Desktop Firewall ASaP

Service complet de sécurisation par firewall – il surveille, contrôle et tient l'historique de l'activité réseau de votre PC

La plupart des utilisateurs d'ordinateurs personnels (PC) ignorent qu'une fois en ligne, ils sont exposés aux attaques et aux intrusions de la part de pirates informatiques. Ces derniers sont à même d'observer vos faits et gestes sur le réseau, de voler le numéro de votre carte de crédit ou d'accéder à vos informations financières personnelles. Mais les utilisateurs de PC, qu'il s'agisse de petites entreprises ou d'utilisateurs privés, peuvent protéger leurs données en mettant en place un firewall personnel sur leurs postes de travail. En effet, un firewall matériel « traditionnel » à placer à l'entrée d'un réseau s'avère rapidement très cher et n'est pas simple à configurer, bien au contraire. Avec Desktop Firewall ASaP, McAfee Security offre une solution qui est à la fois économique et pré configurée. Reposant sur une technologie de firewall distribué et de détection des intrusions mise au point par McAfee Security, la solution Desktop Firewall ASaP vous permet de disposer d'un service complet de sécurisation par firewall logiciel et de protéger efficacement votre système contre les pirates et les autres menaces de l'Internet.

Un firewall logiciel personnel permet également aux entreprises d'économiser beaucoup d'argent. En effet, les systèmes installés à domicile constituent souvent des passerelles pour accéder aux réseaux des entreprises par l'intermédiaire d'une connexion distante ou d'un réseau virtuel privé (VPN). En installant un firewall personnel sur les ordinateurs portables de ses employés, l'entreprise évite que ces derniers ne soient victimes de pirates et n'infectent le réseau lorsqu'ils s'y connectent à distance.

Que votre PC dispose d'une connexion LAN, d'une connexion à distance ou des deux, McAfee Desktop Firewall ASaP est pré configuré pour sécuriser efficacement la plupart des systèmes courants. Avec McAfee Desktop Firewall ASaP, l'utilisateur peut sélectionner le niveau de sécurisation de son choix : faible, moyen, élevé ou personnalisé. De plus, McAfee Desktop Firewall ASaP se charge et se met à jour automatiquement ; vous êtes donc protégé 24 heures sur 24 contre les menaces et les virus présents sur le réseau local ou Internet.

Fonctionnalités / Avantages

McAfee Desktop Firewall ASaP, conçu par McAfee Security, est un service complet de sécurisation par firewall qui surveille, contrôle et tient l'historique de l'activité réseau de votre PC. Il offre aux utilisateurs une protection économique contre les intrusions potentiellement dangereuses et coûteuses, grâce à un ensemble complet de fonctionnalités avancées :

- Installation simple et rapide
- Blocage du trafic sur autorisation
- Surveillance continue du trafic en arrière-plan
- Mises à jour automatiques
- Configuration flexible de la sécurité
- Détection des vulnérabilités
- Rapports locaux
- Protection optionnelle des VPN

Installation simple et rapide
Lorsqu'il a souscrit un abonnement à Desktop Firewall ASaP, l'utilisateur reçoit une URL qui lui permettra de télécharger Desktop Firewall ASaP depuis un serveur McAfee Security. Pour cela, il lui suffit de cliquer sur l'URL et d'entrer son adresse émail : l'installation commence aussitôt. Desktop Firewall ASaP est pré configuré selon des paramètres qui assurent une bonne sécurisation dans les situations les plus fréquentes. L'ordinateur sur lequel le produit est installé dispose ainsi d'emblée d'une excellente protection et reste constamment à jour. Desktop Firewall ASaP se déploie, s'installe, s'administre et se met à jour automatiquement, sans intervention d'un technicien. Il bloque tout le trafic suspect, 24 heures sur 24, que l'utilisateur soit actif ou non.

Blocage du trafic sur autorisation
McAfee Desktop Firewall ASaP filtre le trafic au niveau des équipements dont dispose votre système, tels que cartes réseau et modems. Cette solution permet de rejeter le trafic entrant suspect avant qu'il ne puisse s'en prendre à des fonctions vitales de votre PC et détruire de précieuses ressources système. McAfee Desktop Firewall ASaP effectue ce contrôle en vous permettant de définir des applications comme « autorisées » et « non autorisées ». Les utilisateurs peuvent également consulter une liste des applications dont l'accès est autorisé. Lorsqu'une application autorisée doit accéder à un réseau, McAfee Desktop Firewall ASaP en gère le trafic au point d'accès. Si McAfee Desktop Firewall ASaP détecte une tentative d'accès réseau de la part d'une application non autorisée, il bloque tout le trafic en direction ou en provenance de l'application en question.

