McAfee®

personal firewall plus

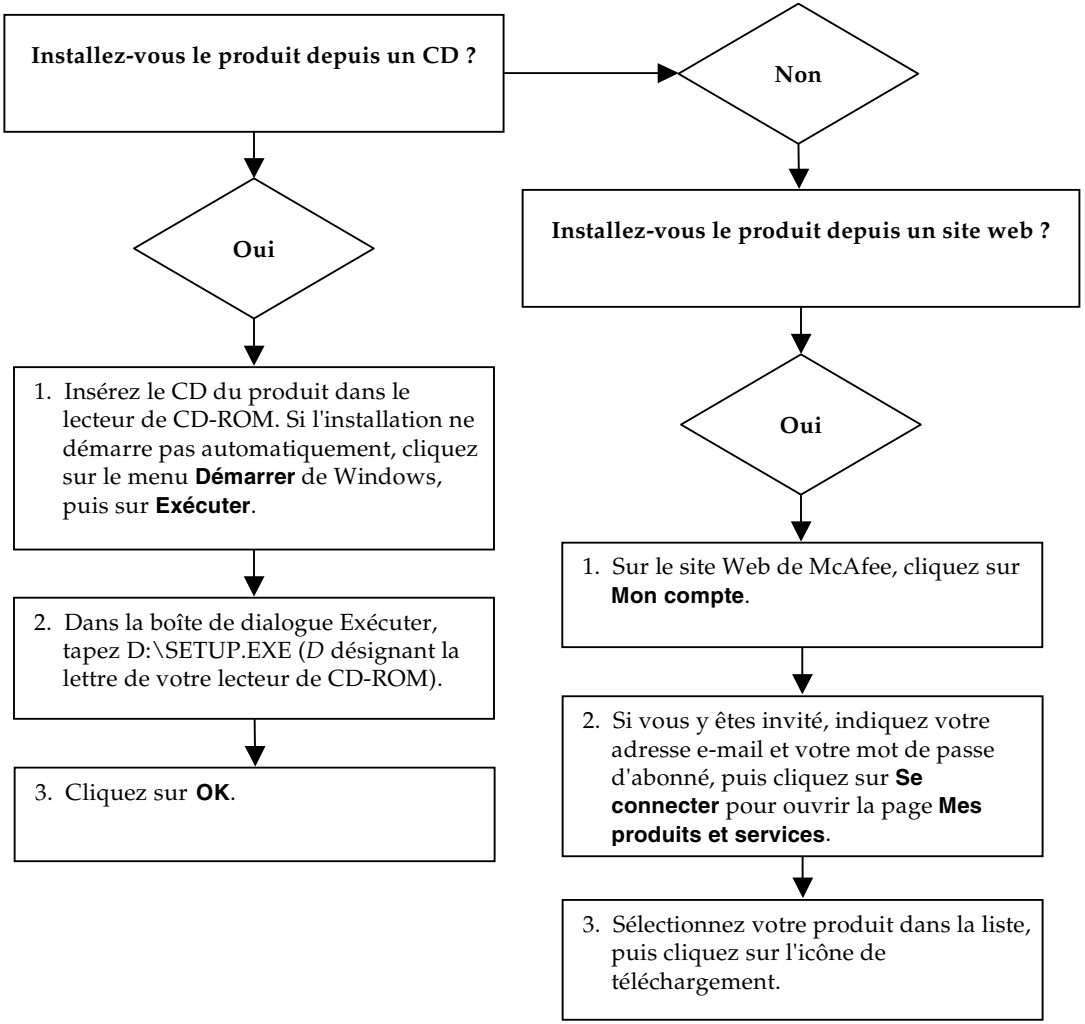
Guide de l’utilisateur

Version 6.0

McAfee®

Carte de configuration rapide

Si vous installez le produit à partir d'un CD ou du site Web, imprimez cette page comme référence.



Pour plus d'informations

Pour pouvoir consulter les Guides d'utilisateurs qui se trouvent sur le CD du produit, assurez-vous qu'Acrobat Reader est installé sur votre ordinateur ; sinon, installez-le depuis le CD du produit McAfee.

1. Insérez le CD du produit dans le lecteur CD-ROM.
2. Ouvrez l'Explorateur Windows : cliquez sur le menu **Démarrer** de Windows, puis sur **Rechercher**.
3. Localisez le dossier Manuals et double-cliquez sur le fichier PDF du guide de l'utilisateur à ouvrir.

Avantages de l'enregistrement

Nous vous conseillons de suivre les instructions fournies dans votre produit pour nous transmettre directement l'enregistrement. Grâce à cet enregistrement, vous bénéficierez d'un support technique compétent et opportun, ainsi que des avantages suivants :

- Un support électronique GRATUIT.
- Des mises à jour des fichiers de définition de virus (.DAT) pendant un an à compter de la date d'installation du logiciel VirusScan si vous achetez ce logiciel.

  Consultez le site http://fr.mcafee.com pour obtenir la tarification d'une année supplémentaire de signatures de virus.
- Une garantie de 60 jours couvrant le remplacement du CD-ROM de votre logiciel si celui-ci est défectueux ou endommagé.
- Des mises à jour des filtres SpamKiller pendant un an à compter de la date d'installation si vous achetez ce logiciel.

  Consultez le site http://fr.mcafee.com pour obtenir la tarification d'une année supplémentaire de mises à jour de filtres.
- Des mises à jour de McAfee Internet Security Suite pendant un an à compter de la date d'installation du logiciel MIS si vous achetez ce logiciel.

  Consultez le site http://fr.mcafee.com pour obtenir la tarification d'une année supplémentaire de mises à jour du contenu.

Assistance technique

Pour toute question relative au support technique, consultez notre site http://www.mcafeeaide.com/. Notre site de support offre 24 h/24 un accès à un Assistant convivial permettant d'obtenir des solutions aux questions de support les plus courantes.

Les utilisateurs confirmés peuvent également essayer nos options avancées, parmi lesquelles une fonction de recherche par mot clé et notre arborescence d'aide. Si vous ne parvenez pas à résoudre votre problème, vous pouvez aussi accéder aux options gratuites de conversation et de courrier électronique. Ces options options vous permettent de communiquer rapidement et gratuitement avec nos ingénieurs du support technique, via Internet. Vous trouverez également des informations relatives à notre service d'assistance téléphonique sur notre site http://www.mcafeeaide.com/.

Numéros de téléphone d’urgence

Pays	Numéro de téléphone
Afrique du Sud	011 700-8216
Allemagne	06 966 404 330
Autriche	017 908 75 810
Belgique	02 27 50 703
Brésil	11 4196-7077
Danemark	03 5258 321
Espagne	901-120 175 (* prix d'un appel normal)
Finlande	09 229 06 000
France	01 70 20 00 08
Italie	02 45 28 15 10
Luxembourg	040 666 15670
Norvège	02 3050420
Pays-Bas	020 504 0586
Portugal	00 31 20 586 6430 (anglais parlé)
République d’Irlande	01 601 55 80
Royaume-Uni	020 794 901 07
Suisse	022 310 1033
Suède	08 57 92 9004

Sommaire

Prise en main 1

Bienvenue dans McAfee Personal Firewall Plus.

Le logiciel McAfee Personal Firewall Plus offre à votre ordinateur et à vos données personnelles une protection avancée. Personal Firewall établit une barrière entre votre ordinateur et Internet. Il surveille silencieusement le trafic Internet et signale toute activité suspecte.

Il fournit les fonctions suivantes :

- Protège efficacement contre les attaques et les tentatives de piratage
- Complète les protections antivirus
- Surveille le trafic Internet et l'activité du réseau
- Donne l'alerte en cas d'événement potentiellement hostile
- Fournit des informations détaillées sur le trafic Internet suspect
- Intègre des fonctionnalités de Hackerwatch.org, telles que les rapports d'événements, les outils d'autotest et la possibilité d'informer par courrier électronique d'autres autorités en ligne des événements signalés
- Inclut des fonctions de traçage détaillé et de recherche d'événement

Nouvelles fonctionnalités

- **Intégration avancée de HackerWatch.org**
  Le signalement de pirates potentiels n'a jamais été aussi simple. McAfee Personal Firewall Plus améliore la fonctionnalité de HackerWatch.org, qui permet de soumettre des événements potentiellement nuisibles dans la base de données.

