des petites entreprises ont besoin de la même protection totale que les plus grandes sociétés, sans la complexité. Désormais, ceci est facilement réalisable grâce à l'appliance de sécurité Firebox® X Edge e-Series de WatchGuard. Le Firebox X Edge est une solution complète de gestion unifiée des menaces (UTM) qui bloque les attaques « zero day », les spywares, les virus, les chevaux de Troie, le spam et les menaces mixtes pour assurer la sécurité des données. Les tunnels VPN ou des succursales/bureaux distants fournissent un accès distant encrypté aux ressources du réseau, tandis que les liens de secours WAN et VPN préservent la connectivité et optimisent les temps de fonctionnement. Ses fonctions réseau souples permettent également une priorisation du trafic et de la bande passante afin d'assurer la performance du réseau et une efficacité maximale. Avec son interface utilisateur avancée et intuitive, l'Edge est la solution idéale pour les entreprises ayant des ressources informatiques limitées. Il est disponible en modèles filaire et sans fil de façon à répondre aux exigences spécifiques de votre réseau.

Prévention proactive des attaques « zero day »

La protection réseau avancée fournie par le Firebox X Edge est basée sur des technologies de proxy sophistiquées qui offrent des défenses proactives intégrées bloquant de nombreux types d'attaques, dont les dépassements de mémoire tampon, le DNS poisoning et les attaques de déni de service (DoS) et de déni de service distribué (DDoS). Ce niveau unique de protection « zero day » est de loin supérieur à celui des produits qui dépendent uniquement du filtrage de paquets et de technologies basées sur les signatures pour bloquer les attaques connues. Il met en place de solides défenses dès que vous allumez votre Firebox.

Protection supplémentaire dans les secteurs d'attaques critiques

Des abonnements de sécurité performants vous apportent des couches de protection supplémentaire. Entièrement intégrés à l'appliance Edge, ils travaillent en collaboration avec les défenses intégrées pour vous offrir une solution complète de gestion unifiée des menaces.

- **spamBlocker**
Bloque jusqu'à 97 % des e-mails indésirables en temps réel, indépendamment du contenu, du format et de la langue.
- **WebBlocker**
Augmente votre productivité, évite que votre responsabilité légale ne soit mise en jeu et limite les risques, en bloquant l'accès au contenu malveillant ou inapproprié sur le réseau.
- **Antivirus de passerelle/service de prévention des intrusions**
Bloque les virus inconnus, les chevaux de Troie, les spywares, les injections SQL et les violations des règles de sécurité au niveau de la passerelle de sécurité.

Gestion centralisée de multiples appliances

Lorsque vous déployez de multiples appliances Firebox X Edge en tant que points d'extrémité d'un réseau Firebox® X Peak™ ou Core™, vos Edge peuvent être administrés de façon centralisée par WatchGuard System Manager (WSM). WSM rationalise la gestion de la configuration et du VPN, ce qui vous permet de déployer les mises à jour logicielles sur tous vos Edge administrés, de définir des règles unifiées sur l'intégralité de votre réseau et de créer des tunnels VPN par

un simple « drag and drop ». WSM vous offre aussi des fonctions de création de journaux, des règles de sécurité flexibles et des outils de contrôle en temps réel.

Fonctions avancées de gestion de réseau

Profitez des fonctions réseau flexibles et fiables nécessaires à votre entreprise, vos succursales et vos bureaux distants pour être toujours connectés et sécurisés.

Une administration sûre et efficace du trafic réseau

- Assure la sécurité de multiples adresses IP externes
- Prend en charge Dynamic NAT, 1:1 NAT et Port Address Translation (PAT)
- Minimise les temps d'immobilisation des réseaux par un lien de secours (failover) WAN vers un port secondaire ou une connexion commutée via le port série
- Optimise la connectivité par un lien de secours VPN complet

Qualité de service (QoS) fiable et configurable

- Etablit des priorités afin d'allouer la bande passante de façon dynamique et de permettre au trafic critique et sensible au temps de l'entreprise, comme la voix sur IP, de prendre le pas sur le trafic moins important.

Convivialité inégalée

Le Firebox X Edge est administré par une interface web intuitive extrêmement simple. Facile à configurer et à utiliser, il fait économiser aux administrateurs réseau de niveau expert un temps précieux, tout en offrant aux moins chevronnés la convivialité indispensable.