Surveillance continue du trafic en arrière-plan
McAfee Desktop Firewall ASaP est une solution idéale pour les connexions toujours ouvertes, telles qu'un modem câble ou une ligne DSL. En effet, Desktop Firewall ASaP protège votre système en continu par le blocage des accès réseau non autorisés et l'arrêt des attaques connues : piratages, bombes, troyens et dénis de service (DoS). McAfee Desktop Firewall ASaP remplit son rôle de contrôleur d'accès en arrière-plan, en bloquant discrètement tout le trafic non autorisé, 24 heures sur 24, que votre ordinateur soit actif ou non.

Mises à jour automatiques
Les mises à jour parviennent automatiquement aux PC protégés grâce à la technologie Rumor© mise en œuvre pour les services ASaP. Les fonctions Rumor© sont intégrées à l'Agent ASaP (client léger sur le poste), que se partAgent VirusScan ASaP et Desktop Firewall ASaP. Le système se met à jour toutes les 24 heures et d'office au démarrage. Le système vérifie son état et, au besoin, met à jour le firewall et apporte les modifications requises au profil de sécurisation de l'utilisateur. L'utilisateur peut également mettre à jour manuellement sa configuration.

Configuration flexible de la sécurité
En fonction de son contexte de travail, l'utilisateur de Desktop Firewall ASaP peut choisir une sécurisation de niveau élevé, moyen ou faible :

- **Niveau élevé.** Pour les PC nécessitant une sécurisation maximale. Ce paramétrage impose une autorisation d'accès pour chaque application, bloque l'accès au partage de ressources et masque les ports non utilisés.

- **Niveau moyen.** Pour les PC qui doivent être protégés contre certaines activités peu sûres. Ce paramétrage permet à l'utilisateur de bloquer l'accès de tiers à ses ressources, tout en autorisant l'utilisation des ressources d'autres ordinateurs. Ce niveau de sécurisation ne masque pas les ports.

- **Niveau faible.** Pour les PC sur lesquels la sécurité n'est pas une priorité. Le trafic de données circule librement vers et en provenance de l'Internet ; les ressources sont partagées et disponibles.

Détection des vulnérabilités
Comme Desktop Firewall ASaP permet aux utilisateurs de tenir la liste des applications qu'ils ont autorisées et celles qu'ils ont bloquées, les programmes cachés sont également détectés lorsqu'ils tentent d'accéder à l'Internet. Desktop Firewall ASaP notifie l'utilisateur de la présence de ces programmes cachés, dont un pirate peut se servir pour se donner un accès distant à votre PC ou qui peut diffuser des informations privées stockées sur votre système.

Rapports locaux
Des rapports locaux permettent à l'utilisateur de vérifier le fonctionnement de son firewall personnel et de consulter l'historique des attaques de pirates.

Protection optionnelle des VPN
En option, Desktop Firewall ASaP permet également de protéger les réseaux privés virtuels (VPN), éliminant la nécessité de configurer manuellement la gestion des protocoles.

McAfee Security introduit Rumor©, une nouvelle technologie ASaP qui fait usage de la distribution Peer-to-Peer (point à point) et du partage de fichiers pour administrer les mises à jour des configurations d'antivirus et de firewalls.

Rumor©, technologie VirusScan ASaP basée sur les transferts point à point, donne aux utilisateurs la possibilité de partager les mises à jour de configuration d'antivirus et de firewalls. Elle permet ainsi de faire des économies de bande passante, de temps d'administration et donc d'argent pour la protection antivirus.

L'Agent VirusScan ASaP passe par des serveurs proxy et des firewalls, sur lesquels la technologie Rumor© de McAfee fonctionne afin de diffuser les mises à jour sur le réseau interne. Cela permet d'augmenter la vitesse d'installation et de mise à jour, et de réduire en la quantité de bande passante utilisée.

Partagez les mises à jour de configuration d'antivirus et de firewalls en utilisant Rumor©

- Diffusion point à point
- Partage de certains types de fichiers uniquement
- Indépendamment de l'application
- Tiquet d'authentification
- Reprise des téléchargements interrompus

QUESTIONS TECHNIQUES FRÉQUEMMENT POSÉES

Basée sur le produit Personal Firewall de McAfee, la solution Desktop Firewall ASaP vous permet de disposer d'un service complet de sécurisation par firewall logiciel et de protéger efficacement votre système contre les pirates et les autres menaces de l'Internet. En cliquant sur les liens ci-après, vous pourrez consulter les réponses à des questions fréquemment posées sur la manière dont Desktop Firewall ASaP peut protéger votre système 24 heures sur 24 contre les attaques des pirates et les menaces virales.