- **Manipulation intelligente et étendue des applications**
  Dès qu'une application cherche à accéder à Internet, Personal Firewall commence par vérifier si elle est reconnue comme une application fiable ou malveillante. Dans le premier cas, Personal Firewall autorise automatiquement (à votre place) une application fiable à accéder à Internet. Cette base de données a été améliorée pour fournir aux utilisateurs plus d'informations sur les applications se connectant à Internet.

- **Détection avancée des chevaux de Troie**
  McAfee Personal Firewall Plus associe une gestion des connexions des applications à une base de données améliorée pour détecter et empêcher davantage d'applications potentiellement malveillantes, telles que les chevaux de Troie, d'accéder à Internet dans le but de transmettre éventuellement vos données personnelles.

- **Amélioration du suivi visuel**
  McAfee Personal Firewall Plus est livré avec un outil de suivi des intrus actualisé, connu sous le nom de Visual Trace. Visual Trace inclut des cartes graphiques faciles à lire indiquant la source des attaques hostiles et le chemin qu'elles empruntent à travers les réseaux du monde entier, notamment des informations détaillées sur le contact et le propriétaire des adresses IP d'origine, ainsi que toutes les étapes suivantes jusqu'à votre ordinateur. La fonction Visual Trace de McAfee Personal Firewall Plus contient désormais un plus grand nombre de données géographiques, affinant ainsi les informations relatives à la situation géographique et une description visuelle améliorée des lieux où se trouvent les intrus. Visual Trace permet aux utilisateurs de tracer visuellement l'origine des intrusions et d'obtenir, grâce à ces nouvelles données, une meilleure visualisation graphique de leurs recherches.

- **Amélioration de la convivialité**
  McAfee Personal Firewall Plus comprend un Assistant de configuration et un Didacticiel utilisateur pour guider les utilisateurs dans la configuration et l'utilisation de leur pare-feu. Bien que le produit soit conçu pour fonctionner sans intervention, McAfee apporte à ses utilisateurs une grande quantité d'informations pour comprendre et se rendre compte de ce que le pare-feu leur apporte.

- **Amélioration de la détection d'intrusions**
  Le système de détection d'intrusions (IDS) de Personal Firewall détecte les méthodes d'attaque connues et toute autre activité suspecte. Dans chaque paquet de données, le système de détection d'intrusions recherche des transferts ou des méthodes de transferts de données suspects et consigne les résultats dans un journal d'événements.

- **Amélioration de l'analyse du trafic**
  McAfee Personal Firewall Plus permet aux utilisateurs de visualiser les données entrantes et sortantes de leur ordinateur, et d'afficher les connexions des applications, notamment les applications qui sont activement « à l'écoute » des connexions ouvertes. Les utilisateurs peuvent ainsi visualiser et agir sur les applications susceptibles de faire l'objet d'une intrusion.

Configuration système requise

- Microsoft® Windows 98, Me, 2000 ou XP
- Ordinateur personnel avec processeur
  Windows 98 ou Me : Pentium 150 MHz ou supérieur
  Windows 2000 ou XP : Pentium 233 MHz ou supérieur
- Mémoire vive
  Windows 98 : 32 Mo (64 Mo recommandés)
  Windows Me, 2000 ou XP : 64 Mo (128 Mo recommandés)
- 35 Mo d'espace disque
- Microsoft® Internet Explorer 5.5 ou ultérieur

REMARQUE
Pour mettre à niveau Internet Explorer vers la version la plus récente, consultez le site Web de Microsoft à l'adresse http://www.microsoft.com/worldwide.

Désinstallation d'autres pare-feux

Avant d'installer le logiciel McAfee Personal Firewall Plus, vous devez désinstaller de votre ordinateur tout autre pare-feu. Pour ce faire, suivez les instructions de désinstallation de votre pare-feu.

REMARQUE
Si vous utilisez Windows XP, il n'est pas nécessaire de désactiver le pare-feu intégré avant d'installer le logiciel McAfee Personal Firewall Plus. Il est toutefois recommandé de désactiver le pare-feu intégré. Sinon, vous ne recevrez pas les événements dans le journal d'événements entrants de McAfee Personal Firewall Plus.

Définir le pare-feu par défaut

McAfee Personal Firewall peut gérer les autorisations et le trafic des applications Internet sur votre ordinateur, même s'il détecte que le pare-feu Windows s'y exécute.

Lorsqu'il est installé, McAfee Personal Firewall désactive automatiquement le pare-feu Windows et devient votre pare-feu par défaut. Vous découvrez alors exclusivement les fonctionnalités et la messagerie de McAfee Personal Firewall. Si vous activez ensuite le pare-feu Windows via le Centre de sécurité Windows ou le Panneau de configuration de Windows en laissant les deux pare-feux s'exécuter sur votre ordinateur, vous constaterez peut-être une perte partielle de consignation dans McAfee Firewall, ainsi qu'une duplication des messages de statut et d'alerte.

REMARQUE
Si les deux pare-feux sont activés, McAfee Personal Firewall ne montre pas toutes les adresses IP bloquées dans son onglet Événements entrants. Le pare-feu Windows intercepte la majorité de ces événements et les bloque, en empêchant McAfee Personal Firewall de les détecter ou de les consigner. Mais McAfee Personal Firewall peut bloquer du trafic supplémentaire en fonction d'autres facteurs de sécurité. Ce trafic sera alors consigné.

Dans le pare-feu Windows par défaut, la consignation est désactivée, mais si vous choisissez d'activer les deux pare-feux, vous pouvez l'activer. Le journal par défaut du pare-feu Windows est C:\Windows\pfirewall.log

Pour assurer que votre ordinateur est protégé par au moins un pare-feu, le pare-feu Windows est automatiquement réactivé lorsque McAfee Personal Firewall est désinstallé.

Si vous désactivez McAfee Personal Firewall ou que vous fixez ses paramètres de sécurité sur **Ouvert** sans activer manuellement le pare-feu Windows, toute protection par pare-feu sera supprimée, sauf pour les applications déjà bloquées.

Définir le niveau de sécurité

Vous pouvez configurer des options de sécurité pour indiquer la manière dont Personal Firewall doit réagir lorsqu'il détecte un trafic indésirable. Par défaut, le niveau de sécurité **Standard** est activé. Utilisez ce paramètre si vous êtes un utilisateur débutant. Si vous êtes un utilisateur expérimenté du pare-feu, vous pouvez utiliser d'autres paramètres. Au niveau de sécurité **Standard**, si une application requiert un accès Internet et que vous lui accordez, cela revient à lui accorder un accès total. L'accès total permet à l'application d'envoyer ou de recevoir des données non sollicitées sur des ports non-système.

Pour configurer les paramètres de sécurité :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis cliquez sur **Utilitaires**.
2. Cliquez sur l'icône **Paramètres de sécurité**.
3. Pour définir le niveau de sécurité, faites glisser le curseur jusqu'au niveau souhaité.

Si vous êtes un utilisateur débutant, acceptez le paramètre **Standard** proposé par défaut. Les niveaux de sécurité vont de Verrouillage à Ouvert :

- **Verrouillage —** Tout le trafic est arrêté. Cela équivaut à débrancher votre connexion Internet. Vous pouvez utiliser ce paramètre pour bloquer les ports que vous avez configurés comme ouverts dans la page Services système.
- **Niveau de sécurité élevé —** Une application ne demande que le type d'accès à Internet dont elle a explicitement besoin (par exemple, Accès sortant uniquement), et soit vous l'autorisez, soit vous le bloquez. Si par la suite l'application demande un accès total, vous pourrez soit accorder cet Accès total, soit conserver l'Accès sortant uniquement. Utilisez ce paramètre uniquement si vous êtes un utilisateur averti en matière de pare-feu.
- **Niveau de sécurité Standard (conseillé) —** Lorsqu'une application requiert un accès Internet et que vous lui accordez, cela revient à lui accorder un accès total. L'Accès total permet à l'application d'envoyer ou de recevoir des données non sollicitées sur des ports non-système. Utilisez ce paramètre si vous êtes un utilisateur débutant.
- **Niveau de sécurité faible —** Toutes les applications sont automatiquement à ce niveau de sécurité lorsqu'elles essaient d'accéder à Internet pour la première fois. Toutefois, vous pouvez choisir d'être averti par une alerte lorsque de nouvelles applications sont autorisées. Utilisez ce paramètre si vous constatez que certains jeux ou transmissions multimédia en temps réel ne fonctionnent pas.
- **Ouvert —** Votre pare-feu est réellement désactivé. Ce paramètre autorise tout le trafic par l'intermédiaire du Personal Firewall sans filtrage.

