# BITDEFENDER SECURITY FOR ISA SERVERS

## PASSERELLES INTERNET – PREMIÈRE LIGNE DE DÉFENSE

Les entreprises offrent aujourd'hui à la plupart de leurs employés un accès partagé à Internet, ce qui rend utiles les services proxy pour gérer l'utilisation de la bande passante et le trafic en mettant les données en cache localement. La recherche d'informations pour des motifs personnels ou professionnels augmente beaucoup le volume du trafic Internet et par conséquent le risque d'exposition aux menaces. C'est pourquoi le déploiement par les entreprises de solutions comme Microsoft® Internet Security and Acceleration (ISA) peut permettre d'enregistrer des gains considérables au niveau de la rapidité d'accès à Internet, et au niveau du fonctionnement de base du pare-feu qui consiste à assurer la défense de première ligne.

## LA PROTECTION DES PASSERELLES D'ACCÈS A INTERNET

Les entreprises qui déploient des passerelles d'accès à Internet bénéficient effectivement de la protection supplémentaire du pare-feu, mais cette protection reste limitée en raison de règles statiques du pare-feu et du manque de visibilité des données franchissant la passerelle. Il en résulte que l'invasion du réseau d'une entreprise par des codes malveillants, due à l'absence de contrôle de certaines applications ou de vérification des contenus peuvent entraîner de considérables pertes de temps, d'argent et de ressources lorsque une infection se produit.

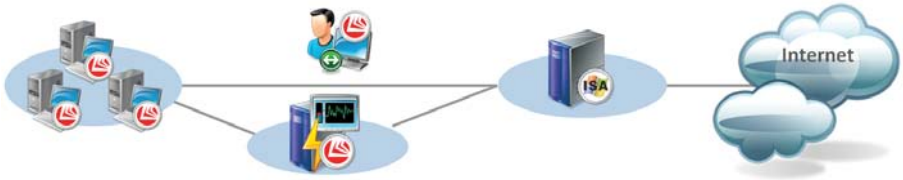
Les services Internet posent des problèmes de sécurité, avec différentes catégories de menaces :

- Sites web ou fichiers téléchargés infectés par des codes malveillants
- Téléchargement de documents infectés joints à des e-mails sur des services en ligne
- Téléchargement de fichiers infectés par l'intermédiaire du service FTP
- Infection propagée par l'intermédiaire d'un lecteur réseau mappé

Les passerelles constituent un goulet d'étranglement des contenus basés en ligne et aident les entreprises à élaborer des politiques de trafic entrant et sortant, qui s'appliquent aux utilisateurs du réseau. Pour optimiser la sécurité et augmenter l'efficacité du déploiement d'un serveur ISA – sans pour autant perturber les performances ni les délais de réponse des opérations essentielles à l'activité de l'entreprise – des solutions complémentaires sont nécessaires pour garantir le maintien de votre efficacité opérationnelle.

## SÉCURISATION DES PASSERELLES INTERNET AVEC BITDEFENDER

BitDefender Security for ISA Servers permet aux entreprises de protéger leur serveur ISA Microsoft® en bloquant certains types de sites web et en filtrant les fichiers téléchargés et les pièces jointes des e-mails en provenance de services de messagerie web. L'application des politiques de sécurité devient alors plus simple, ce qui permet aux entreprises de conserver le contrôle de leurs données sensibles, qui pourraient autrement être divulguées en dehors de l'entreprise.




BitDefender Security for ISA Servers analyse le trafic FTP et HTTP entrant et sortant et applique un ensemble de règles de filtrage configurables via un serveur d'administration centralisée

## PRINCIPALES FONCTIONNALITÉS ET AVANTAGES-CLÉS

- Détection primée des virus, nettoyage et mise en quarantaine
- Limitation du temps d'arrêt du réseau pour améliorer l'efficacité opérationnelle
- Réduit les risques de menaces à la sécurité, ainsi que les coûts et les frais généraux et améliore la productivité
- Technologie de gestion des navigateurs (Browser comforting) pour l'analyse et le téléchargement de gros fichiers par petits blocs
- Facilité d'administration par mots clés des listes noires FTP ou de sites web, et aussi des listes blanches de sites sûrs.
- L'analyse du trafic de fichiers assure une protection antimalware en temps réel qui minimise le risque de propagation des malwares sur le réseau
- Processus d'analyse optimisé et accéléré par l'intégration aux règles du pare-feu et de la mise en cache de Microsoft via l'interface d'analyse antivirus de Microsoft (ISAPI)
- Rapports sur l'activité virale, les statistiques d'analyse et le volume du trafic
- Configuration possible des mesures à prendre face aux événements pour déclencher des alertes ou d'autres types de réaction
- Compatible avec les serveurs ISA déployés en grappes utilisés dans un environnement de trafic dense afin de répartir les charges
- Permet la configuration à distance à partir de n'importe quel ordinateur de l'entreprise via une console d'administration centralisée

bitdefender®

## TECHNOLOGIES BITDEFENDER

b-have Toutes les solutions BitDefender intègrent B-HAVE , qui analyse le comportement des codes potentiellement malveillants au sein d'un ordinateur virtuel, élimine les faux positifs et augmente de manière significative le taux de détection des malwares inconnus.