- Qu'est-ce que Desktop Firewall ASaP ?
- En quoi Desktop Firewall ASaP diffère-t-il d'un firewall classique ?
- Comment Desktop Firewall ASaP est-il géré ?
- Quelles sont les options de sécurité et de filtrage de Desktop Firewall ASaP ?
- En cas de modification de mon niveau de sécurité ou de filtrage, dois-je redémarrer mon ordinateur pour appliquer les nouveaux paramètres ?
- Puis-je utiliser Desktop Firewall ASaP avec mes connexions Internet et LAN ?
- Desktop Firewall ASaP a-t-il une incidence sur les performances des mon système ?
- Quelles sont les plates-formes prises en charge par Desktop Firewall ASaP ?
- Qu'est-ce qu'un paquet fragmenté ? Comment savoir si je dois les bloquer ou les consigner ?
- Quelle est la fonction du bouton « Adaptateurs » dans la configuration des zones de sécurité ?
- Comment empêcher l'affichage de la fenêtre Autoriser / Refuser (au cours d'un jeu par exemple) ?
- Qu'en est-il d'une application qui tente une connexion réseau alors que les notifications sont désactivées ?
- Où sont stockés mes historiques ?
- Quand faut-il utiliser le bouton « Paramètres avancés » pour personnaliser la configuration de mon produit Desktop Firewall ASaP ?
- Quand faut-il effacer mon historique d'activité ?
- Quelles sont les applications acceptées automatiquement ?
- Comment paramétrer Desktop Firewall ASaP pour bloquer tout le trafic ?

Qu'est-ce que Desktop Firewall ASaP ?

Desktop Firewall ASaP est un service complet de sécurisation par firewall, qui surveille, contrôle et enregistre l'historique de l'activité réseau de votre PC. Ce firewall personnel administre et protège votre système 24 heures sur 24 et 7 jours sur 7 par le blocage des accès réseau non autorisés et l'arrêt des attaques connues : piratages, bombes, troyens et dénis de service (DOS).

En quoi Desktop Firewall ASaP diffère-t-il d'un firewall classique ?

Desktop Firewall ASaP contrôle le flux de données à destination et en provenance de votre ordinateur. Le service se configure automatiquement et ne nécessite pas de connaissances préalables en matière de ports ou de protocoles. Desktop Firewall ASaP propose par défaut trois configurations à différents niveaux de sécurisation (élevée, moyenne et faible) ; de ce fait, il est nettement plus simple à mettre en place que les firewalls traditionnels. Desktop Firewall ASaP est également très simple à installer : inutile de monter des équipements matériels spécifiques, il suffit de télécharger un logiciel sous forme de client léger (l'Agent ASaP).

Comment Desktop Firewall ASaP est-il géré ?

Desktop Firewall ASaP se charge automatiquement au démarrage de votre ordinateur. Il est configuré par défaut pour prendre en charge des environnements courants tels que le système d'exploitation Microsoft Windows. Lors des premières utilisations, le programme vous demandera d'autoriser ou de refuser d'autres applications lorsqu'elles tentent un accès réseau.

Quelles sont les options de sécurité et de filtrage de Desktop Firewall ASaP ?

Desktop Firewall ASaP propose trois niveaux de sécurité : Elevé, Moyen et Faible.

- Niveau élevé. Ce réglage est recommandé pour disposer d'une sécurisation maximale.
  - Chaque programme utilisé doit être muni d'un niveau d'autorisation
  - Blocage de l'accès au partage de ressources
  - Masquage des ports non utilisés

- Niveau moyen. Ce paramétrage est recommandé pour bloquer certaines activités peu sûres.
  - Chaque programme utilisé doit être muni d'un niveau d'autorisation
  - Blocage de l'accès partagé aux ressources de votre ordinateur
  - Utilisation permise des ressources d'autres ordinateurs
  - Pas de masquage des ports.

- Niveau faible. Paramétrage minimal pour les systèmes sur lesquels la sécurité n'est pas une priorité.
  - Autorisation des applications
  - Trafic autorisé en direction et en provenance de l'Internet
  - Ressources partagées / disponibles
  - Pas de masquage des ports.

En cas de modification de mon niveau de sécurité ou de filtrage, dois-je redémarrer mon ordinateur pour appliquer les nouveaux paramètres ?

Non. Lorsque votre niveau de sécurité ou le paramétrage du filtrage sont modifiés, Desktop Firewall ASaP charge immédiatement la nouvelle configuration.

Puis-je utiliser Desktop Firewall ASaP avec mes connexions Internet et LAN ?

Oui. Desktop Firewall ASaP fonctionne avec les types de connexions réseau suivants : connexion distante (modem et ligne téléphonique), Ethernet (10/100), DSL via Ethernet, Câble via Ethernet et PPPoE.

Desktop Firewall ASaP a-t-il une incidence sur les performances de mon système ?

Desktop Firewall ASaP n'a pratiquement pas d'incidence sur les performances de votre système. Le programme nécessite un espace de 5 Mo sur le disque dur, soit beaucoup moins que d'autres firewalls personnels disponibles dans le commerce.