REMARQUE
Les applications qui étaient bloquées le seront toujours lorsque le pare-feu sera paramétré sur le niveau de sécurité **Ouvert** ou sur **Désactivé**. Pour empêcher ceci de se produire, vous pouvez soit modifier les autorisations des applications en **Accès total** ou simplement supprimer la règle d'autorisation **Bloqué** dans la liste **Autorisations**.

4 Sélectionnez d'autres paramètres de sécurité :

REMARQUE
Si vous utilisez Windows XP et que plusieurs utilisateurs XP ont été ajoutés, ces options ne sont disponibles que si vous êtes connecté à votre ordinateur en tant qu'administrateur.

- **Enregistrer les événements du système de détection d'intrusion (IDS) dans le journal des événements entrants —** Si vous sélectionnez cette option, les événements détectés par IDS apparaîtront dans le journal d'événements entrants. Le système de détection d'intrusions détecte les types d'attaque classique et d'autres activités suspectes. Le système de détection d'intrusions contrôle chaque paquet de données entrant et sortant afin de détecter les transferts de données ou les méthodes de transfert suspects. Il les compare à une base de données de signatures et y dépose automatiquement les paquets provenant de l'ordinateur en cause.

  IDS recherche des schémas de trafic spécifiques utilisés par les attaquants. IDS contrôle chaque paquet reçu par votre machine afin de détecter le trafic suspect ou connu comme une attaque. Par exemple, si Personal Firewall détecte la présence de paquets ICMP, il les analyse pour rechercher des schémas de trafic suspects en comparant le trafic ICMP aux schémas d'attaque connus.

- **Accepter les requêtes de ping ICMP** — Le trafic ICMP est principalement utilisé pour réaliser des suivis et des pings. Les pings sont fréquemment utilisés pour effectuer un test rapide avant d'initier des communications. Si vous utilisez, ou avez utilisé dans le passé, un programme de partage de fichiers d'égal à égal (peer-to-peer), vous risquez de recevoir un grand nombre de requêtes ping. Si vous sélectionnez cette option, Personal Firewall autorise toutes vos requêtes ping sans les consigner dans le journal des événements entrants. Si vous ne sélectionnez pas cette option, Personal Firewall bloque toutes vos requêtes ping et les inscrit dans le journal des événements entrants.

- **Autoriser les utilisateurs disposant d'un accès restreint à modifier les paramètres de Personal Firewall** — Si vous utilisez Windows XP et que plusieurs utilisateurs XP ont été ajoutés, assurez-vous que cette case est cochée si vous voulez autoriser les utilisateurs XP disposant d'un accès restreint à modifier les paramètres de Personal Firewall.

5 Cliquez sur **OK** lorsque vous avez terminé.

Test de McAfee Personal Firewall Plus

Pour tester Personal Firewall :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee  , choisissez **Personal Firewall**, puis cliquez sur **Tester le firewall**.
2. Personal Firewall ouvre Internet Explorer et va sur l'adresse http://www.hackerwatch.org/, site Web géré par McAfee. Suivez les indications figurant sur la page de test Hackerwatch.org afin de tester Personal Firewall.

REMARQUE
Si vous vous connectez à Internet via un serveur proxy ou un serveur de translation des adresses réseau (NAT, Network Address Translation), comme c'est le cas dans la plupart des réseaux d'entreprise (LAN), vous n'obtiendrez pas les bons résultats. Le testeur de pare-feu de Hackerwatch.org recherche quel ordinateur a demandé le test et teste cet ordinateur. Avec une connexion via un serveur proxy ou NAT, il se contente de transmettre la demande de test de pare-feu provenant de votre ordinateur, si bien que Hackerwatch.org teste un ordinateur, mais pas le bon. Les résultats obtenus sont ceux du serveur proxy, pas de votre ordinateur.

Utilisation de McAfee SecurityCenter

McAfee SecurityCenter est votre centre de sécurité unifié, accessible à partir de son icône dans la barre d'état système Windows ou depuis votre bureau Windows. Il vous permet d'exécuter les tâches utiles suivantes :

- Obtenir une analyse gratuite de la sécurité de votre ordinateur.
- Lancer, gérer et configurer tous vos abonnements McAfee à partir d'une seule icône.
- Consulter des alertes de virus et des actualités produits continuellement mises à jour.
- Recevoir des abonnements d'essai gratuits pour télécharger et installer des versions d'essai directement depuis McAfee à l'aide de notre processus breveté de fourniture de logiciels.
- Obtenir des liens rapides vers le forum de questions et les détails de votre compte sur le site Web de McAfee.

REMARQUE
Pour plus d'informations sur ses fonctions, cliquez sur **Aide** dans la boîte de dialogue **SecurityCenter**.

Lorsque vous exécutez SecurityCenter et que toutes les fonctionnalités McAfee installées sur votre ordinateur sont activées, une icône M rouge apparaît dans la barre d'état système Windows. Cette zone se trouve dans l'angle inférieur droit du bureau Windows et contient l'horloge.

Si une ou plusieurs des applications McAfee installées sur votre ordinateur sont désactivées, l'icône McAfee devient noire .

Pour ouvrir McAfee SecurityCenter :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee .
2. Cliquez sur **Ouvrir SecurityCenter**.

Pour accéder à une fonction de Personal Firewall :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee .
2. Pointez sur **Personal Firewall**, puis cliquez sur la fonction que vous souhaitez utiliser.

Utilisation de McAfee Personal Firewall Plus 2

Pour ouvrir Personal Firewall :

Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis cliquez sur **Afficher le résumé**, **Applications Internet**, **Événements entrants** ou **Utilitaires**.

À propos de la page Résumé

Le Résumé de Personal Firewall comporte quatre pages : Résumé principal, Résumé des applications, Résumé des événements et HackerWatch Summary (Résumé HackerWatch). Les pages de résumé contiennent différents rapports sur les événements entrants récents, l'état des applications et les activités d'intrusion dans le monde entier répertoriées par HackerWatch.org. Vous y trouverez également des liens vers les tâches couramment effectuées dans Personal Firewall.

Pour ouvrir les pages de résumé de Personal Firewall, cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis cliquez sur **Afficher le résumé**. La page Résumé principal apparaît (Figure 2-1).

Figure 2-1. Page Résumé principal

Pour naviguer entre les pages de résumé, utilisez les boutons suivants :

Élément	Description
Modifier l'affichage	Cliquez sur **Modifier l'affichage** pour accéder à la liste des pages de résumé, puis sélectionnez une page dans la liste.
 Flèche droite	Cliquez sur la flèche droite pour passer à la page de résumé suivante.
 Flèche gauche	Cliquez sur la flèche gauche pour revenir à la page de résumé précédente.
 Accueil	Cliquez sur l'icône Accueil pour revenir à la page **Résumé principal**.

La page Résumé principal fournit les informations suivantes :

Élément	Description
Paramètre de sécurité	L'état des paramètres de sécurité vous indique le niveau de sécurité sur lequel le pare-feu est défini. Cliquez sur ce lien pour modifier le niveau de sécurité.
Événements bloqués	L'état des événements bloqués affiche le nombre d'événements ayant été bloqués aujourd'hui. Cliquez sur ce lien pour afficher les détails des événements à partir de la page Événements entrants.
Modifications des règles d'application	L'état des règles d'application affiche le nombre de règles d'applications récemment modifiées. Cliquez sur ce lien pour afficher la liste des applications autorisées et bloquées et pour modifier les autorisations des applications.
Nouveautés	**Nouveautés** désigne la dernière application à laquelle a été accordé un accès total à Internet.
Dernier événement	**Dernier événement** affiche les derniers événements entrants. Vous pouvez cliquer sur un lien pour tracer l'événement ou pour autoriser l'adresse IP. Le fait d'autoriser une adresse IP autorise tout le trafic provenant de cette adresse IP à arriver sur votre ordinateur.
Rapport quotidien	**Rapport quotidien** affiche le nombre d'événements entrants bloqués par Personal Firewall aujourd'hui, cette semaine-ci et ce mois-ci. Cliquez sur ce lien pour afficher les détails des événements à partir de la page Événements entrants.
Applications actives	**Applications actives** répertorie les applications, ouvertes sur votre ordinateur, qui accèdent à Internet. Cliquez sur une application pour voir les adresses IP auxquelles elle se connecte.
Tâches communes	Cliquez sur un lien dans **Tâches communes** pour accéder aux pages de Personal Firewall qui présentent l'activité du pare-feu et vous permettent d'exécuter des tâches relatives aux applications.

