

Antivirus de passerelle/service de prévention d'intrusions

Un abonnement à un service de sécurité intégré pour les appliances for Firebox® X e-Series



Ce que le Gateway AV/IPS apporte à votre réseau et votre entreprise

L'antivirus de passerelle/service de prévention d'intrusions (Gateway AV/IPS) est un service de sécurité par abonnement entièrement intégré pour les appliances Firebox X e-Series. Il fonctionne en tandem avec l'inspection du contenu de la couche applicative du Firebox pour offrir une protection en temps réel contre les spywares, virus, exploits et menaces mixtes connus.

Pourquoi ajouter un abonnement Gateway AV/IPS ?

L'antivirus de passerelle/service de prévention d'intrusions analyse le trafic sur tous les principaux protocoles, en utilisant des signatures constamment mises à jour pour déceler et bloquer les menaces envoyées dans des formats non suspects.

Et comme il est intégré à l'appliance de sécurité Firebox X, vous disposez d'une solution rentable et simple à gérer, sans matériel supplémentaire à acquérir.

Disposer d'une solution de sécurité tout-en-un « ... a considérablement facilité le travail de notre service informatique interne. »

Martin Korn
Responsable du service informatique et service central
Novoferm GmbH

Il bloque à la passerelle les virus, vers et chevaux de Troie véhiculés par le courrier électronique

- Le trafic SMTP et POP3 est analysé à la passerelle afin de bloquer les menaces avant qu'elles n'atteignent vos serveurs et n'exécutent leur charge dangereuse
- Les e-mails suspects peuvent être marqués pour être mis en quarantaine, ce qui permet à l'administrateur de restreindre l'accès ou d'autoriser les utilisateurs à passer en revue les fichiers en quarantaine via des avertissements automatiques par e-mail
- Les fichiers compressés et encodés joints aux e-mails sont décompressés pour être inspectés, de nombreux formats de compression étant pris en charge, notamment les fichiers ZIP, TAR et GZIP

Les intrusions dans le réseau sont identifiées et bloquées

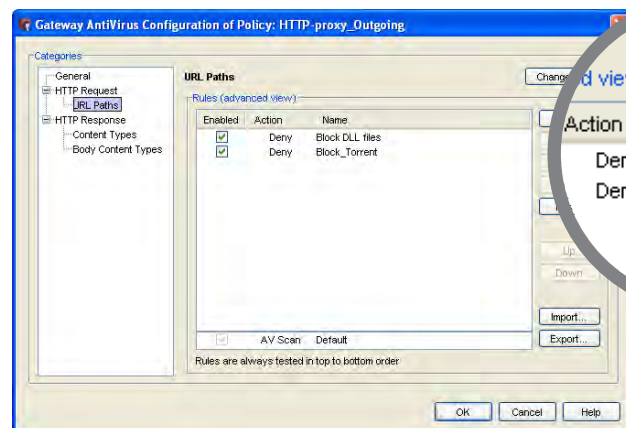
- Analyse tous les principaux protocoles de trafic, dont HTTP, HTTPS, FTP, TCP, DNS, SMTP et POP3, pour bloquer les attaques basées sur le réseau, les applications et les protocoles
- Maintient les spywares en dehors du réseau en bloquant les adresses IP des spywares connus et de ceux qui tentent de contacter leur hôte ou de pénétrer intempestivement dans le réseau à la suite d'une navigation sur Internet
- Une liste des sites bloqués garantit que, lorsqu'une adresse IP est identifiée avec certitude comme la source d'une attaque, les attaques futures provenant de cette même adresse seront bloquées de façon dynamique
- La base de données des signatures constamment mise à jour assure une couverture étendue en temps voulu

Une gestion simple avec une mise en application centralisée des règles

- Vous gérez toutes les fonctions de sécurité de votre appliance Firebox X, dont le Gateway AV/IPS, à partir d'une seule console intuitive, ce qui vous assure une efficacité et une simplicité d'emploi optimales
- Toute l'activité, en termes de sécurité, identifiée par le Gateway AV/IPS est consignée dans un journal et conservée pour permettre d'établir facilement des rapports et donc de prendre immédiatement des mesures correctives ou préventives
- Vous pouvez définir la mesure à adopter lorsqu'un logiciel malveillant est identifié, ce qui permet au réseau d'autoriser, de bloquer ou de verrouiller le trafic douteux selon le type, l'utilisateur/le groupe, le protocole et la gravité

