

McAfee®

personal**firewall**plus

Guide de l'utilisateur

McAfee®

COPYRIGHT

Copyright © 2005 McAfee, Inc. Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, transmise, transcrite, stockée dans un système d'archivage ou traduite dans toute autre langue, sous quelque forme ou par quelque moyen que ce soit sans l'autorisation écrite de McAfee, Inc., de ses fournisseurs ou de ses sociétés affiliées.

MENTION DES MARQUES

ACTIVE FIREWALL, ACTIVE SECURITY, ACTIVESECURITY (ET EN KATAKANA), ACTIVESHIELD, ANTIVIRUS ANYWARE AND DESIGN, CLEAN-UP, DESIGN (STYLIZED E), DESIGN (STYLIZED N), ENTERCEPT, ENTERPRISE SECURECAST, ENTERPRISE SECURECAST (ET EN KATAKANA), EPOLICY ORCHESTRATOR, FIRST AID, FORCEFIELD, GMT, GROUPSHIELD, GROUPSHIELD (ET EN KATAKANA), GUARD DOG, HOMEGUARD, HUNTER, INTRUSHIELD, INTRUSION PREVENTION THROUGH INNOVATION, M AND DESIGN, MCAFEE, MCAFEE (ET EN KATAKANA), MCAFEE AND DESIGN, MCAFEE.COM, MCAFEE VIRUSSCAN, NA NETWORK ASSOCIATES, NET TOOLS, NET TOOLS (ET EN KATAKANA), NETCRYPTO, NETOCTOPUS, NETSCAN, NETSHIELD, NETWORK ASSOCIATES, NETWORK ASSOCIATES COLLISEUM, NETXRAY, NOTESGUARD, NUTS & BOLTS, OIL CHANGE, PC MEDIC, PCNOTARY, PRIMESUPPORT, RINGFENCE, ROUTER PM, SECURECAST, SECURESELECT, SPAMKILLER, STALKER, THREATSCAN, TIS, TMEG, TOTAL VIRUS DEFENSE, TRUSTED MAIL, UNINSTALLER, VIREX, VIRUS FORUM, VIRUSCAN, VIRUSSCAN, VIRUSSCAN (AND IN KATAKANA), WEBSCAN, WEBSHIELD, WEBSHIELD (ET EN KATAKANA), WEBSTALKER, WEBWALL, WHAT'S THE STATE OF YOUR IDS?, WHO'S WATCHING YOUR NETWORK, YOUR E-BUSINESS DEFENDER, YOUR NETWORK. OUR BUSINESS. sont des marques déposées ou des marques de McAfee, Inc. et/ou de ses sociétés affiliées aux États-Unis et/ou dans d'autres pays. La couleur rouge utilisée pour identifier des fonctionnalités liées à la sécurité est propre aux produits de marque McAfee. Toutes les autres marques, déposées ou non, mentionnées dans ce document sont la propriété exclusive de leurs détenteurs respectifs.

INFORMATIONS SUR LA LICENCE

Accord de licence

À L'ATTENTION DE TOUS LES UTILISATEURS : LISEZ ATTENTIVEMENT L'ACCORD JURIDIQUE CORRESPONDANT À LA LICENCE QUE VOUS AVEZ ACHETÉE. IL DÉFINIT LES CONDITIONS GÉNÉRALES D'UTILISATION DU LOGICIEL SOUS LICENCE. SI VOUS IGNOREZ LE TYPE DE LICENCE QUE VOUS AVEZ ACQUIS, REPORTEZ-VOUS AUX DOCUMENTS COMMERCIAUX ET AUTRES DOCUMENTS D'OCTROI DE LICENCE, OU AU BON DE COMMANDE, QUI ACCOMPAGNENT VOTRE PRODIGEIL OU QUI VOUS ONT ÉTÉ TRANSMIS SÉPARÉMENT DANS LE CADRE DE VOTRE ACHAT (SOUS LA FORME D'UN LIVRET, D'UN FICHIER INCLUS DANS LE CD DU PRODUIT OU D'UN FICHIER DISPONIBLE SUR LE SITE WEB À PARTIR DUQUEL VOUS AVEZ TÉLÉCHARGÉ LE PRODIGEIL). SI VOUS N'ÊTES PAS D'ACCORD AVEC CERTAINS TERMES DE CET ACCORD, N'INSTALLEZ PAS LE LOGICIEL. LE CAS ÉCHÉANT, VOUS POUVEZ RENVoyer LE PRODUIT À MCAFEE, INC. OU À L'ENDROIT OÙ VOUS L'AVEZ ACHETÉ AFIN D'EN OBTENIR LE REMBOURSEMENT INTÉGRAL.