Pour afficher la page Résumé des applications, cliquez sur **Modifier l'affichage**, puis sélectionnez **Résumé des applications**. La page Résumé des applications fournit les informations suivantes :

Élément	Description
Moniteur de trafic	Le **Moniteur de trafic** présente les volumes de trafic entrant et sortant sur votre connexion Internet au cours des dix dernières minutes. Cliquez sur le graphique pour afficher les détails du suivi du trafic.
Applications actives	**Applications actives** présente la largeur de la bande passante utilisée par les applications les plus actives au cours des dernières 24 heures. **Application** : nom de l'application qui accède à Internet. **%** : pourcentage de la bande passante utilisé par l'application. **Autorisation** : type d'accès à Internet accordé à l'application. **Règle créée** : date de création de la règle d'application.
Nouveautés	**Nouveautés** désigne la dernière application à laquelle a été accordé un accès total à Internet.
Applications actives	**Applications actives** répertorie les applications, ouvertes sur votre ordinateur, qui accèdent à Internet. Cliquez sur une application pour voir les adresses IP auxquelles elle se connecte.
Tâches communes	**Tâches communes** : ces liens vous amènent aux pages Personal Firewall qui présentent l'état des applications et vous permettent d'exécuter des tâches relatives aux applications.

Pour afficher la page Résumé des événements, cliquez sur **Modifier l'affichage**, puis sélectionnez **Résumé des événements**. La page Résumé des événements fournit les informations suivantes :

Élément	Description
Comparaison des ports	L'option **Comparaison des ports** affiche un graphique à secteurs des ports de votre ordinateur les plus fréquemment sollicités au cours des 30 derniers jours. Vous pouvez cliquer sur le nom d'un port pour afficher les détails de la page Événements entrants. Vous pouvez également déplacer le pointeur de votre souris sur le numéro de port pour afficher sa description.
Premiers attaquants	**Premiers attaquants** affiche les adresses IP les plus fréquemment bloquées, le dernier événement entrant de chaque adresse et le nombre total d'événements entrants au cours des trente derniers jours pour chaque adresse. Cliquez sur un événement pour afficher les détails des événements à partir de la page Événements entrants.

Élément	Description
Rapport quotidien	**Rapport quotidien** affiche le nombre d'événements entrants bloqués par Personal Firewall aujourd'hui, cette semaine-ci et ce mois-ci. Cliquez sur un nombre pour afficher les détails des événements à partir du journal des événements entrants
Dernier événement	**Dernier événement** affiche les derniers événements entrants. Vous pouvez cliquer sur un lien pour tracer l'événement ou pour autoriser l'adresse IP. Le fait d'autoriser une adresse IP autorise tout le trafic provenant de cette adresse IP à arriver sur votre ordinateur.
Tâches communes	**Tâches communes** : ces liens vous amènent aux pages Personal Firewall qui présentent les détails des événements et vous permettent d'effectuer des tâches relatives aux événements.

Pour afficher la page Résumé HackerWatch, cliquez sur **Modifier l'affichage**, puis sélectionnez **HackerWatch Summary**. La page Résumé HackerWatch fournit les informations suivantes :

Élément	Description
Activité mondiale	**World Activity** affiche une carte mondiale qui identifie les activités récemment bloquées et surveillées par HackerWatch.org. Cliquez sur la carte d'analyse des menaces globales dans HackerWatch.org pour l'ouvrir.
Volume des événements	**Event Tracking** affiche le nombre d'événements entrants soumis à HackerWatch.org.
Activité globale des ports	**Global Port Activity** affiche les premiers ports qui, au cours des 5 derniers jours, ressemblent à des menaces. Cliquez sur un port pour afficher son numéro et sa description.
Tâches communes	Cliquez sur un lien dans **Common Tasks** pour accéder aux pages de HackerWatch.org, où vous pourrez obtenir davantage d'informations sur les activités de piratage dans le monde entier.

À propos de la page Applications Internet

Utilisez la page Applications Internet pour afficher la liste des applications autorisées et bloquées.

Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis cliquez sur **Applications Internet**. La page Applications Internet s'ouvre (Figure 2-2).

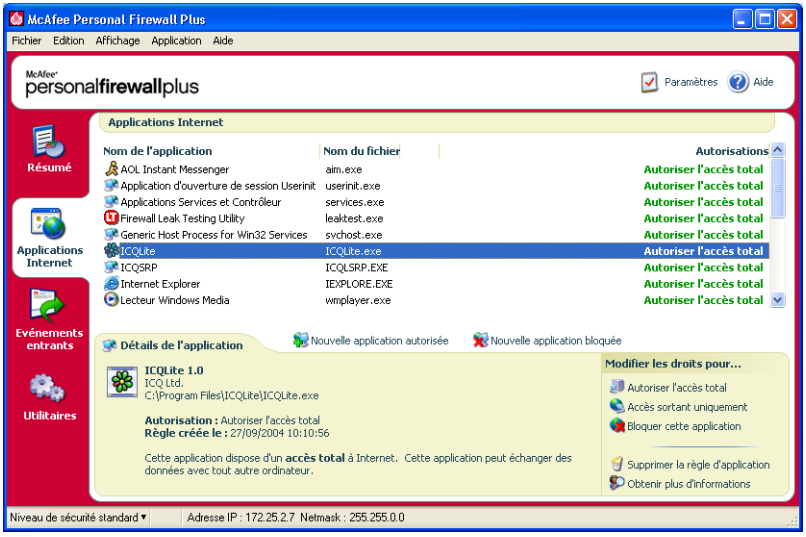


Figure 2-2. Page Applications Internet

La page Applications Internet fournit les informations suivantes :

- Nom des applications
- Nom des fichiers
- Niveaux d'autorisation actuels
- Détails de l'application : chemin d'accès, horodatage des autorisations et description des types d'autorisation

Modification des autorisations

Personal Firewall vous permet de définir le niveau d'autorisation de chaque application demandant l'accès à Internet.

Pour modifier un niveau d'autorisation, procédez comme suit :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis cliquez sur **Applications Internet**.
2. Dans la liste **Autorisations**, cliquez avec le bouton droit de la souris sur le niveau d'autorisation d'une application, puis choisissez un niveau différent :
   - **Autoriser l'accès total** permet à l'application d'envoyer et de recevoir des données.
   - **Accès sortant uniquement** empêche l'application de recevoir des données.
   - **Bloquer cette application** empêche l'application d'envoyer ou de recevoir des données.

     REMARQUE
     Les applications qui étaient bloquées le seront toujours lorsque le pare-feu sera fixé sur le niveau de sécurité **Ouvert** ou sur **Désactivé**. Pour empêcher ceci de se produire, vous pouvez soit modifier les autorisations des applications en **Accès total** ou simplement supprimer la règle d'autorisation **Bloqué** dans la liste **Autorisations**.

Pour supprimer un niveau d'autorisation, procédez comme suit :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis cliquez sur **Applications Internet**.
2. Dans la liste **Autorisations**, cliquez avec le bouton droit de la souris sur le niveau d'autorisation d'une application, puis cliquez sur **Supprimer la règle d'application**.

La prochaine fois que cette application demandera l'accès à Internet, vous pourrez définir son niveau d'autorisation afin de l'ajouter de nouveau à la liste.

Modification des applications

Pour modifier la liste des applications Internet autorisées et bloquées, procédez comme suit :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis cliquez sur **Applications Internet**.
2. Dans la liste **Nom de l'application**, ajoutez ou supprimez des applications :
   - Pour ajouter une application « autorisée », cliquez sur **Nouvelle application autorisée**, sélectionnez l'application à autoriser, puis cliquez sur **Ouvrir**.
   - Pour ajouter une application « bloquée », cliquez sur **Nouvelle application bloquée**, sélectionnez l'application à bloquer, puis cliquez sur **Ouvrir**.
   - Pour supprimer une application de la liste, cliquez sur **Supprimer la règle d'application**.

À propos de la page Événements entrants

La page Événements entrants vous permet d'afficher le journal d'événements entrants généré lorsque Personal Firewall bloque un trafic Internet non sollicité.

Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis cliquez sur **Événements entrants**. La page Événements entrants s'affiche (Figure 2-3).