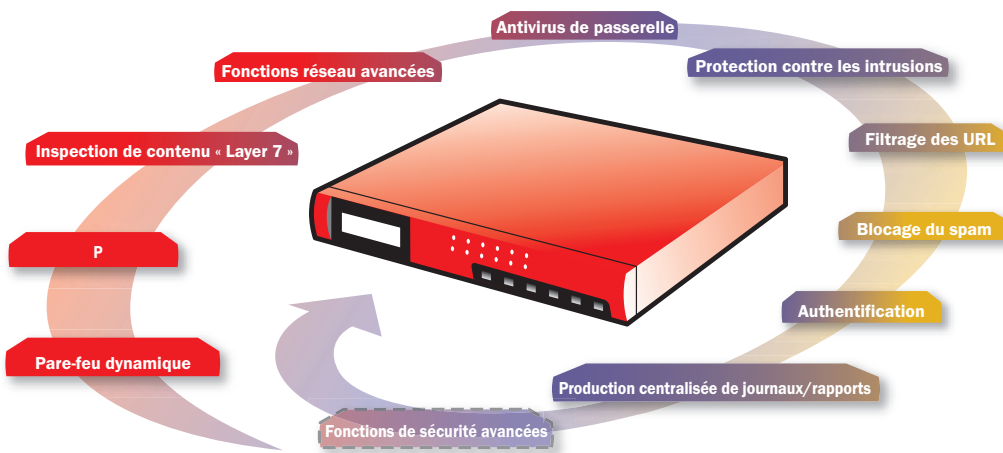
Filtrage Internet rentable

- Assurez la protection, sur l'ensemble de votre réseau, de tous les utilisateurs configurés derrière votre pare-feu Firebox X avec un seul abonnement Gateway AV/IPS
- Pour faire des économies, achetez le Gateway AV/IPS avec notre suite d'abonnements à des services de sécurité performants



Configurer le Gateway AV/IPS est un jeu d'enfant. Vous définissez l'action à adopter à l'aide d'une interface intuitive.

Une solution de sécurité entièrement intégrée pour une protection totale



Solution de sécurité « tout-en-un »

Les appliances Firebox X se conjuguent avec des abonnements à des services de sécurité performants pour vous offrir une protection complète contre les logiciels malveillants. Toute les fonctions de sécurité sont gérées à partir d'une seule console intuitive, y compris la production de journaux et de rapports, afin d'offrir une vue immédiate de l'activité en termes de sécurité. Comme les menaces ne cessent d'évoluer, les solutions WatchGuard XTM et Firebox X sont conçues de façon à prendre facilement en charge l'ajout de nouvelles fonctions de protection par des abonnements à des services de sécurité, ce qui évite de coûteuses montées en gamme.

Achetez le bundle et profitez de ses avantages

Tout ce qu'il vous faut pour une gestion unifiée des menaces complète est réuni dans un bundle de gestion unifiée des menaces (UTM) pratique de WatchGuard®, comprenant un pare-feu, un VPN, des abonnements à des services de sécurité et un support technique.

Chaque bundle UTM comprend tout ce qui suit :

- Une appliance Firebox X e-Series (Peak, Core ou Edge) au choix*
- spamBlocker avec détection des virus émergents
- WebBlocker avec inspection HTTP et HTTPS
- L'antivirus de passerelle/service de prévention d'intrusions assurant une protection contre les menaces connues, basée sur les signatures
- Service LiveSecurity® avec garantie du matériel, support technique 24h/24 et 7j/7, mises à jour logicielles gratuites, alertes de sécurité et ressources pour la formation.

Dès le départ, ce bundle facilite et améliore la gestion et l'efficacité de votre sécurité réseau. Vous disposez d'une solution complète à prix intéressant, sans frais supplémentaires, ni contrats, ni matériel à acquérir.

*Des formules d'abonnement de 1, 2 et 3 ans sont disponibles.

Vous avez le boîtier ? Optez pour la Suite logicielle UTM

Faites de votre appliance WatchGuard Firebox X une solution de gestion unifiée complète des menaces (UTM) avec la Suite logicielle UTM. Un moyen efficace et rentable d'avoir une protection complète contre les vecteurs d'attaques sur Internet, avec toute votre sécurité réseau gérée depuis une seule console centralisée. Cette suite inclut également un support technique 24h/24 et 7j/7 imbattable sur le marché.

La Suite logicielle UTM WatchGuard® comprend :

- spamBlocker
- WebBlocker
- Antivirus de passerelle/service de prévention des intrusions
- Service LiveSecurity®

Une bonne affaire quand vous les achetez tous ensemble !

*Aucune appliance n'est incluse dans la Suite logicielle UTM.

**Essai
GRATUIT
de 30 jours**

Essayez gratuitement pendant 30 jours l'antivirus de passerelle/
service de prévention d'intrusions, spamBlocker et WebBlocker.
Renseignez-vous auprès de votre revendeur.

Adresse : WatchGuard Technologies France, La Grande Arche - Paroi Nord, 92042 Paris La Défense • Site Internet : www.watchguard.fr • Tél. : +33 1 40 90 30 35
• E-mail : 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, LiveSecurity et Core sont des marques non déposées ou déposées de WatchGuard Technologies, Inc. aux États-Unis et/ou dans d'autres pays. Toutes les autres marques appartiennent à leurs propriétaires respectifs. Numéro de référence WGC66236_042009