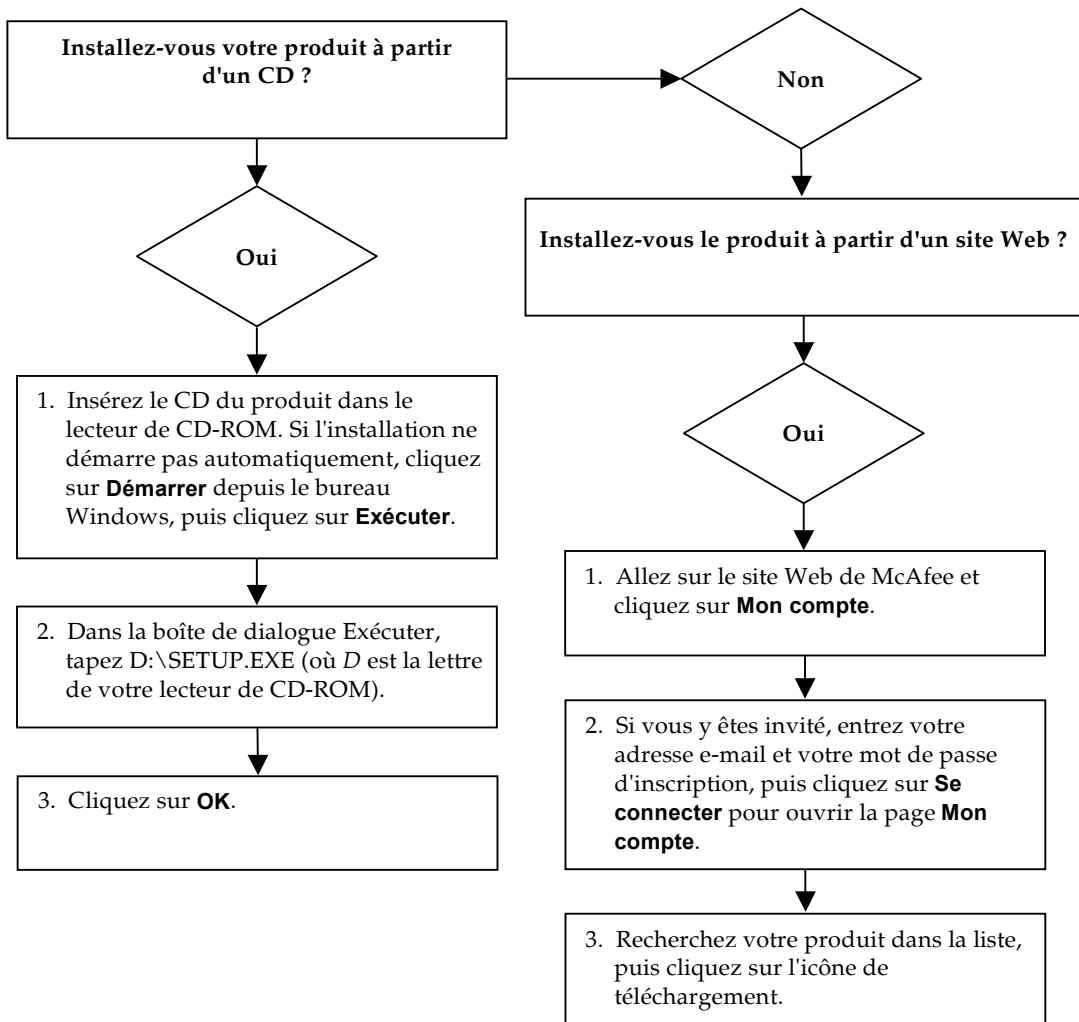
Mentions

Ce produit contient ou peut contenir :

- ♦ Un logiciel développé par le projet OpenSSL à utiliser avec la boîte à outils OpenSSL (<http://www.openssl.org/>).
- ♦ Un logiciel cryptographique écrit par Eric Young et un logiciel écrit par Tim J. Hudson.
- ♦ Certains logiciels couverts par un accord de licence (ou de sous-licence) conclu avec l'utilisateur dans le cadre de la General Public License (GPL) GNU ou d'autres licences de logiciels libres similaires autorisant l'utilisateur à, entre autres, copier, modifier et redistribuer certains programmes ou certaines parties de programmes et à accéder au code source. La GPL stipule que, pour tout logiciel couvert distribué à d'autres utilisateurs dans un format binaire exécutable, le code source doit également être mis à disposition. Pour tous ces logiciels couverts par la Licence Publique Générale, le code source est disponible sur ce CD. Si des licences de logiciels libres requièrent que McAfee, Inc. accorde un droit d'utilisation, de copie ou de modification d'un logiciel plus étendu que celui octroyé dans cet accord, ce droit prime sur les droits et restrictions de cet accord.
- ♦ Un logiciel initialement écrit par Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer.
- ♦ Un logiciel initialement écrit par Robert Nordier, Copyright © 1996-7 Robert Nordier.
- ♦ Un logiciel initialement écrit par Douglas W. Sauter.
- ♦ Un logiciel développé par l'Apache Software Foundation (<http://www.apache.org/>). Une copie de l'accord de licence de ce logiciel est disponible à l'adresse www.apache.org/licenses/LICENSE-2.0.txt.
- ♦ International Components for Unicode ("ICU") Copyright © 1995-2002 International Business Machines Corporation et autres.
- ♦ Un logiciel développé par CrystalClear Software, Inc., Copyright © 2000 CrystalClear Software, Inc.
- ♦ Technologie FEAD® Optimizer®, Copyright Netopsystems AG, Berlin, Allemagne.
- ♦ Outside In® Viewer Technology © 1992-2001 Stellant Chicago, Inc. et/ou Outside In® HTML Export, © 2001 Stellant Chicago, Inc.
- ♦ Un logiciel protégé par les droits d'auteur de Thai Open Source Software Center Ltd. et Clark Cooper, © 1998, 1999, 2000.
- ♦ Un logiciel protégé par les droits d'auteur d'Expat maintainers.
- ♦ Un logiciel protégé par les droits d'auteur de The Regents of the University of California, © 1989.
- ♦ Un logiciel protégé par les droits d'auteur de Gunnar Ritter.
- ♦ Un logiciel protégé par les droits d'auteur de Sun Microsystems®, Inc. © 2003.
- ♦ Un logiciel protégé par les droits d'auteur de Gisle Aas. © 1995-2003.
- ♦ Un logiciel protégé par les droits d'auteur de Michael A. Chase, © 1999-2000.
- ♦ Un logiciel protégé par les droits d'auteur de Neil Winton, © 1995-1996.
- ♦ Un logiciel protégé par les droits d'auteur de RSA Data Security, Inc., © 1990-1992.
- ♦ Un logiciel protégé par les droits d'auteur de Sean M. Burke, © 1999, 2000.
- ♦ Un logiciel protégé par les droits d'auteur de Martijn Koster, © 1995.
- ♦ Un logiciel protégé par les droits d'auteur de Brad Appleton, © 1996-1999.
- ♦ Un logiciel protégé par les droits d'auteur de Michael G. Schwern, © 2001.
- ♦ Un logiciel protégé par les droits d'auteur de Graham Barr, © 1998.
- ♦ Un logiciel protégé par les droits d'auteur de Larry Wall et Clark Cooper, © 1998-2000.
- ♦ Un logiciel protégé par les droits d'auteur de Frodo Looijaard, © 1997.
- ♦ Un logiciel protégé par les droits d'auteur de la Python Software Foundation, Copyright © 2001, 2002, 2003. Une copie de l'accord de licence de ce logiciel est disponible à l'adresse www.python.org.
- ♦ Un logiciel protégé par les droits d'auteur de Beman Dawes, © 1994-1999, 2002.
- ♦ Un logiciel écrit par Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame.
- ♦ Un logiciel protégé par les droits d'auteur de Simone Bordet & Marco Cravero, © 2002.
- ♦ Un logiciel protégé par les droits d'auteur de Stephen Purcell, © 2001.
- ♦ Un logiciel développé par Indiana University Extreme! Lab (<http://www.extreme.indiana.edu/>).
- ♦ Un logiciel protégé par les droits d'auteur de International Business Machines Corporation et autres, © 1995-2003.
- ♦ Un logiciel développé par l'University of California, Berkeley et ses donateurs.
- ♦ Un logiciel développé par Ralf S. Engelschall <rs@engelschall.com> dans le cadre du projet mod_ssl project (<http://www.modssl.org/>).
- ♦ Un logiciel protégé par les droits d'auteur de Kevin Henney, © 2000-2002.
- ♦ Un logiciel protégé par les droits d'auteur de Peter Dimov et de Multi Media Ltd. © 2001, 2002.
- ♦ Un logiciel protégé par les droits d'auteur de David Abrahams, © 2001, 2002. Consultez le site <http://www.boost.org/libs/bind/bind.html> pour obtenir de la documentation.
- ♦ Un logiciel protégé par les droits d'auteur de Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, © 2000.
- ♦ Un logiciel protégé par les droits d'auteur de Boost.org, © 1999-2002.
- ♦ Un logiciel protégé par les droits d'auteur de Nicolai M. Josuttis, © 1999.
- ♦ Un logiciel protégé par les droits d'auteur de Jeremy Siek, © 1999-2001.
- ♦ Un logiciel protégé par les droits d'auteur de Daryle Walker, © 2001.
- ♦ Un logiciel protégé par les droits d'auteur de Chuck Allison et Jeremy Siek, © 2001, 2002.
- ♦ Un logiciel protégé par les droits d'auteur de Samuel Krempp, © 2001. Consultez le site <http://www.boost.org> pour obtenir des mises à jour, de la documentation et l'historique des révisions.
- ♦ Un logiciel protégé par les droits d'auteur de Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002.
- ♦ Un logiciel protégé par les droits d'auteur de Cadenza New Zealand Ltd., © 2000.
- ♦ Un logiciel protégé par les droits d'auteur de Jens Maurer, © 2000, 2001.
- ♦ Un logiciel protégé par les droits d'auteur de Jaakko Järvi (jaakko.jarvi@cs.utu.fi), © 1999, 2000.
- ♦ Un logiciel protégé par les droits d'auteur de Ronald Garcia, © 2002.
- ♦ Un logiciel protégé par les droits d'auteur de David Abrahams, Jeremy Siek, et Daryle Walker, © 1999-2001.
- ♦ Un logiciel protégé par les droits d'auteur de Stephen Cleary (shammah@voyager.net), © 2000.
- ♦ Un logiciel protégé par les droits d'auteur de Housermark Oy <<http://www.housermark.com>>, © 2001.
- ♦ Un logiciel protégé par les droits d'auteur de Paul Moore, © 1999.
- ♦ Un logiciel protégé par les droits d'auteur du Dr. John Maddock, © 1998-2002.
- ♦ Un logiciel protégé par les droits d'auteur de Greg Colvin et Beman Dawes, © 1998, 1999.
- ♦ Un logiciel protégé par les droits d'auteur de Peter Dimov, © 2001, 2002.
- ♦ Un logiciel protégé par les droits d'auteur de Jeremy Siek et John R. Bandela, © 2001.
- ♦ Un logiciel protégé par les droits d'auteur de Joerg Walter et Mathias Koch, © 2000-2002.