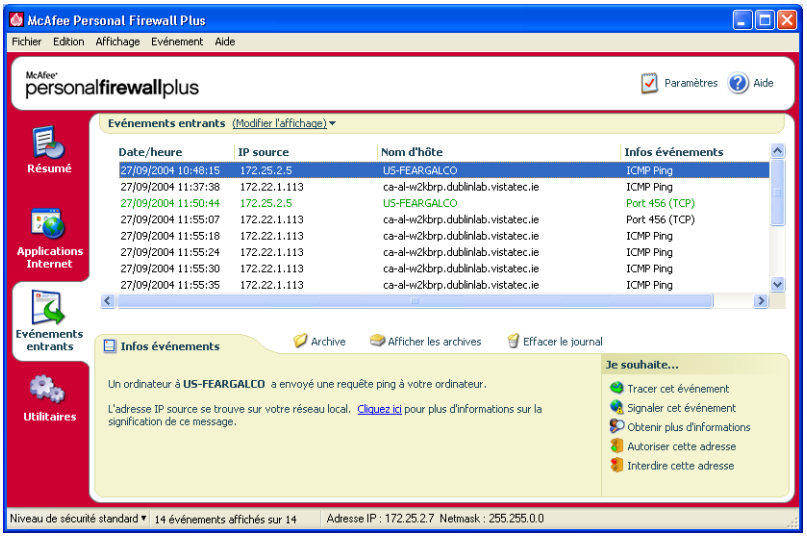


Figure 2-3. Page Événements entrants

La page Événements entrants fournit les informations suivantes :

- Horodatage
- Adresses IP source
- Noms d'hôte
- Noms de service ou d'application
- Détails de l'événement : types de connexion, ports de connexion, description des événements de port

Mieux comprendre les événements

À propos des adresses IP

Les adresses IP sont des nombres. Plus précisément, chaque adresse IP est constituée de quatre nombres compris entre 0 et 255, qui identifient un lieu spécifique vers lequel le trafic peut être dirigé sur Internet.

Adresses IP spéciales

Certaines adresses IP se présentent différemment pour diverses raisons :

Adresses IP non routables : elles sont également appelées « Espace d'adressage IP privé ». Ces adresses IP ne peuvent pas être utilisées sur Internet. Les blocs d'adresses IP privées sont 10.x.x.x, 172.16.x.x - 172.31.x.x et 192.168.x.x.

Adresses IP en boucle : ces adresses sont utilisées à des fins de test. Le trafic envoyé à ce bloc est renvoyé au périphérique qui a généré le paquet. Il ne quitte jamais le périphérique et est essentiellement utilisé à des fins de tests matériels et logiciels. Le bloc d'adresses IP en boucle est 127.x.x.x.

Adresse IP nulle : adresse non valide. Elle apparaît lorsque l'adresse IP du trafic était vierge. De toute évidence, cela n'est pas normal et cela signifie souvent que l'expéditeur masque délibérément l'origine du trafic. L'expéditeur n'aura de réponse à son trafic que si le paquet est reçu par une application en mesure de comprendre son contenu, qui comprend notamment des instructions spécifiques à l'application en question. Toute adresse commençant par 0 (0.x.x.x) est une adresse nulle. 0.0.0.0 est, par exemple, une adresse IP nulle.

Événements provenant de 0.0.0.0

Si vous détectez des événements provenant de l'adresse IP 0.0.0.0, il existe deux causes probables. La première est la plus courante : pour une raison indéterminée, votre ordinateur a reçu un paquet au format non valide. Internet n'est pas toujours fiable à 100 % et des paquets au format non valide peuvent se présenter. Comme Personal Firewall détecte les paquets avant que ceux-ci ne soient validés par TCP/IP, il risque de les signaler comme événement.

L'autre cas de figure se présente lorsque l'adresse IP source est usurpée ou fausse. Les paquets usurpés peuvent signifier que quelqu'un est à la recherche d'un cheval de Troie et teste votre ordinateur. Puisque Personal Firewall a bloqué ces tentatives, rassurez-vous : votre ordinateur est protégé.

Événements provenant de l'adresse 127.0.0.1

Les événements indiquent parfois une adresse IP source de type 127.0.0.1. Il s'agit d'une adresse IP spéciale, appelée adresse de bouclage.

En fait, 127.0.0.1 désigne toujours l'ordinateur sur lequel vous vous trouvez, quel qu'il soit. Cette adresse est également appelée « localhost » (hôte local), car le nom d'ordinateur localhost sera toujours traduit par l'adresse IP 127.0.0.1.

Cela signifie-t-il que votre ordinateur tente de s'auto-pirater ? Un cheval de Troie ou un logiciel espion cherche-t-il à prendre le contrôle de votre ordinateur ? C'est peu probable. De nombreux programmes légitimes utilisent l'adresse de bouclage à des fins de communication entre leurs composants. Par exemple, de nombreux serveurs de messagerie ou serveurs Web personnels sont configurables via une interface Web, généralement accessible depuis une adresse de type http://localhost/.

Toutefois, Personal Firewall autorise le trafic émanant de ces programmes ; par conséquent, si vous détectez des événements provenant de 127.0.0.1, il est fort probable que l'adresse IP source soit usurpée ou fausse. Les paquets usurpés indiquent généralement un utilisateur à la recherche d'un cheval de Troie. Puisque Personal Firewall a bloqué ces tentatives, rassurez-vous : votre ordinateur est protégé. De toute évidence, il est inutile de signaler les événements provenant de 127.0.0.1.

Ceci dit, certains programmes, dont Netscape 6.2 et ultérieur vous demandent d'ajouter 127.0.0.1 à la liste des adresses IP autorisées. Les composants de ces programmes communiquent entre eux de telle manière que Personal Firewall ne peut pas déterminer si le trafic est local ou non.

Par exemple, avec Netscape 6.2, vous devez autoriser l'adresse 127.0.0.1 pour pouvoir utiliser votre liste d'amis. Si vous détectez du trafic provenant de 127.0.0.1 et que toutes les applications sur votre ordinateur fonctionnent normalement, vous pouvez bloquer ce trafic en toute sécurité. Toutefois, si un programme (tel que Netscape) rencontre des difficultés, ajoutez 127.0.0.1 à la liste des adresses IP autorisées de Personal Firewall, puis regardez si cela résout le problème.

Si cela résout le problème, vous serez confronté à l'alternative ci-après : si vous autorisez 127.0.0.1, votre programme fonctionnera, mais vous serez davantage exposé aux attaques par usurpation ; si vous n'autorisez pas cette adresse, votre programme ne fonctionnera pas, mais vous demeurerez protégé contre ce trafic malveillant.

Événements provenant d'ordinateurs sur votre réseau local LAN

Des événements peuvent être générés à partir d'ordinateurs de votre réseau local (LAN). Pour indiquer que ces événements proviennent d'un emplacement « proche de chez vous », Personal Firewall les affiche en vert.

Lorsque l'on configure un réseau local d'entreprise, il est généralement préférable de sélectionner l'option **Autoriser tous les ordinateurs du réseau LAN** de la page Adresses IP autorisées.

Toutefois, il est important de noter que dans certaines situations, votre réseau « local » peut être aussi dangereux, voire plus, que le réseau extérieur. Ceci se vérifie notamment lorsque vous êtes connecté à un réseau public à large bande passante, par exemple, via un modem ADSL ou câble. Dans ce cas, il est préférable de ne pas cocher l'option **Autoriser tous les ordinateurs du réseau LAN**.

De même, si vous utilisez une connexion de réseau domestique à large bande, vous devrez ajouter manuellement les adresses IP de vos ordinateurs locaux à la liste Adresses IP autorisées. N'oubliez pas que vous pouvez utiliser des adresses de type .255 pour autoriser un bloc entier. Par exemple, vous pouvez autoriser votre réseau ICS (réseau de partage de connexion Internet) entier en autorisant l'adresse IP 192.168.255.255.

Événements provenant d'adresses IP privées

Les adresses IP au format 192.168.xxx.xxx, 10.xxx.xxx.xxx et 172.16.0.0 - 172.31.255.255 sont appelées adresses IP non routables ou privées. Ces adresses IP ne quittent jamais votre réseau et vous pouvez leur faire confiance la plupart du temps.

Le bloc 192.168 est utilisé avec le Partage de connexion Internet de Microsoft (ICS). Si vous utilisez ICS et que vous détectez des événements provenant de ce bloc d'adresses IP, vous voudrez peut-être ajouter l'adresse IP 192.168.255.255 à votre liste d'adresses IP autorisées. Vous autoriserez ainsi la totalité du bloc d'adresses 192.168.xxx.xxx.