Sécurité sans fil flexible

Les modèles sans fil comprennent un point d'accès sans fil 802.11b/g avec des options de sécurité WPA, WPA2 et WEP.

- Trois zones de sécurité sans fil (VAP) distinctes confèrent aux administrateurs un contrôle précis des privilèges d'accès à Internet pour différents groupes d'utilisateurs.

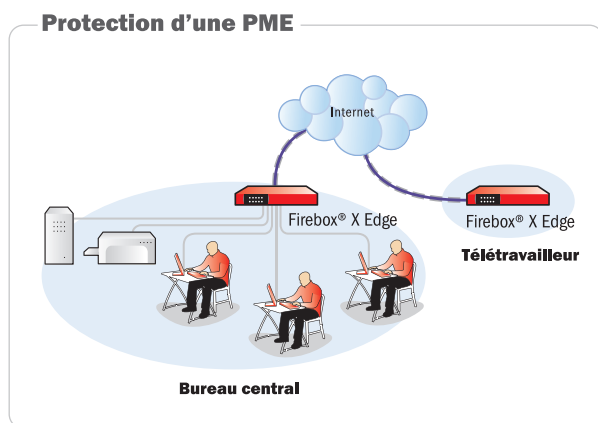
Protection de votre investissement dans la sécurité

Au fur et à mesure de l'essor de votre entreprise, vous pouvez passer à la capacité et aux fonctions de sécurité d'un modèle supérieur à l'aide d'une simple clé logicielle. C'est aussi facile que cela. Pas besoin d'acheter du matériel supplémentaire.

Assurez en permanence la connexion et la sécurité du réseau de votre PME

Gérer le réseau d'une PME n'est pas une tâche facile. Face à la kyrielle de menaces sur Internet, il vous faut une solide protection incluant une prévention proactive des attaques, ce qui ne peut être assuré par simple routeur. Votre solution doit intégrer des défenses multicouches qui combattent le spam, les spywares, les virus et les exploits basés sur Internet. Les PME sont confrontées, dans une large mesure, aux mêmes préoccupations que les grandes entreprises, notamment les demandes d'applications multiples, le haut volume de trafic et une connectivité sécurisée pour les utilisateurs distants. En raison de leurs ressources généralement plus limitées, elles recherchent des solutions réellement conviviales et abordables, susceptibles d'évoluer quand elles prennent de l'essor.

La solution : le **Firebox X Edge** de WatchGuard conçu pour les réseaux des PME.



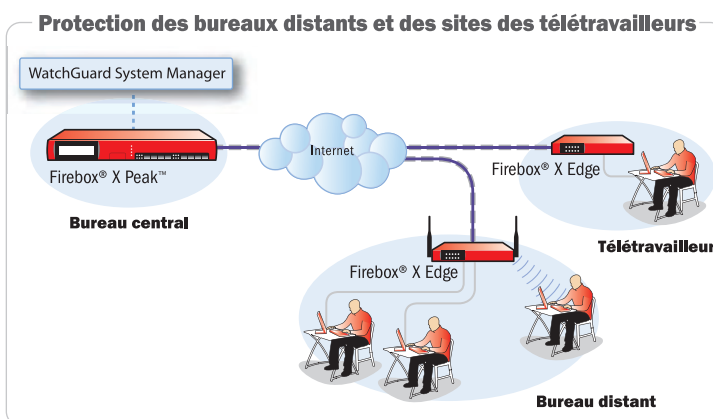
L'intérêt de choisir un Firebox X Edge pour votre PME