Carte de configuration rapide

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



McAfee se réserve le droit de modifier ses politiques et plans de support et de mise à niveau à tout moment et sans préavis. McAfee et ses noms de produit sont des marques déposées de McAfee, Inc. et/ou de ses filiales aux États-Unis et/ou dans d'autres pays.

© 2005 McAfee, Inc. Tous droits réservés.

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

McAfee vous conseille de suivre les instructions fournies avec le produit pour vous enregistrer directement. 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 si vous achetez le logiciel VirusScan.
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 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.

Support technique

Pour toute question relative au support technique, consultez notre site

<http://www.mcafeeaide.com/>.

Notre site de support offre, 24 heures sur 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 à l'option gratuite de conversation et de courrier électronique. Ces options vous permettent de communiquer rapidement et gratuitement avec nos ingénieurs du support technique, via Internet. Vous trouverez également des informations relatives à nos services d'assistance téléphonique sur notre site

<http://www.mcafeeaide.com/>.

Table des matières

Carte de configuration rapide	iii
1 Prise en main	7
Nouvelles fonctions	7
Configuration système requise	9
Désinstallation d'autres pare-feux	10
Configuration du pare-feu par défaut	10
Définition du niveau de sécurité	11
Test de McAfee Personal Firewall Plus	13
Utilisation de McAfee SecurityCenter	13
2 Utilisation de McAfee Personal Firewall Plus	15
À propos de la page Résumé	15
À propos de la page Applications Internet	20
Modification des règles d'application	21
Autorisation et blocage d'applications Internet	21
À propos de la page Événements entrants	22
Mieux comprendre les événements	23
Affichage des événements dans le journal d'événements entrants	25
Options de réponse aux événements entrants	27
Gestion du journal d'événements entrants	31
À propos des alertes	33
Alertes rouges	34
Alertes vertes	39
Alertes bleues	41
Index	43

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 vous offre 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 fonctions

- **Amélioration de la prise en charge des jeux**
McAfee Personal Firewall Plus protège votre ordinateur contre des tentatives d'intrusion et toutes autres activités douteuses durant vos parties de jeu en plein écran, mais peut masquer les alertes s'il détecte de telles tentatives ou activités. Les alertes rouges apparaissent une fois que vous quittez le jeu.
- **Amélioration de la gestion de l'accès**
McAfee Personal Firewall Plus permet aux utilisateurs d'accorder dynamiquement aux applications un accès temporaire à Internet. La durée de l'accès est limitée au temps écoulé entre le lancement de l'application et sa fermeture. Lorsque Personal Firewall détecte un programme inconnu ou tente de communiquer avec Internet, une alerte rouge offre la possibilité d'accorder à l'application un accès temporaire à Internet.

- **Amélioration du contrôle de sécurité**

En exécutant la fonctionnalité de verrouillage de McAfee Personal Firewall Plus, vous bloquez instantanément l'ensemble du trafic Internet entrant et sortant entre un ordinateur et Internet. Les utilisateurs peuvent activer et désactiver l'option de verrouillage à partir de trois zones dans Personal Firewall.
- **Amélioration des options de récupération**

Vous pouvez exécuter les options de réinitialisation pour rétablir automatiquement les paramètres par défaut de Personal Firewall. Si Personal Firewall s'avère ne pas être stable et que vous restez sans solution face à cette difficulté, vous avez la possibilité d'annuler vos paramètres actuels et de rétablir ceux par défaut du produit afin d'exécuter une version stable et opérationnelle de Personal Firewall.
- **Protection de la connectivité Internet**

Pour empêcher qu'un utilisateur ne désactive sa connexion Internet par mégarde, l'option permettant d'interdire des adresses IP est exclue d'une alerte bleue lorsque Personal Firewall détecte que la connexion Internet provient d'un serveur DHCP ou DNS. Si le trafic entrant ne provient pas d'un serveur DHCP ou DNS, l'option apparaît.
- **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.
- **Détection avancée des chevaux de Troie**

McAfee Personal Firewall Plus combine la gestion de connexion des applications à une base de données améliorée afin de détecter et de bloquer davantage d'applications potentiellement nuisibles (les chevaux de Troie par exemple), les empêcher d'accéder à Internet et de transmettre vos données personnelles.
- **Amélioration du suivi visuel**

Visual Trace inclut des cartes graphiques. Faciles à lire, elles indiquent la source et le cheminement des attaques (à l'échelle internationale). En particulier, elles fournissent des informations détaillées sur le contact et le propriétaire des adresses IP d'origine.