Si vous n'êtes pas connecté à un réseau privé et si vous détectez des événements provenant de ces plages d'adresses IP, il se pourrait que l'adresse IP source soit usurpée ou falsifiée. Les paquets usurpés signifient généralement que quelqu'un est à la recherche d'un cheval de Troie. Puisque Personal Firewall a bloqué ces tentatives, rassurez-vous : votre ordinateur est protégé.

Puisque les adresses IP privées désignent des ordinateurs totalement différents selon le type de réseau sur lequel vous vous trouvez, le fait de signaler ces événements sera sans effet ; par conséquent, il est inutile de le faire.

Affichage des événements dans le journal d'événements entrants

Le journal d'événements entrants vous permet d'afficher de manière pratique les événements de différentes manières. L'affichage par défaut limite l'affichage aux événements survenus le jour même. Vous pouvez également afficher les événements survenus au cours de la semaine passée, voire le journal complet.

Personal Firewall vous permet également d'afficher les événements entrants de jours spécifiques, d'adresses Internet spécifiques (adresses IP) ou bien encore des événements contenant les mêmes informations.

Pour plus d'informations sur un événement, cliquez sur l'événement : les informations s'affichent alors dans la zone **Infos événements**, au bas de la page Événements entrants.

Affichage des événements de la journée

Pour afficher uniquement les événements survenus dans la journée :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis cliquez sur **Événements entrants**.
2. Dans le menu **Affichage**, cliquez sur **Afficher les événements de la journée**.

   Le journal d'événements entrants affiche uniquement les événements survenus aujourd'hui.

Affichage des événements de la semaine

Pour afficher les événement survenus la semaine passée :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis cliquez sur **Événements entrants**.
2. Dans le menu **Affichage**, cliquez sur **Afficher les événements de cette semaine**.

   Le journal d'événements entrants affiche uniquement les événements survenus cette semaine.

Affichage du journal d'événements entrants complet

Pour afficher tous les événements dans le journal d'événements entrants :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis cliquez sur **Événements entrants**.
2. Dans le menu **Affichage**, cliquez sur **Afficher le journal complet**.

   La page Événements entrants affiche tous les événements du journal, mais sans les archives.

Affichage des événements du jour sélectionné uniquement

Cette fonction vous permet de consulter les événements survenus tel ou tel jour. Tous les événements n'ayant pas eu lieu ce jour-là sont masqués.

Pour afficher tous les événements survenus tel ou tel jour

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis cliquez sur **Événements entrants**.
2. Dans le menu **Affichage**, cliquez sur **Afficher uniquement les événements du jour sélectionné**.

   Les événements de la journée apparaissent dans le journal d'événements entrants.

Affichage des événements relatifs à l'adresse Internet sélectionnée uniquement

Cette fonction est utile lorsque vous devez consulter d'autres événements provenant d'une adresse Internet spécifique. Tous les autres événements sont masqués.

Pour afficher tous les événements provenant d'une adresse Internet spécifique :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis cliquez sur **Événements entrants**.
2. Dans le menu **Affichage**, cliquez sur **Afficher uniquement les événements relatifs à l'adresse Internet sélectionnée.**

   Les événements provenant de l'adresse Internet sélectionnée s'affichent dans le journal d'événements entrants.

Affichage des événements dont les informations sont identiques uniquement

Cette option permet de voir si le journal d'événements contient d'autres événements dont les informations (colonne **Infos événements**) sont identiques à celles de l'événement sélectionné. Vous pouvez ainsi déterminer si cet événement revient plusieurs fois et s'il provient de la même source. La colonne Infos événements fournit une description de l'événement et, le cas échéant, le nom du programme ou du service qui utilise ce port.

Pour afficher tous les événements ayant les mêmes informations :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis cliquez sur **Événements entrants**.
2. Dans le menu **Affichage**, cliquez sur **Afficher uniquement les événements dont les informations sur les événements sont identiques**.

   Les événements présentant les mêmes informations apparaissent dans le journal d'événements entrants.

Options de réponse aux événements entrants

Vous pouvez non seulement obtenir des détails sur les événements du journal d'événements entrants, mais aussi effectuer un traçage visuel des adresses IP impliquées dans un événement, ou encore obtenir des informations depuis le site Web HackerWatch.org (communauté anti-piratage en ligne).

Traçage de l'événement sélectionné

Vous pouvez effectuer un traçage visuel des adresses IP associées à un événement entrant consigné dans le journal. Procédez comme suit :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis cliquez sur **Événements entrants**.
2. Cliquez avec le bouton droit de la souris sur l'événement à tracer, puis sélectionnez **Tracer l'événement sélectionné**.

   Vous pouvez aussi double-cliquer sur l'événement.

   Par défaut, Personal Firewall lance un traçage visuel à l'aide du programme intégré Visual Trace.

Consultation du site HackerWatch.org

Vous pouvez également essayer d'obtenir plus d'informations sur un événement en allant sur le site de la communauté anti-piratage HackerWatch.org :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis cliquez sur **Événements entrants**.
2. Localisez et sélectionnez l'événement sur lequel vous souhaitez obtenir plus d'informations.
3. Dans le menu **Événement**, choisissez **Plus d'informations sur l'événement**.

Votre navigateur Web s'ouvre. Vous pouvez alors accéder au site HackerWatch.org (à l'adresse http://www.hackerwatch.org/) pour obtenir des détails sur le type de l'événement et déterminer s'il est nécessaire ou non de le signaler.

Notification d'un événement

Pour signaler un événement représentant, selon vous, une attaque de votre ordinateur :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis cliquez sur **Événements entrants**.
2. Cliquez sur l'événement à signaler, puis sur **Signaler cet événement** dans le volet inférieur droit.

   Personal Firewall transmet l'événement au site Web HackerWatch.org en utilisant votre ID unique.

Abonnement à HackerWatch.org

Lorsque vous ouvrez la page Résumé de Personal Firewall pour la première fois, celui-ci contacte le site HackerWatch.org afin de générer votre ID utilisateur unique. Si vous êtes déjà inscrit, votre abonnement est automatiquement validé. Si vous êtes un nouvel utilisateur, vous devez entrer un pseudonyme et une adresse électronique. Il vous faudra ensuite cliquer sur le lien de validation dans le courrier électronique de confirmation envoyé par HackerWatch.org pour pouvoir utiliser les fonctions de filtrage/transmission électronique d'événements à ce site Web.

Vous pouvez signaler des événements à HackerWatch.org sans valider votre ID utilisateur. Cependant, pour filtrer des événements et les transmettre par e-mail, vous devez vous abonner au service.

Votre abonnement au service permet le suivi de vos envois ; il nous permet de vous prévenir lorsque HackerWatch.org a besoin de plus d'informations ou lorsqu'une intervention de votre part est nécessaire. En outre, il nous permet de confirmer, et de valider, les informations que nous recevons.

Toutes les adresses électroniques fournies à HackerWatch.org restent confidentielles. Si un FAI soumet une requête en vue d'obtenir des informations supplémentaires, sa demande est routée via HackerWatch.org ; votre adresse électronique n'est jamais divulguée.

Autorisation d'une adresse

Si le journal d'événements entrants consigne un événement contenant une adresse IP que vous souhaitez autoriser, vous pouvez configurer Personal Firewall pour qu'il autorise de façon permanente les connexions provenant de cette adresse :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis cliquez sur **Événements entrants**.
2. Cliquez avec le bouton droit de la souris sur l'événement dont vous voulez autoriser l'adresse IP, puis cliquez sur **Autoriser l'adresse IP source**.
3. Vérifiez que l'adresse IP affichée dans le message de confirmation Autoriser cette adresse est correcte, puis cliquez sur **OK**.

   L'adresse IP est ajoutée à la liste **Adresses IP autorisées**.

Pour vérifier que l'adresse IP a été ajoutée, procédez comme suit :

1. Cliquez sur l'onglet **Utilitaires**.
2. Cliquez sur l'icône **Adresses IP autorisées ou interdites**, puis sur l'onglet **Adresses IP autorisées**.

   L'adresse IP apparaît dans la liste **Adresses IP autorisées**.