- **Simple à configurer et à administrer** grâce à une interface utilisateur web intuitive. Pas besoin d'être un expert en informatique pour l'installer et le faire fonctionner !
- **Une haute sécurité assurée par une appliance prête à l'emploi** avec des paramètres par défaut intelligents et des assistants de configuration qui vous assurent une solide protection dès le premier jour
- **Les options antispam, antispyware, antivirus, prévention des intrusions et filtrage des URL** assurent une gestion unifiée des menaces complète pour protéger votre réseau.
- **Options de gestion réseau flexibles et fiables pour les bureaux indépendants** dont la prise en charge de 1:1 NAT, Dynamic NAT, PAT (Port Address Translation) ainsi que de multiples adresses IP externes
- **Les fonctions de gestion de trafic et qualité de service (QoS)** garantissent au trafic essentiel à l'entreprise, tel que la voix sur IP, une priorité sur la bande passante administrée
- **Temps d'immobilisation du réseau réduit** grâce au lien de secours (failover) WAN/WAN en cas de déconnexion de la ligne sur le port WAN principal
- **Services hôtes et sécurité sans fil** permettant aux entreprises d'offrir un accès Internet contrôlé à des utilisateurs invités sans compromettre la sécurité de leur réseau
- **Accès sécurisé aux ressources critiques du réseau** pour les télétravailleurs opérant sur des stations de travail hors site, avec une authentification et un VPN utilisateur mobile
- **Possibilité d'accroître la capacité et les fonctions réseau/sécurité** au fur et à mesure de l'augmentation de vos besoins par une simple clé logicielle, sans remplacement de matériel

Protégez le périmètre de votre réseau

L'extension aux succursales et bureaux distants de la haute sécurité dont est doté votre bureau central ne doit pas être un poids pesant sur les ressources de votre service informatique. Il faut que vous puissiez bénéficier de la même protection puissante dans le périmètre de votre réseau, tout en garantissant l'intégralité du système à partir d'un seul point central. Pour optimiser l'efficacité et la rentabilité de votre solution de sécurité, tous ses composants doivent être facilement interopérables, afin de vous permettre d'établir des règles de sécurité uniformes pour l'ensemble de votre réseau, susceptible d'être mises à jour partout en quelques clics de souris. Parallèlement, l'appliance avec ou sans fil de votre succursale ou de votre bureau distant doit être dotée de fonctionnalités réseau avancées pour garantir la priorisation et la bonne gestion du trafic entre vos bureaux et de votre bande passante.

La solution : le **Firebox X Edge** de WatchGuard, l'appliance idéale pour étendre la performance du Firebox X Core ou Peak de votre bureau central à vos succursales/bureaux distants.



L'intérêt de choisir le Firebox X Edge pour vos succursales/bureaux distants

- **Les fonctions de gestion unifiée des menaces** dont une vraie protection « zero day », l'antispyware, l'antispam, l'antivirus, la prévention des intrusions et le filtrage des URL constituent des défenses multicouches puissantes au périmètre de votre réseau
- **La gestion centralisée de la configuration** assurée par WatchGuard System Manager (WSM) sur votre Firebox X Core ou Peak rationalise fortement l'administration de vos succursales/bureaux distants
- **Vous pouvez sécuriser la connectivité entre vos bureaux** avec des tunnels VPN pour succursales/bureaux distants faciles à configurer. En effet, WSM vous permet de créer des tunnels VPN en trois étapes par simple « drag and drop », ce qui vous fait gagner un temps précieux en termes de configuration et de maintenance
- **Les mises à jour logicielles des appliances** peuvent être déployées sur vos appareils Edge distants avec WSM de façon à ce que vos règles de sécurité soient rapidement et universellement renforcées et que les logiciels de vos appliances soient toujours à jour
- **Les fonctions réseau avancées** du Firebox X Edge incluent notamment la prise en charge de 1:1 NAT, Dynamic NAT, PAT (Port Address Translation) ainsi que de multiples adresses IP externes, afin de vous offrir des options flexibles et fiables
- **Avec la qualité de service (QoS) et la gestion dynamique du trafic**, vous savez que votre bande passante est administrée et que le trafic sensible au temps, comme la voix sur IP, a la priorité sur le trafic moins important
- **Vous permet d'offrir à des hôtes un accès contrôlé et sécurisé sans fil à Internet**, sans compromettre la sécurité de votre réseau, en utilisant le point d'accès sans fil de l'appliance Edge