Quelles sont les plates-formes prises en charge par Desktop Firewall ASaP ?

Windows 95, Windows 98/SE, Windows ME et Windows NT4.

Qu'est-ce qu'un paquet fragmenté ? Comment savoir si je dois les bloquer ou les consigner ?

La fragmentation de paquets est une technique couramment utilisée par les pirates pour attaquer un système informatique. Il est recommandé de bloquer les paquets fragmentés.

Quelle est la fonction du bouton « Adaptateurs » dans la configuration des zones de sécurité ?

Les réglages relatifs aux adaptateurs se rapportent aux trois « zones » protégées par Desktop Firewall ASaP : Internet, Réseau local (Local Area Network – LAN) et Néant (zone non protégée par Desktop Firewall ASaP). En cliquant sur le bouton « Adaptateurs », vous pouvez sélectionner un autre adaptateur réseau. L'adaptateur sélectionné est identifié par l'icône « LAN (2 ordinateurs) », « Internet (globe) » ou « Néant (point d'interrogation) ».

Comment empêcher l'affichage de la fenêtre Autoriser/Refuser (au cours d'un jeu par exemple) ?

Dans la barre d'état système, cliquez à l'aide du bouton droit sur l'icône de l'Agent ASaP et choisissez « Firewall ». Une liste déroulante vous propose alors plusieurs options, dans lesquelles vous pouvez choisir la désactivation ou l'activation des notifications qui vous invitent à autoriser ou à refuser l'accès réseau pour une application. (Si l'icône a l'aspect d'un signal de stop rouge, toutes les notifications d'applications sont bloquées.) Pour activer les notifications, cliquez sur « Activer notification ».

Qu'en est-il d'une application qui tente une connexion réseau alors que les notifications sont désactivées ?

Lorsque les notifications sont désactivées, toutes les applications qui tentent un accès réseau sont temporairement bloquées. Lorsque vous réactivez les notifications, Desktop Firewall ASaP vous signalera à nouveau les tentatives d'accès réseau de la part de ces applications, et vous pourrez les autoriser ou les refuser.

Où sont stockés mes historiques ?

Vos fichiers d'historique d'activité réseau sont archivés lorsque leur taille atteint 500 Ko. Ils sont alors sauvegardés dans le répertoire myCIO/Reports et renommés comme suit : <nom de zone>-<date initiale>-<date finale>.htm (par exemple : internet-2000.08.09-2000.10.10.htm).

Quand faut-il utiliser le bouton « Paramètres avancés » pour personnaliser la configuration de mon produit Desktop Firewall ASaP ?

Pour la plupart des utilisateurs, les niveaux de sécurité pré configurés (Faible, Moyen et Elevé) suffisent pour protéger adéquatement le système. La fonction de personnalisation, ou paramétrage avancé, est destinée aux utilisateurs qui ont une bonne connaissance de différents protocoles tels que DHCP, RIP et PPTP. Si la manipulation de ces protocoles ne vous est pas familière, EVITEZ D'EFFECTUER DES REGLAGES MANUELS. Lorsque vous configurez manuellement Desktop Firewall ASaP, il se peut que la sécurité de votre système ne soit plus assurée correctement.

Quand faut-il effacer mon historique d'activité ?

Effacez votre fichier d'historique lorsqu'il devient trop long ou trop difficile à lire. Certains utilisateurs parcourent leur historique une fois par jour, notent les anomalies éventuelles, puis en effacent le contenu. Il s'agit bien sûr d'une préférence personnelle : vous pouvez effacer le contenu de votre fichier d'historique aussi souvent que vous le souhaitez.

Quelles sont les applications acceptées automatiquement par Desktop Firewall ASaP?

- **MYAGTSVC** (Agent Rumor©)
- **UPDDLG** (Moteur de mise à jour)
- **MCUPDATE** (Agent de mise à jour de VirusScan win32)
- **MSTASK** (Système d'exploitation Windows)
- **MSDTC** (Système d'exploitation Windows)
- **SERVICES** (Système d'exploitation Windows)
- **RPCSS** (Système d'exploitation Windows)
- **TCPSVS** (Système d'exploitation Windows)

Comment paramétrer Desktop Firewall ASaP pour bloquer tout le trafic ?

Dans la barre d'état système, cliquez à l'aide du bouton droit sur l'icône et choisissez « FireWall ». Dans la liste déroulante, choisissez « Configuration ». Dans l'écran de configuration, cliquez sur l'onglet « Global ». Placez le curseur du niveau de filtrage sur « Tout bloquer ». Cliquez sur « Appliquer » ou sur « OK » pour confirmer vos modifications. ** *REMARQUE : Cette opération vous déconnecte en principe du réseau.