Interdiction d'une adresse

Si une adresse IP apparaît dans votre journal d'événements entrants, cela signifie que le trafic en provenance de cette adresse est bloqué. Par conséquent, l'interdiction d'une adresse ne vous apportera aucune protection supplémentaire, sauf si votre ordinateur est doté de ports délibérément ouverts à l'aide de la fonction Services système ou exécute une application autorisée à recevoir du trafic.

N'ajoutez une adresse IP à votre liste de sites interdits que si un ou plusieurs ports sont délibérément ouverts sur votre ordinateur et que, pour une raison ou une autre, vous estimez nécessaire d'empêcher cette adresse d'accéder aux ports ouverts.

Si le journal d'événements entrants contient un événement relatif à une adresse IP que vous voulez interdire, vous pouvez configurer Personal Firewall pour qu'il bloque définitivement les connexions provenant de cette adresse :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis cliquez sur **Événements entrants**.
2. Cliquez avec le bouton droit de la souris sur l'événement dont vous voulez interdire l'adresse IP, puis cliquez sur **Interdire l'adresse IP source**.
3. Vérifiez que l'adresse IP affichée dans le message de confirmation Interdire cette adresse est correcte, puis cliquez sur **OK**.

   L'adresse est ajoutée à la liste **Adresses IP interdites**.

Pour vérifier que l'adresse IP a été ajoutée à la liste des adresses interdites, procédez comme suit :

1. Cliquez sur l'onglet **Utilitaires**.
2. Cliquez sur l'icône **Adresses IP autorisées ou interdites**, puis sur l'onglet **Adresses IP interdites**.

   L'adresse IP apparaît dans la liste **Adresses IP interdites**.

Gestion du journal d'événements entrants

La page Événements entrants vous permet de gérer les événements du journal d'événements entrants généré lorsque Personal Firewall bloque un trafic Internet non sollicité.

Archivage du journal d'événements entrants

Vous pouvez archiver le journal d'événements entrants dans un fichier sur votre disque dur. Nous vous recommandons d'archiver régulièrement le journal d'événements car il peut devenir très volumineux.

Pour archiver le journal d'événements entrants, procédez comme suit :

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis cliquez sur **Événements entrants**.
2. Dans le menu **Fichier**, cliquez sur **Archiver le journal**.
3. Un message de confirmation s'affiche. Cliquez sur **Oui**.
4. Cliquez sur **Enregistrer** pour enregistrer l'archive à l'emplacement par défaut, ou naviguez jusqu'à l'emplacement de votre choix.

Affichage des journaux d'événements entrants archivés

Vous pouvez afficher des journaux d'événements entrants précédemment archivés.

> **REMARQUE**
> Avant d'afficher vos archives, vous devez archiver le journal d'événements entrants en cours. Si vous négligez cette opération, le journal d'événements entrants en cours sera effacé lorsque vous afficherez une archive.

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis cliquez sur **Événements entrants**.
2. Dans le menu Fichier, cliquez sur **Afficher les journaux archivés**.
3. Cliquez sur le nom du fichier d'archive (vous devrez peut-être naviguer dans le système pour y accéder), puis cliquez sur **Ouvrir**.

   Les données archivées s'affichent dans le journal d'événements entrants.

Effacement du contenu du journal d'événements entrants

Vous pouvez effacer la totalité du contenu du journal d'événements entrants.

> **REMARQUE**
> Une fois les entrées du journal d'événements entrants effacées, vous ne pourrez plus les récupérer. Si vous pensez en avoir besoin ultérieurement, archivez-les.

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis cliquez sur **Événements entrants**.
2. Dans le menu **Fichier**, cliquez sur **Effacer le journal**.
3. Un message de confirmation s'affiche. Cliquez sur **Oui**.

   Le journal d'événements ne contient plus aucune entrée.

Exportation des événements affichés

Vous pouvez exporter votre journal d'événements dans un fichier texte pour les besoins de votre FAI, de votre support technique ou des personnes chargées de faire appliquer la loi.

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis cliquez sur **Événements entrants**.
2. Dans le menu Fichier, cliquez sur **Exporter les événements affichés**.
3. Placez-vous sur le répertoire dans lequel vous voulez enregistrer les événements.
4. Renommez le fichier si nécessaire, puis cliquez sur **Enregistrer**.

   Vos événements sont enregistrés dans un fichier au format .txt à l'emplacement choisi.

Copie d'un événement dans le Presse-papiers

Vous pouvez copier un événement dans le presse-papiers pour ensuite le coller dans un fichier texte à l'aide du Bloc-notes.

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis cliquez sur **Événements entrants**.
2. Dans le journal d'événements entrants, cliquez sur l'événement à exporter.
3. Dans le menu **Édition**, cliquez sur **Copier l'événement sélectionné dans le Presse-papiers**.
4. Ouvrez le Bloc-notes :

   Cliquez sur le bouton Démarrer de Windows, choisissez Programmes, puis Accessoires et cliquez sur Bloc-notes.
5. Dans le menu **Édition**, cliquez sur **Coller**. L'événement s'affiche dans le Bloc-notes. Répétez cette procédure pour tous les événements souhaités.
6. Sauvegardez le fichier Bloc-notes en lieu sûr.

Suppression de l'événement sélectionné

Vous pouvez supprimer des événements du journal d'événements entrants.

1. Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis cliquez sur **Événements entrants**.
2. Dans le journal d'événements entrants, cliquez sur l'événement à supprimer.
3. Dans le menu **Édition**, cliquez sur **Supprimer l'événement sélectionné**.

   L'événement est supprimé du journal.

À propos des alertes

Nous vous recommandons vivement de vous familiariser avec les différents types d'alerte que vous pouvez rencontrer en utilisant Personal Firewall. Passez en revue les types d'alerte pouvant s'afficher (voir ci-dessous) et les diverses réponses possibles, de façon à y répondre en toute confiance.

REMARQUE
Firewall peut afficher des recommandations pour vous aider à décider du traitement à appliquer à une alerte. Pour afficher les recommandations dans les alertes, cliquez sur l'onglet **Utilitaires**, puis sur l'icône **Paramètres d'alerte** ; dans la liste **Recommandations intelligentes**, sélectionnez **Utiliser les recommandations intelligentes** (option par défaut) ou **Afficher uniquement les recommandations intelligentes**.

Alertes rouges

Les alertes rouges contiennent des informations importantes à traiter immédiatement.

- **L'application Internet a été bloquée !** — Cette alerte s'affiche lorsque Personal Firewall a empêché une application d'accéder à Internet. Par exemple, si une alerte relative à un cheval de Troie s'affiche, McAfee refuse automatiquement l'accès à Internet au programme et vous recommande d'analyser votre ordinateur afin de détecter d'éventuels virus.
- **L'application demande l'accès à Internet —** Cette alerte s'affiche lorsque Personal Firewall détecte du trafic Internet ou réseau pour de nouvelles applications (Niveau de sécurité standard ou élevé).
- **L'application a été modifiée —** Cette alerte s'affiche lorsque Personal Firewall détecte qu'une application préalablement autorisée à accéder à Internet a été modifiée. Si vous n'avez pas mis à niveau l'application en question depuis longtemps, réfléchissez bien avant de lui accorder l'accès à Internet (Niveau de sécurité faible, standard ou élevé).
- **L'application demande l'accès au serveur —** Cette alerte s'affiche lorsque Personal Firewall détecte qu'une application préalablement autorisée à accéder à Internet demande un accès en qualité de serveur (Niveau de sécurité élevé).

REMARQUE
Le paramètre par défaut de Windows XP SP2 Mises à jour automatiques télécharge et installe des mises à jour pour le système d'exploitation Windows et d'autres programmes Microsoft qui s'exécutent sur votre ordinateur sans vous en informer. Lorsqu'une application a été modifiée à partir d'une des mises à jour silencieuses de Windows, des alertes McAfee Personal Firewall apparaîtront lors de la prochaine exécution de cette application.

IMPORTANT
Vous devez autoriser l'accès à Internet aux applications qui en ont besoin pour des mises à jour de produits en ligne (par exemple, les services McAfee).

L'application Internet a été bloquée !

Si une alerte relative à un cheval de Troie s'affiche (Figure 2-4), Personal Firewall refuse automatiquement l'accès à Internet au programme suspect et vous recommande de rechercher d'éventuels virus sur votre ordinateur.

Figure 2-4. L'application Internet a été bloquée !