Spécifications

Spécifications	Firebox® X10e WG50010	Firebox® X10e-W WG50011 Amér. du Nord WG50012 International WG50015 Chine WG50012-JP Japon	Firebox® X20e WG50020	Firebox® X20e-W WG50021 Amér. du Nord WG50022 International WG50025 Chine WG50022-JP Japon	Firebox® X55e WG50055	Firebox® X55e-W WG50056 Amér. du Nord WG50057 International WG50060 Chine WG50057-JP Japon
Évolutivité du modèle	vers X20e ou X55e	vers X20e-W ou X55e-W	vers X55e	vers X55e-W	N/A	N/A
Débit du pare-feu†	100 Mbps		100 Mbps		100 Mbps	
Débit du VPN†	35 Mbps		35 Mbps		35 Mbps	
AV de passerelle/Prévention d'intrusions	En option		En option		En option	
Blocage du spam	En option		En option		En option	
Filtrage des URL	En option		En option		En option	
Ports série	1		1		1	
Interfaces 10/100	6		6		6	
Zones de sécurité (incl.)	2		2		2	
Sessions simultanées	6 000		8 000		10 000	
Nœuds pris en charge (LAN IP)	15 (avec montée à 20 possible)		30		Illimités	
Tunnels VPN pour les succursales/bureaux distants	5		15		25	
Tunnels VPN pour les utilisateurs mobiles (incl./max)	1/11		5/25		5/55	
Limite d'authentification DB de l'utilisateur local	200		200		200	
Lien de secours (failover) WAN	En option		En option		Inclus	
Lien de secours (failover) VPN	Inclus		Inclus		Inclus	

†Le débit varie selon l'environnement et la configuration

Fonctions
Fonctions de sécurité

- Pare-feu dynamique
- Inspection de la couche applicative pour le trafic sortant
 - HTTP
 - FTP
 - POP3
- Inspection de la couche applicative pour le trafic entrant
 - SMTP
- Détection des anomalies de protocole
- Appariement de formes
- Protection du réassemblage de paquets fragmentés
- Protection contre les paquets malformés
- Liste statique de sources bloquées

VPN

- Encryptage (DES, 3DES, AES)
- IPSec
 - SHA-1, MD5
 - IKE : clé pré-partagée, certificat Firebox, certificats de tiers (x.509)
- Émulation IPSec
- Dead Peer Detection (RFC 3706)
- Encryptage basé sur le hardware
- Support PPTP (10 utilisateurs)

Authentification des utilisateurs

- XAUTH
 - LDAP
 - Windows® Active Directory
- Authentification locale
- Windows® NT
- Windows® 2000
- Windows® 2003

Affectation d'adresses IP

- Statique

- Client PPPoE
- Serveur DHCP
- Client DHCP
- Relais DHCP

Fonctions de redondance

- Lien de secours (failover) WAN
- Lien de secours WAN vers modem série
- Lien de secours VPN

Gestion et priorisation du trafic

- Priorisation du trafic basée sur des règles
- Priorisation du trafic VPN
- Support complet pour le marquage
 - Diffserv
 - Services IP
- Qualité de service (4 files de priorisation)
 - Interactive
 - Élevée
 - Moyenne
 - Faible

Fonctions réseau avancées

- NAT statique
- NAT dynamique
- 1:1 NAT
- IPSec NAT Traversal
- Règles basées sur PAT (Port Address Translations)
- Jusqu'à 8 adresses IP externes
- Routes statiques : jusqu'à 100
- DNS dynamique

Modes de fonctionnement

- Commutateur intégré 3 ports (couche 2)
- Mode routé (couche 3)

Logiciel d'administration

- Interface utilisateur graphique web
- WatchGuard System Manager (WSM) v9.1 ou supérieure

Création de journaux/rapports

- Rapports d'activité et sécurité WSM
- Rapports d'activité sur les abonnements de sécurité basés sur Internet
- Syslog
- Rapports compatibles WebTrends® (disponibles pour les utilisateurs de WSM)
- Rapports HTML (disponibles pour les utilisateurs de WSM)
- Canal de connexion crypté

Logiciel d'exploitation des appliances

- Version 8.x ou supérieure

Fonctions de sécurité sans fil

- Services hôtes sans fil
- 802.11b/g
- 3 Virtual Access Points (VAPs)
- WPA
- WPA2
- WEP

Certifications

- Certifié ICSA Labs : IPSec
- West Coast Labs Checkmark
 - Pare-feu niveau 1, VPN, Filtrage Internet, Prévention d'intrusion, Antispam

Support et maintenance

- Matériel garanti 1 an
- Abonnement initial de 90 jours ou abonnement d'un an au service LiveSecurity®