- **Amélioration de la convivialité**
McAfee Personal Firewall Plus comprend un assistant de configuration et un didacticiel utilisateur destinés à guider les utilisateurs lors de la configuration et de 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 offre à ses utilisateurs une visibilité sur les données entrantes/sortantes et affiche les connexions d'applications, notamment de celles 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, Windows Me, Windows 2000 ou Windows XP
- Ordinateur personnel avec processeur compatible Pentium
Windows 98, 2000 : 133 MHz minimum
Windows Me : 150 MHz minimum
Windows XP (Édition familiale et Professionnelle) : 300 MHz minimum
- RAM
Windows 98, Me, 2000 : 64 Mo
Windows XP (Édition familiale et Professionnelle) : 128 Mo
- 40 Mo disponibles sur le disque dur
- Microsoft® Internet Explorer version 5.5 ou ultérieure

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.

Configuration du 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.

Définition du 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. 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 sur l'icône McAfee  avec le bouton droit de la souris dans la barre d'état système de Windows, pointez sur **Personal Firewall** et sélectionnez **Options**.
- 2 Cliquez sur l'icône **Paramètres de sécurité**.
- 3 Pour définir le niveau de sécurité, faites glisser le curseur jusqu'au niveau souhaité.

Les niveaux de sécurité vont de Verrouillage à Ouvert.

- ◆ **Verrouillage** — Toutes les connexions Internet de votre ordinateur sont interdites. Vous pouvez utiliser ce paramètre pour bloquer les ports que vous avez configurés comme ouverts dans la page Services système.
- ◆ **Niveau de sécurité élevé** — Lorsqu'une application demande un certain type d'accès à Internet (par exemple, Accès sortant uniquement), vous pouvez soit l'autoriser, soit l'interdire. Si par la suite l'application demande un accès total, vous pourrez alors lui accorder cet Accès total ou conserver l'Accès sortant uniquement.
- ◆ **Niveau de sécurité standard (recommandé)** — Lorsqu'une application requiert un accès Internet et que vous lui accordez, l'application bénéficie d'un accès total à Internet qui lui permet de gérer le trafic entrant et sortant.
- ◆ **Niveau de sécurité faible** — Toutes les applications reçoivent automatiquement une autorisation lorsqu'elles essaient d'accéder à Internet pour la première fois. Toutefois, vous pouvez configurer Personal Firewall pour qu'il vous avertisse 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 désactivé. Ce paramètre autorise tout le trafic par l'intermédiaire du Personal Firewall, sans le filtrer.

REMARQUE

Les applications qui étaient bloquées le seront toujours lorsque le pare-feu sera paramétré sur le niveau de sécurité **Ouvert** ou sur **Verrouillage**. Pour éviter cela, vous pouvez soit modifier les autorisations des applications en **Autoriser l'accès total** ou supprimer la règle d'autorisation **Bloqué** dans la liste **Applications Internet**.

- 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 des événements de détection d'intrusion (IDS) dans le journal d'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 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 des utilisateurs disposant d'un accès restreint à modifier les paramètres de Personal Firewall** — Si vous utilisez Windows XP ou Windows 2000 Professionnel et que plusieurs utilisateurs 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

Vous pouvez tester votre installation de Personal Firewall pour détecter d'éventuelles vulnérabilités face aux intrusions et à d'autres activités suspectes.

Pour tester votre installation de Personal Firewall à partir de l'icône McAfee dans la barre d'état système :

- Cliquez avec le bouton droit de la souris sur l'icône McAfee  située dans la barre d'état système de Windows, puis sélectionnez **Tester le firewall**.

Personal Firewall ouvre Internet Explorer et se rend à 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.


Utilisation de McAfee SecurityCenter

McAfee SecurityCenter est votre centre de sécurité unique, accessible à partir de son icône dans la barre d'état système Windows ou de 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 continuellement mises à jour et les informations les plus récentes sur les produits.
- 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 fonctions 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 , puis sélectionnez **Ouvrir SecurityCenter**.

Pour ouvrir Personal Firewall à partir de McAfee SecurityCenter :

- 1 Dans SecurityCenter, cliquez sur l'onglet **Personal Firewall Plus**.
- 2 Sélectionnez une tâche dans le menu Je souhaite.


Pour ouvrir Personal Firewall à partir de Windows :

- 1 Cliquez avec le bouton droit de la souris sur l'icône McAfee  située dans la barre d'état système Windows, puis pointez vers **Personal Firewall**.
- 2 Sélectionnez une tâche.

Utilisation de McAfee Personal Firewall Plus

2

Pour ouvrir Personal Firewall :

- Cliquez sur l'icône McAfee  avec le bouton droit de la souris dans la barre d'état système de Windows, pointez sur **Personal Firewall** et sélectionnez une tâche.


À propos de la page Résumé

Le Résumé de Personal Firewall comporte quatre pages :

- ◆ Résumé principal
- ◆ Résumé des applications
- ◆ Résumé des événements
- ◆ 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 la page Résumé principal dans Personal Firewall :

- Cliquez sur l'icône McAfee  avec le bouton droit de la souris dans la barre d'état système de Windows, pointez sur **Personal Firewall** et sélectionnez **Afficher le résumé** (Figure 2-1).

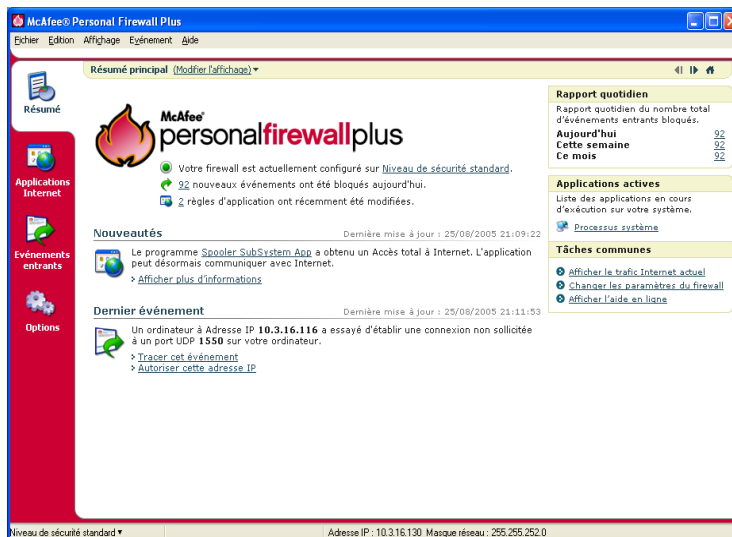





Figure 2-1. Page Résumé principal

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.