Consultez la description générale de l'événement, puis sélectionnez l'une des options suivantes :

- Cliquez sur **Obtenir plus d'informations** pour afficher les détails de l'événement via le journal d'événements entrants de Personal Firewall (pour plus de détails, reportez-vous à la section *À propos de la page Événements entrants* à la page 23).
- Cliquez sur **Lancer McAfee VirusScan Online** pour procéder à la recherche de virus.
- Cliquez sur **Continuer l'opération en cours** si l'action entreprise par Personal Firewall vous convient.

L'application demande l'accès à Internet

Si vous avez sélectionné un niveau de sécurité **Standard** ou **Élevé**, Personal Firewall affiche un message d'alerte (Figure 2-5) lorsqu'il détecte du trafic Internet ou réseau correspondant à des applications nouvelles ou modifiées.

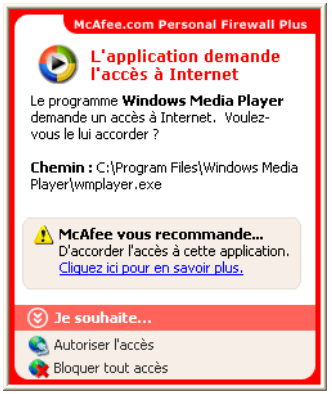


Figure 2-5. L'application demande l'accès à Internet

Lorsqu'un message vous conseille d'être prudent si vous autorisez l'application à accéder à Internet, vous pouvez obtenir plus d'informations sur l'application en choisissant le lien **Cliquez ici pour en savoir plus**. Ce lien n'est disponible que si Personal Firewall est configuré pour utiliser les recommandations intelligentes.

Il se peut que McAfee ne reconnaisse pas l'application qui tente d'accéder à Internet (Figure 2-6).

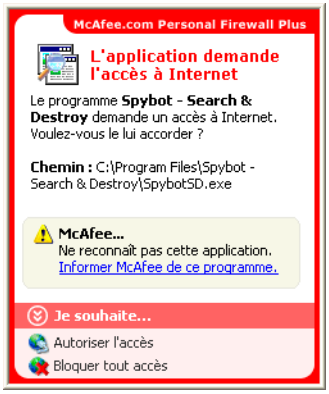


Figure 2-6. Application non reconnue

McAfee n'est donc pas en mesure de vous conseiller sur la manière de traiter l'application. Vous pouvez signaler l'application en question à McAfee en cliquant sur **Informer McAfee de ce programme**. Une page Web apparaît et vous demande des informations liées à l'application. Veuillez fournir toutes les informations que vous détenez.

Nos opérateurs HackerWatch combinent les informations envoyées avec d'autres outils de recherche pour déterminer si une application mérite d'être répertoriée dans notre base de données d'applications connues et, le cas échéant, la manière dont elle doit être traitée par Personal Firewall.

Consultez la description générale de l'événement, puis sélectionnez l'une des options suivantes :

- Cliquez sur **Autoriser l'accès** pour permettre à l'application d'envoyer ou de recevoir des données non sollicitées sur des ports non-système.
- Cliquez sur **Bloquer tout accès** pour empêcher l'application d'envoyer ou de recevoir des données.

L'application a été modifiée

Si vous avez sélectionné le niveau de sécurité **Faible**, **Standard** ou **Élevé** dans les paramètres de sécurité, Personal Firewall affiche une alerte (Figure 2-7) lorsqu'il détecte qu'une application autorisée à accéder à Internet a été modifiée. Si vous n'avez pas récemment mis à niveau l'application en question, réfléchissez bien avant de lui accorder l'accès à Internet.

Figure 2-7. L'application a été modifiée

Consultez la description générale de l'événement, puis sélectionnez l'une des options suivantes :

- Cliquez sur **Autoriser l'accès** pour permettre à l'application d'envoyer ou de recevoir des données non sollicitées sur des ports non-système.
- Cliquez sur **Bloquer tout accès** pour empêcher l'application d'envoyer ou de recevoir des données.

L'application demande l'accès au serveur

Si vous avez choisi un niveau de sécurité **Élevé** dans les options Paramètres de sécurité, Personal Firewall affiche une alerte (Figure 2-8) lorsqu'une application autorisée à accéder à Internet demande l'accès au serveur.

Figure 2-8. L'application demande l'accès au serveur

Ainsi, une alerte s'affiche lorsque MSN Messenger demande l'accès au serveur pour envoyer un fichier au cours d'une discussion en ligne.

Consultez la description générale de l'événement, puis sélectionnez l'une des options suivantes :

- Cliquez sur **Autoriser l'accès au serveur** pour permettre à l'application d'envoyer et de recevoir des données.
- Cliquez sur **Autoriser uniquement l'accès sortant** pour empêcher l'application de recevoir des données.
- Cliquez sur **Bloquer tout accès** pour empêcher l'application d'envoyer ou de recevoir des données.

Alertes vertes

Les alertes vertes vous informent de modifications apportées à Personal Firewall. Par exemple, elles vous indiquent le nom des applications auxquelles Personal Firewall a automatiquement accordé un accès à Internet ou vous signalent de nouvelles règles d'application.

Programme autorisé à accéder à Internet — Cette alerte s'affiche lorsque Personal Firewall autorise automatiquement l'accès à Internet à toutes les applications nouvelles ou modifiées, puis vous envoie une notification (niveau de sécurité faible). Une application modifiée sera, par exemple, une application dont les règles ont été modifiées pour lui accorder un accès automatique à Internet.

Application autorisée à accéder à Internet

Si vous avez sélectionné le niveau de sécurité **Faible** dans les options de Paramètres de sécurité, Personal Firewall autorise automatiquement l'accès à Internet à toutes les applications nouvelles ou modifiées, puis émet une alerte (Figure 2-9).

Figure 2-9. Programme autorisé à accéder à Internet

Consultez la description générale de l'événement, puis sélectionnez l'une des options suivantes :

- Cliquez sur **Afficher le journal des applications** pour afficher les détails de l'événement via le journal d'applications d'Internet (pour plus d'informations, reportez-vous à la section *À propos de la page Applications Internet* à la page 21).
- Cliquez sur **Désactiver ce type d'alerte** pour empêcher l'affichage des alertes de ce type.
- Cliquez sur **Continuer l'opération en cours** si l'action entreprise par Personal Firewall vous convient.

Alertes bleues

Les alertes bleues ne sont qu'informatives. Elles ne nécessitent aucune réponse.

- **Tentative de connexion bloquée**—Cette alerte s'affiche lorsque Personal Firewall bloque du trafic Internet ou réseau indésirable. (Niveau de sécurité faible, standard ou élevé).

Tentative de connexion bloquée

Si vous avez sélectionné un niveau de sécurité **Faible**, **Standard** ou **Élevé**, Personal Firewall affiche une alerte (Figure 2-10) lorsqu'il bloque du trafic Internet ou réseau non sollicité.

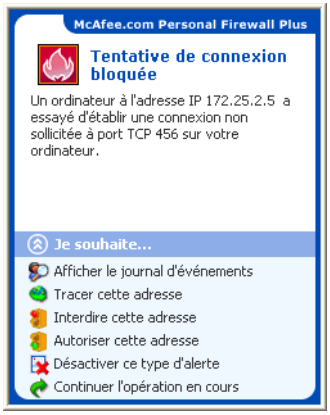


Figure 2-10. Tentative de connexion bloquée

Consultez la description générale de l'événement, puis sélectionnez l'une des options suivantes :

- Cliquez sur **Afficher le journal d'événements** pour consulter les détails sur l'événement dans le journal d'événements entrants de Personal Firewall (pour plus de détails, reportez-vous à la section *À propos de la page Événements entrants* à la page 23).
- Cliquez sur **Tracer cette adresse** pour effectuer un traçage visuel des adresses IP relatives à l'événement.
- Cliquez sur **Interdire cette adresse** pour empêcher cette adresse d'accéder à votre ordinateur. L'adresse est ajoutée à la liste Adresses IP interdites.
- Cliquez sur **Autoriser cette adresse** pour autoriser cette adresse IP à accéder à votre ordinateur.
- Cliquez sur **Continuer l'opération en cours** si l'action entreprise par Personal Firewall vous convient.

Index

N

P

T

Pour plus d'informations sur
les produits, les services dans
le monde entier et l'assistance,
contactez votre représentant
agréé McAfee
ou rendez-nous visite à
l'adresse suivante :

McAfee
International BV
PO Box 58326, 1040 HH
Amsterdam
Pays-Bas

fr.mcafee.com

http://www.mcafeeaide.com

NA-671-0010-FR-1