## MISES À JOUR AUTOMATIQUES

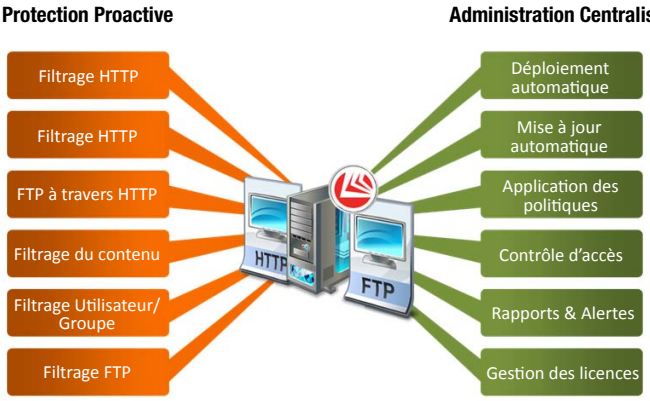
BitDefender Security for ISA Servers fournit des mises à jour intelligentes toutes les heures avec les nouvelles définitions de virus et une base de données à contenu restreint, assurant que votre serveur de messagerie Microsoft® ISA Server est bien équipé de la toute dernière protection anti-menaces.

## DÉFENSE EN PROFONDEUR

BitDefender Security for ISA Servers n'est qu'un des éléments d'un ensemble complet de solutions assurant la protection globale du réseau, depuis la passerelle jusqu'à la station de travail. Les produits proactifs et multi-plateformes de BitDefender détectent et bloquent les menaces que les virus, le spyware, le adware et les chevaux de Troie peuvent faire peser sur l'intégrité de votre réseau.

## CONFIGURATION REQUISE

- Windows Server 2003 avec SP1, Windows Server 2003 R2
- Windows Server 2008, Windows Server 2008 R2
- Microsoft ISA Server 2000/2004/2006 Standard Edition
- Microsoft ISA Server 2004/2006 Enterprise Edition
- Internet Explorer version 6.0 ou supérieure




BitDefender Security for ISA Servers offre des fonctionnalités de détection antivirus, d'administration et de reporting qui permettent de partager des fichiers en toute sécurité

## ANALYSE ET FILTRAGE MULTI-NIVEAUX

Les moteurs d'analyse primés de BitDefender ont étérécompensés par les principaux organismes de certification –y compris ICSA Labs, Virus Bulletin et West Coast Labs – pour leur protection proactive antimalware inégalée. BitDefender offre des méthodes d'analyse et de filtrage à de multiplesniveaux pour détecter les codes malveillants, et protéger vos données confidentielles.

**Trafic web (HTTP)** Le moteur d'analyse détecte en temps réel les virus et les malwares quand les utilisateurs naviguent sur Internet, accèdent à des services de messagerie ou à d'autres applications Internet.

**Téléchargement FTP (montant et descendant)** L'analyse permet de détecter les virus et les malwares en temps réel à chaque fois que les utilisateurs téléchargent des fichiers, en utilisant un service FTP.

**Filtrage du contenu** Le filtrage du contenu permet la détection d'informations prédéfinies de type : numéro de carte ou de compte bancaire, noms de rapports, bases de données clients, etc. et de les empêcher de sortir de manière incontrôlée de l'entreprise. Le filtrage du contenu repose sur des restrictions personnalisées basées sur des adresses de serveurs de sites web ou FTP, des mots clés et la taille des contenus.

**Listes noires et blanches** Pour bloquer les sites web en fonction de mots clés, ou en utilisant une liste de sites reconnus pour être soit dangereux soit sans danger.

**Politiques** Elles permettent de moduler les restrictions qui doivent s'appliquer dans les réseaux d'entreprises, en fonction d'une base d'adresses IP, de types de contenus, ou de protocoles.

## PROTECTION CONTRE LES MENACES ENTRANTES ET SORTANTES

- Détection primée des virus, nettoyage et mise en quarantaine
- Processus d'analyse optimisé et accéléré par l'intégration aux règles du pare-feu et de la mise en cache de Microsoft via l'interface d'analyse antivirus de Microsoft (ISAPI)
- Analyse des fichiers et du contenu web en temps réel pour minimiser les risques de propagation de malware sur le réseau.
- Facilité d'administration par mots clés des listes noires FTP ou de sites web, et aussi des listes blanches de sites sûrs.

## OPTIMISATION, GESTION ET RAPPORTS

- Réduit la charge administrative en permettant la centralisation de la gestion des notifications par intégration des alertes BitDefender au module d'alertes du serveur ISA
- Compatible avec les serveurs ISA déployés en grappes utilisés dans un environnement de trafic dense afin de répartir les charges
- Technologie de gestion des navigateurs (Browser comforting) pour l'analyse et le téléchargement de gros fichiers par petits blocs
- Rapports sur l'activité virale, les statistiques d'analyse et le volume du trafic
- Configuration possible des mesures à prendre face aux événements pour déclencher des alertes ou d'autres types de réaction

bitdefender®