Élément	Description
Modifications des règles d'application	L'état des règles d'application affiche le nombre de règles d'application 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, en cours d'exécution 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 :


- 1 Cliquez sur l'icône McAfee  avec le bouton droit de la souris dans la barre d'état système de Windows, pointez sur **Personal Firewall** et sélectionnez **Afficher le résumé**.
- 2 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 connexions Internet entrantes et sortantes au cours des quinze dernières minutes. Cliquez sur le graphique pour afficher les détails du suivi du trafic.
Applications actives	<p>Applications actives présente la largeur de la bande passante utilisée par les applications les plus actives au cours des dernières 24 heures.</p> <p>Application—nom de l'application qui accède à Internet.</p> <p>%—pourcentage de la bande passante utilisé par l'application.</p> <p>Autorisation—type d'accès à Internet accordé à l'application.</p> <p>Règle créée—date de création de la règle d'application.</p>

Élément	Description
Nouveautés	Nouveautés désigne la dernière application à laquelle a été accordé un accès total à Internet.
Applications actives	Applications actives répertorie les applications, en cours d'exécution 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 :

- 1 Cliquez sur l'icône McAfee  avec le bouton droit de la souris dans la barre d'état système de Windows, pointez sur **Personal Firewall** et sélectionnez **Afficher le résumé**.
- 2 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.
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 :

- 1 Cliquez sur l'icône McAfee  avec le bouton droit de la souris dans la barre d'état système de Windows, pointez sur **Personal Firewall** et sélectionnez **Afficher le résumé**.
- 2 Cliquez sur **Modifier l'affichage**, puis sélectionnez **Résumé HackerWatch**.

La page Résumé HackerWatch fournit les informations suivantes.

Élément	Description
Activité mondiale	Activité mondiale 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.
Suivi des événements	Suivi des événements affiche le nombre d'événements entrants soumis à HackerWatch.org.
Activité globale des ports	Activité globale des ports 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 Tâches communes 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.

Pour ouvrir la page Applications Internet :

- Cliquez sur l'icône McAfee **M** avec le bouton droit de la souris dans la barre d'état système de Windows, pointez sur **Personal Firewall** et sélectionnez **Applications** (Figure 2-2).

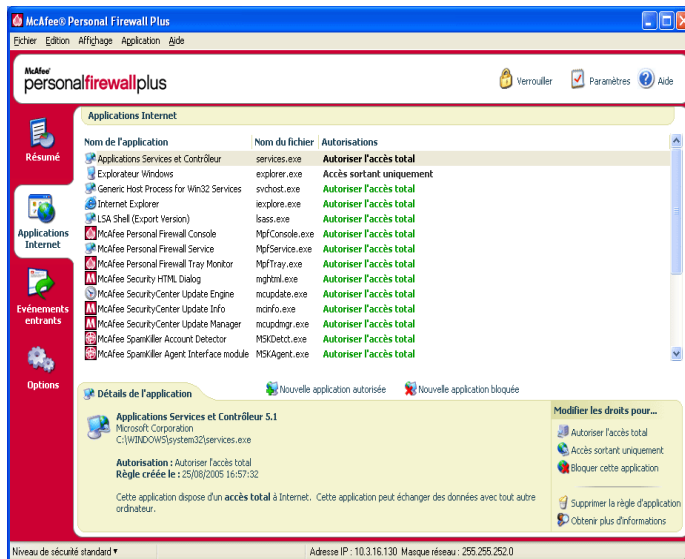


Figure 2-2. Page Applications Internet

La page Applications Internet fournit les informations suivantes :

- Nom des applications
- Nom des fichiers
- Niveaux d'autorisation actuels
- Détails de l'application : nom et version de l'application, nom de la société, chemin d'accès, autorisation, horodatage et description des types d'autorisation.

Modification des règles d'application

Personal Firewall vous permet de modifier les règles d'accès des applications.


Pour modifier une règle d'application :

- 1 Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis sélectionnez **Applications Internet**.
- 2 Dans la liste **Applications Internet**, cliquez avec le bouton droit de la souris sur la règle d'application d'une application, puis choisissez un niveau différent :
 - ◆ **Autoriser l'accès total** — permet à l'application d'établir des connexions Internet entrantes et sortantes.
 - ◆ **Accès sortant uniquement** — permet à l'application d'établir uniquement des connexions Internet sortantes.
 - ◆ **Bloquer cette application** — empêche l'application d'accéder à Internet.

REMARQUE

Les applications qui étaient bloquées continuent de l'être lorsque le pare-feu est paramétré sur le niveau de sécurité **Ouvert** ou **Verrouillage**. Pour empêcher ceci de se produire, vous pouvez soit modifier la règle d'accès de l'application en **Accès total**, soit supprimer la règle d'autorisation **Bloqué** dans la liste **Applications Internet**.


Pour supprimer une règle d'application :

- 1 Cliquez sur l'icône McAfee  avec le bouton droit de la souris dans la barre d'état système de Windows, pointez sur **Personal Firewall** et sélectionnez **Applications Internet**.
- 2 Dans la liste **Applications Internet**, cliquez avec le bouton droit de la souris sur la règle d'application, puis choisissez **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.

Autorisation et blocage d'applications Internet


Pour modifier la liste des applications Internet autorisées et bloquées :

- 1 Cliquez sur l'icône McAfee  avec le bouton droit de la souris dans la barre d'état système de Windows, pointez sur **Personal Firewall** et sélectionnez **Applications Internet**.
- 2 Sur la page Applications Internet, cliquez sur l'une des options suivantes :
 - ◆ **Nouvelle application autorisée** — accorde à l'application un accès total à Internet.
 - ◆ **Nouvelle application bloquée** — empêche l'application d'accéder à Internet.
 - ◆ **Supprimer la règle d'application** — supprime une 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 des connexions Internet non sollicitées.

Pour ouvrir la page Événements entrants :

- Cliquez sur l'icône McAfee  avec le bouton droit de la souris dans la barre d'état système de Windows, pointez sur **Personal Firewall** et sélectionnez **Événements entrants** (Figure 2-3).

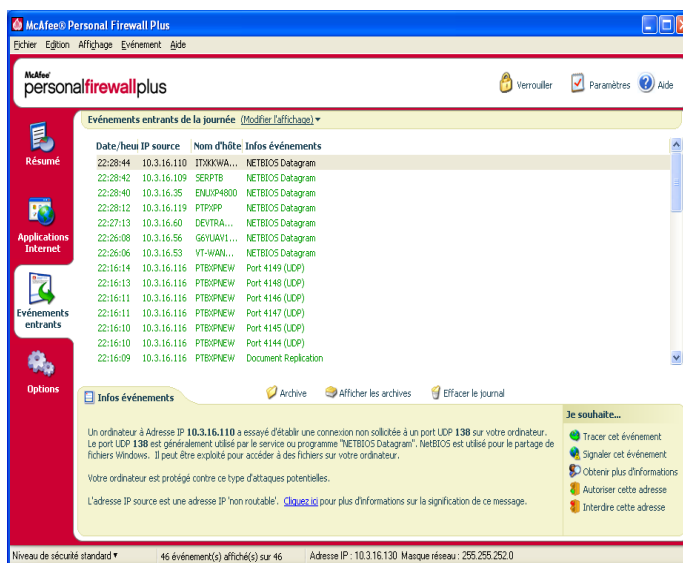


Figure 2-3. Page Événements entrants

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, nom d'hôte ou IP, 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.

Types d'adresses IP

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 d'adresses IP 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. Lorsqu'il le détecte, Personal Firewall indique que l'adresse IP du trafic était vierge. 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 : 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 fautive. Les paquets usurpés peuvent indiquer que quelqu'un est à la recherche d'un cheval de Troie sur votre ordinateur. Puisque Personal Firewall bloque ce genre d'activité, 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 en boucle, également appelée « localhost ».

De nombreux programmes légitimes utilisent l'adresse en boucle à des fins de communication entre leurs composants. Par exemple, vous pouvez configurer de nombreux serveurs de messagerie ou serveurs Web personnels via une interface Web. Pour accéder à l'interface, vous tapez « `http://localhost/` » dans votre navigateur Web.

Personal Firewall autorise le trafic émanant de ces programmes ; par conséquent, si vous détectez des événements provenant de 127.0.0.1, il est probable que l'adresse IP source soit usurpée ou fausse. Les paquets usurpés signifient généralement qu'un autre ordinateur est à la recherche d'un cheval de Troie sur votre ordinateur. Puisque Personal Firewall bloque ces tentatives d'intrusion, votre ordinateur est protégé.

Certains programmes, dont Netscape 6.2 et ultérieur vous demandent d'ajouter 127.0.0.1 à la liste des adresses IP autorisées et leurs composants 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 sont générés par votre réseau, 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.

Dans certaines situations, votre réseau « local » peut être aussi dangereux qu'Internet, notamment lorsque vous êtes connecté à un réseau à large bande passante, par exemple, via un modem ADSL ou câble. Dans ce cas, ne sélectionnez pas l'option **Autoriser tous les ordinateurs du réseau LAN**, mais ajoutez les adresses IP de vos ordinateurs locaux à la liste Adresses IP autorisées.

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.xxx.xxx 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 affiche 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 le volet **Informations sur les événements**.

Affichage des événements de la journée

Utilisez cette option pour examiner les événements du jour.

Pour afficher les événements de la journée :

- 1 Cliquez sur l'icône McAfee avec le bouton droit de la souris dans la barre d'état système de Windows, pointez sur **Personal Firewall** et sélectionnez **Événements entrants**.
- 2 Dans le journal d'événements entrants, cliquez avec le bouton droit de la souris sur une entrée, puis cliquez sur **Afficher les événements de la journée**.

Affichage des événements de la semaine

Utilisez cette option pour examiner les événements de la semaine.

Pour afficher les événements de la semaine :

- 1 Cliquez sur l'icône McAfee avec le bouton droit de la souris dans la barre d'état système de Windows, pointez sur **Personal Firewall** et sélectionnez **Événements entrants**.
- 2 Dans le journal d'événements entrants, cliquez avec le bouton droit de la souris sur une entrée, puis cliquez sur **Afficher les événements de la semaine**.

Affichage du journal d'événements entrants complet

Utilisez cette option pour examiner tous les événements.

Pour afficher tous les 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 avec le bouton droit de la souris sur une entrée, puis cliquez sur **Afficher le journal complet**.

Le journal affiche tous les événements du journal d'événements entrants.

Affichage des événements survenus un certain jour

Utilisez cette option pour examiner les événements survenus un certain jour.

Pour afficher les événements survenus un certain jour :

- 1 Cliquez sur l'icône McAfee avec le bouton droit de la souris dans la barre d'état système de Windows, pointez sur **Personal Firewall** et sélectionnez **Événements entrants**.
- 2 Dans le journal d'événements entrants, cliquez avec le bouton droit de la souris sur une entrée, puis cliquez sur **Afficher uniquement les événements du jour sélectionné**.

Affichage des événements provenant d'une adresse Internet spécifique

Utilisez cette option pour examiner les autres événements provenant d'une adresse Internet spécifique.

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

- 1 Cliquez sur l'icône McAfee avec le bouton droit de la souris dans la barre d'état système de Windows, pointez sur **Personal Firewall** et cliquez sur **Événements entrants**.
- 2 Dans le journal d'événements entrants, cliquez avec le bouton droit de la souris sur une entrée, puis cliquez sur **Afficher uniquement les événements relatifs à l'adresse Internet sélectionnée**.

Affichage des événements dont les informations sont identiques

Utilisez cette option pour voir si le journal d'événements contient d'autres événements dont les informations (colonne Informations sur les 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 Informations sur les événements fournit une description de l'événement et, le cas échéant, le nom du programme ou du service qui utilise ce port.

Pour afficher des événements dont les informations sont identiques :

- 1 Cliquez sur l'icône McAfee avec le bouton droit de la souris dans la barre d'état système de Windows, pointez sur **Personal Firewall** et cliquez sur **Événements entrants**.
- 2 Dans le journal d'événements entrants, cliquez avec le bouton droit de la souris sur une entrée, puis cliquez sur **Afficher uniquement les événements dont les informations sur les événements sont identiques**.

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.

Pour tracer un événement sélectionné :

- 1 Cliquez sur l'icône McAfee avec le bouton droit de la souris dans la barre d'état système de Windows, pointez sur **Personal Firewall** et sélectionnez **Événements entrants**.
- 2 Dans le journal d'événements entrants, cliquez avec droit de la souris sur l'événement à tracer, puis cliquez sur **Tracer l'événement sélectionné**. Vous pouvez aussi double-cliquer sur un événement pour le tracer.

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

Consultation du site HackerWatch.org

Pour consulter le site HackerWatch.org :

- 1 Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis sélectionnez **Événements entrants**.
- 2 Sélectionnez l'entrée de l'événement dans la page Événements entrants, puis cliquez sur **Obtenir plus d'informations** dans le volet **Je souhaite**.

Votre navigateur Web par défaut s'ouvre et accède au site 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 sur l'icône McAfee avec le bouton droit de la souris dans la barre d'état système de Windows, pointez sur **Personal Firewall** et sélectionnez **Événements entrants**.
- 2 Cliquez sur l'événement à signaler, puis sur **Signaler cet événement** dans le volet **Je souhaite**.

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 dans 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

Vous pouvez utiliser la page Événements entrants pour ajouter une adresse IP à votre liste d'adresses IP autorisées afin de l'autoriser en permanence.

Si la page 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.

Pour ajouter une adresse IP à la liste Adresses IP autorisées :

- 1 Cliquez sur l'icône McAfee avec le bouton droit de la souris dans la barre d'état système de Windows, pointez sur **Personal Firewall** et sélectionnez **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**.

Vérifiez que l'adresse IP affichée dans la boîte de dialogue de confirmation Autoriser cette adresse est correcte, puis cliquez sur **OK**. L'adresse est ajoutée à la liste Adresses IP autorisées.

Pour vérifier que l'adresse IP a été ajoutée à la liste :

- 1 Cliquez sur l'icône McAfee avec le bouton droit de la souris dans la barre d'état système de Windows, pointez sur **Personal Firewall** et sélectionnez **Options**.
- 2 Cliquez sur l'icône **Adresses IP autorisées ou interdites**, puis sur l'onglet **Adresses IP autorisées**.

Une coche apparaît en regard de l'adresse IP 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 d'adresses IP interdites 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 la page 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.

Vous pouvez utiliser la page Événement entrants, qui affiche les adresses IP de l'ensemble du trafic entrant, pour interdire une adresse IP que vous suspectez être la source d'une activité Internet indésirable ou douteuse.

Pour ajouter une adresse IP à la liste Adresses IP interdites :

- 1 Cliquez sur l'icône McAfee avec le bouton droit de la souris dans la barre d'état système de Windows, pointez sur **Personal Firewall** et sélectionnez **Événements entrants**.
- 2 La page Événements entrants répertorie les adresses IP de l'ensemble du trafic Internet entrant. Sélectionnez une adresse IP, puis effectuez l'une des opérations suivantes :
 - ♦ Cliquez sur l'adresse IP avec le bouton droit de la souris, puis sélectionnez **Interdire l'adresse IP source**.
 - ♦ Dans le menu **Je souhaite**, cliquez sur **Interdire cette adresse**.

- 3 Dans la boîte de dialogue Ajouter une règle d'adresse IP interdite, utilisez un ou plusieurs des paramètres suivants pour configurer la règle d'adresse IP interdite :
 - ◆ **Une seule adresse IP** : l'adresse IP à interdire. Par défaut, il s'agit de l'adresse IP que vous avez sélectionnée dans la page Événements entrants.
 - ◆ **Une plage d'adresses IP** : les adresses IP comprises entre l'adresse spécifiée dans le champ De l'adresse IP et celle spécifiée dans le champ À l'adresse IP.
 - ◆ **Cette règle expire le** : date et heure d'expiration de la règle d'adresse IP interdite. Utilisez les menus déroulants appropriés pour sélectionner la date et l'heure.
 - ◆ **Description** : description facultative de la nouvelle règle.
 - ◆ Cliquez sur **OK**.
- 4 Cliquez sur **Oui** dans la boîte de dialogue de confirmation. Cliquez sur **Non** pour revenir à la boîte de dialogue Ajouter une règle d'adresse IP interdite.

Si Personal Firewall détecte un événement provenant d'une connexion Internet interdite, il vous le signale de la manière que vous avez spécifiée à la page Paramètres d'alerte.

Pour vérifier que l'adresse IP a été ajoutée à la liste :

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

Une coche apparaît en regard de l'adresse IP 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 en cours pour enregistrer tous les événements entrants consignés, accompagnés de la date et de l'heure, des IP source, des noms d'hôte, des ports et des informations sur l'événement. Il est recommandé d'archiver régulièrement le journal d'événements entrants pour éviter qu'il ne devienne trop volumineux.

Pour archiver le journal d'événements entrants :

- 1 Cliquez sur l'icône McAfee avec le bouton droit de la souris dans la barre d'état système de Windows, pointez sur **Personal Firewall** et sélectionnez **Événements entrants**.

- 2 Dans la page Événements entrants, cliquez sur **Archive**.
- 3 Dans la boîte de dialogue Archiver le journal, cliquez sur **Oui** pour continuer l'opération.
- 4 Cliquez sur **Enregistrer** pour enregistrer l'archive à l'emplacement par défaut, ou naviguez jusqu'à l'emplacement de votre choix.

Remarque : Par défaut, Personal Firewall archive automatiquement le journal d'événements entrants. Cochez ou décochez la case **Archiver automatiquement les événements consignés** dans la page Paramètres de journalisation des événements pour activer ou désactiver cette option.

Affichage des journaux d'événements entrants archivés

Vous pouvez afficher des journaux d'événements entrants précédemment archivés. L'archive enregistrée inclut la date et l'heure, les IP source, les noms d'hôte, les ports et les informations relatives aux événements.

Pour afficher un journal d'événements entrants archivé :

- 1 Cliquez sur l'icône McAfee avec le bouton droit de la souris dans la barre d'état système de Windows, pointez sur **Personal Firewall** et sélectionnez **Événements entrants**.
- 2 Dans la page Événements entrants, cliquez sur **Afficher les archives**.
- 3 Sélectionnez le nom de fichier de l'archive ou parcourez l'arborescence pour le trouver et cliquez sur **Ouvrir**.

Effacement du contenu du journal d'événements entrants

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

AVERTISSEMENT : 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.

Pour effacer les entrées du journal d'événements entrants :

- 1 Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis sélectionnez **Événements entrants**.
- 2 Dans la page Événements entrants, cliquez sur **Effacer le journal**.
- 3 Cliquez sur **Oui** dans la boîte de dialogue pour effacer le journal.

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.

Pour copier un événement dans le Presse-papiers :

- 1 Cliquez avec le bouton droit de la souris sur l'icône McAfee, pointez sur **Personal Firewall**, puis sélectionnez **Événements entrants**.
- 2 Cliquez sur l'événement avec le bouton droit de la souris dans le journal d'événements entrants.
- 3 Cliquez sur **Copier l'événement sélectionné dans le Presse-papiers**.
- 4 Lancez le Bloc-notes.
 - ♦ Tapez `notepad` sur la ligne de commande ou cliquez sur le bouton **Démarrer** de Windows, pointez sur **Programmes**, puis **Accessoires**. Sélectionnez **Bloc-notes**.
- 5 Cliquez sur **Edition**, puis sur **Coller**. Le texte de 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.

Pour supprimer des événements du journal d'événements entrants :

- 1 Cliquez sur l'icône McAfee avec le bouton droit de la souris dans la barre d'état système de Windows, pointez sur **Personal Firewall** et sélectionnez **Événements entrants**.
- 2 Dans la page Événements entrants, cliquez sur l'entrée de l'événement à supprimer.
- 3 Dans le menu Edition, cliquez sur **Supprimer l'événement sélectionné**. L'événement est supprimé du journal d'événements entrants.

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 **Options**, 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.

- **Application Internet 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 concernant de nouvelles applications.
- **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 récemment mis à niveau l'application en question, réfléchissez bien avant de lui accorder l'accès à Internet.
- **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.

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).

Application Internet 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. Si McAfee VirusScan n'est pas installé, vous pouvez lancer McAfee SecurityCenter.



Figure 2-4. Application Internet 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 22](#)).
- Cliquez sur **Lancez McAfee VirusScan** pour procéder à la recherche de virus.
- Cliquez sur **Continuer l'opération en cours** si l'action entreprise par Personal Firewall vous convient.
- Cliquez sur **Autoriser l'accès sortant** pour autoriser la connexion sortante (niveau de sécurité élevé).

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 des connexions 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 **Informez McAfee de ce programme**. Une page Web apparaît et vous demande des informations concernant 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 autoriser l'application à établir des connexions Internet entrantes et sortantes.
- Cliquez sur **Autoriser l'accès une seule fois** pour accorder à l'application un accès temporaire à Internet. La durée de l'accès est limitée au temps écoulé entre le lancement de l'application et sa fermeture.
- Cliquez sur **Bloquer tout accès** pour interdire la connexion à Internet.
- Cliquez sur **Autoriser l'accès sortant** pour autoriser la connexion sortante (niveau de sécurité **élevé**).
- Cliquez sur **Aide sur le choix** pour afficher les rubriques relatives aux autorisations d'accès des applications dans l'aide en ligne.

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 autoriser l'application à établir des connexions Internet entrantes et sortantes.
- Cliquez sur **Autoriser l'accès une seule fois** pour accorder à l'application un accès temporaire à Internet. La durée de l'accès est limitée au temps écoulé entre le lancement de l'application et sa fermeture.
- Cliquez sur **Bloquer tout accès** pour interdire la connexion à Internet.
- Cliquez sur **Autoriser l'accès sortant** pour autoriser la connexion sortante (niveau de sécurité **élevé**).
- Cliquez sur **Aide sur le choix** pour afficher les rubriques relatives aux autorisations d'accès des applications dans l'aide en ligne.

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 un accès en qualité de 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 une seule fois** pour accorder à l'application un accès temporaire à Internet. La durée de l'accès est limitée au temps écoulé entre le lancement de l'application et sa fermeture.

- Cliquez sur **Autoriser l'accès au serveur** pour permettre à l'application d'établir des connexions Internet entrantes et sortantes.
- Cliquez sur **Autoriser uniquement l'accès sortant** pour empêcher toute connexion Internet entrante.
- Cliquez sur **Bloquer tout accès** pour interdire la connexion à Internet.
- Cliquez sur **Aide sur le choix** pour afficher les rubriques relatives aux autorisations d'accès des applications dans l'aide en ligne. Alertes vertes

Alertes vertes

Les alertes vertes vous informent des événements qui se produisent dans Personal Firewall. Par exemple, elles vous indiquent le nom des applications auxquelles Personal Firewall a automatiquement accordé un accès à Internet.

Programme autorisé à accéder à Internet — Cette alerte s'affiche lorsque Personal Firewall autorise automatiquement l'accès à Internet à toutes les nouvelles applications, 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 du firewall, 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 de Personal Firewall (pour plus d'informations, consultez la section [À propos de la page Applications Internet à la page 20](#)).
- 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.
- Cliquez sur **Bloquer tout accès** pour interdire la connexion à Internet.

L'application a été modifiée

Si vous avez sélectionné le niveau de sécurité **Faible** dans les options du firewall, Personal Firewall autorise automatiquement l'accès à Internet à toutes les applications modifiées. 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 de Personal Firewall (pour plus d'informations, consultez la section [À propos de la page Applications Internet à la page 20](#)).
- 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.
- Cliquez sur **Bloquer tout accès** pour interdire la connexion à Internet.

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.

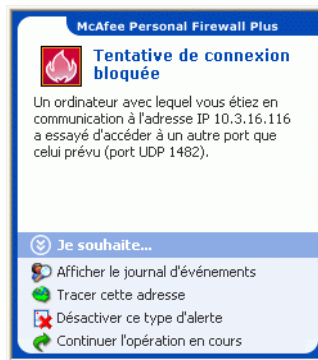


Figure 2-10. Tentative de connexion bloquée

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

- Cliquez sur **Afficher le journal des applications** pour consulter les détails sur l'événement dans le journal d'événements entrants de Personal Firewall (pour plus de détails, consultez la section [À propos de la page Événements entrants à la page 22](#)).
- 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

A

adresses IP

- à propos de, 23
- autorisation, 29
- interdiction, 30

affichage des événements dans le journal d'événements, 25

alertes

- Application Internet bloquée, 34
- L'application a été modifiée, 34
- L'application demande l'accès à Internet, 34
- L'application demande l'accès au serveur, 34
- Nouvelle application autorisée, 39
- Tentative de connexion bloquée, 41

applications Internet

- à propos de, 20
- autorisation et blocage, 21
- modification des règles d'application, 21

C

- Carte de configuration rapide, iii
- configuration système requise, 9

D

désinstallation

- autres pare-feux, 10

E

événements

- à propos de, 22
- actions en cas de, 27
- affichage
 - d'une adresse sélectionnée, 27
 - de la journée, 25
 - de la semaine en cours, 26
 - dont les informations sont identiques, 27
 - du jour sélectionné, 26
 - tous, 26

archivage du journal d'événements, 31

consultation de HackerWatch.org, 28

copie, 33

effacement des entrées du journal d'événements, 32

en boucle, 24

exportation, 33

notification, 28

plus d'informations, 28

provenant d'adresses IP privées, 25

provenant d'ordinateurs sur le réseau local LAN, 24

provenant de 0.0.0.0, 23

provenant de 127.0.0.1, 24

suppression, 33

traçage

affichage des journaux d'événements archivés, 32

compréhension, 22

H

HackerWatch.org

abonnement, 29

consultation, 28

notification d'un événement à, 28

J

Journal des événements

à propos de, 22

affichage, 32

gestion, 31

M

McAfee SecurityCenter, 13

mises à jour automatiques de Windows, 34

N

notification d'un événement, 28
nouvelles fonctions, 7

P

page Résumé, 15
pare-feu par défaut, paramétrer, 10
Pare-feu Windows, 10
Personal Firewall
 test, 13
 utilisation, 15
prise en main, 7

T

test de Personal Firewall, 13
traçage d'un événement, 28